Navigating the Digital Age

THE DEFINITIVE CYBERSECURITY GUIDE FOR DIRECTORS AND OFFICERS | THIRD EDITION

paloalto NETWORKS

Navigating the Digital Age

THE DEFINITIVE CYBERSECURITY GUIDE FOR DIRECTORS AND OFFICERS | THIRD EDITION

paloalto NETWORKS

Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers Third Edition

Publisher: Palo Alto Networks

Editors: Aleksandra Miljus, Mike Perkowski, Al Perlman, and Flora Zhang

Copy Editor: Rupal Shah

Design and Composition: Tim Heraldo, Ryan Catlett, and Caitlynn Wightman

Produced with Grateful Thanks to: Deirdre Beard, Paul Calatayud, Christopher Coccagna, Zoë Crawford, John Davis, Sean Duca, Kevin Dunbar, Karine Gidali, Rick Howard, Prem Iyer, Danielle Kriz, Andria Leaf, Katie Levine, Dana Loof, Rossana Monzon, Mara Mort, Aryn Pedowitz, Indelisa Pereida, Jeffrey Rennacker, and Abbi Tatton.

Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers, Third Edition is published by:

Palo Alto Networks, 3000 Tannery Way, Santa Clara, CA 95054, USA

Phone: +1 408-753-4000 | www.navigatingthedigitalage.com

First published: 2020

Disclaimer

Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers, Third Edition contains summary information about legal and regulatory aspects of cybersecurity governance and is current as of the date of its initial publication October 2020. Although the Guide may be revised and updated at some time in the future, the publishers and authors do not have a duty to update the information contained in the Guide, and will not be liable for any failure to update such information. The publishers and authors make no representation as to the completeness or accuracy of any information contained in the Guide.

This guide is written as a general guide only. It should not be relied upon as a substitute for specific professional advice. Professional advice should always be sought before taking any action based on the information provided. Every effort has been made to ensure that the information in this guide is correct at the time of publication. The views expressed in this guide are those of the authors. The publishers and authors do not accept responsibility for any errors or omissions contained herein. It is your responsibility to verify any information contained in the Guide before relying upon it.

Preface

Nikesh Arora — Chief Executive Officer and Chairman, Palo Alto Networks

Welcome to the third edition of *Navigating the Digital Age.* Fueled by the pace of technological advancement and the growth of digital connections, we can all relate to the axiom—the world moves fast. Then, in early 2020, the world faced an unprecedented global pandemic. Virtually overnight the challenges involved in navigating the Digital Age changed, likely forever. Fast became faster. We immediately started hearing from our customers.

There was an energy company that had to equip and secure 80,000 work at home employees over a single weekend. There was a health organization that needed to deliver critical public health services uninterrupted. There was a school district that had to quickly shift to distance learning for its students.

And there was our own company. Palo Alto Networks has long been at the forefront of innovation—and that spirit of innovation has in many ways better prepared us to weather such a crisis. We implemented a remote flexible work program to ensure the safety of our employees and empower them with more choice. Our systems and applications allow employees to work securely anywhere in the world, including our SOC analysts. And we leveraged automation and cloud delivery to scale seamlessly.

Today, connected digital technologies are a lifeline. They ensure that supply chains can function smoothly, and medical equipment can be tracked and monitored. They enable businesses to keep the lights on and adapt rapidly to serve the evolving needs of customers. They allow teachers to educate children online, scientists to share data in real time, and government agencies to keep their constituents informed.

For technologies to truly live up to their promise, the people using them must feel safe. Cybersecurity is as fundamental to our way of life in the 21st century as the quality of the air we breathe and the water we drink.

With the ground shifting quickly for everyone, it became obvious that the time was at hand to create a new edition of *Navigating the Digital Age.* As a leader in cybersecurity, we believe it is part of our mission to provide a platform for voices of expertise, guidance, and vision. We also proudly embrace our responsibility to do what we can to help the cyber community, as we secure today, for a better tomorrow.

While the global pandemic has been a catalyst, this book deals with challenges far beyond those related to COVID-19. The pandemic has accelerated trends we had already been witnessing and expe-

riencing in cybersecurity, such as the shift to cloud models, the need for extensive automation, the embrace of machine learning and artificial intelligence, to name just a few.

But the pandemic has also shined a harsher, brighter, and more urgent light on vital cybersecurity challenges that were already churning at the time we published the second edition of *Navigating the Digital Age* in 2018. These include the needs to strengthen communication between business and technology leaders and to embed cybersecurity into every aspect of our organizations.

What you will find in this third edition of *Navigating the Digital Age* is a mix of new chapters, updates to existing ones, and chapters that we kept intact as their relevance is as pressing as when they were first written. This edition contains new themes such as inspiring a new generation to safeguard our digital life, leading with emotional agility, budgeting in times of economic uncertainty, and of course, securing the future.

With 50 illustrious leaders from around the world sharing their ideas and experiences on cybersecurity, it is our sincere hope that you find the book instructive, illuminating, and thought-provoking.

With shared experience comes the opportunity for transformation. We can transform as individual organizations, industries, or countries—or we can transform together. We can look at our common challenges and build a foundation where we are all better prepared to be responsive and resilient in facing whatever crises may confront us in the future. *Navigating the Digital Age* is more than just a title for this book; it is a 21st century strategic imperative.

Table of Contents

Strategy

People

Process

Contributor Profiles

PART 1
The Future of Threat and Risks

Part 1 – Introductions

1

Ensuring a Safe, Secure, and People-Centered Internet

Vint Cerf — Vice President and Chief Internet Evangelist, Google

I am a passionate advocate for widespread access to an internet that works for all. Yet even with all that is being done around the globe to connect people, it seems hard to believe that half the world today still doesn't have reliable access to the internet. Some people might have thought that internet access was simply an option before the COVID-19 pandemic. But now I'm assuming we are all convinced that internet access for all is as critical as many of the other baseline needs for people.

Yet no matter how much we do our best to ensure that every single person on the planet has regular access, we must also ensure that what they are accessing is a safe and secure online environment. The best way to do that is to enlist the help, today, of the people who will run and use it tomorrow. So, how can we inspire future generations so they can be custodians of a shared digital future and a more people-centered internet? We need them to understand what the internet was designed for in the first place, and how to maintain the openness and innovation for which it was intended.

How can we do this? Today's young have only known a mobile internet available to them around the clock. We need them to appreciate that the internet is as fragile as the collective will of all of us. Each of us needs to be a leader in helping to create a global culture that will help to ensure a safe and secure online future.

Why I Designed an Open Internet

As an assistant professor at Stanford University, Robert Kahn and I co-designed the TCP/IP protocol suite, which became the foundational underpinnings of the internet.

Now, I sometimes get criticized for having designed a system where everything can talk to everything else. Of course, it was very deliberate, because, at the time, back in the early 1980's, we didn't know what devices would need to talk to what other devices, and we wanted to make sure there were no barriers to communication. That gave people the freedom to try all kinds of things out. You didn't have to worry about doing a deal, or negotiating with somebody, in order to interact. And even though you could send information from one device to another, the receiving device could always just ignore you.

Security, we decided, would be layered on top of that widespread communications infrastructure. For example, we knew that you could eventually insist on strong authentication and a variety of

other security tactics that could be introduced. So I felt comfortable with the idea that anything should be able to talk to anything.

Of course, as we know now, there are side effects to that kind of ubiquitous communications, such as distributed denial of service attacks, disinformation campaigns, ransomware, and the like. But these are the costs of an open internet.

Some people think the solution is to strongly clamp down on what can talk to what. I worry about that response a lot. How is this all going to come out if it turns out that we can't maintain an essentially open and widely interconnected network? If the internet is going to turn into islands that are difficult to bridge, then a lot of the utility, excitement, and potential of the internet is going to evaporate. So we need great cybersecurity to continue to have a free and open internet.

Cybersecurity Means Freedom from Harm

When we speak of freedom in the online environment, we often look at the Universal Declaration of Human Rights. We hear about the freedom to speak, the freedom to assemble, the freedom to share information. But we don't often speak of freedom from harm.

When we think about the kinds of harm that can come to people on the Net, we worry about privacy, safety, and sustainability. We worry about malware. We worry about Internet of Things (IoT) devices. We worry about personal security behavior. There are literally millions of different discovered vulnerabilities that are maintained in a giant, freely available database called VirusTotal that Google acquired in 2012. As much as possible, we need to be free from all of these many different kinds of harms.

Some people tell me that "freedom from harm" is not very well defined. It could mean that a regime wants to protect itself from harm by suppressing any kind of public debate by its citizens. But generally speaking, I think "freedom from harm" is a good guiding principle.

Unfortunately, there are many bad behaviors that you cannot necessarily defend against using purely technical means. So we need a way to think about a set of interlocking approaches that help with freedom from harm. There are three legs to the stool that apply to this problem.

The first approach is that, if there is harmful behavior that you could stop through technical means, then it's generally a good thing to use that technology. Strong authentication and two-factor authentication are examples of technologies that can help to prevent certain kinds of bad behaviors and harmful actions, as is Zero Trust. And today's operating systems are typically crafted to defend themselves against various kinds of attack.

Second, when technical solutions alone can't stop harmful behavior, the next thing you can do is to say, "if we can detect these behaviors, then there will be consequences." So we might agree on some basis that if a party is caught violating online security, or causing some other harm, there will be consequences. If that's within one country's jurisdiction, then that country's law enforcement hopefully takes effect. Or maybe it's an international agreement, and there's some kind of cooperation, such as when Interpol tracks down people who are behaving criminally.

Unfortunately, laws and regulations don't necessarily guarantee freedom from harm. Lots of people speed when they drive a car, and they aren't caught, even though they know that speeding is illegal. But of course they know if they are caught there will be consequences.

So the third leg of the stool is to just tell people, "Don't do that, it's wrong." Many people say, "Well, that sounds very

wimpy." That's when I remind them that gravity is the weakest force in the universe, but if you have enough mass, it's amazing how powerful it can be. Gravity keeps us from flying off the planet, and keeps the Earth from flying away from the sun.

In the same way, if you have enough social mass to agree on certain norms and behaviors in a society, then there can be a lot of pressure on the remainder of the society to behave according to those norms. Under the right circumstances, that can help to reduce the amount of misbehavior that arises.

Let me describe each of these three approaches in more detail.

Nuggets of Technology

The first leg of the stool is technology. I know that other chapters of this book will delve into a variety of technical approaches to ensuring better cybersecurity in the post-COVID era. What I'm looking for are small nuggets that are enablers of a desirable outcome.

An example of a nugget of security technology is strong authentication. The reason that's important is that you don't want someone to take action on your behalf without your permission. If it's too easy to pretend to be you, then you will not be protected against that possible outcome.

When you start looking at the IoT, whether it's security in the house, or HVAC (heating, ventilation and air conditioning), or some other device, you don't want a device you're depending on to be controlled by an unauthorized party. You certainly don't want your webcam to be releasing video to somebody who shouldn't get it.

So the device needs to know, "From which party should I be granting control? And to which party should I be sending data? And how do I verify that? How do I reject all other attempts?" For that kind of cybersecurity, strong authentication is the best tool that we have available. And public-key cryptography is a very powerful way of implementing that.

Across the board, you have a safer and more secure internet when devices are protected from various and sundry forms of attack. The only way you can do that is to build in resistance to the various kinds of attack. Happily, there are a number of other tools available to do that. Sometimes cryptography is your friend. Sometimes detection of malware is your protector. Sometimes it's about a Zero Trust approach.

But the problem I foresee is that many IoT devices are made by folks who are just trying to sell a product, get their money, and then not pay any attention to that device anymore. Which means that bugs don't get fixed, and devices become increasingly vulnerable. As a customer, you may not have any recourse to deal with that problem, especially if you can't find the party that built and sold the device in the first place.

Think about the example of medical instrumentation and the need for privacy. You don't want all of your medical data to be released, so you need proper cryptographic protection for the data being transferred. There's no question that we need to encourage innovation in many industries and arenas. But if a device attaches to the internet, the innovators need to remain responsible for guaranteeing the cybersecurity of that device.

Cybersecurity Depends on Unifying Policy

In order to get more internet out in the world, I think policy decisions are currently much more important than technical ones. The way that policy decisions develop today will have quite an impact on the way the internet functions tomorrow. And we are seeing pressure towards fragmentation of the internet for a number of different reasons.

The real question we need to address now is, what policies will be adopted, and will those policies be coherent and compatible? There are many different policies to be concerned about, and they appear in different layers in the internet's architecture.

Take, for example, misinformation and disinformation. What should a social media application company do about content that is judged to be harmful, or judged to be essentially wrong and potentially disruptive? Who has the authority to decide if this information should not be further propagated? Do we want private-sector companies to make those decisions? Or do we want to have common standards on an international basis? Could we even get those agreements on an international basis, given the diversity of political regimes, cultures, and preferences? It's not clear how uniform we could make those kinds of policies.

What about law enforcement? How are we going to deal with the fact that somebody in Country A can be harming somebody in Country B? What if they don't have any kind of reciprocal agreement about extradition? What is considered to be enforceable in different jurisdictions? Or look at digital signatures, if you and I create an online contract, and we each digitally sign it, and one or the other of us fails to meet the terms and conditions of the contract, in which jurisdiction will our digital signatures be treated as binding? What requirements will there be for the release of a digital signature capability, including a public and private key pair that would be binding to both of us? What are the terms and conditions that we would all recognize in different courts and different jurisdictions?

One approach to these questions is the work being done by the Global Commission on the Stability of Cyberspace, which has been working to formulate norms to encourage consistent governance across the internet. But eventually many of these issues will need to find their way into multilateral laws. The European Union's consistent approach to regulating market dynamics is one example of collaborative, multi-country, internet governance. But it builds from the EU's existing governance processes. Working across many countries around the world is a much more challenging endeavor.

The norms that The Global Commission has been proposing are not treaties, although they could be prelude to those kinds of agreements. They're intended to explore a space of common value that might be agreed upon by at least a subset of the countries in the world. For example, their first norm was to argue that we should agree not to interfere with, or harm, or damage, the public core of the internet. That fundamentally means all of the basic infrastructure that allows the internet to function, such as routers, the domain name system, the servers, and the undersea cables. The Global Commission suggests that all of that basic infrastructure should be considered hands off, in the same way that we agree that we don't attack schools and hospitals even in wartime.

My hope is that these various potential norms might lead to common agreement among some subset of the countries of the world that would make the internet function more effectively, and create a safer and more secure environment.

Creating Social Mass

When it comes to creating "social mass," the third leg of the stool, it's very important that the citizens, the users of the network, feel some responsibility for their own behavior. It sounds simple, but it really does mean things like not picking "password" as your password, or using the same password for every online account that you have.

In that regard, personal cybersecurity isn't too different from wearing a mask to help protect against COVID. The mask is not just protecting you from others, it's protecting others from you. The security penetration of some systems is a consequence of someone choosing bad passwords, or creating other risks such as accessing questionable websites, or using insecure software, or not using a Virtual Private Network (VPN) when accessing sensitive corporate networks. When you are exhibiting vulnerable behaviors, the harms may actually come to other parties besides yourself.

I'll give you a business example that was in the news. A retailer was using certain devices to read customer credit cards at the point of sale. They acquired these devices from a manufacturer whose software turned out to be insecure. Hackers were able to break the security code on those devices and reprogrammed them, so that whenever a credit card was swiped at the point of sale, at the same time the credit card information was being sent to a bank it would also go to the bad guy. That's an example of a company's security practices having an effect on a large number of people whose own behavior didn't create any cyber risk.

Achieving social mass is as much a function of leadership as anything else. As business and technology leaders, we have a responsibility to set both an example and an agenda. We have to communicate the value and beauty of a free and open internet but we must also be clear about the risk and about the types of behaviors that can both cause and mitigate risk. We need to inspire everyone as individuals and organizations, citizens and communities, to encourage the social mass that can help us all shoulder our own responsibility for safe and secure behavior.

Toward a More People-Centered Internet

As we work to make the internet more safe, reliable, and secure, and to inspire the next generation of users and leaders, I want to emphasize how important it is to assure the actual utility of the system to a broad range of people. It provides very little value to many kinds of people around the world, to install internet access somewhere, making it sustainable and affordable, if there is no utility in it.

What applications are available to the parties who finally get access? What information is available in local languages? What accommodations are being made for disabilities? Can we turn the internet into an economic engine for many different kinds of people, providing options for work that they might not have had before?

During the COVID pandemic, there has been a very significant digital divide. Many people of means were able to use the internet to continue doing their work from home. Yet many other people who had to be on site to make a living had no such opportunity, and were, in fact, placed at even greater risk of exposure. So the pandemic shone a very bright spotlight on these kinds of fissures in the social and economic systems around the world.

We should take those lessons from the pandemic to heart when we work to build a more people-centered internet. We need to redesign much of the lower-paid work around the world, and leverage the power of the internet, to help even out those economic disparities.

To ensure the utility of the internet for coming generations, I am hopeful that there will be broad and international agreement that the internet should continue to be as open as we can make it, while we are trying to protect people from

harm. If we are successful in finding ways to do that, then we can look back and say we did today what was right.

Coming generations need to believe two things. First of all, they have to believe that it's possible to do new things on the internet—and I guarantee you that there are always new ideas coming. But the second thing is that they need to believe that there's an environment in which their new ideas can thrive. And for that we need to have a collective will to create a safer and more secure infrastructure that's as reliable as possible, and as affordable as possible, so that everybody can benefit from it.

2

Forget About the New Normal. We're in the New Now.

Lieutenant General Bruce T. Crawford — Retired Chief Information Officer, U.S. Army, Department of Defense

Since the COVID-19 pandemic changed our lives in early 2020, we have all intellectually been in search of ways to remain centered and focused on essential tasks. Our lives have become far more complex, and we have all been consumed with "the mission (personal and professional)," whether that is protecting against cybersecurity threats or ensuring that our families are safe and healthy. Some long for the comfort and predictability of the past and are searching for ways to fit the uncertainty of the COVID environment into that template. The reality is we are likely in the midst of a cascading series of future states that mandates a fundamentally different approach to maintain our competitive advantage, regardless of the roles we play.

It is the magnitude and intensity of the mission that requires us to find ways to stay grounded, alert, aware, and optimistic for those we are privileged to lead … and, truth be told, for ourselves. One way I like to do that is by getting in an early-morning run, thinking about the many facets and complexities of the mission to keep our organization safe, secure, and functioning at optimal efficiency. Like so many of my teammates in the military—and like many others in the private sector—my thoughts were dominated on one typical morning run by a recurring theme:

The new normal.

We've all heard, and probably uttered that phrase so often this year that it has the potential to become stale and meaningless. While I believe that many people have defaulted to that phrase as a way to explain what we're going through and what may be around the corner, the reality is that a return to normalcy may be unachievable. We may talk about the new normal as a way to improve our comfort with our current challenges, but I feel it's time that we all need to embrace the change and begin posturing our people and our organizations to rapidly adapt, at speed, and at scale. My sense is the time has come to forget the new normal and embrace the realities of the new now.

Everything Feels Different

What do I mean by the new now, and how is it different from the new normal narrative that has dominated the headlines? Let me use what we experienced as a result of the national tragedy of September 11, 2001 to explain.

As fate would have it, I was in the Pentagon on that horrific day. The next day,

we all knew that many things were going to be different. New rules were quickly developed to ensure the physical security of our people and our national assets. In the military, this included things like installing concrete barriers at the entrances to our bases and tightening up security checks before we could pass through checkpoints. For anyone traveling, we enacted new airport security measures, including taking our shoes off at security gates. All necessary steps, and they undoubtedly helped to keep us safe amid uncertainty. This became our new normal. And arguably even conceptually, we are still doing many of the same things, in the same manner today, with relatively few adjustments or updates over the past nineteen years.

Now, by contrast, in what I describe as the new now, everything feels different. My instincts tell me that things have changed in ways and magnitudes we could not have imagined. The mood of our organizations, our businesses, and our workforces are very different. New variables are constantly being introduced into the equations of our daily lives, forcing us all to continuously adapt to the here and "new" now.

Our focus has to rapidly shift from regaining normalcy, to real-time adaptation to rapidly changing conditions affecting what we do, and how we do it, now.

The New Now and Cybersecurity

What does this have to do with cybersecurity? Nothing. Well, nothing if you are rooted in traditional thinking around threats, user environments, tools, and processes. But if you appreciate just how much things have changed and will continue to change, then welcome to the new now of cybersecurity. We must rethink how we will leverage cyber capabilities. How we will run and defend operational and business networks, and data critical to the achievement of the near and long-term goals of our organizations.

More than a decade ago, I read a quote from General Stanley McChrystal, who at that time was leading all U.S. Forces in Afghanistan. His lesson was simple but powerful:

> *"We have to start getting comfortable being uncomfortable."*

Although I've never had the pleasure of meeting him in person, his thinking resonates with me now more than ever. In the complex environment of COVID, where the dawning of each day introduces new variables into the equation, we can't allow ourselves to just keep doing things the same way and expecting a different outcome. The conditions never remain static, and new complexities continuously emerge. And those complexities are often so disruptive that status quo is unobtainable.

Over this time, I've had many occasions to talk to my colleagues in the enterprise IT and cybersecurity space, including those in corporate America. Initially we were all yearning for the predictability of the pre-COVID good old days where everyone pretty much knew the rules, the structure of the marketplace, and the demands of our jobs. In the past, with few exceptions, we all had the ability to determine what was secure and what was at risk, but now I don't think we are going to have that comfort for quite a while—or if ever at all.

Whether you are ensuring that your organization can retain its footing, or in my case protecting the U.S. Army's digital assets, it's important to understand what "uncomfortable" feels like so you can get comfortable being uncomfortable in the new now.

Let this sink in: As an example, in the Army, overnight we went from defending the traditional network perimeters at 288 posts, camps, and stations and the Penta-

gon in 143 countries, to literally defending the living room. Who among us could honestly say they saw that one coming? Business and organizations continued to function, many with increased efficiency, but the dramatic expansion of the cyberattack surface, impacted by a teleworking workforce, created a different set of challenges, never before imagined at this speed and scale.

Well, get used to that, because in the new now, at some point there will be no such thing as telework. Having witnessed the rapid acceptance of the virtual space, my prediction is it will be culturally accepted as just work. Almost overnight, "the office" has become wherever the user happens to be. Location is fast becoming irrelevant. Because in the new now, the office is where the user is. This mandates an institutional shift in how we think about cybersecurity in the rapidly changing world of the new now.

Now, we need to deal with some hard truths.

The People Problem: Reimagining the Workforce of the Future in the Race for Talent

If there is a silver lining to the pandemic and its impact on those of us charged with cybersecurity, it is that it has forced us to be more innovative, bold, and resourceful in embracing new ideas. At the very top of that list of new ideas is the need to shift our focus to, what I consider to be, the absolute center of gravity for delivering cybersecurity capabilities and all things related to digital modernization integration: Our people.

Right before our eyes, the values of the future workforce and next generation of leaders is evolving at speed and at scale, and is heavily influenced by how they digest information, mainly in the virtual space.

It is no secret, regardless of your line of business, that sustaining a skilled workforce is a key to our ability to maintain our competitive advantage. In a world where money is no longer the key variable in the race for talent equation, the fundamental question for us all is do we have the talent to compete? If not, how will we adapt traditional HR to rapidly upskill (existing capacity), reskill (legacy capacity), recruit, and retain the very best and brightest in the global race for talent? It's a very complex question, but my instincts are that the answer lies in our ability to embrace next generation virtual training platforms and a fundamental shift in our thinking that places more institutional training emphasis on skills, rather than legacy certifications.

According to a 2019 report by the Center For Strategic And International Studies, the number of unfilled cybersecurity positions has grown by more than 50% since 2015. We all know about the huge cybersecurity and enterprise IT skills gap that exists, and I can confirm we have the same issues in the military that you face in the private sector. Automation, machine learning algorithms, and AI tools help a lot, but you still need intellectually curious, adaptive, and resourceful people to create and execute our cybersecurity and enterprise IT strategies. That means recruiting and retaining the best people, and to do that, we all need to pay a lot more attention to creating a better organizational environment, one that accounts for the ideas and issues today's (and tomorrow's) workforce cares about. In addition to the work/life balance I mentioned earlier, we need to put in place more substantial, meaningful and committed mentorship programs and commit to an organizational culture that puts more value on skills than on legacy certifications.

This certification issue is an important one to me, and it's not that I don't value traditional certifications for cybersecurity or for any technical requirement;

I definitely do. But at the end of the day in the new now, all we can count on is that things are going to change, and probably dramatically so. So, certifications that are built on baselines of knowledge and competence will only go so far; in the end, smart people with a passion and superior skills make all the difference.

So how do you transition your organization, to rapidly increase the cybersecurity skillset of the workforce? To properly scale your abilities in the new now, speed, flexibility, and agility matter; you can't achieve that by simply sending people to traditional certification programs. Think of the Army and its 15,000 IT professionals, and consider how long it would take, and how much it would cost, to up-skill and reskill that workforce? What is needed is institutional acceptance of post-COVID AI, machine learning-enabled virtual training platforms that not only leverage online training but also provide a virtual means to assess the current state of skills in our organizations. We need to focus on skills from the start in our training and recruiting efforts, especially in a segment where the rules of the game change so dramatically and so rapidly as cybersecurity. The world of academia is changing and so should we. Nano degrees and AI-enabled online training in the virtual space are critical enablers to winning the race for talent.

We also have to keep in mind that although defending traditional enterprise networks is still of the utmost importance, the insatiable appetite for data associated with the ever-changing environment of the new now demands more emphasis on protecting our data. We need data scientists, data analysts, data engineers, because data is the common fabric in our cybersecurity defenses. It's the reason hackers hack—to get at our data. I've heard and read a lot in recent years about "data being the new oil" of the global economy, and that makes a lot of sense. But I do have a somewhat different angle on that axiom, one that fits for the military but also for any sector: Data is the new ammunition of the future fight and the fuel in the global era of great power competition.

Cybersecurity in the Business Value Proposition

For business and technology leaders, living and thriving in the new now requires understanding and confronting a few fundamental issues about cybersecurity today:

- **Cybersecurity must be integrated horizontally into the culture, mindset, and DNA of your organizations.** That means it must be considered as a part of every corporate action, which includes all strategy and investment decisions. From the boardroom to the conference room, especially given the dispersed nature of our workforce, cybersecurity must be horizontally integrated across all workflows and functions.

- **Cybersecurity, as well as the broader set of IT initiatives, must stop being viewed through only a technology lens.** Whether you run a construction company, a technology company, or a military command post, cybersecurity and IT must be aligned with the organization's mission and value proposition. I know you'll probably read about this issue in other chapters of this book, but it is so important and so existential to accomplishing our respective missions that it bears repeating.

- **IT and cybersecurity are too important to be left to the technologists (and I say this with full acknowledgement of my status as a "recovering technologist").** Embracing cybersecurity challenges goes far beyond making sure employees don't write their

passwords on sticky notes left on their computer. Just like DevOps quickly evolved into DevSecOps as organizations realized cybersecurity's critical impact on the business, we must commit ourselves to a greater level of collaboration among and between the business leaders and the techies.

Make Mobility a Core Business Tenet

One of my final thoughts on the new now is the primacy of mobility as a core business tenet, and the mandate to include mobility as a foundational element of future cybersecurity strategies. It wasn't that long ago that mobility was a way for organizations to make themselves look more attractive to Gen Z and millennial employees. "And you can work from home," went the HR sales pitch, with the often-unspoken caveat "If your manager OKs it." That was mobility in the new normal.

In the new now, as I previously mentioned, the office is now wherever the user happens to be. Mobility is an absolute must-have, not a perk. Mobility must be as much a part of business processes as your intellectual property, marketing messages and corporate culture. You can't operate if you don't have mobility at the core of your workflows, and you can't be mobile without the right security mindset at the edge of the enterprise, where the user literally lives.

Again thinking back to the onset of the pandemic, it was astonishing how quickly the cyberattack surface expanded. In the Pentagon, we went from about 1% telework to 90%-plus telework almost overnight. We went from traditional boundary cyber defenses to defending our personal space where our kids previously shared our networks, our devices, and our cloud services.

While leaders in business, education, the military, and all walks of life tried to keep up with this exponential rate of change, those who would do us harm have been watching our actions (or inactions) very closely. We must begin our cybersecurity strategies in the new now with that assumption—that all operating spaces will be contested; nothing is safe, and nothing is off-limits to our adversaries.

Redefining Normal

Let's set aside any notion that we will return to anything that approaches our traditional definition of normal—not in work, not in many of our usual personal activities, and certainly not in cybersecurity.

Instead, embrace the new now. When you understand that tomorrow may likely be very different from today, and next week and next month and next year will be even more different, you'll understand and appreciate the strategic shift in our institutional thinking that is required to secure our networks, our data, our identities, and our lives.

To help me reset my ideas and expectations, I still rely on my morning run. It may be one of the few remaining "normal" things in my life, especially as I transition from my life in the military to my life as a private citizen. But I'm OK with setting aside normal. Bring on the new now.

Seizing the Opportunities, Understanding the Challenges

3

Why Our Digital DNA Must Evolve—Quickly

Salim Ismail — Founder, ExO Foundation; Board Member, XPRIZE

Our world is about to go from less than a billion connected sensors to 20 billion to more than a trillion, all in a time frame that will, in retrospect, seem like the veritable blink of an eye. In many ways, we are moving faster than our ability to keep pace with the change. Thus, we are seeing a disconnect between what we *can* do and what we *want* to do.

Here are two small, but illustrative, examples: Nearly two-thirds of executives say boards of directors have a vital role to play in digital transformation, yet only 27% say their boards are advocates for current strategies.[1] At the same time, 70% of CEOs say the move to the cloud and digitization is outpacing their ability to understand and define the risks.[2]

The opportunity before us is too important for these types of gaps to continue. The entire human race is at the threshold of an era of exponential change, when technology will transform all aspects of humanity into a digital environment—right down to our very DNA and cerebral cortexes. Moreover, as data continues to grow exponentially, it will become interconnected in the cloud to form a cyber mesh of data.

Our Immune Systems Are Causing Disconnects

We are experiencing these disconnects because, fundamentally, our systems are not designed to absorb this amount of dramatic and rapid change. We all rely on protective measures to adapt to change and mitigate risk, whether we are talking about the biological systems in our bodies or the cultures and processes we have built into our organizations. I refer to these protective measures as immune systems, and they are built into our business and institutional practices just as surely as they are built into bodies.

In business, these immune systems comprise governance procedures we've put in place, restrictions on how we utilize personnel, processes or technologies, or rules that specify how new ideas are presented within the organization. Whatever they are, they serve the purpose of slowing down and regulating our corporate metabolism. And, in many ways, they work for us. Until they don't.

In today's environment, these immune systems are contrary to our need to move quickly and keep up with technology innovation, particularly as we

embrace exponentially accelerating technologies, such as artificial intelligence and quantum computing. If we are to fulfill the promise of the Digital Age, we must overcome the limitations caused by our organizational immune systems.

To Fix Cybersecurity, We Must Remove Roadblocks to Innovation

We must also, finally and fundamentally, address the immense cybersecurity challenges of this new world order and ensure that our immune systems don't slow us down or stop us from making the necessary changes. We must remove roadblocks to cybersecurity innovation.

For example, many organizations still have a large number of point products in place that are not connected with one another and don't offer sufficient security against modern attack methods. The organization may think they are protected, when they actually have gaps. Relying on older technologies and not getting rid of solutions that don't work is an obstacle to innovation. The cyber mesh is growing exponentially; cybersecurity must keep pace.

Why? Here's the reality: As we expand our cyber mesh of data, as we transform to a world of more than a trillion sensors, we are exposing ourselves to a potential cyberattack surface the likes of which we have never seen. We are already struggling to deal with the world's existing attack surface. If we don't figure out the cybersecurity challenges of our expanding cyber mesh of data, we run the risk of being victims of our progress, rather than beneficiaries.

How do we move forward? How do we embrace progress? How do we create a new digital DNA that our immune systems won't reject? And, perhaps most importantly, how do we ensure that our digital interactions and activities are suitably safe in a world where our very bodies are exposed to the potential of a cyberattack?

Getting Ready for Exponential Disruption

Data has already become our most valuable currency and will remain the defining differentiator between organizations that thrive in the Digital Age and those that disappear. We've seen virtually every industry disrupted by connected digital technologies—transportation, media, advertising, healthcare, music, photography, communications, finance, entertainment, retail. The list goes on—and we're still at the beginning stage.

As we move from less than a billion sensors to 20 billion to a trillion and beyond, the potential for dynamic disruption expands exponentially, accelerated by the shift from the read phase of digitization to the write phase. In this next phase, we are talking about the capability of writing code to our bodies, brains, and genomes. From a biotech standpoint, we are probably within two years of more widespread deployment. From a neuroscience standpoint, we are perhaps five or six years away.

Real-World Examples, Real-World Risks

We are already seeing examples of how this next advance in the Digital Age will affect our lives, health, leisure, and work. Think about healthcare in an age when we can each have a tiny sensor injected into the fatty area between our thumb and forefinger, whereby clinicians can easily access identity data, medication information, and emergency information. Or when an alert automatically sends a message to our physician at the first sign of a clogged artery or a leukemia cell entering into our bloodstream.

Look at what has been accomplished by Neil Harbisson, who had a "cyborg

antenna" implanted in his brain to help him deal with an extreme form of color blindness. The antenna allows him to feel and hear colors as audio vibrations inside his head.[3] Think about extending the capabilities of our human memories with petabytes of data stored somewhere deep within the cortexes of our brains.

We are also, unfortunately, seeing some of the risks of this new world. In 2017, the U.S. Food and Drug Administration recalled nearly half a million pacemakers because of security flaws that made them vulnerable to cyberattack.[4] Nations are already collecting the DNA of government leaders to prepare for the possibility of a targeted cyber-based bio attack.[5] And before we see self-driving cars on the road, we have to be comfortable that the level of vulnerability is acceptable. We can only imagine the potential chaos and harm a fleet of unmanned vehicles could create if they were controlled by adversarial forces.

It's Time to Think Big

Yet, forward we progress. We are creating exponentially more volume and variety of data, seemingly by the second. If we go about our business without making any changes, we are heading for disaster.

If you want to address big problems, you need to think big. Our organization has studied common traits among the world's fastest growing startup companies and has identified that each of these organizations is able to articulate a Massive Transformative Purpose. This is defined as the higher aspirational purpose of the organization.

If data is a resource like oil, then we need to start thinking about it that way. Do we have a Massive Transformative Purpose? Can we create one? What would it be? One thing is clear: When it comes to cybersecurity, our current frameworks, mindsets, and immune systems hamper us and need to be addressed.

Can We Break Down Our Immune Systems to Empower Innovation Securely?

Immune systems protect us against radical change. They are wired to give us time to adjust and figure out the right outcomes. Governance is designed to be compliant with process and regulation because we know it is necessary. But what works in one context doesn't work so well in another. Immune systems can sometimes be roadblocks to innovation.

To move forward with cybersecurity in the Digital Age, we need to break down our current immune systems so that we are encouraging, embracing, and empowering rapid change and innovation.

It is certainly possible to engineer our immune systems to respond quickly. When a doctor performs a kidney transplant, she administers an immunosuppressant drug so the new kidney has time to bed down. Can we create similar results in our organizations, whereby the normal attack on the status quo is suppressed and new ideas have time to find a foothold?

Can We Create a Process to Solve the Immune System Problem?

The simple answer is "yes." I know because our organization has created and implemented a successful model that works. The process works as follows:

- Bring together senior management from across the organization. Showcase new technologies, threats, and opportunities—very much shock and awe—to show that disruptive threats are on the horizon and something must be done. This creates a burning platform for change.
- Gather 25 young leaders/future lieutenants to do the real work over 10 weeks. Divide them into two streams:

» One stream looks at disruptive new ideas in adjacent industries that could grow the business by 10x or more;

» The second stream examines the existing organization and chooses mechanisms to improve the status quo.

At the end of the 10 weeks, they present their ideas. Senior management funds the ideas that they believe are worth it. We have seen conclusively that management, leadership, and culture can leapfrog three years ahead in that 10-week period.

In analyzing why it works, we found that the opening workshop acts like an immunosuppressant drug, similar to a doctor performing a kidney transplant. By having the future leaders create new ideas (with coaching support), they champion and own those ideas, increasing chances of adoption in the future. In the past, disruptive ideas got funded about 10–15% of the time; now, when you break down the immune systems, we find more than 90% of new ideas get fully funded.

Can We Apply the Process to Cybersecurity?

Absolutely. There are many different ways to approach and implement the process. Individual organizations could take one approach, regulatory bodies could take another, and organizations in different industries can implement the model based on their own challenges. Heavily regulated industries, such as financial services and healthcare, have different challenges than organizations in industries where regulation is less of a factor. While the same basic processes and principles apply, the specifics of each engagement can change, based on the organization and its goals.

An approach we took in the public sector provides an illustrative model that could be applied to cybersecurity. We set a deliberately aggressive objective: Drop the cost of an existing problem by 10 times. Perhaps this is not as audacious as making a safe, secure, and people-centered internet, but it is a worthy and difficult goal, nonetheless. We formed teams to take a problem space—such as transportation, healthcare, or affordable housing—through four phases:

1. **Technology layer:** The goal was to examine breakthroughs that will drive the future, looking at new technologies and working with maker spaces, biohacking labs, and fabrication laboratories. Areas explored included sensors, 3D printing, robotics, artificial intelligence, synthetic biology, and eco-friendly technologies, such as green building construction and low-carbon energy sources.
2. **Design layer:** The goal was to picture, imagine, design, and describe technology solutions. We worked with artists, science fiction writers, designers, and media experts to envision and paint a future with technologies in mind. Design experts then used human-centered design techniques to integrate that vision into possible products and services.
3. **Entrepreneurial layer:** The goal was to ensure economic sustainability. We looked at developing funding mechanisms to help entrepreneurs raise money; created models to ensure the sustainability of potential solutions (via business or taxes); and designed business models to solve major problems through the combination of design and technology.
4. **Social layer:** The goal was to ensure that the solutions could be implemented into society. We worked with sociologists, anthropologists, regulatory experts, and legal thinkers. We explored public-private partnerships, conducted experiments and trials, and incorporated community leaders representing different social groups, classes, and interests.

In the City of Miami, we were able to create four components to address the specific problem of traffic congestion. Perhaps most important, funding has been made available for immediate development and employment.

Are We Ready to Transform Our Cybersecurity DNA?

We know the model works, and we know it can work in the cybersecurity space. First, we need the motivation to change, which should be well apparent to everyone reading this chapter and this book.

One of the characteristics that makes this era's progress exponential is hyper-connectivity. Because we are all digitally connected, ideas and innovations can spread quickly. This can be used for the greater good and, as we have seen, can also serve malevolent purposes. As we deploy models to transform our immune systems, hyper-connectivity can be used as a point of leverage. For example, it gives us the opportunity to work at the edges, where immune systems are less likely to create insurmountable obstacles.

Another important point is that we don't have to solve the problem all at once, all of us at the same time, all in unison. Although there is a definite urgency to the cybersecurity challenge, we can adopt the principles we have developed in specific organizations and then share them across a broader spectrum. For example, what we learned from our engagement in Miami can be applied to other cities, thus accelerating change by providing ideas, inspiration, and proven implementation techniques.

Finally, we have to recognize that when it comes to cybersecurity, we all share a collective purpose, whether we define that as a Massive Transformative Purpose in capital letters, or whether we collectively and individually create a pathway, step-by-step, toward a more secure future—a future in which we can fully embrace the Digital Age without fear that a cyber mesh will entrap us, rather than empower us.

Conclusion

In some ways, the journey ahead of us is clear. We *will*, without doubt, move forward in our inexorable march toward exponential digitization: We *will* go from a billion to more than a trillion sensors; we *will* leverage artificial intelligence and other exponential technologies; we *will* digitize our brains and bodies; we *will* transform all aspects of humanity into a digital environment. As a species, we are programmed to proceed, always seeking to embrace innovation and progress.

At the same time, however, the volume, velocity, and pace of change in today's Digital Age is without historical precedent. We are moving at a speed that threatens to overwhelm us if we don't put the proper protections and safeguards in place. To fulfill the promise of the Digital Age, we must overcome the limitations of the immune systems we have built to protect us. In particular, we must transform our digital DNA so we can move forward creatively and innovatively to address the cybersecurity challenge before us. Now's the time.

---

1 "The Board of Directors You Need for a Digital Transformation," Harvard Business Review, July 13, 2017.

2 "Cybersecurity and the cloud," Vanson Bourne 2018.

3 "Neil Harbisson: the world's first cyborg artist," The Guardian, May 6, 2014.

4 "Three reasons why pacemakers are vulnerable to hacking," The Conversation, Sept. 4, 2017.

5 "Hacking the President's DNA," The Atlantic, November 2012.

4

The Exhilarating, Exciting, and Sobering World of the Internet of Things: Imagine the Opportunities, and Realize the Risks

Jennifer Steffens — Chief Executive Officer, IOActive

Few technologies have the potential to impact the way we work, live, play, shop, and interact like the Internet of Things. Imagine the ability to use sensors, embedded chips, process inputs, and other ways to "smarten" everything, from our cars and our health to our physical communities.

At the same time, let's keep the excitement of connected things in perspective. Smart cities, intelligent dialysis machines, and self-replenishing retail shelves all are examples of using IoT to enhance our lives at work and at home. An IoT-enabled hairbrush is not.

Capturing, analyzing, and leveraging seemingly infinite volumes and varieties of data are exhilarating and can help fuel innovation for more life-enhancing IoT products. But it also can cause well-founded alarm for executives and consumers if care is not taken to account for bad actors and other threats to intelligent devices and processes.

Fortunately, best practices are emerging to address these IoT issues today, even as the technology is still in its infancy. The successful organizations will be the ones that can stay ahead of the curve in spotting opportunities. They will need to open their minds to find innovative ways to stop threats and build a safe digital environment for consumers.

Can You Imagine It? Imagine the Heady Stuff

There's no need to recite gaudy statistics—and there are oceans of them—about the explosive growth of IoT market expenditures, the number of connected devices, and the economic impact of an IoT-infused market ecosystem. Forget about clichés like "the tip of the iceberg." We're looking at the Marianas Trench—which is deeper than Mount Everest is high—of IoT market development. Many of us can't begin to imagine how big IoT is going to become because, like the Marianas Trench, we really don't see it. Stuff like computerized automotive emissions controls, cashless tolling systems, and retail loss prevention packaging are so much a part of our everyday lives that we don't even think of them as IoT applications.

For people like me, the heady stuff is trying to figure out where IoT will take us in the future, and what it will mean for society—for better or for worse.

Obviously, there are tons of business-to-business applications where IoT has only scratched the surface, such as inventory control in retailing and wholesale distribution, manufacturing floor workflows, RFID in third-party logistics, and smart power grids. And consumer applications are even more plentiful and fanciful because of the way they impact our lives, including sensor-controlled traffic management, intelligent medical devices, smart homes, and connected cars. These and similar applications are fast becoming commonplace, and our children will have trouble imagining a time when they didn't download music from the internet to their GoPro camera while gliding down the mountain on auto-leveling skis.

And then, there are the odd, eccentric, and downright weird (to some people whose imaginations don't always stretch that far), like "bovine management" (AKA, smart farming), internet-connected toys and, yes, even intelligent hairbrushes.

But, let your imagination run wild, and you'll begin to consider the vast array of possibilities to make things more efficient, affordable, and interesting for us. And for business executives and board members who care less about the technology behind those solutions and more about the financial opportunities it affords, these are exciting times.

Just imagine it:

- Machine-learning-enabled telemedicine (think of it as digital house calls on steroids), where doctors can receive real-time updates on a patient's heart condition before the patient even feels anything, and the doctor can fix the problem remotely using a smartphone.
- Store managers who uncover an organized retail-theft plot by matching an employee's digital ID with merchandise removed from a shelf, but not accounted for as a sale.
- Consumers who learn that their credit card numbers are being used 1,000 miles away—before their banks' fraud departments notify them and cancel their cards.
- City officials who spot a terrorist's attempt to poison municipal water sources from across the world using malware uploaded from a burner cell phone.

Undoubtedly, business executives and board members reading this chapter can envision countless other applications and use cases—if they can just let their imaginations run free.

Of course, there are significant implications for these and other soon-to-emerge IoT applications. Regulatory, legal, privacy, and cultural concerns weigh heavy on everyone's minds—and they should. Still, it's important for decision-makers to not let fear, uncertainty, and doubt cloud innovation and opportunity.

And that's why it's crucial that executives and boards keep in mind their leadership responsibilities: to question and to ensure their organizations stay ahead of rapidly emerging threats, at all stages of IoT product innovation and development.

IoT Threats and Risks: Look Before You Leap and Make a Connection

Here's a two-part premise for business executives, government leaders, and board members about IoT:

> **Part 1:** Let's agree that just because something *can* be connected doesn't mean it *should* be connected.
>
> **Part 2:** If something is connected because it has the potential to improve our work or personal lives—or generate revenue for our businesses—we need to understand that there are always risks involved.

In Part 1, my point is that we now have the ability to embed, attach, or integrate technology with everything from industrial equipment and our municipalities' most important services to household devices and our children's toys. Our electronics are smaller and more functional, our algorithms more intelligent and flexible, our packaging more inconspicuous and even attractive. But organizations and their leaders need to really think twice about whether intelligent food or robotic office plants—although technically feasible—are what we all need. We all know that consumers, in particular, love shiny new things. But the "if you build it, they will come" philosophy has never proven to be a sound and profitable business strategy.

But Part 2 is where we need to really put our energies, talents, and imaginations. Any time you connect something to another device, a computer network or the internet, you are opening up potential new avenues for intrusions and breaches. As business leaders, we naturally worry about the financial, operational, and legal impact of hacking IoT systems.

But what about other kinds of more personal risks? How about the risks to our children when their smart toys are hacked by bad actors to track their locations? *The New York Times,* in a lengthy article about smart toys for the holiday season, pointed out numerous instances of chip- and sensor-based toys that exuded vulnerabilities; some of them were even banned by various European government regulators.[1]

And then there are even potentially more widespread, insidious, and catastrophic risks. What if hackers were to access a city's water purification system through Wi-Fi-based controllers? Or if someone's electronic pacemaker was corrupted through an RFID-enabled watch? Or foreign powers manipulated a country's national voting systems by downloading malware from a smartphone to an electronic voting booth? Or if computerized braking systems on our cars and trucks were disabled over the internet?

These are not hypothetical scenarios. Our company has long been involved in testing security vulnerabilities of IoT-based systems, and our experts have determined that all the scenarios—and more—are not only possible, but in many cases have actually happened.

Our researchers have repeatedly demonstrated that cars can be disabled while they are being driven, vulnerabilities of internet-connected toys can be exploited, and pacemakers can be maliciously hacked. And as for smart cities—well, let's just say our researchers have determined that those cities aren't always as smart—or as "digitally safe"—as they'd like to think.

Therefore, it's important to remember a few undeniable facts about IoT risks:

- The more "things" we connect to our network and the public internet, the more vulnerabilities are created. This is particularly true with what our technical colleagues call "unmanaged endpoints," which often lack the robust and automated security our traditional computer endpoints now include as second nature.
- The bad guys are working together, sharing information, tips, tricks, and shortcuts. They are even jointly funding efforts through their own flavor of crowdsourcing on the dark web.
- The good guys, by comparison, are usually going it alone. Companies and governments around the world rarely feel comfortable collaborating on security because it exposes their risks to others, presumably eroding what they see as competitive advantage.

- The potential for more and more risks is going to expand in direct proportion to the dramatic increase in connected devices, systems, and business processes.

In short, doing nothing is not a sound business strategy. I'm sure the regulators would agree, as well.

Addressing IoT's Problems and Fulfilling Its Potential

Let me be clear about what I am *not* saying: I am not advocating that businesses and public organizations pump the brakes on IoT solutions development and deployment. Far, far from it. I am so excited about the potential for IoT to enhance our lives, our businesses, our institutions, and our society that I want to see research, development, manufacturing, marketing, and sales proceed as quickly as possible in order to meet consumer and business demand.

In order to do that, those of you reading this chapter—and in fact, this entire book—should keep a few principles in mind about IoT risk management, remediation, and security best practices. It also is important for business and public sector leaders to consider the broader implications of where IoT is going in the future, as it relates to societal and cultural trends.

These suggestions are intended for the entire IoT ecosystem, from technology creators and enterprises integrating IoT into products and services, to governments, regulators, and "fixers."

- **Security should be designed into IoT solutions from the start, not after a breach.** I know, it sounds easy, right? But in our euphoria over discovering the ability to connect everything to anything, we must not lose track of the increased risk profile our businesses, government institutions, and citizens can face. Fixing security breaches after the fact is very costly and inefficient. In fact, looking at how regulators are clamping down on organizations that suffer a security breach, no matter how well-intended everyone may have been, it's vital for security in IoT systems to become an essential feature, just as important as what a connected device can do. Some of you may balk at the idea of doing early-stage security integration into inexpensive electronic devices because of the perceived costs and potential impact in time to market. But I can assure you that costs and time to market will be much worse if and when you suffer a breach. Get it done right from the initial design phase.
- **Don't throw a broad, one-size-fits-all security blanket over your IoT innovations.** As big an advocate for IoT security and vulnerability defense frameworks as I am, I am completely open-eyed about the need to balance security requirements with product functionality that delivers an outstanding customer experience. The good news is that those two ends of the spectrum are not mutually exclusive—you can and should have rock-solid security on all connected devices without making businesses, consumers, or citizens jump through hoops in order to take advantage of these exciting technologies.
- **Collaboration is good for everyone.** Industry players, governments, regulators, consumer groups, standards bodies: All of these parts of the IoT ecosystem should work together to explore exciting new opportunities and to balance those opportunities with known and potential new security frameworks to protect everyone. Technology companies have often found ways around their latent competitiveness to create technology roadmaps and solutions guides that grow their market opportunity and

give customers viable, productive solutions. Besides, we already know that the bad guys have put their heads together to find ways to muck things up. Don't let them get a leg up on our efforts because we are too proud or too stubborn to work together.

- **Customers are willing to make tradeoffs on things like privacy in order to use IoT for fun and profit. Don't let them go too far.** Not that long ago, Facebook members were reluctant to reveal too many personal details on their walls. Now, they promote every aspect of their lives (sometimes to their detriment) in order to enjoy the full experience of social media. This means your organizations need to be careful not to let customers' exuberance in adopting the "next new thing" put them—or your organization—in harm's way. Make sure your customers and consumers are aware of best practices and smart IoT hygiene in order to remain secure while still getting the most out of technology integrated into everyday work and home lives.

A Few Ways for Business Leaders and Board Members to Stretch Their Imaginations

Whether you're a CISO at a global financial institution, a board member of a nonprofit educational foundation, or the CEO of a technology company committed to connecting every node on the global network, there are five things I recommend you do now to prepare yourself for the heady times that await us.

1. Boards should bring in a security expert—either as a member or as a consultant—so the security voice is heard loud and clear as new IoT development programs are discussed and planned.
2. Decisions about security are too often made too low in the organization, by security technicians, IT staff, or others "close to the flame." Security is a strategic initiative and needs to be treated as such by non-technical executives and business leaders.
3. Don't stifle innovation by giving in to fears about corporate-wide breaches and blaring headlines. You didn't get to this level of achievement in your careers by being timid. Be bold, but be smart. Balancing risk with reward is what leaders do.
4. If anyone answers your question about security as you roll out IoT solutions with, "That's how we've always done it," show them the door.
5. "Smart security" approaches are being implemented every day at companies such as Microsoft, the Mayo Clinic, and General Motors, to name just a few. Strive to add your organization's name to this impressive and growing list.

Conclusion

IoT isn't about to transform our society; it's already doing it. Every day, more and more applications emerge that make everyday devices smarter and more utilitarian than one could have ever imagined.

Which brings us back to one of our core themes: Imagine.

Nearly 50 years ago, John Lennon sang about a different kind of world, one with infinite possibilities for all of us. I'm pretty sure he didn't specifically envision the role that sensors, self-driving cars, and intelligent household products would play in changing how we live, work, and play. But he did encourage us to stretch our imaginations:

"You may say I'm a dreamer
But I'm not the only one."

Unlike Lennon, I'm a business executive who loves finding the intersection between technology, customers, employees, work, and play. But just like the famous Beatle, I'm a dreamer. I can imagine the powerful and transformative role that IoT—and its eventual spin-off technologies—will play in our society.

Just don't ask me why we need a smart chip in a hairbrush.

---

[1] "Don't Give Kids Holiday Gifts That Can Spy on Them," The New York Times, December 8, 2017.

5

How Data Grids Will Power the Economy and Influence Our Future

Rama Vedashree — Chief Executive Officer, Data Security Council of India

Within just two decades, since the beginning of the third millennium, digital data has transformed everything.

It started with the sheer volume of data, which became multiplied by the many digital formats and media forms. The internet and cloud have enabled digital data to become connected into a global data grid, which has enabled us to gain intricate insights into one another, as well as how our world works, plays, interacts, and governs. It has reshaped the very nature of our communities at the local, regional, and global levels—enriching our economies, enabling collaboration across the world, and allowing us to enjoy more productive lives at work and at home.

In turn, accessibility to this cyber mesh of connected and connectable data has elevated the potential for cyber risk and "digital deluge." It has created an important sense of urgency for an ecosystem of enablers—governments, enterprises, educational institutions, and advocacy groups—to work together toward the common goal of making our digital universe safer.

When I took on the role of CEO of the Data Security Council of India four years ago, I was optimistic about the commitment of interested stakeholders in ensuring that the digital economy and, in fact, our digital lives, would be safe and secure. However, a number of factors are coalescing to give us concern. The fast-paced digitization momentum across the world, rapidly growing economies like India's and China's, and the World Economic Forum's "Global Risks Report 2018," which cites cyber risks and data theft/fraud as global risks, are together a wake-up call for action at the global, regional, and national levels.

Still, four years later, I am even more optimistic about our ability to harness this massive wave of data, in all its many forms and connections, for the good of our global societies. Of course, I am also realistic about the need for intelligent cyber risk identification and mitigation practices in order for us to build and prosper from the "digitization of everything."

At the core of this ability to build and benefit from a cyber mesh of data are five key concepts:

1. Developing a global data grid to shape and fuel the global economy.
2. Using data as the new currency for today and, especially, the future.

3. Weighing the ramifications of Big Data in shaping the enterprise and consumer of the future.
4. Balancing our innovation ecosystem with the reality of data monopolies.
5. Enabling cybersecurity and privacy imperatives to co-exist in a data-driven world.

Where we go from here is dependent on a whole host of factors, many of which have yet to emerge and are difficult to predict with certainty. But we know this for sure: Digital data is going to change the world in even more dramatic ways than it has done since the invention of first-generation computing.

Data Grids: Powering the Global Economy

The concept of grids—interwoven, mesh-like systems and processes for a wide range of industries and applications—is well known and widely understood in our societies. Grids exist and function smoothly for such applications and sectors as power and electric, financial systems, aviation, and many others.

Now, a new type of grid has emerged—a global data grid—which merges the tremendous surge of information with all the connected points in other grids. This creates exciting, powerful business models that weren't available just a few years ago. For instance, think of how the free flow of data across physical and digital storefronts has spawned the age of multi-channel retailing that knows no geographic boundaries.

Global data grids also exist for the amazing growth in user-generated content—everything from social media platforms, wikis, blog sites, and personal e-diaries—that encompasses everything from family genealogy and hobbies to open source software communities.

In global data grids, information will increasingly be shared from sector grid to sector grid, promoting increased collaboration that utilizes common information or generates new insights from previously unseen data. This will rapidly evolve into a global, real-time data grid, with companies, government agencies, and consumers collaborating on data creation and access.

Think about the promise offered by data-centric compliance mandates, such as the U.S. Health Insurance Portability and Accountability Act (HIPAA), which allows patients to take their personal health information with them, regardless of which doctor, medical facility, insurance company, or healthcare service they use. Now, multiply that potential exponentially across industries and around the world. We see similar global data grids being formed in areas such as higher education, tying together both physical and virtual learning centers, as well as university-sponsored research laboratories, public policy think tanks, and community development programs. Consider, for instance, the increasingly global footprint of major universities, such as Harvard, Stanford, Oxford, and Le Sorbonne—all of which have built and are leveraging their own global data grids.

That is where we are going.

Data as the Currency of the Future

A generation ago, there was a lot of talk about, "Oil as the new currency." Today, however, there is increasing evidence that data is, in fact, becoming our new currency; and that trend is likely to accelerate. Consider these data points from industry research:

- By 2025, the value of the European Union data economy is projected to hit 1,054 billion Euros, representing 6.3% of European Union gross domestic product (GDP)—more than double its portion of GDP just five years earlier.[1]

- "Digital industry"—global data-centric market segments—will increase its annual profit margin potential by more than $1.4 trillion annually by 2030.[2]
- Digital transformation will contribute more than $1 trillion to the Asia Pacific GDP by 2021, driven heavily by artificial intelligence, the Internet of Things, Big Data, and other data-driven initiatives.[3]

Of course, trying to get a handle on the financial contribution of digital data isn't new. In fact, global consulting giant McKinsey wrote about this issue as far back as 2013, when it raised the notion of separating the economic impact of digital capital from that of tangible technology assets, such as hardware, software, and IT-enabled services.

It is clear, however, that it will not be long before we no longer are writing articles or papers with the headline, "Data is the New Currency" for a very pragmatic reason: Data is rapidly establishing itself as the currency of record for all global industries. It is, in fact, becoming the "new oil." In healthcare, financial services, manufacturing supply chains, retail, utilities, government services, and in all other market sectors, data is being monetized in a wide range of applications. And we have only tapped the surface.

Perhaps typical of the impact of data on markets, industries, and economies is a blog post by banking industry consultant Chris Skinner, who wrote:

> *"If all the things we used to do (in banking) make no profit anymore, where is the money to be made in the future? And the answer is: data."*

The Big Impact of Big Data Will Get Even Bigger

It is easy to be amazed at the massive growth of digital information. The much-discussed Big Data movement is now mainstream, and it has enjoyed enormous popularity as organizations learn how to harness this growing amount of data for a wide range of use cases.

But the sheer volume of data growth is not the issue. Organizations need to find new ways to efficiently access the right data from the right point in the global data grids in order to make a real difference in how we work, play, and interact. Without a strategic plan—and the right tools—for harnessing all that data, organizations will drown trying to "drink from the fire hose."

Big Data—augmented by related data-generation trends, such as mobility, wearables, virtualized infrastructure, e-commerce, IoT, distributed workforces, collaboration platforms, enterprise content management, and others—has only begun to scratch the surface of what it can do. That's due to a number of factors, such as the formative stages of data-mining tools and the early development of powerful, secure algorithms that turn raw data into actionable insights. Big data's growth, as impressive as it is, also has been limited by enterprises' desire to keep capital expenses as low as possible, which is problematic for Big Data use cases that require more compute power, more storage capacity, more network bandwidth, and more data centers.

But as prices on IT infrastructure continue to fall, and as cloud service providers become the new data centers for large and small enterprises alike, Big Data will accelerate its ability to capture, store, manage, analyze, and share data from a wider and more diverse set of inputs.

Take healthcare as an example. To say that data is exploding in the healthcare space is stating the obvious. One recent study said healthcare data is growing faster than ever—nearly 50% annually.[4] That is due to a variety of factors, including regulatory mandates, digitization of healthcare business processes and workflows, the rise of applications such as telemedicine, and the insistence of healthcare practitioners on using their own personal devices to create and share information about their patients and their practices.

Healthcare is just one prime example of an enormous opportunity for improvements, touching on both patient benefits (in the form of improved medical outcomes and better long-term health) and commercial success for hospitals, practitioners, and insurers. Public health, for instance, is a fast-growing specialty that relies heavily on data from across the healthcare data grid, as are other exciting use cases, such as global telehealth practices and infectious disease control. And applications around medical imaging, such as PACS and DICOM, are in the early stages of both commercial opportunity and dramatic improvements in patient care. Managing radiology images and other unstructured data in a global healthcare grid is literally a life-saving development and helps realize the vision of universal healthcare.

Whether it's healthcare data, information about banking transactions, up-to-the-minute feeds on traffic congestion, or real-time insights into the health of common household appliances, Big Data is going to reshape the very nature of how organizations in all industries do business and serve their commercial and consumer customers. For example:

- Analytics engines are going to become considerably more powerful, more affordable, and easier to use, often integrating with analytics engines of social media feeds and other consumer platforms.
- Consumers will make real-time decisions based on multiple data feeds shaped by independent—yet connected—analytics engines. This will expose them to more new products, services, suppliers, and relationships than ever—and they will not have to invest a dime of their own money to take advantage of those analytics engines.
- Delivering services to commercial and consumer clients will become faster and more personalized than ever, improving the user experience and driving enhanced customer satisfaction—leading to even more consumption.

As that happens, the Big Data trend we're currently experiencing will not seem so big after all, compared to what we will experience in just 5 to 10 years from now.

How big could it be? Consider the fact that the worldwide population stands at about 7.8 billion people in 2020. Now, how many "things" do each of us use every day that could have important information that we access or share? 10? 50? More?

Are Data Monopolies and Innovation Mutually Exclusive?

With so much attention and energy stemming from important developments, such as the internet, social media, and cloud computing, it should come as no surprise that "data monopolies" have emerged—disproportionately large collections of data held and managed by a handful of innovative, ambitious, and powerful enterprises.

The commercial success of companies like Facebook, Google, Twitter, Amazon Web Services, Alibaba, Tencent, and other industry titans are remarkable examples of the combination of smart business decisions, commitment to innovation and research, bold bets on new technologies, and a little bit of good luck. The fact that these and a relatively small number of other organizations collect, hold, and leverage massive amounts of data is not, by definition, something to fear. It is, of course, something to acknowledge; we must understand its implications.

After all, the broad collection of personal data undoubtedly sparks concern over privacy rights and confidentiality. That was a big driver behind the European Union's landmark General Data Protection Regulation (GDPR), which may influence and shape data privacy regulations in other regions of the world.

And, if data is the new global currency, it's not surprising that some people are raising concerns about "whoever controls the data has the power." But there is an important balance that needs to be struck between preserving the privacy of individual data and allowing businesses and governments to use data in a responsible, innovative way to better serve their constituents.

This is not a black-or-white issue. It's highly nuanced, with the need for a delicate balance to ensure that protecting data doesn't lock out innovation, or that harvesting data to create new goods and services doesn't imperil our individual identities and rights.

The tension among companies, governments, regulators, and consumers is inevitable, with each group trying to promote its own interests. But we need to keep in mind that this doesn't need to be an "I-win-you-lose" scenario.

We also need to understand the appropriate role of government in protecting individual rights and avoiding the deleterious effect of data monopolies. Our governmental agencies and regulators should avoid going down the path of heavy penalties and overly regulated data access and usage, opting instead for collaboration among all stakeholders to strike that delicate balance between commercial innovation and individual privacy of personal data.

In fact, I believe industry players will increasingly band together to collaborate on smarter, more efficient compliance protocols, and will team with government agencies, regulators, privacy advocates, and standards bodies to do so. While this may seem like an unusual alliance, I believe it is a more efficient and effective way to ensure responsible compliance measures without stifling innovation.

Protecting Our World and Our Data Against Digital Threats

As excited as I am about the possibilities of using all this data for the common good of our societies, I am also realistic about the growing footprint of cyber threats. Every year, the incidence, impact, and innovation of cyberattacks increase, and there's no reason to think they will abate in the coming years.

Again, data—and proper access to it—is key to ensuring that applications, services, and entire economies are safe and secure. If that sounds like "data that protects data," you are right. In order to protect our most important data—personally identifiable information, financial records, medical records, intellectual property, and more—we will need to develop new tools and services to discover and remediate data vulnerabilities.

Yes, threat intelligence and other subscription-based services help to identify threats and promote joint problem solving. But we need to do more. Too often, we have incident feeds that are limited in

their impact or ability to promote remediation because they lack access to critical data about threat sources, points of attack, weak points at the network's edge, indicators of compromise, and more.

Again, the notion of balancing security needs with privacy expectations is relevant here. But it goes even farther. After all, there's nothing preventing us from locking down everything tighter and tighter—servers, mobile devices, applications, cloud services, and more. Doing so, however, seriously degrades the user experience and stifles innovation in data-driven goods and services.

Data must continue to flow, reliably and securely, through networks that are increasingly global and susceptible to the efforts of bad actors. Restricting data traffic to the point of choking it impacts our data economy locally, regionally, and globally. That's why the European Union is working on regulations to unlock the data held by European institutions, and the U.S. federal government has an open data initiative.

This concept is evident in the rise of data marketplaces, or data supermarkets, which enable new companies to build markets where public data is available. In these scenarios, specific users can easily combine that data with other, free data sets for improved insights and unearthing new business opportunities and societal value.

Ensuring this cross-border data flow is going to require a more collaborative effort among commercial, governmental, regulatory, and consumer bodies. In fact, to promote best practices in cybersecurity and to protect individuals, businesses, and governments, we must find ways to promote more data sharing and greater collaboration. Take terrorism, for example. Fighting both physical and digital terrorism requires cooperation among a vast network of agencies, organizations, and data sources, all around the world. We must continue to push for ways in which governments, particularly in areas of law enforcement and national defense, work together.

We should also strive to step up deliberations and consensus building around the application of international law and governing states in cyberspace, at both the UNGGE (UN Group of Governmental Experts) and bilateral levels. The recently mooted "Digital Geneva Convention" and other proposals need attention to ensure that states do not violate established norms in cyberspace. This is necessary, not only to identify and weed out cyber criminals, but also to protect and preserve individual liberties, particularly as many governments have built offensive cyber capabilities.

In an era of digital economies and digital lifestyles, we need to treat security as a core feature and requirement in all products and services, from the onset of the design phase. Our communities, economies, and constituents demand it, and it will be on our hands if we don't deliver it.

Conclusion

Our societies and our lives have been dramatically impacted by developments as basic as the discovery of fire, as well as simple and complex inventions such as the wheel and hydroelectric power. But I believe there is no development with greater long-term implications for our world as new applications for digital data.

Data is more than seemingly random collections of ones and zeros. It is information, currency, social fabric, safety, knowl edge, confidence, and innovation. When created, shared, and managed for the good of our communities, our families, and our industries, it acts as an exhilarating source of hope for a better world. And when combined with smart, collaboratively developed security safeguards, it gives our best and our brightest the opportunity to continue to use data in heretofore unimaginable ways for the common good.

Technological advancements may allow us to connect more things to each other, but the real power and beauty of a connected society is its ability to use grids of data to bring us closer together as people, as communities, and as nations.

---

[1] "Building a European Data Economy," Digital Single Market 2019.

[2] "Digital Industry: The True Value of Industry 4.0," Oliver Wyman and Marsh & McLennan, 2016.

[3] "Digital Transformation to Contribute More Than US$1 Trillion to Asia Pacific GDP By 2021," Microsoft and IDC, 2018.

[4] "Report: Healthcare Data is Growing Exponentially, Needs Protection," Healthcare Informatics, 2014.

6

The Future of Cloud

Ann Johnson — Corporate Vice President, Cybersecurity Solutions, Microsoft

When I think of the future of cloud computing, I automatically think of my teenager. Then I smile. Broadly.

Cloud and my teenager have a lot in common, especially as they continue to grow in size and capabilities. The rate of their physical advancement is nothing short of astonishing, and every time you look around, they are doing amazing things that seemed inconceivable just a short time ago.

Just as I marvel at my teenager's rapid physical and intellectual development, the skyrocketing adoption rates and widespread embrace of cloud for mission-critical applications are noth-ing short of inspirational.

Of course, my teenager doesn't improve organizational agility, scale exponentially to keep up with new workloads, or come with a predictable subscription-pricing model. And as much as I hope and plan for a smooth transition to a lifetime of health, happiness, and a solid career path for my child, I truly don't have a clue what the future holds.

Not so for the cloud, however.

I don't need a crystal ball to predict what the future holds for the cloud. Oh, I may not be able to see around the corner for every technical nuance that will add more value to the cloud or to pinpoint the economic value of the cloud economy.

But I have seen the future of cloud, and it is bright. (Yes, even accounting for the harsh reality of cyber threats. I'll explain why in a bit.)

Good News for Business Leaders: Cloud Will Transform Your Organization

My vision of the cloud's future starts in the past—when enterprises began experimenting with cloud-based services, such as SaaS, or when employees began deploying early versions of shadow IT by storing work data on cloud-base file-sync-and-share sites. Organizations soon realized that the cloud was a good resource for doing things like application testing and development, or promoting cross-group collaboration without having to deploy dedicated infrastructure.

In this phase, I thought of the cloud as *helpful.* It was an interesting and opportunistic tactical resource that allowed organizations to reduce the cost and speed the time of delivering IT resources. It helped us keep a handle on FTEs that would otherwise need to be allocated to support new digital initiatives.

Our positive experiences in using the cloud gave us confidence that we could start using it for more important services and applications that were at the very heart of our day-to-day business activities. Soon, our most important applications were migrated to the

cloud—building on the tactical benefits of first-generation cloud, becoming a strategic asset in increasing IT and organizational agility, and instantly scaling resources in reaction to new business opportunities or challenges.

Today, cloud has morphed from helpful to *important,* a strategic way to not only let us do more with less, but to ensure we can utilize our people for the things that make a difference.

In the future, however, cloud will take the next step. In fact, the cloud's utility, capability, and resilience are rapidly accelerating—due in no small part to a few key technologies I'll introduce shortly. In a few years from now, we will look at the things that make us excited about cloud today as quaint. That's how much things will change.

In short, the future of cloud will complete its revolution from helpful and important to a difference-maker. The cloud of the near future will be *transformational.* It will open up all kinds of possibilities in the era of digital transformation that will not only improve IT and business efficiency, but will also change the way we work, live, and play.

The cloud of the future will make our organizations and our communities more connected, more useful, more agile, and, yes, more secure. It won't be easy, of course. It will take a continued commitment to experimentation, investment of time, money, and people; a willingness to change decades-long organizational and personal behavior; and an ability to create a vision based on what you can't yet see, but you can begin to imagine.

Brad Smith, Microsoft's President, has put the cloud's future into a framework that is aspirational, inspirational, and yet practical. In "A Cloud for Global Good," he talks in very pragmatic terms about the intersection of the cloud, emerging technologies, and all stakeholders in creating a society that benefits more people in new, transformative ways.

This vision will be supported by the integration of such technical trends as artificial intelligence (AI), machine learning, quantum computing, and mixed reality. Already, these factors are changing the very nature of the cloud, with bigger and better changes to come.

The Symbiosis of Cloud and AI

Not surprisingly, the global push for deeper insights into all that data flooding our networks and the cloud has driven organizations to turn to artificial intelligence. AI, as well as machine learning and other derivatives, is transforming what we can do with data, enabling us to make better decisions, with bigger impact, faster, and more reliably. And we have only scratched the surface.

In many ways, cloud is the ultimate sandbox for AI-enabled workloads and AI application development. The ability to handle massive and rapidly growing amounts of rich data makes the cloud an ideal laboratory for AI solutions.

Consider just a handful of possibilities still emerging or soon to take shape, thanks to the marriage of AI and the cloud:

- **Healthcare:** Hospitals, practitioners, and related organizations need to solve the interoperability problem that is still hampering the delivery of coordinated care. In the face of EMR mandates, a growing regulatory footprint, and the drive for essential applications like telemedicine and population health, healthcare organizations will turn more to the cloud and AI to use that mountain of data more efficiently. Or, just consider the possibility of predicting and preventing future pandemics before they take their devastating toll on our societies and our planet.

- **Retail:** Brick-and-mortar retailers and online sellers want to sharply reduce, or even eliminate, merchandise theft, fraud, and shrinkage—a $100 billion-a-year problem for physical stores and potentially much larger in the era of an increased swing toward e-commerce and omnichannel retail. More robust and turbo-charged analytics will allow them to link inputs from IP surveillance, inventory management systems, item-level RFID, and anti-theft packaging—all in the cloud.
- **Government:** Municipalities all around the world are striving to re-engineer how they deliver social services, such as identifying and remediating sources of domestic abuse. The marriage of the cloud's infinite computing horsepower and AI's deep insights into cascades of seemingly disconnected data makes that not only possible, but highly likely.
- **Financial services:** Can the industry eradicate insurance fraud and securities trading violations, absent mountains of paperwork or without trampling on individual privacy rights? The combination of cloud and AI will make it happen, all without necessitating tons of CapEx and on-premises systems development.
- **Education:** While there is no question that infusing technology into educational curricula and arming our teachers, staff, and students with technology have helped to bridge the much-discussed digital divide, more work needs to be done. The cloud is going to be the linchpin in bringing new educational opportunities to students in rural communities with historically limited access to transformative technologies, due to factors such as location, culture, or budget.
- **Transportation:** Airlines spend billions of dollars annually simply due to an inability to keep operations intact—and revenue flowing—during bad weather. Using an AI-hypercharged cloud will give them instantaneous knowledge about rapidly changing weather conditions, which will enable them to be more predictive in scheduling and routing, with less inconvenience and danger to passengers and work crews.

At the same time, AI is turning the cloud into a richer, more functional, more efficient environment for knowledge creation, collaboration, and utility. Over the next few years, cloud service providers and private cloud developers will benefit from AI in eye-popping ways.

For instance, AI will make cloud adoption and utilization more appropriate and efficient for regulated environments, particularly for demonstrating compliance and for spotting potential anomalies before they become regulatory headaches. Audit trails will become cleaner, more precise, and more efficient in the cloud through the use of AI and machine learning engines.

This is heady stuff—a true symbiosis. Not only will AI, machine learning, natural language processing, and cognitive computing advance rapidly because of the cloud, but the cloud will become richer, more robust, and more useful as its ecosystem is embedded with AI-related technology. It will be the ultimate win-win scenario.

Turbo-Charging the Cloud of the Future With Quantum Computing

Remember how excited we used to get when a new family of microprocessors came out, allowing us to have faster PCs and take advantage of new software functionality? We have Moore's Law to thank for much of that, as well as the very

smart engineers at chip-maker and software companies.

Now, get ready for a quantum leap—pun intended—in power. Quantum computing is going to transform the cloud of the future with an infrastructure overhaul we've never seen before.

I won't get into the physics of qubits or what quantum computing will mean for your data center operations. What you need to know, however, is that the cloud is about to become even faster and more useful for applications that will be developed, deployed, and run in the cloud.

For instance, consider research laboratories looking for new ways to calculate nuclear binding energy. If you don't know anything about nuclear binding energy, you're not alone. But what you can probably surmise is that this is an application that is fed by massive amounts of data, and also needs more horsepower than ever to execute and turn that data into something actionable. Enter quantum computing. Already, researchers at Oak Ridge National Laboratory are using cloud-based quantum computers to conduct simulations and calculations that would otherwise have required untold investments in hardware, software, and FTEs, just in the experimental stage.

Of course, quantum computing has yet to become commercialized, but that's not far off. So, when the technology becomes mainstream, quantum-driven applications will find their home in the world's biggest data center—the cloud.

And you can only imagine what kind of mind-blowing advancements we'll see in cloud computing's performance and scalability when we introduce quantum computing into the cloud's infrastructure.

Consider the opportunities a quantum-spiked cloud environment can support:

- Development of new clean energy sources that are more cost-efficient and that produce better yields than current generations of wind and solar energy.
- Research into new food production processes that will literally wipe out global famines.
- Uncovering exciting new ways to predict, prevent, and treat potential health problems years before they surface.
- Delivering personalized, customized, affordable one-on-one education that is motivating to students and invigorating to teachers.

Quantum computing is going to be the new physical engine of the cloud. And the cloud will never be the same.

Securing the Cloud of the Future

I worry about security. A lot. And not just because "security" is in my job title. Because when I think of security, I again think of my teenager.

Parents are hardwired to worry about their children's security. Our worries evolve, become more complex and closer to the surface as the kids get older. Not surprisingly, I have broken out in a cold sweat more than once when I think about my teenager's security.

Yes, I worry all the time about my teenager's physical and emotional security. But I also have a measured sense of optimism and confidence about the future of digital security. And that's because I'm incredibly upbeat about what the cloud community of suppliers, agents, and users has been able to do with security, and what we are all likely to do as we move into the transformative future of the cloud.

Let's be clear: I'm no Pollyanna when it comes to the target-rich environment that the cloud has become and what it will be in the future.

Those of us who have studied technology are very familiar with Metcalfe's

Law, which posits that the value of a network increases exponentially in relationship to the number of people attached to it. Think about the hundreds of millions of people using the cloud every day. Now, multiply that by whatever number you like. Five? Twenty? One hundred? Think about a much, much larger cloud community, measured not only in the number of users but also, more importantly, in the number and diversity of "things" connected to the cloud. The potential threat vectors presented by hackers, organized cyber-criminal gangs, and bad state actors over the next several years are breathtaking. Not breathtaking as in surveying the Alps, trekking through the rain forest, or roaming the American heartland. I mean breathtaking as in "gulp."

So, it's important for all of us to know what we'll be up against as we necessarily and deliberately rely and depend on the cloud.

With more and more data—and with more of that data deemed mission critical—created, stored, and managed in the cloud, bad actors will naturally take aim. Developments like the Internet of Things are a great example of why: The fact that the IoT represents a multi-trillion-dollar target makes it a gigantic target for the bad guys. This is becoming even more an issue as "smart things" are connected to the cloud without sufficient integrated security or as users fail to adopt proper security hygiene.

With such a broad attack surface, in an always-on environment, fraudsters have already exfiltrated data and caused cyber mischief. So it's up to us to do more. A lot more.

Already, some things are happening. One of the best is the imminent demise of passwords. Whether you store your dozens or hundreds of passwords in a spreadsheet, on sticky notes, or in a digital wallet, passwords no longer are sufficient cybersecurity defenses.

So passwords are giving way to biometrics and other steps in multi-factor authentication, making it harder for bad guys to penetrate our firewalls and grab our personally identifiable information, intellectual property, and digital assets of every format. Still, we cannot underestimate the intelligence, creativity, and determination of hackers, whether they are lone wolves (which they rarely are), part of digital crime syndicates, or state-sponsored bad actors.

They are coming after us in the cloud, and they will amp up their efforts in the cloud of the future. There's good news, however: We're all ramping up and fortifying our cloud security frameworks in anticipation of more penetration attempts.

First, a fundamental truism is that AI will be a big-step change for cloud security, which we desperately need.

Already, cloud environments are being fortified with machine language engines to analyze global data points in the hundreds of billions of cloud-based transactions. AI and machine learning normalize the data (remember, it's all unstructured, from spreadsheets and email to cat videos on Facebook) and push out attack indicators that are more meaningful, timely, and accurate. This will make our detection efforts far better—an order of magnitude better, in fact.

Using AI on top of those machine language engines will speed scenario modeling, giving already-stretched security analysts the ability to spot trends faster and make better decisions.

Then, you'll be able to take virtual reality technology and let your security experts—and your business users, too—visualize the threats in a consumer-friendly manner.

And none of that happens without a global cloud operating at hyper-scale speed.

Security is one area that really benefits from a large, wide, and deep cloud envi-

ronment, because with the right analytics tools and enough processing power, global decision-making becomes easier and more accurate.

Cloud security also will become much more automated; again, machine language tools will drive huge process improvements in developing and deploying automated defenses. This will take considerable pressure off overworked security administrators and security operations centers to manually detect and thwart attempted intrusions as simple as garden-variety viruses or as insidious as malevolent ransomware.

In short, the cloud of the future is going to be a digital fortress, more robust and resilient than ever. Cloud security will be more intelligent, more automated, and more discerning, driven by advances in AI, machine learning, quantum computing, and other transformative technologies. Cloud security also will be designed and implemented with more of an eye toward a positive user experience, making security steps less obtrusive to the user and less likely to impact our business productivity or our personal enjoyment.

I'm not predicting that we'll never have breaches or that we won't have blaring headlines about loss of personally identifiable information. But I have seen the future of cloud, and it is secure.

Now, if I could only feel more confident about my teenager's security when I'm not there, too.

Conclusion

After my child was born, I was overwhelmed with a sense of amazement for that tiny life-form. But I was so consumed by my new child's everyday needs—eating, changing, bonding, sleeping—that I rarely allowed myself the luxury of dreaming about the future.

But as my child entered the exciting world of teenage-dom, I began to focus on what the future held and how my teenager would make a mark on the world.

I feel the same about cloud. In its formative years, I was thrilled by the many benefits of cloud computing to extend the resources of traditional IT organizations, to let business users take charge of their digital destinies, and to let billions of people connect, collaborate, and build global communities. In those days, that was enough to keep most of us really busy.

Now, as the cloud has evolved from a helpful business tool to an important resource, to the point where it is now transforming so much of our work and personal lives, I am exhilarated when I allow my imagination to run free and envision what the cloud of the future looks and feels like.

Maybe my teenager will even help shape the cloud of the future in some meaningful way. But I know one thing for sure: The cloud will change the world much, much more profoundly in the coming years than it already has changed mine.

Why and How We Must Change Our Roles and Behaviors

7

Understanding the Exciting, Exponential, and Terrifying Future of Cybersecurity

Marc Goodman — Author and Global Security Advisor

I used to be a cop. It was a great job, and I loved it. Then one day, my policing career changed drastically—all because I knew how to use the spell-check feature in WordPerfect.

Yes, that impressive demonstration of technical acumen put me among the "digital elite" in policing back in the day, and it became the catalyst for a highly enjoyable and challenging career in cyber criminology. Now, as I spend my time researching and consulting about next generation cybersecurity threats in the real world, I have to admit: I'm profoundly concerned. Concerned about the seemingly limitless ways we are dependent on technology and the equal number of ways it can all go wrong.

However, despite these worries, I remain optimistic about the future and our ability to make significant strides in the battle against cybercrime. In order to get there, a few things need to happen, which we'll cover in this chapter:

First, you must **understand the enemy**—specifically, the threats, the vulnerabilities, and the criminals.

Next, you must **acknowledge and evaluate the traditional, tried-and-not-so-true reactions** of executives and boards of directors to cyberattacks.

Finally, you need to find and exploit the secrets that will help you change the balance of power between the good guys (you) and the bad guys (the ones robbing you) by throwing out the old playbook on cybersecurity and beginning anew.

The Power of Exponentials

Learning about the power of exponentials can change your view of the threats, your responsibilities, and most importantly your cybersecurity strategies for the future.

What do I mean by exponentials? Exponential technologies—computers, robotics, AI, synthetic biology—all obey Moore's Law and thus double in their capabilities every year or so. To conceptualize what these rapid changes look like, business leaders have devised a number of terms to describe the phenomenon, including non-linear thinking, inflection points, hockey-stick curves, or force multipliers.

Conversely, linear point-to-point advancement of actions and developments is comforting to us. It's reassuring to believe that we have some knowledge—or perhaps even some control—of where we are headed. Linear expectations and predictions are comforting, but they

are dead wrong when applied to technology, a serious mistake that has direct implications on how we approach cyber risk.

Understand Your Enemies: They're Different Than You Think

Most organizations look at recent attacks on their information assets and usually think linearly. "Yes, DDoS attacks are increasing, and so are phishing attempts," the CISO may tell the CEO or the board. "But we're on top of it, and here's what we're doing." In other words, most organizations see the problem as having a linear path, requiring a linear approach to solutions. Spend slightly more money on malware prevention, conduct more training on security hygiene practices, have users change their passwords more often. Last year the problem was this, now it's that, so let's plot our defenses based on the fact that threats are increasing in an orderly linear fashion.

Wrong. Linear thinking about threats and enemies must give way to exponential thinking, because the pace of everything is accelerating, and it's doing so way, way faster than we had imagined. Linear thinkers believe autonomous vehicles are pure hype and will never take off. Exponential thinkers know they are already here.

When it comes to the bad guys, there's a big problem. They are thinking and acting exponentially, while we're defending ourselves linearly. Moore's Law means nothing to them. They're Moore's Outlaws.

The second thing to keep in mind about the impact of exponentials on cyber risk is the rate at which automation is taking place. You want to talk about a force multiplier? Automation in its many forms—algorithms, scripts, machine learning, and natural language systems—is creating cyber crime at scale. They're using our smart tools against us in order to scale their malevolence at a rate far greater than we could have imagined. Well, start imagining.

There is a ton of software out there to automate cyberattacks. Distributed denial-of-service (DDoS) is a great example: It's automated mischief. They've even weaponized the cloud—*our cloud*—to execute DDoS attacks and other digital warfare.

The automation of cyberattacks represents a disturbing and highly problematic development, adding mightily to the arsenal of cyber criminals, enabling bad actors to fully automate even the most complicated of crimes, such as hijacking and ransom offenses, combined with great effect the explosion of ransomware attacks in recent years.

Holding someone or something hostage for money has been around for millennia, but the analog version of ransom-based crimes took a lot of work. You needed to identify the target and study their movements, then hire some guys with guns, stalk and grab the victim, stow them away, reach out to the family, warn them not to contact the police, agree on a location for the money exchange, line up a pigeon to actually pick up the money instead of you, arrange a getaway vehicle, and hope you're not caught.

Exponentials in the form of automated threats make it much, much easier. They're taking a highly complex crime and encoding it in software. It's pretty easy to do—you don't need a PhD in computer science—and it's really cost efficient. You can buy a ransomware kit on the Dark Web for about $10, and the average ransomware payout is pegged at $163,000. Now that's what I call a return on investment.

And there's no limitation on how much ransomware you can launch. Again, exponentials are at work.

Now, let's raise the stakes way, way higher—the Internet of Things. Talk about a potential bonanza for the bad guys thinking and acting exponentially. Actually, the IoT itself is a great object lesson in exponentials. Look at the exponential growth in the number and diversity of connected things; tell me that doesn't look like a classic hockey stick. And the incremental economic value of IoT is going to run into the trillions of dollars. Think that's not an inviting target?

I call this the third dimension of cyber threats. In the beginning, we had computers. They were these big, ugly, gray boxes shoved into climate-controlled data centers or parked on someone's desk. Then we got mobile—notebooks, tablets, and smartphones. And finally, we realized we could put a chip in everything. TV used to be a vacuum tube, now it's a smart, ultra-high-resolution display with more intelligence than a supercomputer.

Computing is now fully mobile and ubiquitous, and all those endpoints are vulnerable. Your kids' toys have become turned against them; chips for speech synthesis and cloud connectivity have become ways to triangulate your child's location by truly evil people. We're going to add 50 billion new devices—probably more—to the internet by 2020, and it's all being done insecurely.

Is there anything you can do about it? Read on.

Consider Your Biases and Your Actions: It's Time for a Refresh

For CISOs, C-suite executives, and board members to defeat an increasingly sophisticated and determined cyber adversary, new ideas and dramatically different approaches are necessary. Forget about thinking outside the box. In fact, throw the box out. You'll need to think outside a geodesic dome embedded in a kaleidoscope. That's how many new angles, dimensions, and perspectives you'll need.

One thing I learned many years ago when I got into law enforcement was to try and understand the mindset of the person I was trying to catch. I was taught great lessons about profiling and getting inside the head of the bad guys, and the veterans on the force shared great knowledge with me about suspects' "tells" in their behavior and appearance.

Not surprisingly, there has been a lot of effort trying to get into the minds of cyber criminals: What makes them tick? What are their motivations? What are their fears? All great questions. Unfortunately, there aren't a lot of easy answers.

Remember the popular meme of the early days of the internet: "On the internet, no one knows you're a dog." Well, when you're being attacked, you are rarely sure who is doing the attacking, so pondering the mindset and motivation of the attacker doesn't do you a lot of good. Bits and bytes are flying at your corporate network, and you're not really sure if it's a competitor, a member of an organized cyber-crime ring, a disgruntled employee, or a state actor.

Here's where our new friends—exponentials—come into play. My experience has taught me that many business executives and boards still cling to the old stereotype of the attacker profile. They too often think it's some pimply kid in his parents' basement. He (or on rare occasions, she) is imagined as a lone wolf with social problems or feelings of inadequacy in traditional institutions such as schools or businesses. I'm here to tell you: Come to that conclusion at your own risk.

You must discard those stereotypes and adopt a new mindset of your own that is radically different from that most executives have historically used. You must consider that your latest cyber adversary is fully capable of, and committed to, taking down your organization. The sooner

you accept that notion, the sooner you'll be on your way toward a more relevant and potent cybersecurity strategy.

Another example of exponential thinking you should employ in an effort to break down old biases and consider new actions is the notion of fear. (Not your fear, the cyber criminal's fear.)

Your strategies should not be built on ways to heighten their fear of being caught and prosecuted; they won't work. And the reason they won't work is devilishly simple: The criminals have nothing to lose.

There's a very pragmatic reason for that by my own estimations: The chances of a cyber criminal being arrested, prosecuted, and jailed is something along the lines of one in a million. Literally.

The chance that they're going to be caught and punished is the exception rather than the rule, due to the nature of international law. A cop in Milwaukee simply can't arrest somebody in Russia, France, or China—and all cybercriminals know this. They do not fear you, your defense strategies, your detection tools, law enforcement, or the criminal justice system.

Finally, business executives—and especially corporate boards and board members—need to adopt an exponentially different posture when it comes to taking responsibility for cybersecurity.

First, let's acknowledge that, while boards are made up of very smart and successful people, they are not digital natives, for the most part. They are probably 55 to 70 years old, on average, and have not grown up in business or in life attached to digital devices. Many of them are not up to speed on technology, so they rely on "trusted partners" to filter questions of technology for them. That might be the CISO, CIO or a technical consultant, but the result is the same: They are counting on the tech people to ensure the organization is cybersecure.

That has to change. If board members lack the skill set to ask the right questions or to push back on issues they don't understand, they need to find a way to get those skills into the boardroom. Remember: Even if board members want to ask probing questions, the CISO has been known to push back. They may make their case before the board, but the CISO often answers board members' seemingly elementary questions with buzzwords and industry speak. And because the board members don't want to come off as uniformed, they don't probe further and assume all is well.

Instead, board members need to do more to understand their cyber risk posture and exposure. They need to educate themselves and not be intimidated by technical experts who may throw around buzzwords to block them.

Boards also should consider establishing a dedicated cybersecurity committee with a tech-savvy board member as its chair. After all, boards have committees for compensation, governance, and audit. Isn't cybersecurity just as essential a board responsibility?

Another idea—and this one is radical, not because it's so strange but because it's so rarely used—is the notion that boards and senior executives need to practice their responses and reactions to data breaches. All companies have been hit with data breaches; some know about it, some don't. But boards must lead the way in preparing for that eventuality so they can limit the financial, operational, legal, and brand damage that often occurs.

I don't mean having a cybersecurity response playbook or a disaster recovery protocol that gets dusted off and updated once a year. I'm talking about digital war games.

As we all know, these are routinely done in other industries, markets, and walks of life. Law enforcement and the military practice them all the time, often

with terrifyingly real approaches that often make it nearly impossible to tell if the scenario is real or simulated. Of course, the airline industry does this routinely. Do you think an airline pilot suddenly asks himself after 10 years of flying, "Hmmm ... I wonder what would happen if an engine were to go out at 35,000 feet over the Pacific?" Of course not—they practice for this event all the time.

Organizations need to run exercises that include members of the board, CEO, CISO, general counsel, heads of marketing and sales, CFO, and investor relations team. The board should actually run the exercise and take it very seriously. Actions should be monitored, recorded, evaluated, and shared with team members, and corrective measures should be taken to address inadequacies.

Reasons for Some Optimisim

I've talked a lot about threats, challenges, roadblocks, and hurdles. Many of these have been magnified and spiked in urgency, frequency, and impact as a result of the concept of exponentials. And you'll remember early on in this chapter that I expressed my deep concern over what's happening. I think you'll agree I have good reason to think this way when it comes to cyber threats.

But remember: I'm also very optimistic about what the future holds, especially to all the positive benefits technologies will undoubtedly yield to the world of medicine, education and the global economy. While I have highlighted many of the threats from cyber threat actors, there is also room for hope, given the tremendous amount of attention these threats are receiving. I am heartened by the increasing understanding I am seeing and hearing from many executives, board members, and technical experts about addressing the issue of cybersecurity.

In particular:

1. The questions I'm being asked by executives and CISOs are much smarter, more focused, and more results-oriented. Many of you reading this chapter have come to grips with the understanding that legacy approaches bring legacy results—and that the bad guys are playing with algorithms while too many cybersecurity defenses were designed in an era of mainframe computers.
2. There is a heightened sense of urgency on nearly everyone's part. Some of it is motivated by a desire to avoid banner headlines in *The Wall Street Journal* or having executives paraded in yellow jumpsuits out of federal courthouses. But whatever the motivation, everyone is taking this very, very seriously and has a wide-open appreciation of the heightened stakes.
3. Organizations are starting to come around to the sophistication, intelligence, creativity, and determination of cyberattackers. Stereotypes about attackers' mindsets and motivations, so deeply rooted in digital folklore and some really bad movies, are finally melting away.
4. There is a growing understanding and acknowledgement that being cyber-secure isn't about having the best technology—as important as that is—but it's more about exponentially changing the way we think and behave collectively.

A Few New Rules for Changing the Rules

One of the biggest areas of concern among both technical and business leaders is the startling, yawning chasm between the

number of cybersecurity professionals needed today and over the coming years and the actual number of digital experts available to fill those positions. Some estimates put this gap at 1 million people by 2020, while others think it may be several times higher. I encourage you to plan for the high end of that shortfall range—and then increase it.

We also know, from the basic economic theorem of supply and demand, that salaries of cybersecurity professionals are rising much faster than IT industry norms. That means that even the people you have on staff—men and women you've already invested in heavily—are being approached and poached by headhunters as you read this. That also means that even if you are fortunate to hire good people, chances are you will not be able to keep them too long.

Organizations therefore need to take dramatic steps to ensure they have a pipeline of talent constantly coming to their firms to fill these positions. I'm not just talking about upping your college graduate recruiting budget for computer security majors (although you should certainly do that).

Re-evaluate how you identify candidates. I'm talking about rethinking the profile of the kinds of people you hire and train for those roles. For instance, think about the kinds of people who succeed in any organization: What qualities do they possess? Intelligence. Work ethic. Communications skills. A willingness to ask "dumb" questions. An ability to learn from mistakes.

These and other qualities are not necessarily limited to computer science grads from MIT or Berkeley. Think about recruiting people with these demonstrated skills from non-traditional corners of your organization. People like field service engineers or accounts payable clerks. Or truck drivers and copywriters. There are tons of people in your organizations with the requisite personal attributes and mindsets—if not necessarily the deep technical expertise—that can be harnessed to fill that growing gap. Don't worry. I'm sure you'll have a ton of great security engineers who will be at the top of their field when it comes to knowledge about tunneling or reverse malware engineering. But you're going to need a lot more assets and greater diversity of those assets. So think exponentially.

Focus on the user experience of security. Another part of cybersecurity that needs an exponential shift in mindset is the cybersecurity user experience and design. This is an area that is ripe for innovation, if for no other reason than so much of what has passed for security alert software has been woefully inadequate.

How many times do your employees get some pop-up message on their screens while they're looking on the internet or working on email, and what they see is ugly and confusing? The design of security warnings is abysmal and painful. Users too often default out of the windows because the warnings get in the way of them doing their work, and they don't see why it's a big deal to let the warning slide.

It's not enough that our security protocols work in theory—they have to work where the rubber meets the road at the end of a keyboard used by somebody in your company in sector 4G. And that requires a good understanding of human behavior, something infrequently accounted for in organizational cybersecurity strategies. Setting a policy is only the first step. Making sure it is reasonable, understood, and followed is a whole different ball of wax.

Rethink and re-architect the organizational chart. Lastly, rethink your organizational approach to cybersecurity by getting rid of whatever you call the cybersecurity department on your organiza-

tional chart. When you put a nice, neat box around cybersecurity, you're sending a message: These are the ninjas of cybersecurity. They have the magic potion, the elixir that will defeat the cyber thieves. It's their concern, not yours.

Throughout this chapter, I have argued that we need a much broader and more radical way of thinking about your cyber defense team, one that takes into account the exponential nature of our world. Cybersecurity needs to be crowdsourced to include all hands on deck. It's not just the responsibility of a few dozen or even a few hundred technical experts locked up in your IT organization.

Cybersecurity is not just "their" problem. It's an "everybody" problem. It's not a department; it's an attitude. If you don't expand your idea of how to solve the problem by ensuring that everyone has skin in the game, you are on your way to losing the game. And the stakes of losing, already quite high, are about to become astronomical.

The good news is, there is much we can do to protect ourselves and our organizations from digital threats. The first, and perhaps most important, step is to begin to think exponentially—because in the age of Moore's Law, every minute counts.

8

Dealing with the Evolving Adversary Mindset

James C. Trainor — Senior Vice President, Cyber Solutions Group, Aon

The views presented in this chapter are my own and not those of the Federal Bureau of Investigation.

Incident #1: On Nov. 24, 2014, employees at Sony Pictures opened their computers to the sound of gunfire, scrolling threats, and a skeletal image now commonly referred to as the "Screen of Death." By the time the cyberattack was over, more than 3,200 computers and 830 servers were destroyed, highly confidential files were released worldwide, and 47,000 Social Security numbers were compromised.[1]

Incident #2: In 2010, the FBI announced that hackers were using passwords and other security measures to illegally transfer thousands of dollars at a time, from bank account to bank account. The attack, known as GameOver Zeus, affected hundreds of thousands of computers to the tune of more than $100 million.[2]

Incident #3: In the Fall of 2015, a hacker impersonating a phone company employee gained access to the private email account of John O. Brennan. At the time, Brennan happened to be the director of the U.S. Central Intelligence Agency.[3]

Incident #4: In January 2018, a former U.S. National Security Agency contractor, named Hal Martin, pleaded guilty to stealing a massive amount of confidential security information, including NSA cyber-hacking tools. While there are ongoing questions about the plea agreement, there is no question that the stolen tools were used in the devastating WannaCry ransomware attack in May of 2017.[4]

Incident #5: In September 2016, a Kosovo citizen named Ardit Ferizi was sentenced to 20 years in a U.S. prison. He pled guilty to accessing a protected computer without authorization to steal personal identifiable information from approximately 1,300 individuals, including members of the military and government personnel. Ferizi stole the information with the goal of handing it over to ISIS.[5]

What these five incidents have in common is that they caused extensive financial and reputational damage and/or had the potential to significantly compromise a country's national security.

Different Types of Attacks

Here's what they *don't* have in common: the motivation and mindset of the perpetrators. Each of these incidents rep-

resents a different category of cyberattack that businesses, governments, and law enforcement agencies must be prepared to prevent and address. These are:

1. **Nation-State:** North Korea targeted Sony Pictures because of the pending release of a comedy called *The Interview.*
2. **Criminal:** GameOver Zeus was one of many criminal attacks that earned the alleged mastermind, Evgeniy M. Bogachev, a $3 million bounty from the FBI for his capture.
3. **Hacktivist:** The Brennan attack was the work of an organization called Crackas with Attitude (CWA). The five alleged perpetrators ranged in age from 15 to 24.
4. **Insider:** The Hal Martin attack is viewed by many in law enforcement as a potential catastrophic event because it makes all potential adversaries more dangerous.
5. **Terrorist:** Ferizi was captured after posting a tweet that stated, "We are extracting confidential data and passing on your personal information to the soldiers of the khilafah, who soon with the permission of Allah will strike at your necks in your own lands!"

Understanding the Evolving Adversary Mindset

I spent more than 20 years at the U.S. Federal Bureau of Investigation, and in my last role as Assistant Director of the Cyber Division in Washington, D.C., I led the team that developed and implemented the FBI's national strategy to combat cybercrime. One of the cases I worked on was the Sony attack, which was historic for many reasons.

For one, it involved a wide range of malicious acts against Sony, including intrusion, destruction, and threats to employees and the public. The government was able to respond quickly. Within days, the FBI identified the perpetrators and, within six weeks, President Obama signed an executive order issuing sanctions against three North Korean organizations and 10 individuals.

Responding to this type of breach required an understanding of the legal and regulatory environment, the technical environment, privacy issues, media-related issues, and more. Preventing a breach of this size and scope is just as challenging, if not more so. It has been difficult enough to understand the mindsets of each of the individual types of adversaries. It becomes even harder when these adversaries have multiple motivating factors and sponsors, such as government-backed attacks for both profit and geo-political warfare.

Another reason I consider the Sony attack to be historic is because it portends what we can expect in the future, where there is a blending of mindsets, behaviors, motivations, and techniques from all types of adversarial actors. We are already seeing examples across the globe from various nation-state actors—principally from North Korea, but also from Russia and China.

At the same time, those who would do harm for profit, politics, or principle are becoming more sophisticated all the time, with easier and cheaper access to tools and technologies. We are even seeing the emergence of cybercrime-as-a-service. And we are giving our adversaries a larger potential attack surface, with innovations such as the Internet of Things (IoT), the growth of big data analytics, and our exponential use of massive social media platforms.

Responding to the Evolving Environment

As the threat landscape evolves, and as it becomes harder to distinguish between a threat from a nation-state and a threat from a criminal enterprise, the onus is

on all of us to be better prepared so we can prevent attacks and respond quickly and appropriately when there is a breach. Of course, that is much easier said than done.

In my experience, many company executives feel that cybersecurity is too broad and all-encompassing, and that it can be overwhelming. They don't know where to start; they have a hard time measuring the return on investment for cybersecurity; and they are concerned about escalating costs. An exception to this is companies that have experienced a cyberattack. Those are the companies that have a sense of great urgency and purpose.

All of us reading this book, all of us who are passionate about protecting our future and making it safe to navigate the Digital Age—we all need to adopt a similar sense of urgency. Our adversaries are getting bolder and more sophisticated. We have gone from Sony, where there was an attack on freedom of expression and business operations, to attacks on democratic processes and elections. It won't stop there. We are seeing an increase in ransomware, extortion and, eventually, we can expect to see more attacks that threaten the loss of human life.

Given the changes in the mindsets, motivations, tools, technologies, and behaviors of our adversaries, how do we respond? What are the steps we can take now to be better prepared, to be true to the exciting promise of the Digital Age, while recognizing and fighting back against the inherent dangers of an evolving adversary mindset?

I suggest we start by focusing on these key areas:

Connectivity: As we expand our connectivity, we also expand our attack surfaces. Adversaries can harness IoT devices as botnets, causing heightened concern over a potential distributed denial-of-service (DDoS) attack on critical infrastructure. One company has warned about a massive botnet that is recruiting IoT devices to create a cyber storm that could take down the internet.[6] This is not to say we shouldn't move forward with IoT innovation. But we must be aware of increased vulnerabilities. Securing IoT devices is different from securing traditional PCs, laptops, and smartphones. We must quickly get smart about how we use these devices and how we secure them. Do we really want to create an army of toasters that our adversaries can use to attack us?

Regulatory/Legal: The risk of fines, negative publicity, and other penalties tends to be a fairly strong motivator for organizations to focus on cybersecurity with a greater degree of urgency. In Europe, we are seeing that compliance with General Data Protection Regulation (GDPR) is forcing organizations to do a full assessment of their security profiles to ensure a variety of protections. These include providing data breach notifications, anonymizing data to protect privacy, safely handling the transfer of data across borders, and others. It is important to recognize that while GDPR is a product of and requirement within the European Union, it impacts any company around the world that possesses the personal data of EU residents. This is a good thing. In the U.S., questions are being raised whether any regulations—and what kind of regulations—could have been used to either prevent or mitigate the massive Equifax cyberattack that affected more than 140 million Americans. It is the hope of many that Equifax turns out to be a cautionary tale of what can happen when there is a lack of government oversight.[7]

Vulnerability awareness: Ransomware attacks are continuing to grow, with many instances still going unreported or underreported. We are also seeing that spear phishing and social engineering tactics are getting more crafty, more targeted, and more advanced. In 2017, attackers deployed new spear phishing

tactics against organizations across all sectors, including major technology companies and government agencies. Hackers tricked employees at international energy companies into opening documents to harvest usernames and passwords, granting access to power switches and computer networks. Fraudsters targeted UK students with an email scam to steal personal and banking details. At the same time, the spread of misinformation continues, and data integrity attacks are on the rise—impacting the market value of companies and our ability to respond to natural disasters, and influencing public opinion.

Disrupting the Attack Lifecycle

This is also an important time to invest in cybersecurity education, awareness, and training. The more we understand about how attacks work, the better job we can do at lessening their impact—regardless of the motivation and mindset of the adversary, and regardless of our roles and responsibilities within our organizations. The way attackers work is to follow a series of six stages that comprise what we refer to as the "attack lifecycle."[8] These are:

1. **Reconnaissance:** This is the planning stage, during which attackers research, identify, and select targets.
2. **Weaponization and delivery:** Attackers determine which methods to use to deliver malicious payloads, such as automated tools, exploit kits, and spear phishing attacks with malicious links or attachments.
3. **Exploitation:** Attackers deploy an exploit against a vulnerable application or system, typically using an exploit kit or weaponized document. This allows the attack to gain an initial entry point.
4. **Installation:** Once they've established a foothold, attackers install malware to conduct further operations, such as maintaining access, persistence, and escalating privileges.
5. **Command and control:** With malware installed, attackers then actively control the system, instructing the next stages of the attack. They establish a command channel to communicate and pass data between infected devices and their own infrastructures.
6. **Actions on the objective:** With control, persistence, and ongoing communication, adversaries can act upon their motivations. This could be data exfiltration, destruction of critical infrastructure, theft, extortion, criminal mischief, or some combination of all the above.

Being able to leverage knowledge about the attack process provides an advantage for defenders because attackers must be successful at each step to succeed. The defender only has to "see and stop" the adversary at any stage to cause the adversary to fail. To be able to do this successfully, an organization needs to have a holistic approach to addressing cyber risks. In general terms, this includes:

- **Increase visibility.**
- **Reduce the attack surface.**
- **Prevent known threats.**
- **Discover and prevent unknown threats.**
- **Quantify risk.**
- **Transfer risk.**

When discussing cybersecurity, I often compare it to healthcare. If I eat well, exercise, don't smoke, and see the doctor regularly, I reduce the likelihood

of getting sick. But we all get sick, and that's when health insurance comes in to cover the costs associated with an illness. The same thing applies in cyber. If an organization performs the first four steps successfully, then a safety net of cyber insurance can help mitigate catastrophic financial consequences.

How do you accomplish these objectives? Disrupting the attack lifecycle and reducing risk relies on a combination of technology, people, and processes.

- **The technology** must be highly automated and integrated across all network environments, including fixed, mobile, physical, on-premises, and cloud, from the perimeter to data centers, branches, endpoints, and IoT devices.
- **The people** must receive ongoing security-awareness training and be educated in best practices to minimize the likelihood of an attack progressing past the first stage.
- **The processes** and policies must be in place and enforced for rapid remediation should an attacker successfully progress through the entire attack lifecycle.

Preparing for the Future

One of the ideas that recurs throughout this book is the maxim that cybersecurity is everyone's responsibility, as discussed in chapter 10. Investing in cybersecurity education, training, and awareness is a necessary step in that direction. But there is more work to be done.

As participants in a global economy, as nations, as individual companies, and even as individuals, we can all create an atmosphere of cybersecurity cooperation and collaboration. A model for the future, at the policy level, is the U.S.-China cybersecurity agreement, which was signed in 2015 and renewed in 2017. Under terms of that pact, the countries have agreed to refrain from state-sponsored cyberattacks on one another's private-sector companies.

As organizations and institutions—companies, academia, government agencies—we can all be more proactive in sharing threat intelligence so we can prevent attacks and react in real time to minimize the damage of successful attacks. As individuals, we can take advantage of cybersecurity education and training to ensure that we are following best practices, based on our roles, responsibilities, and vulnerabilities within our organizations.

For example, I strongly encourage board members to be aware of and adhere to the five principles of cyber-risk oversight developed by the National Association of Corporate Directors in the U.S. These are:

1. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
2. Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.
3. Boards should have access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas.
4. Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequatestaffing and budget.
5. Board-management discussions about cyber risk should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.

Conclusion

We live in interesting times. Each day, it seems, brings headlines of a new cyberattack or threat (see graphic on page 73). In 2016 alone, the FBI's Internet Crime Complaint Center (IC3) received nearly 300,000 complaints.[9] In February 2018, the Center for Strategic and International Studies estimated that global losses of cybercrime in 2016 were approximately $600 billion. This is an increase from $445 billion in 2015.[10]

Exacerbating the challenge is the reality that the mindsets of our adversaries are a moving target. While adversarial motivations and intentions may have been identifiable in the past, we are now dealing with an environment where there is a melding of the mindsets. What may seem like a cybercrime for profit, or a hacktivist attack, may in reality turn out to be a state-sponsored event or an attack initiated by a company insider.

Recognizing that the motivations of our adversaries are evolving is an important step in the right direction. It helps us all to be more aware. This awareness should also translate into a professional and personal responsibility to take action: Whether that is to undertake cybersecurity training, to hire experts for board meetings, or even just to make sure we are using two-factor authentication.

We can't always predict criminal behavior. But we can be educated, aware, and proactive in making sure that we are doing everything we can to mitigate and minimize risk. As we look to the future of cybersecurity in the Digital Age, that should be our mindset.

---

1 "The Attack on Sony," 60 Minutes, April 12, 2015.

2 "GameOver Zeus Botnet Disrupted," FBI.gov, June 2, 2014.

3 "Student pleads guilty in hacking ring that targeted CIA Director John Brennan," Politico.com, Jan. 6, 2017.

4 "A Stolen NSA Tool Is Being Used in a Global Cyberattack," The Atlantic, May 12, 2017.

5 "ISIL-linked Hacker Sentenced to 20 Years in Prison," The United States Attorney's Office, Eastern District of Virginia, Sept. 23, 2016.

6 "New botnet could take down the Internet in 'cyberstorm,'" says Checkpoint, Internet of Business, Oct. 23, 2017.

7 "Equifax Breach Puts Credit Bureaus' Oversight in Question," NPR, Sept. 21, 2017.

8 Lockheed Martin has registered the term: Cyber Kill Chain®, which describes a similar framework in seven phases: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, Actions on Objectives.

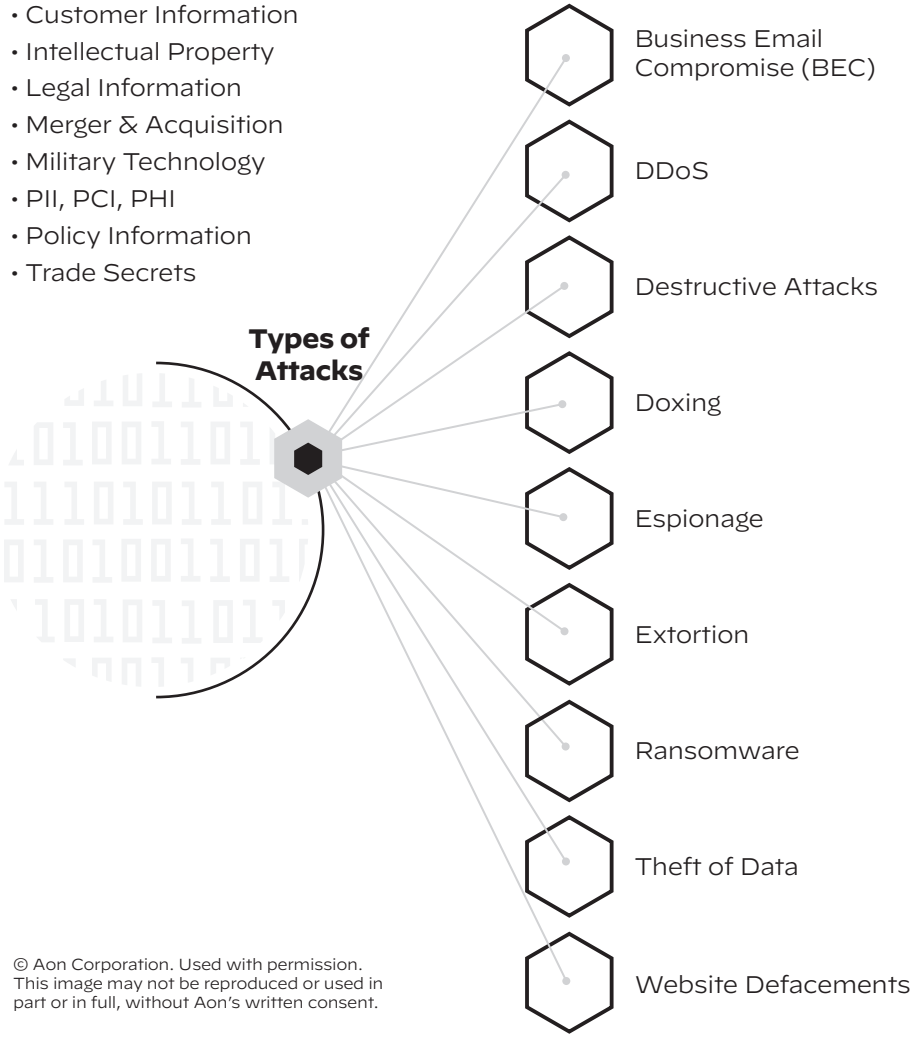
9 "2016 Internet Crime Report," FBI Internet Crime Complaint Center (IC3), June 2016.

10 "Economic Impact of Cybercrime: At $600 Billion and Counting—No Slowing Down," Center for Strategic and International Studies, Feb. 21, 2018.

TYPES OF ATTACKS AND DATA

Types of Data

- Customer Information
- Intellectual Property
- Legal Information
- Merger & Acquisition
- Military Technology
- PII, PCI, PHI
- Policy Information
- Trade Secrets



9

The Evolving Role of the CISO: From Risk Manager to Business Enabler

Justin Somaini — Chief Security Officer, Unity Technologies

One of the first things I do in my role as Chief Security Officer is reach out to the heads of other departments to find out how I can integrate myself into their operations. In one more extreme instance, I asked if I could join the sales department on a part-time basis. Not as a salesman, thank goodness, but in my role as CSO. The head of sales was a bit perplexed, but agreed. For a year I participated in sales meetings and even went on sales calls.

I learned about conversion rates and vicariously experienced the unimaginable thrill of closing a big sale and the crushing pain of losing one. By the time the year was up, I had a solid understanding of how our sales organization worked and, perhaps even more importantly, I had developed close working relationships with a number of key people in the department.

You may be thinking: You're a chief security officer. Why would you spend a year in the sales department, even part time, when your job is to protect the company from security breaches and ensure that it remains compliant?

I would answer that merely protecting the company from security breaches and ensuring compliance is actually not a very good description of my job, nor the job of my peers and colleagues around the globe. Not in 2017, not in 2018, and certainly not in the years ahead.

The role of the CSO, or as many prefer, the chief information security officer (CISO), has come a long way in the 20-plus years since the CISO title was first created. Today it is evolving at a faster pace than ever before. The CISO now must identify himself or herself as a business enabler and, just as critically, he or she must be recognized in the same way by others—from the boardroom to the executive suite to the various lines of business and departments that keep the organization focused, functioning, and moving forward on a day-to-day basis.

How could I enable sales if I didn't understand sales? Or marketing, human resources, finance? How can I enable the business if I don't have a firm understanding of how the business works, what motivates the teams, what the corporate culture feels like in the trenches?

These may seem like fairly obvious questions, but they are not necessarily the questions most CISOs have asked in the past. Looking to the future, I believe these are the kinds of questions that will increasingly define how CISOs oper-

ate. They will also be a factor in who fills those key roles and how security practitioners interact and collaborate within their departments and across the organizations at large. If the CISO is empowered to enable the business, he or she must speak the language of business and be conversant with the basic activities and values of the business.

The Transition to Business Enabler

The CSO is a continuously evolving role that drives a continuously evolving skill set. In order to be successful, practitioners need to be proactive in maturing the role as well as themselves. Twenty years ago, the job was basically to manage the firewall and secure the perimeter. You didn't have to know much about what you were protecting, as long as you knew which technology solutions would do the best job of keeping the bad guys at bay.

The world today is much different. Digital technologies and connectivity have infused every aspect of the business. This elevates risk, but it also elevates the value and importance of the cybersecurity function. The CISO increasingly has a seat in the executive suite because security is no longer just about risk; it's also about competitive differentiation.

The most fundamental way in which security can act as a differentiator is by removing hurdles to enable and empower the sale of products and services to the customer. When I think of my objective at SAP, it was to have a secure company and a secure customer. It's pretty straightforward, yes. But making it happen is anything but simple.

For example, security should be able to empower faster, more agile and more reliable product development. That is one reason organizations are more inclined to include security early on in development processes and why we are seeing the rise of SecDevOps. In addition, security must support business and technology innovation—think Big Data analytics, the Internet of Things, social networking, and machine learning, to name a few—to enable true competitive differentiation and potential market disruption.

There are other ways to drive business enablement. If we build better, more reliable security protections into solutions than our competitors do, we can build customer loyalty and help retain existing customers. If we can create security solutions that are seamlessly aligned with the company's direction, we can create differentiated products, services, and potential revenue streams. For example, the company comes out with a new service that offers advanced security monitoring and alerts for an additional $10 a month. If we can drive operational efficiencies and effectiveness, we can help the organization accelerate speed to market and reduce overall costs.

The Evolution of the CISO

How do we get there from here? What are the skill sets that will differentiate the best CISOs from the rest? What do business leaders and board members expect from their CISOs, now and in the future? How can we ensure that we are truly enabling the business, while still performing our fundamental responsibility of having a secure company and a secure customer?

I suggest we start by focusing on three specific areas:

1. **Ensuring that we are extremely disciplined in the things that are known:** This should encapsulate the basic tasks of the cybersecurity domain—controls, vulnerability scanning, patch management, application security, and more. We need to be absolute professionals in these tasks and functions. If you can't deliver on the basics, you can't deliver, period.

2. **Becoming proficient in addressing today's more expansive expectations:** For example, we can talk about risk management, but we need to actually define it and articulate it for our organizations, so decision-makers understand what they are investing in, and why. We must be proficient in empowering specific initiatives that are impelling our organizations forward, such as cloud computing, modernizing legacy applications or enabling secure mobility, digital transformation, and other organizational imperatives.
3. **Analyzing, predicting, and preparing for the future:** Technology is moving at a rapid pace, to be sure, but there are certain things we can predict about the future with pretty clear certainty. We know that the Internet of Things is something we must make secure. We know that IT consumerization will continue to redefine customer expectations. We know that jurisdictional fiefdoms are continuing to impact how we think about security. We know that technologies such as artificial intelligence and machine learning will help drive innovation, within our own organizations and among our adversaries.

We must be thoughtful and proactive in advancing security into these domains before they become a problem. Business enablement is more than merely being aware of these responsibilities and challenges; it also requires that we become excellent and proficient in communicating, collaborating, interacting, and managing our inter-relationships within the organization.

Clearing the Lines of Communication

It is not simple to evolve from the kind of cloistered, poorly communicative security department that has characterized many organizations into an operation that is fully engaged and adapted. You need to have the buy-in, support, and prioritization of the security function across the organization, whether that is sales, marketing, development, customer support, or any other business function or department.

The only way to get that buy-in is through translating and communicating the language of security so that business people understand it. CISOs have to step outside of the security domain and see what value they can add throughout the organization. In my experience, there are four fundamental objectives the CISO must be thinking of when communicating within the organization:

1. How can cybersecurity help generate, protect, and ensure revenue?
2. How can cybersecurity help retain existing customers?
3. How can cybersecurity help differentiate against competitors?
4. How can cybersecurity drive operational efficiencies and effectiveness?

To do this, you need a security team that is transparent, forward-leaning in engagement with the organization and, perhaps most important, deeply knowledgeable about how the business is run and what the various departments truly do. How can the CISO expect the company to understand the risks, if we can't transparently explain what the reality is? We need the rest of the organization to see the world through our eyes.

CISO: The Next Generation

Every business and every culture is different. A for-profit organization is not going to have the same goals and objectives as a non-profit. A company with a global customer base is going to operate differently than a company whose customers are regionally located.

One of the many things I learned in my year with the sales organization was that our sales teams in South America had much different motivations and ways of operating than our sales teams in North America. Would I have been able to truly understand this if I hadn't taken the time—and had the interest—to learn in great detail how the organization worked?

Tomorrow's CISOs will have to be on intimate terms with every aspect of the organization. I think it is wise for security professionals to follow the intent of an MBA rotation program and spend a quarter inside the marketing organization, a quarter inside sales, a quarter inside finance, a quarter inside HR or manufacturing, or some other department central to the overall operations of the business. You get a basic, simple education over time. It's not academic. It's real. You get to watch the everyday lives of your constituents. It helps you change your security model and mindset.

People often ask what characteristics to look for in potential CISOs. The first thing I look for is someone with a strong moral compass. I look for people who will do things beyond their responsibilities. If she sees something wrong, she fixes it, without looking for credit. I look for people who have a basic curiosity. We are a horizontal function across the business. I want someone who wants to ask: How does the business operate? How does it grow? And I certainly want someone who is curious about security technology. If you're not curious about new technology, you're not going to take the time to explore new ways of doing things. In cybersecurity, we always have to be willing to adopt new technologies and new solutions to solve new problems.

If I have to go around telling people what they should be doing, I am not doing my job very well. I want people to be unsatisfied with what they have, who are waiting for me to move on so they can step into my role. You can't teach someone to be a CISO; they have to be able to do the job, to learn, and to adapt, and they have to be forced to grow. They have to be self-critical and very open mentally. Curiosity is amazingly important. In order for you to convince the rest of the business to take security seriously, you must understand what motivates them and how you can better influence them. In order to do that, you've got to get to know them.

Steps to Take Now

How does any executive get defined as being successful? You have to make your number, whatever it is. In security, because we don't generate revenue, we're often measured in terms of risk mitigation, not necessarily business enablement. If you are successful, you may have no incidents. If you have no incidents, people will think there's no need to invest in security. So you have to communicate: Let us show you how we are being attacked and how we are blocking these attacks.

Once you really understand the business, you can talk the talk much more effectively in the language of business enablement. For example, many companies are looking to drive business in China. Security needs to be part of that discussion. We have the power and potential to help the company overcome hurdles, and if we can overcome those hurdles, we can help the company acquire new customers and open up new revenue streams. That is how you win the hearts and minds of executives and that is how you motivate them to give you a seat at the table.

Here's one more measure of success that may not be obvious to CISOs who are not yet focused on business enablement: Do your peers in the organization include you in relevant discussions? Do they like you or hate you? Do they see you as

obstructionist or do they see you as part of the culture of change? If people don't want to include you, you are not going to be able to help them. It puts the onus on CISOs and their teams to be more engaging, open, and inclusive.

The path to business enablement is a journey. There are simple steps we can each take immediately, and it doesn't necessarily mean spending a year in the sales department, although, if you haven't done it, I highly recommend it. The things security professionals can do now to be more proactive in supporting business enablement include:

- Send an email to the heads of sales and marketing, and tell them you want to learn. Ask if you can sit in on weekly sales calls. That one step will go a long way. They will understand who you are and what you do. Right now, they probably have no concept. Identify people in the organization with whom you need to build relationships, and ask them what you can do to help.
- If you don't already do this, read the company's financial reports religiously. They will give you valuable information about your business that you won't always be aware of during the normal course of day-to-day activities.
- Reach out to your peers and build some kind of "state of the union" report, or annual cybersecurity report, or a compelling infographic. Give them something that is interesting and informative, so that people with either little time or lack of interest will spend some time with it and learn something from it. We must be looking at how we change our language so that it resonates with non-security people. Develop a cadence of different deliverables and materials, using all of your resources, including online. Then track what works best in your organization, both with your peers and with the executive board.
- Look at your team and your culture. Are you open about the problems of cybersecurity? If necessary, have a cybersecurity town hall meeting. Keep open office hours for everyone to come by and air grievances or simply communicate about real issues and opportunities. Your team will see the change in tone and direction, and they will naturally follow suit.
- Take a hard look at yourself. Do you love what you do? What really motivates you? Are you curious about the overall business? Where do you spend your time on a monthly basis? Most of us avoid the things we hate and go to the things we like. Are you self-critical? What do you resist, what do you find to be stressful, do you avoid having critical conversations with your boss or peers?

Conclusion

This is a great time to be a cybersecurity professional. Our role in our organizations, and the world, is becoming more critical and more highly valued. It also means we take on more pressure and have more responsibility. Doing things the way we've done them in the past just won't cut it in today's environment.

To prepare ourselves and our organizations for the future, we must understand and speak the language of business enablement. We must be curious about how the business works, and we must be articulate in explaining how we can help. We must evolve and we must do it quickly. The Digital Age isn't waiting for anyone.

How Work Requirements and Ethical Responsibilities Come Together

10

The Great Reset: The Future of Work and Cybersecurity

Gary A. Bolles — Chair for the Future of Work, Singularity University

Until early 2020 much of the ongoing debate about the shifting landscape of human work focused on whether technology or globalization was having a greater impact on our work. Were robots and software digesting jobs? Or did offshore production and distributed supply chains have a greater effect? Economists and pundits throughout the world weighed in.

Then along came a virus. We know now that neither globalization nor automation compares to the sudden appearance of a global health crisis, which dramatically changed work as we know it. Yet this great shift masked two even more powerful forces: the pace of change and the spread of change. Even though automation, globalization and the pandemic are all jockeying for top honors for disruption, it's actually the *speed* and the *distance* of change that are causing the greatest ripple effects on human work. At the same time, they have also contributed to an exponential increase in the potential complexity of enterprise security. As a result, these are the two forces that are fueling some of the greatest challenges—and opportunities—for cybersecurity.

The Pace and Spread of Change

As the pandemic gripped the world, we entered into what I called, "The Great Reset," a tectonic shift in how, when, and where we worked. That reset has ended up being one of the most profound lessons on the pace and spread of change for virtually every industry, business, leader, and worker.

Of course, dramatic change isn't new. Over the past few decades, many industries had already been subject to disruptive change. The internet revamped businesses such as media and retail. Shifting global supply chains reshaped manufacturing. Breakthrough technologies transformed markets ranging from dating to personal transportation. Yet all of these market shifts paled against the abrupt change driven by The Great Reset.

Enabled by communications technologies, workgroup apps and online work platforms, many organizations already had experimented with distributed work. Companies such as IBM and Yahoo at one point had robust work from home (WFH) policies. Yet the traditional approach to leadership has leaned heavily on what I call "management by surveillance," with

a strong bias toward a manager's role as the command-and-control supervisor whose trust only extends as far as her hourly view of a team's work. In part because of that lack of trust, many companies shut down their WFH programs, calling workers back to their mother-ship offices. From a cybersecurity standpoint, this simplified preparation and response models, since the majority of work would continue inside the physical corporate sphere.

That didn't last. As the lockdown strategies of The Great Reset took hold in one country after another, suddenly managers had to supervise distributed teams, and adapt with a speed that few before would have thought possible.

But rapid change alone can ultimately be manageable. If the change is to a predictable future state that's not significantly different from today, then speed by itself doesn't have to be a huge barrier. However, the other twin tower of disruption is the spread of change. The more different tomorrow is from today, the more problems morph and the more a new skill set is needed to solve those problems, the greater the potential challenge.

For example, a large conference or concert business with a few unpopular events simply needs to adjust its offerings. But a producer that can't fill a single stadium needs to rapidly experiment to find out what its customers and performers will want through digital offerings. A showroom furniture store may have to adjust its prices by season. But a showroom with no onsite customers must make the leap to a digital-only business and offer a compelling online experience, which requires an entirely new skill set. And where lockdowns continued, many businesses had to reconsider whether their entire approach to the market needed to change permanently.

The same, of course, is true of work. Driven by the sudden appearance of dot-com competitors or the rapid evaporation of the market demand for certain skills, some workers, in the past, needed to rapidly adapt to new demands. But, though many denizens of the hi-tech arena say that we thrive on change, as humans few of us are truly prepared for really rapid change. And few of us are prepared to learn entirely new skills in a dramatically different arena.

It turns out that a lot of our human preconceptions of what is possible are driven by routine and familiarity. We are each capable of extraordinary accomplishments, given the right requirements or incentives. Maintaining our businesses and our jobs seems to be the right combination of incentives.

But in the rapid shift to distributed work, many leaders are gaining the growing realization that they have broken the seal on the traditional organization. The result: Their workforces are becoming fluid right before their eyes.

The Suddenly Fluid Workforce

In the "Survive Phase" of The Great Reset, much of the discussion in the zeitgeist focused on the rapid adoption of distributed communications. Many workers who rarely or never used video calls suddenly found themselves completely dependent on a daily stream of back-to-back-to-back webcam meetings. Yet this process masked what was already happening to workers and teams, fueling a new workforce framework for the enterprise.

In many industries and organizations, work and jobs were already becoming atomized by technology. Work tasks were being split up among workers in dynamic ways, as teams continually faced new problems. Work responsibilities and roles were being adjusted accordingly. Some

organizations responded by committing to programs that could help workers become adaptive learners. But many companies continued to follow less-agile processes that kept workers from being able to effectively adapt.

That less-flexible mindset of the past can be thought of as somewhat binary. Workers are either employees or they're not. While there might be a range of work roles within the organization, a binary approach reduced the number of use cases for work, making it comparatively easier to hire, develop, and promote workers.

The Great Reset has forced organizations to embrace a far more fluid mindset about workers and work roles. While market leaders in the past could simply reinforce existing processes and work roles, even traditional incumbents are now realizing they must embrace more agile processes. This will inevitably mean a far more fluid mindset about the range of roles that workers will perform.

From a management standpoint, the vision of the kind of "boundaryless" organization has been around for decades. In G.E.s' 1990 annual report, Jack Welch expounded on a vision of a new kind of organization. "Our dream for the 1990s is a boundaryless company," Welch said, "a company where we knock down the walls that separate us from each other on the inside and from our key constituencies on the outside."

Think of it as a "soft-walled organization," with people in a range of contexts easily, and rapidly traversing the former edges of the company. But how can business and IT leaders get their minds around this kind of shift? Rather than a binary mindset, a more useful perspective may be fuzzy thinking.

In mathematics, a binary set is straightforward. Membership in the set is either 0 or 1. But an element in a fuzzy set is defined by its *degree of membership* in the set.

Look at the range of roles in an organization. At any point, your organization may, of course, have traditional full-time employees. But it may also leverage the energies of part-time workers, temporary workers, contractors, sub-contractors, consultants, work consortia, industry consortia, online gig workers, apprentices, students, cloud workers, crowdsourced workers, partners, and even former employees. And all of these might be performing their work in an unlimited number of physical locations, and collaborating with each other in an N-dimensional number of relationships.

Full-time employees with benefits might be thought of as having 100% membership in the work of the organization. But a gig worker who drops off a pizza to the office (assuming you have an office) would have only the slightest percentage of membership in an organization's work. Every other role would be something in between 0 and 100%.

Fuzzy set thinking also needs to be subjective and multi-directional. For example, let's say that I think you and I are friends and co-workers. You, however, think we are just co-workers. So when the arrow points from me to you, there's an additional "friend" set. But it only works one way, since you don't feel the same.

The same can be true for work relationships. I may have tremendous loyalty and affinity to the organization. But if I'm a contractor, the organization may think of me as a disposable worker. That kind of subjectivity and ambiguity is hard enough in simple interpersonal interactions; it is especially problematic in a constantly changing workforce.

Some leaders may find this breathtaking complexity such an overwhelming problem to solve, even from a pure HR management standpoint, they may believe that existing business processes are simply not up to the task. They can't possibly hire and manage large numbers

of workers in fluid and ambiguous relationships. Worse, line managers within many organizations are ill-prepared to directly manage this kind of complexity as they try to coordinate team members in a series of increasingly ambiguous work roles.

Yet the response by many organizations to The Great Reset actually shows that this kind of fluid mentality is indeed possible. What is critical is that IT leaders have the same approach to the organization's cybersecurity model.

Fuzzy Ways of Thinking About Cyber Risk

Users in the old enterprise security model were essentially managed by standard set theory. A worker could be thought of as occupying a position in a set, such as "employee." That "employee set" had a limited number of use cases associated with it. Cyber-risk models related to work would typically be based on the layering of tasks, resources, interactions, and geography.

Any worker's responsibilities results in a set of tasks they regularly perform. Each worker needs access to certain *resources,* such as information, hardware, and software. Invariably there are some kinds of *interactions* with other workers, both inside and outside the organization. And workers perform those tasks in one or more physical *locations.*

In the past, these factors could be relied upon to be relatively static for many work roles. Sure, some people changed work roles and tasks regularly, requiring new resources and interactions. But in many organizations this was a small subset of the workforce. Some workers operated from home or performed as nomads, but in most organizations these were limited to sales and business development functions.

However, The Great Reset has shown that virtually all of these—tasks, resources, interactions, and geographies—can change dramatically. And they can, and will continue to morph, both in terms of the pace and spread of change.

How, then, should leaders think about cyber risk in the era of the fluid organization?

In the early 1990s, when I was the editorial director for *Network Computing* magazine, the risk model for the organization focused on the perimeter. If an organization could simply manage the edges of its technology and physical infrastructure, anything within those virtual and physical walls could be considered part of the trust domain. But the advent of public networks erased the perimeter, and with it went perimeter security strategies.

To incorporate a range of use cases that included remote and mobile workers, the new model focused on endpoints. Secure every endpoint and the connections between them, and trusted communications could ensue. But because organizations of any scale still had large offices, a substantial percentage of workers could be assumed to operate within the trust bubble much of the time.

Today, however, the organization is perpetually distributed, and likely perpetually fluid. Suddenly someone who was a contributor to a cloud-based crowdsourcing competition becomes a contractor working on a sensitive project. How does the organization recognize that transition? How can it flexibly and easily adapt its security model, practices, and tools to ensure that the appropriate levels of security are maintained?

In addition to these challenges, The Great Reset has introduced at least one new security factor to consider: Health risk. An enterprise information security strategist might have cared about worker health in the abstract. But suppose now that a worker comes into the office, and a week later her co-workers fall ill. Is it the organization's responsibility to track

those interactions, and trace back to find out who was in contact with whom? Does that have an impact on how the organization will manage resource access and co-worker interactions? Would a worker who has tested positive for a disease be flagged on building entry in the same way as someone who had breached information security?

The new enterprise cybersecurity model needs to be built on fuzzy thinking. The constantly changing landscape of workers, tasks, roles, resources, and geographical location itself will remain fuzzy for some time. Even when many organizations ultimately shift into the Thrive phase of the Great Reset, hopefully with the capacity to build their businesses even better than before, leaders will find their organizations have become inevitably and perpetually fluid.

Those organizations that embrace this new model in their businesses—as well as in their approach to cybersecurity—are the ones that will truly thrive from the insights gained in and around The Great Reset. Many of these lessons to be learned and adopted are eloquently discussed in subsequent chapters of this book, exploring a variety of ways to articulate cyber risk and offering insights for ways to adjust and innovate in a world characterized by an increasing pace and spread of change.

Anticipating the Next Great Reset

Look down the road a few years. What happens if a sudden modification to an international trade law means your organization can't continue to function in its primary market? How would your organization respond if its customers rapidly adopted a competitor's new product or service? How will any organization react when generalized artificial intelligence suddenly performs a range of new business processes at a tiny percentage of existing worker costs? What could happen to your organization's entire security function if quantum computing renders most security keys ineffective?

Granted, of course, that many of these are unlikely. But to many of us, so was a global pandemic.

From a cybersecurity standpoint, suppose you work at a gig-worker company operating in a geography that overnight becomes subject to a law redefining every independent contractor as an employee. How could the organization's cybersecurity model rapidly incorporate potentially thousands of workers whose "degree of membership" in the company increased from 2% to 100%? Would your existing model adapt, or collapse?

Not to mention, of course, that automation and globalization haven't gone away as seismic forces. Each of these will continue to have a substantial impact on workforces, forcing continuous changes in work roles and business dynamics. No matter what tomorrow's drivers will be, there is no foreseeable time when the pace and spread of change will slow.

At the beginning of 2020, few business continuity plans anticipated the impact of a global pandemic. Yet organizations that managed themselves with a fluid workforce found they were in a far more advantageous position to anticipate new shocks to the system. Today, the opportunity for leaders is not just to adapt to having a more fluid organization, but to embrace the capacity to continually adapt—and to ensure that the organization's approach to cyber risk is just as adaptive.

11

The Ethics of Technology and the Future of Humanity

Gerd Leonhard — Author; Executive "Future Trainer;" Strategist; Chief Executive Officer, The Futures Agency

The Next 20 Years Will Bring More Change Than the Previous 300

If this statement sounds somewhat preposterous, please keep in mind that we are now crossing a crucial threshold that was previously unthinkable. Technology is no longer simply changing our environment, i.e., what is *around or outside us*, or what hardware we use. No more is it just a tool. Technology is well on its way to becoming a creative force—and a thinking machine, as well.

Technology is now gearing up to go *inside us*, thereby changing who we are and rapidly redefining what it means to be human. All this, as some of my fellow futurists are fond of saying, to allow us to "transcend the limitations of humanity."

If intelligent machines are to perform our routine work for us, we will have to train them, teach them, connect them to us—in effect making digital copies of ourselves, cloning our knowledge (and possibly some of our unique human intelligences) in the cloud. This will alter us; and it will alter our view of what we are and what we could be, as well as what the machines are. And this is only the first step. Try to imagine:

- Nanobots in your bloodstream monitoring and even regulating cholesterol levels.
- Augmented virtual or mixed reality devices that look like regular eyeglasses or even contact lenses, giving you ready access to the world's knowledge, at the blink of an eye.
- The ability to connect your neocortex directly to the internet and transform thoughts into action or record what you think.
- Developing a relationship with your digital assistant or robot because it seems so real, so very human.

None of this is as far away as you may think, and the societal, cultural, human, and ethical implications will be mind-boggling. Clearly we must prepare for this challenge today, or we will find ourselves ill-equipped to handle these new realities. If we are not able to clearly define and articulate an agreed upon set of Digital Age ethics, we run the risk that unfettered technology expansion will not only be dangerous, it will also cause us to question the very nature of our existence: What is it that makes us human?

Defining Ethics

Before we venture further into why ethics in technology is critical to our future, first let us attempt to define what ethics is. Riffing off the late U.S. Supreme Court judge Potter Stewart, I propose this as a working definition:

> ***Ethics is knowing the difference between what you have a right or the power to do and what is the right thing to do.***

If we accept this definition and apply it to what is coming in the next 10 years, we can quickly see a serious challenge emerging.

The Future Is Exponential, Convergent, and Combinatorial—and So Are the Resulting Ethical Challenges

Right now, we are at the take-off point of exponential progress. Henceforth, change is no longer gradual but sudden, in almost all scientific and technological progress—such as quantum/3D computing, nanotechnology, biotechnology, cloud computing, hyper-connectivity and the Internet of Things (IoT), AI, geoengineering, solar energy, 3D printing, autonomous vehicles, and pretty much everything else.

What's more, most of these exponential technologies are dual-use—meaning they can be harnessed for incredible, positive innovations as well as for evil purposes. As William Gibson, the science fiction writer widely credited with pioneering cyberpunk, likes to say, "Technology is morally neutral until we apply it."

Let's imagine the world a mere 10 years from now—some 50 to 100 times more advanced—a world where most science fiction has become science fact. It is likely to be a world where literally everyone and every*thing* around us is connected, observed, recorded, measured, and tracked. I estimate there will be something like one trillion devices on the IoT by then, where IA (intelligence augmentation) has truly become AI (artificial intelligence), and where at least 80 percent of the 10 billion earthlings are connected at high speeds, on cheap devices, wearables, and via digital assistants and robots that we can communicate with, as if we are speaking to a good friend. Add genetic engineering and the rapid convergence of technology and biology to this equation, and the sky is the limit—literally—in terms of possibilities (see page 89).

Exponential thinking, therefore, becomes mission-critical, both to realize opportunities and to foresee and address the consequential ethical challenges and moral quandaries.

A Perfect Storm of Combinatorial Forces

Even more important, the true challenge to humanity lies in the fact that while all these technologies are unfolding exponentially, they are also causing traditionally unrelated industries (and the sciences underneath them) to converge. These so-called megashifts, such as datafication, cognification, automation, and virtualization (see megashifts.com) are already combining with each other to create entirely new possibilities and challenges.

These convergent and combinatorial forces will soon create a perfect storm of immense progress and enormous challenges that transcend the realms of technology and business by impacting society, culture, and humanity as a whole.

Get Ready for the Next Generation of Unicorns

Looking back at the warp-drive success of the unicorns of the past seven years (i.e., those companies that were or are privately valued at over $1 billion, pre-IPO, such as Uber, Xiaomi, Palantir, Airbnb, and Spotify), we can already see

examples of the exponential-combinatorial-convergent story. And this is just the beginning.

For instance, Spotify's business model became feasible only because of exponential and combinatorial technological change: Streaming 20 million songs to 150 million users is now doable, thanks to the fact that we finally have cheap yet powerful smartphones connected to fast mobile networks. In addition, we now have new ways of paying online, AI/algorithms that create playlists, and last but not least, sufficient market pressure on the record companies to provide the licenses. It is quite revealing to note in this context that Spotify is no longer really in the business of "selling music." Rather, it sells convenience, intelligence, interface, and curation—the result of a convergent and exponential outlook on the future, something that apparently is always reserved for industry outsiders.

Airbnb makes for another great example. It boasts a vast, global database of users' short-term rental listings, with mobile devices as the primary use case. It employs intelligent rating and pricing technology (AI once more, if you will), has social media built in to the system, offers digital payment options, and has been propelled by the rise of the sharing economy. Put all this together, and you have warp-drive growth.

While these tech innovations are all mostly positive developments that often enrich our lives, we must brace ourselves for what is about to come: new superstar, exponential, unicorn organizations that combine AI and biotechnology—thus achieving the complete convergence of technology and biology—or fuse AI, nanotechnology, and the material sciences.

Understanding the Urgency to Construct Ethical Frameworks

However, the prospect of such exponential growth puts us on the horns of another dilemma. We must now urgently construct ethical frameworks that will keep up with this furious pace. Without these ethical frameworks in place, unfettered and thereby socially destructive growth will become increasingly toxic and disastrous.

Clearly we must prepare for this challenge today, or we will find ourselves ill-equipped to handle these new realities. Business ought to take a lead on this, and so must savvy politicians and public officials. Whoever is the thought leader in these thorny issues will be more influential than Warren Buffett has been in matters of investing.

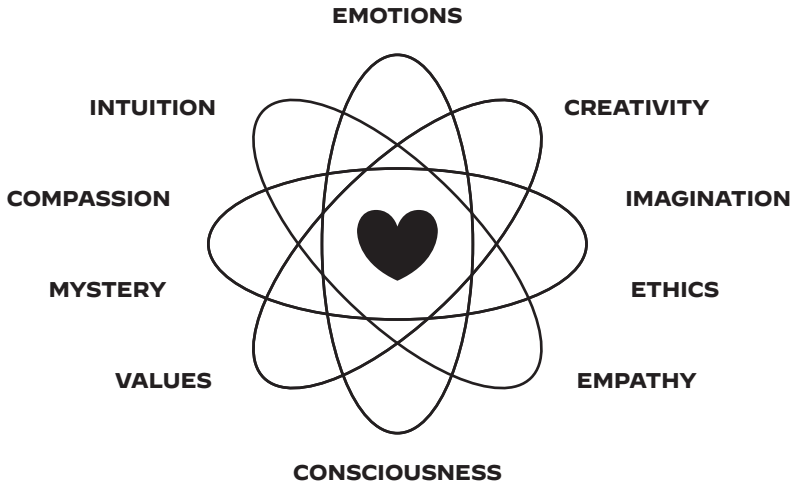
Donald Ripley in the 1995 movie Powder: *"It has become appallingly clear that our* ***technology*** *has surpassed our* ***humanity.****"*

Every Extension Is Also an Amputation—but What Should We *Not* Amputate?

Marshall McLuhan talked about this in his landmark 2001 book *Understanding Media,* and it rings even more true in the present day: Every technological extension of ourselves is also an amputation of another part of us (or another extension).

If we continue to have closer relationships with our screens than we have with other people, if we will indeed "transcend human limitations" by spending our lives in augmented or virtual spaces, or if we are to connect our neural networks directly with an AI in the cloud, then we will certainly lose—i.e., *amputate*—many things that make us human. I firmly believe this is a consequence we must reckon with.

We stand to lose human elements, such as emotions (which can be emulated by but are fundamentally incomprehensible to computers); imperfections (smart machines won't tolerate errors); surprises and serendipity (machines don't enjoy them), and mysteries (machines hate them).



Generally, it would become nearly impossible to retain what I call "the androrithms," all the things that actually make us human. We might end up extended in many different ways, but also our basic human expressions could end up amputated. We'd be extremely intelligent, but totally dehumanized. That strikes me as a bad idea.

Who will decide what we can safely amputate—such as, maybe, the ability to read maps or drive a car ourselves? Who will define the limits of when we will no longer be human? Who is mission control for humanity?

Getting an Ethics Upgrade—From If and When to *Why* and Who

The bottom line is that we are now moving to an entirely different era as far as technology is concerned. Sometime in the next five to 10 years, it will no longer be about *if* we can do something, i.e., technical feasibility, cost or time, can something be done, will it actually work, how expensive will it be, and how will it make money? Rather, it will be about *why* we are doing it (context, purpose, values, goals) and *who* is doing it (control, security, governance, power). In other words, it will be about ethics, ultimately. This is a crucial shift in society, brought about by exponential, convergent, and combinatorial change.

Are you ready to shift from an emphasis on science and technical feasibility to an emphasis on meaning, purpose, and human governance?

What Does Digital Ethics Have to Do With Security? The Digital Ethics Moonshot

In my opinion, technological security can only be as good as the moral, ethical, and political frameworks that surround and define it. The most advanced security technology will be useless if those who hold the key and those who use it, act unethically, with evil intent, or with great negligence. In fact, the very same technology that is employed to protect consumers and users can be used to spy on them. Some of the most potentially beneficial technologies, such as the IoT, can be used to form the biggest and most powerful Panopticon ever constructed.

It will therefore not be enough to simply improve technological firepower as

the world gears up for exponential technological growth; we must also redesign and embolden our ethical frameworks. We have to reach a global agreement on what is good for humanity, at large, and what is clearly not—and, also, how we would enforce such tenets.

In many ways, this task might even be harder than the technological challenges ahead of us.

Ethics in Technology, aka Digital Ethics, Will Very Quickly Become the No. 1 Issue in This Industry

Defining ethical standards on a global scale is not easy. It may even be impossible *if* we attempt to address very detailed convictions, i.e., values and beliefs that are particular to specific societies, countries, regions, or religions. But if we stay at the very top level, on a global scale, I believe we can indeed define some crucial ethical standards for humans. The key will be to focus on HUMANITY, and to act with what ancient Greeks called *phronesis* (practical wisdom) in order to ensure that all technological progress results in collective human flourishing—which is the underlying paradigm we need to adopt.

On the topic of religion and ethics, Albert Einstein (a big source of inspiration for me) repeatedly set forth that morality does not require a divine source. Rather, morality (yet another term to describe something like ethics) is a purely natural and human creation; it is simply a part of being human. The Dalai Lama wrote an entire book on his belief that ethics is more important than religion. Take note.

Meta-level ethics would, for example, assume that pretty much everybody wants to remain human, retain human qualities, and enjoy basic human rights, such as the right to free will, free decision-making, and choice (notwithstanding the few but also very noisy transhumanists and extreme singularitarians who seem overly keen on becoming cyborgs or robots as soon as possible).

Who would enjoy having their digital (or real) identity stolen, or their DNA used to program a super-soldier halfway around the world? Does anybody want his or her data and information out in the public sphere? Everybody enjoys the ability to have mystery, secrets, mistakes, and privacy in their lives.

For Your Consideration: An Ethics Framework for the Digital Age

These are the kinds of general digital ethics principles that could be the framework for a global "ethics in technology" manifesto—a kind of digital human rights declaration. In fact, I suggest five core human rights that could form the basis of a future digital ethics manifesto:

1. **The right to remain natural, i.e., biological.** We need to retain the right to be employed, use public services, buy things, and function in society without a requirement to deploy technology on or inside our bodies.
2. **The right to be inefficient if and where it defines our basic humanness.** We must have the choice to be slower than technology and not make efficiency more important than humanity.
3. **The right to disconnect.** We must retain the right to switch off connectivity, go dark on the network, and pause communications, tracking, and monitoring.
4. **The right to be anonymous.** In our coming hyperconnected world, we should still have the option of not being identified and tracked, such as when using a digital application or platform, when it doesn't pose a risk to or impose upon others.

5. **The right to employ or involve people instead of machines.** We should not allow companies or employers to be disadvantaged if they choose to use people instead of machines—even if it's more expensive and less efficient.

Conclusion

What are we without ethics? Can we still assert and own our humanity, particularly as we barrel headlong toward a future in which technology will give us the ability to blur the lines between what is human and what is machine? Just because we *can* do it, *should* we do it? And if we do, how will we define what is the *right* way to do it?

I believe we urgently need to tackle this challenge because the future could be heaven, or it could be hell (I call this 'HellVen'), depending on the decisions we make today. Technology does not have ethics, but societies depend on them. Let us remind ourselves that civilizations are driven by their technologies and defined by their humanity. Technology is not *what* we seek, but *how* we seek.

A BRIEF HISTORY OF THE NEXT DECADE BY GERD LEONHARD

2024: The world is becoming hyperconnected, automated, and uber-smart—and everyone benefits. Nine billion people are "always on," around the planet, each of us seeing different information and content all the time. We interact with platforms via augmented reality, virtual reality, holographic screens, or via intelligent digital assistants (IDAs).

2025: Our own digital egos have moved to the cloud and are developing a life of their own. Swarms of IDAs and software bots live in the cloud and take care of routine tasks. No more searching for restaurants or hotels; no more updating the doctor on what's wrong. Our bots know us and our desires, and they communicate infinitely better than we can by typing questions into a computer.

2027: Goodbye privacy and anonymity. We are constantly connected to machines, and they are getting better and better at reading our minds. Technology has become so fast, powerful, and pervasive that we cannot avoid being tracked, observed, recorded, and monitored—ever.

2028: Automation is widespread, and social norms are being rewritten. Gone are the days when routine tasks—whether blue collar, white collar, manual, or cognitive—are done by humans. Machines have learned how to understand language, images, emotions, and beliefs. Machines can also speak, write, draw, and simulate human emotions. Machines cannot *be,* but they can *think.*

2029: Free will and free choice are only for the privileged. Our lives have become tracked, guided, and curated. Because everything we do, say, see— and increasingly, feel and think—can be tracked and measured, we see a waning in the importance of free will. We can no longer easily divert from what the system thinks is best for us, because everything is observed. This makes for healthier and more responsible lives, lowers the costs of medical care, and makes near-perfect security possible. Yet, many of us are unsure whether this is heaven or hell.

2030: 90 is the new 60. Because we have analyzed the DNA of billions of connected humans via cloud biology and quantum computing, we can now determine with great certainty which exact gene is responsible for triggering which exact disease. In another five years or so, we will be able to prevent cancer. Longevity has exploded, completely changing our social systems, as well.

PART 2
Lessons from Around the World

Part 2 – Introductions

12

If You're Not Collaborating with Colleagues and Competitors on Cyber Threat Intelligence, Beware: The Bad Guys Are Way Ahead of You

Sherri Ramsay — Cybersecurity Consultant; Former Director of the U.S. National Security Agency / Central Security Service Threat Operations Center

I worked at the U.S. National Security Agency for 33 years, during the time when we first saw just how big a target the Department of Defense and the rest of the federal government was for hackers and bad actors all over the world. During those years, I learned firsthand about many of the problems those in private-sector leadership are now struggling with in their attempts to protect their digital domains.

And I learned about the value of sharing threat intelligence information when it came to protecting our networks and our data.

The other lesson I learned is one I want to emphasize throughout this chapter—an organization's success in cybersecurity depends as much on leadership as it does on technology. Maybe more.

Specifically, I learned that cybersecurity requires leadership—whether you're a CIO in a three-letter government agency or a CEO of a global conglomerate. And this leadership means having the confidence, the boldness, and, sometimes, the sheer audacity to share! Sharing tips, vulnerabilities, mitigations, and winning strategies with those outside your organization. Even with your competitors.

Why? Because it's what the bad guys are doing to us, every minute of every hour of every day.

Every day, our computers and networks are being attacked. It takes attackers only minutes to compromise a system, and most of the time, they are able to exfiltrate our data within days, sometimes hours. And when we realize what has happened, often much later and sometimes only when notified by an external party, such as law enforcement, we wonder what went wrong, whether it will happen to us again, and how we could have prevented it. We operate in independent stovepipes, defending ourselves as if each of us was on our own island. The bad guys, the attackers, watch us as we struggle to understand and characterize the attacks.

They watch us. And then they come at us again.

The attackers meet in the dark corners of the internet to share exploits, vulnerabilities, exploitation infrastructure, and

whatever other information might be helpful to those looking to attack our networks for nefarious purposes. To date, we have talked about information sharing, but we have not yet done nearly enough to dramatically move the needle in our favor.

If the bad guys are collaborating, why aren't the good guys? Why do we continue to live with this disadvantage? Are we waiting for a solution to fall in our laps?

How and Why Bad Actors Are Sharing Insights About Your Security

The harsh reality is that there is extensive collaboration among the cyber bad guys; there are few lone wolves. This extends across the entire spectrum of bad actors—nation-states, criminals, hacktivists, and terrorists. Even a single hacker is not really alone.

Why do they collaborate? Why do they share? The answer is simple. It saves them time and it saves them money. According to Etay Moor, Senior Strategist at IBM, "Information sharing is a given on the dark side of the net." That's a big reason the average cost of conducting an attack is decreasing and attacks are spreading across networks at a faster pace, year after year.

Much of the information the bad guys share is easily accessed without them doing anything special. For example, they simply use a search engine to locate spreadsheets with the word "password" in them to get the default password lists for numerous devices of interest.

Bad guys also exploit one of our biggest weaknesses: human error. Information is available on the internet that may have been posted by mistake or by someone who had no idea that the information would be useful for a nefarious purpose. And there is also a significant amount of information that has been stolen or compromised and then posted on legitimate websites, which often are created for the sole purpose of sharing stolen information with others.

There are forums created and used by the bad guys. Some have benign names like "security research forum." They promote these forums as legitimate entities, even displaying ads to cover costs or to actually make money. These forums are used to share all kinds of information that is helpful to the bad guys. They also provide anonymity for their users. This is teamwork.

The Dark Web, by design, provides anonymity for users and is facilitating a thriving underground for the bad guys. Here, everything that a person needs to break in to your networks is available for an astonishingly low cost. How low? Worms can be purchased as cheaply as $10, key loggers for $20, known ransomware for $30–$50. Furthermore, the entire exploitation/attack can now be easily outsourced, from the development of the malware to its distribution and even the conduct of the operations.

And these bad guys are coming after your networks and your data.

Why Organizations Don't Share This Information—and How It Impacts Cybersecurity

Throughout history, we have used strategic alliances to defeat our enemies and to solve our most pressing problems, from minimizing geopolitical conflict to stabilizing financial markets and tackling world hunger. Some say that the true measure of a great civilization is its ability to work together to solve difficult, seemingly intractable problems. Certainly, cybersecurity appears to meet this criterion.

But allying with others is in depressingly sharp contrast with how we are addressing cybersecurity today. Information about "near-misses" and successful attacks are closely guarded secrets. Orga-

nizations rarely share this critical information, collaborate on damage control, or provide early warning to other organizations that may be at risk. It's a losing strategy.

Why do we continue to live with this disadvantage? There are three reasons organizations have been hesitant to participate in meaningful information-sharing initiatives.

- Many of the sharing mechanisms today are associated with federal or state government, and enterprises are concerned that sharing information with the government will lead to increased regulation and oversight. Companies are concerned about the perception of being "in bed" with the government, which might affect their global market opportunities.
- In the private-sector, corporations feel that disclosure may prompt criminal or civil lawsuits. Remember all the legal brouhaha over the Y2K threat and companies' worries over legal exposure?
- Maybe the most important reason for not sharing is concern over market and reputational risk. Even a problem caused by a technical glitch or human error implies data or IT infrastructure problems or poor management. An actual attack just creates additional uncertainty.

Unfortunately, we are failing. Every new cybersecurity headline serves as a warning that no organization is immune from these attacks. Each new breach seems worse than the last. Everything, from our business communications to medical equipment to the cars we drive, is vulnerable. Fighting against network intrusions in disconnected silos and relying upon traditional enterprise security technologies and techniques has gone as far as it can go, and it is not good enough.

Breaking this cycle will require a fundamental shift in thinking. It will require leadership. Just as we evolved from the early days of perimeter defense to today's focus on intelligence, detection, and response, we must move from an individualistic model to one of collaborative "connective defense." We can only make true progress once we share our relevant information, pool our expertise, and connect our responses.

Or we'd better get ready to suffer the consequences.

Getting in Front of the Problem With a "Crowdsourced" Mindset

In building a collaborative connective-defense cybersecurity model, we can take a lesson from the concept of crowdsourcing.

Crowdsourcing, according to *Merriam-Webster,* is the practice of obtaining needed services, ideas, or content by soliciting contributions from a large group of people, especially from the online community. Crowdsourcing has certainly enhanced our travel by car. Not too long ago, we followed the directions provided to us by our GPS devices, unaware of road hazards, accidents, etc., along our routes. Now with crowdsourced information input into our GPS applications in real time, we are aware of these incidents and can take action to avoid them. In fact, the applications provide an alternative route. We are empowered as drivers because we have useful information and mitigations in real time.

Adopting a crowdsourced mindset is a great strategy for fortifying our collective cybersecurity defenses. Because cybersecurity is now everyone's problem, everyone can become part of the solution. We will need strong leadership to move in the direction of sharing relevant information and sharing it quickly.

With its long history as a prime target for cyber criminals and threats, the U.S.

government recognized early on that collaboration and information sharing can make a difference in cybersecurity.

In 1998 the federal government asked each critical infrastructure sector to establish an Information Sharing and Analysis Center (ISAC). These groups were created to help critical infrastructure owners and operators protect their facilities, personnel, and customers from cyber and physical security threats and other hazards. ISACs provide a central resource for gathering and sharing information on cyber threats and network defense best practices. They are a starting point for crowdsourcing a connective defense.

The Comprehensive National Cybersecurity Initiative (CNCI) was initiated in January 2008 by President George W. Bush, and was a significant policy development, especially for its time and the current understanding of the cybersecurity environment. CNCI proposed to establish a frontline of defense against immediate cyber threats by creating and enhancing shared situational awareness of network vulnerabilities, threats, and events. CNCI advocated for making cybersecurity more collaborative and efficient within the federal government; it did so by establishing more empowered cyber centers and extending that expertise to the entire governmental sector by enabling teamwork across state, local, and tribal governments. The initiative remains one of the strongest examples of dedicated government leadership achieving a whole-of-nation approach to tackling shared cybersecurity challenges.

A potentially big roadblock to promoting collaboration in the private sector—fear of running afoul of federal laws and regulations—was mitigated by the passage of The Cybersecurity Act of 2015. This important legislation encourages private organizations to voluntarily share cyber threat indicators and defensive measures without fear of legal liability, public exposure, or antitrust complications. The act not only provides protection for companies that share information with the federal government, but also for companies that exchange cyber incident information with each other, whether or not the government is involved. For CEOs and CISOs, the most significant benefit of this law is that it empowers members of the private sector to begin collaborating with each other on cyber incidents. The private sector can take advantage of this opportunity, redefine information sharing, and create a framework for collaboration that serves its needs.

There are many powerful examples of this new spirit of openness and sharing in the private sector. One demonstration of this is the Columbus Collaboratory, an Ohio-centered consortium of private-sector companies across different industries—from healthcare and financial services to energy and consumer goods. Columbus Collaboratory is committed to using sophisticated analytics, artificial intelligence, and machine learning on a collaborative basis to identify and overcome cybersecurity threats.

Another illustration of how bold leaders have put aside the emotional turmoil of working with competitors is the Cyber Threat Alliance. Look at their roster, and you'll immediately see the participants are often direct competitors. But however fiercely they may compete in the market, all their CEOs ultimately understand the value in jointly being part of the solution.

TruSTAR, the organization where I act as an advisor, is another great example of how adopting a collaborative, crowdsourced model really pays dividends. At TruSTAR, a threat intelligence platform helps organizations—many of which are direct competitors—share information about threats and solutions in order to overcome the organized malevolence promoted by cybercriminals.

I believe it is this crowdsourcing approach to cybersecurity that is a model not only of what can work, but also of what has to happen with far more frequency if we are to beat the bad guys and keep our networks secure and our data safe. And that will take the leadership, confidence, and boldness of those business executives and board members reading this book.

We cannot afford to do any less.

Building a Connective Defense to Share Cybersecurity Information

These efforts demonstrate the benefits of working as a team to defend ourselves against the growing number of attacks against both government and the private sector. This cannot be a feel-good exercise to make us feel warm and fuzzy about teamwork. This is a pragmatic, hard-headed, enlightened approach, accomplished by pooling resources and getting better insight into threats and defenses.

If we don't do this, adversaries will always have the upper hand, and we will continue to endlessly spend money, but never be able to win the battle.

Unfortunately, mention the word "sharing" when it comes to cybersecurity, and many corporate leaders start twitching. But we must take the emotion out of this issue by appreciating the many benefits of crowdsourcing to create a "connective defense."

What are the requirements of connective defense?

- **It must preserve privacy.** Collaboration on cybersecurity should not cost participants the trust of their clients.
- **Participation in it must deliver real value to the individual contributors.** It is not sufficient to create an exchange where sharing is one-directional. Members must be incentivized to participate in a timely exchange of actionable data.
- **The member connections must be fluid.** We cannot limit ourselves by allowing existing personal or industry relationships to define our sharing paradigm. We need to have dynamic connections, driven by the targets of an attack campaign and composed of those in the network who want to contribute to timely active defense.
- **The system has to be transparent and trustworthy.** There cannot be any doubt about the motivations of contributors or the operators of the system itself. There must be transparency around how members are vetted and admitted and how the data is used and protected.

Keep in mind another important issue: What information is being shared? When we talk about sharing intelligence, some ill-informed people may reflexively interpret that as proprietary and private information. But the information that needs to be shared isn't personally identifiable information, health insurance data, context-specific content, or intellectual property. It is information that will identify an attacker in the network and mitigate the attack.

This connective defense by enterprises working together will help all of us detect, investigate, and mitigate emerging threats far more quickly than we ever could working alone.

In doing so, we are taking a page—in fact, the most strategic page—of the cyber attackers' go-to-market plan. We can finally close the gap with our adversaries and change the discussion from embarrassing failures to inspiring successes.

Isn't it about time?

Summary

Let me be very clear about this: The old model for cybersecurity no longer works. It's broken, and it can't be fixed. We must

work together like the bad guys do—only better.

Keeping an incident quiet or sharing only among a few friends potentially exposes others to the same attack, which is a fundamental breach of fiduciary responsibility, whether you're a CEO, board member, CISO, or government official. A true exchange—a connective defense—will give our organizations the best opportunity not only to defend our digital infrastructure against attacks, but it also will enable others to understand the threat landscape and help all of us.

Sharing is best if it is voluntary, not under a government-reporting requirement. An exchange will add value and will enable real-time correlation and mitigation to all participants. Let's learn from government agencies' experience in plotting our paths; those of us who worked in the government's cyber centers know that this collaboration model can and does work.

The technology is advancing, the legal climate is changing, and the opportunity for us, the good guys, to gain the higher ground is here. The lack of effective collaboration among organizations in both the public and private sectors is our Achilles' heel. The bad guys will continue to exploit it as long as we let them.

Let's fix this problem!

13

Partnering to Secure a New Form of Critical Infrastructure

Ryan Gillis — Vice President for Cybersecurity Strategy and Global Policy, Palo Alto Networks

Sean Morgan — Director of Cybersecurity Policy and Partnerships, Palo Alto Networks

The COVID-19 pandemic has wreaked havoc on communities and economies around the world. The loss of lives is heartbreaking, and the disruptions have been disorienting. Cybersecurity attacks have surged too, as bad actors, rogue nations, and cyber criminals have exploited the situation to unleash new attacks on governments, businesses and individuals.

Just a month after the pandemic reared its head, the World Health Organization sent out an ominous warning: Cyberattacks against its staff working on its response to the novel coronavirus spiked five-fold in the form of credentials theft and email spoofing.[1] In July 2020, a joint advisory from the United States, United Kingdom and Canada identified that foreign government actors were conducting a coordinated campaign to target the intellectual property of coronavirus vaccine developers.[2] On a more personal level, cyber risks have impacted many individuals as people are forced to think about the security of their work from home environments, or their children's distance learning platforms.

What we do about these new and insidious attacks matters a great deal. In order to address these new threats fully and efficiently, organizational leaders should embrace two key concepts: A more committed form of public-private cybersecurity collaboration, and an acknowledgement of new risks associated with rapidly evolving definitions of what constitutes critical infrastructure.

A More Robust Commitment to Cybersecurity Collaboration

Every day, our team works to find new and creative ways to foster and contribute to partnerships between the public and private-sectors in order to combat escalating cybersecurity attacks. I know my colleagues and counterparts around the world are doing the same. Creating meaningful partnerships that tangibly improve security outcomes is hard work, but the stakes have never been higher.

We are in constant exchange with global government agencies to work together in identifying, preventing, and remediating threats. Even before the pandemic, the growing scale and sever-

ity of cyber risks drove the public and private-sectors together to prevent and respond to the bad guys.

Around the globe, this commitment to partnership has been especially important in protecting our critical infrastructure. In the United States, for example, critical infrastructure refers to the 16 sectors, as defined by the U.S. Department of Homeland Security (DHS), that provides the essential services that underpin American society. (As we'll cover shortly in this chapter, the shifting definition of "critical infrastructure" adds a new wrinkle for all of us to plan for, even when the pandemic's advance is eventually slowed and, hopefully, halted.)

Now, it's time for all of us to step up our game in confronting these new cyber risks head-on and eradicate threats before they cause even more disruption to our already disrupted new reality. To do that, we must embrace a comprehensive public-private sector collaborative framework, built upon three major pillars: assessing cross-sector risk to critical functions, expanding threat sharing and prevention, and fostering consensus standards for securing our increasingly distributed remote workforces.

Assessing Cross-Sector Risk to Critical Functions

While it's obvious to identify sectors such as energy, communications, healthcare, and transportation as critical infrastructure, COVID has taught us that we have to broaden our field of vision on what constitutes "critical" and "essential" in times of crisis. Government organizations across the world have rethought what constitutes an essential function or sector, and your organizational cybersecurity framework must reflect that.

In this way, COVID largely validated a policy shift that was already underway by government entities like the DHS. Instead of conceiving of critical infrastructure risk as siloed by sector, DHS has introduced the concept of National Critical Functions (NCF)—a new framework that recognizes the highly complex, cross-sector dependencies of modern supply chains.

During COVID, one key national objective was to keep food supply chains operational, in furtherance of the National Critical Functions to "Produce and Provide Agricultural/Food Products, and Services." Executing against this objective required extensive coordination across at least food and agriculture, water, manufacturing, chemical, and transportation sectors. Even small businesses several levels downstream of the national food supply chain were deemed "essential," and quickly realized that any disruption to their operations, including cyber-enabled disruptions, could have a cascading impact on national public safety and security.

Leaders would be wise to assess their own organizational risk with this strategic-level view, aligning people, process and technology against the risks most critical to their organization, or even a broader national security or public safety mission.

Threat Sharing and Prevention

When it comes to understanding the full scope of global cyber threats, no single entity is capable of achieving sufficient visibility. It's not a new principle, but the stakes of the COVID crisis have sharpened the importance of threat sharing collaboration in minimizing disruptions to our collective international response.

Governments bring a unique perspective, with a vantage point to identify the critical sectors, functions, and organization most fundamental to continuity of the national response. Industry, especially cybersecurity companies, can use their cross-sector visibility of global networks to identify trends and evolution of adversary tactics.

In order to properly understand and prioritize cyber risk, organizations need to step outside their own boundaries, biases, and processes to seek out help wherever it comes from. In healthcare, manufacturing, financial services, and other essential sectors, no one organization can possibly know enough about the full breadth of cyberthreats and solutions. They must be prepared to partner with governments, national cyber research centers, cybersecurity technology, and services providers, suppliers, customers, and more to access and understand the widest array of information. And yes, that includes collaboration with organizations that you would consider to be your competition for the good of the broader security ecosystem.

You need more information, better information, and faster information than ever, above, and beyond the malware, ransomware, and zero-day attacks you've run into in the past. On top of that, artificial intelligence, and machine learning technologies can help your organization parse greater numbers and more diverse types of threats and actually translate that information into automated defensive action.

Scaling a Secure Remote Workforce

Just three years ago, U.S. Census data indicated that 5% of the U.S. workforce worked from home. Now, research indicates that more than 40% of the U.S. workforce is working full-time from home.[3] Giant multinational organizations such as Google have made it clear that they expect a larger-than-ever portion of their employees to work from home at least until the middle of 2021.[4] Do you think organizations are going to run counter to this trend? Talk about swimming upstream.

Government and enterprise leaders would be wise to not view this shift as a fleeting trend, and align their cybersecurity priorities, policies, and practices with this new reality. In many ways, COVID merely accelerated network transformation trends that were already underway and will likely continue in some form long after the pandemic recedes. It is now simply a strategic imperative to extend consistent security capabilities you deploy within your internal HQ network to all environments, regardless of where an employee connects from.

Palo Alto Networks saw this happening with our own workforce, so we partnered with governments and multinational entities like the World Economic Forum to share cybersecurity best practices and recommendations for securing remote workforces. In particular, you need to prepare for the possibility—and maybe the inevitability—that your remote workforce will continue to grow. So your cybersecurity infrastructure must evolve in anticipation of this trend. Emerging software-defined and cloud-delivered security capabilities can help organizations rapidly scale and secure increasingly distributed workforces so that their devices, applications and data—your organization's data—are secure.

Reimagining and Redefining Critical Infrastructure

Earlier in this chapter, I said that our lives and livelihoods depend upon getting COVID-related cyber risks under control. That was not hyperbole. Foreign nations and cyber criminals are attempting to infiltrate our efforts to develop, test, and bring to market a safe and reliable vaccine. You can imagine what would happen if cyber criminals undermined those efforts. Think of all the smart healthcare systems driven by the Internet of Things, from dialysis machines to heart monitors. Healthcare, no doubt, is critical infrastructure.

But it's not just the healthcare industry that is at risk. If we let our imaginations run freely, we can understand that,

in the COVID era, cows, and corn have become essential parts of critical infrastructure. Think about computer-controlled irrigation systems that water acres and acres of corn in farmlands around the world. If those irrigation systems are compromised it could impact corn harvests, which are essential for cows' diets. If cows' diets are impacted by a lack of corn due to hacked irrigation systems, food supplies will be disrupted. During the early weeks of the pandemic, also saw a significant constraint in beef and chicken supplies in processing plants, threatening to dislocate food supplies in our homes, grocery stores and restaurants.

COVID has also brought many of the complex security challenges enterprise leaders face to a more easily discernible, household-level. When municipalities closed down in-person classes, in favor of distance learning, many parents had to figure out who would stay home and oversee their children's online learning, and how it would impact their ability to do their own jobs. Many working parents quickly pivoted to work from home collaborative platforms, but cybersecurity risks quickly emerged. Now, not only were worker productivity and sensitive data impacted, but children's identities were at risk of exposure.

We must learn the lessons presented by this pandemic to find smarter, more innovative and more robust ways to fortify our businesses, our communities and our homes against cyber risks.

Next Steps for Business Leaders and Board Members

For C-suite executives, board members and other business leaders, it's time to take action. Even when the current pandemic is brought under control, most scientists, doctors and epidemiologists fully expect other bacterial and viral threats to emerge. While public health issues are undoubtedly paramount, cybersecurity challenges will be near the top of the list of problems to solve to ensure continuity of the nation's operational process.

Here are a few things executives and board members should understand and be prepared to do:

- Take a long hard look at your organization's risk profile, and insist upon full transparency and brutal honesty. Together with your CISO, CIO, CTO and other technical leaders, you must take a full inventory of all cyber risks, assess the likelihood of those risks occurring and calculate the economic, operational and brand impacts of cyberattacks. Risk calculation must become more scientific and more ingrained in your organization's DNA.
- Understand, adopt and "live" the best practices identified in this chapter, as well as those that continue to emerge. This isn't just to ensure that you do all the big things right, but also to avoid having to reinvent the wheel when it comes to putting in place the right cybersecurity framework. Learn from those who have come before you and are doing it right.
- Be committed to a full and open engagement with public and private-sector organizations to more rapidly and fully identify risks and solutions. Now is not the time to become secretive and proprietary, at least not when it comes to cybersecurity.
- Now, more than ever, leadership matters. Whether you're talking about heads of government, CEOs, health and science experts, cybersecurity executives or community leaders, the actions (or inactions) of those in charge have far-reaching consequences. Collaboration is a hallmark of leadership, and in times when sys-

tems and processes are under great stress, you need more collaboration, not less.

I hope that many of you have already put in place smart, efficient and comprehensive plans for managing cybersecurity risks in our new reality. As you go forward, I encourage you to remember one of the most important lessons learned here in the United States in the aftermath of the September 11, 2001; the 9/11 Commission's conclusion that the tragedy was the result of a "failure of imagination."[5] Unfortunately, we learned the hard way what a determined enemy could do to us if we did not think of every conceivable threat—even those that may have seemed so unlikely as to be discarded.

When it comes to cybersecurity, let's stay vigilant. And we can all use greater understanding of, and commitment to, ecosystem-wide collaboration. Don't wait for the next crisis to find out.

---

1 "WHO report fivefold increase in cyber attacks, urges vigilance," World Health Organization, April 2020.

2 "Advisory: APT29 targets COVID vaccine development," July 2020.

3 "Stanford research provides a snapshot of a new working-from-home economy," Stanford University, June 2020.

4 "Google will continue to let employees work from home through the end of June 2021," TechCrunch, June 2020.

5 "Final Report of the National Commission on Terrorist Attacks Upon the United States," 9/11 Commission, July 2004.

Best Practices in Driving Change

14

The Value of Being Prepared For Anything

Mario Chiock — Schlumberger Fellow and Former Chief Information Security Officer Emeritus, Schlumberger

Over the past several years our company, Schlumberger, has undertaken a massive cybersecurity modernization initiative. As part of our plan we:

- Built a next generation Cyber Security Operations Center (CSOC) in Houston, Texas.
- Embraced the cloud as a flexible, fast, cost-efficient, and reliable cybersecurity delivery model.
- Moved towards secure network transformation with software-defined networks (SD-WAN), enhanced data analytics, Zero Trust, and more.
- Deployed a distributed data lake to ensure we could deliver security protections to our employees wherever they are, whenever they need it.
- Created flexible working conditions for our cybersecurity teams, so they could "follow the sun," thus eliminating night shifts and encouraging – at times requiring – that our people work from home.
- Empowered other workers to work from home and provided them with tools, processes, controls, and—importantly—training to be productive and safe.

We took these steps as part of a corporate-driven, strategic imperative to make cybersecurity a competitive differentiator for Schlumberger, in our digital transformation. We did not take these measures with the expectation that in the spring of 2020 there would be a global pandemic that would put all of our efforts to the test immediately.

Yet, that is precisely what happened. When our business leaders made the decision to have our employees work from home in March 2020, our cybersecurity teams were prepared. Over the approximate course of a weekend, we went from about 25,000 simultaneous remote users to about 80,000, including employees and contractors.

The transition was smooth. There were no business interruptions as a result of scaling up our remote workforce, and we maintained business continuity at all times with our customers as they, too, scaled up remote work.

The biggest issues among our workers had nothing to do with cybersecurity or business operations. In fact, the kinds of complaints we heard most often had to do with the comfort of desks, chairs, and the quality of monitors and headsets.

I share this not to boast—although we are admittedly quite proud that our CSOC

was named as the Information Security Executive (ISE) Central Project Award Winner for 2020.

Rather, my goal is to pass on some of the key lessons learned in the process:

- About the importance of business and technology collaboration.
- Being open to new ideas such as next generation CSOC and secure network transformation.
- Setting cybersecurity as a company-wide agenda.
- Critically, working with all of your teams to stress, as I always emphasize, that ***everyone*** is responsible for cybersecurity.

Business and Tech Collaboration

At Schlumberger cybersecurity is a corporate-wide effort. Over the years our board has elevated cybersecurity to a top five priority. This happened because of strong communication and collaboration between the business and technical sides. Our board and executive teams were open to ideas from the tech team and we, on the tech side, focused on communicating a risk-based approach to cybersecurity.

Our strategy was to present both the inherent risk and residual risk to the business side so we could create a strategy based on the risk tolerance of leadership. The more specific the questions you ask, the better: What are our blind spots? Why do we have excessive privilege? How can we minimize human error?

Once you understand risk tolerance, you can build a risk-based strategy with the appropriate mitigation controls and technology investments. For example, we focused on technology visibility across the entire organization in order to identify and eliminate blind spots. We honed in on excess privilege as well as awareness, training, and basic cybersecurity hygiene to mitigate the impact of human error.

In doing so, we didn't compromise on our core corporate goals, nor did we break our cybersecurity budget. Mobile-first was a critical aspect of our digital transformation strategy because management wanted our people to work from anywhere and still have safe access to all of the resources they needed. Our responsibility was to enable and secure that, not to put up obstacles.

We also created a risk-based dashboard, where we showed the board that you don't have to spend a lot of money to improve your risk posture. On the contrary; with our dashboard, we were able to show that we could improve our return on investment based on our plan for risk management and mitigation.

Innovate with Expertise

Technology is key to any successful risk-based cybersecurity strategy. There were many elements involved in our strategy to invest in new technologies, but I will focus on two that were vital in enabling us to implement our company-wide mobile-first strategy, and consequently scaling quickly and easily in response to COVID-19.

Next Generation CSOC

The main impetus for building the next generation CSOC was that our previous solution would not scale. It seemed as if the more people we put on it, the more attacks we would get. And it didn't matter how many people we hired; we could not handle 100% of the work. So we looked at the key issues, starting with our people. Even with extensive automation, the CSOC is only as good as your people.

CSOC analysts are a hot commodity, given the industry-wide skills shortage. If people aren't happy, they can easily just quit and move on to a new job. We realized that investing in automation would help our teams, rather than

replace them. One of our major goals was to retain our people and keep them happy. With our investment in a next generation CSOC, we have been able to:

- **Create flexible hours** and enable our people to work regularly from home as part of their normal day-to-day routine. This was in place before COVID made work from home a necessity, so our teams were already used to it.
- **Eliminate the night shift** for our people everywhere. In addition to our CSOC in Houston, we have another CSOC in Kuala Lumpur, Malaysia, so we can follow the sun. Each CSOC has just two shifts, early and late, so no one has to work the graveyard shift.
- **Leverage extensive automation and next generation tools.** Automation enabled us to increase our capacity by a factor of eight to ten times. Our people tell us one of the reasons they stay is because they are using tools that make them more effective and make their jobs easier.
- **Reduce the risk landscape** by using intelligence and machine learning to prioritize. We have been able to build algorithms to make us aware of the risks that are the highest impact and importance.

Secure Network Transformation

Another area of innovation for us was secure network transformation, including the shift to cloud for cybersecurity and the growing use of SD-WAN to support a rapidly growing "edge" environment. SD-WAN is an architectural model in which the network hardware and software are separated, which means the network can be managed centrally and from the cloud.

This is especially valuable in supporting field operations, because we can make adjustments from a central location, rather than locally. This enables us to deliver performance and bandwidth where needed, as well as the appropriate security protections, without the need for on-site network management software or IT personnel. With SD-WAN you can simplify management and scalability of network and security services, with centralized control of critical capabilities such as Zero Trust, identity management, authentication, authorization, and least-privilege access.

SD-WAN is a part of a broader set of initiatives characterized as "secure access service edge" or SASE. The concept is that the enterprise perimeter is no longer a location but a set of dynamic edge capabilities delivered via the cloud.

As you can see, moving security to the cloud is a critical aspect of our secure network transformation, as well as our next generation CSOC. Many of the security tools we use in the CSOC are cloud native, which makes it simpler for our teams to have access to current versions, as well as the most up-to-date threat intelligence. This was extremely beneficial when we had to rapidly scale and secure remote workers in response to COVID.

With the cloud, we have been able to build a distributed data lake, making it simpler, more efficient, and more cost-effective to have distributed security data delivered where it is needed, whenever it is needed. Cloud and automation are also critical in managing costs. Schlumberger has a lot of resources, but we don't necessarily spend more money or have more people than other companies when it comes to cybersecurity. There are companies half of our size with twice the staff and twice the expenditure.

Preparation, Training and Awareness

I've said it before, and I'll say it again: Everyone is responsible for cybersecurity. If you adopt that as a mantra, it will guide your actions and decision-making pro-

cesses when it comes to the critical areas of preparation, training, and awareness.

Here's an example of what I mean. Very early in the pandemic, before there was even thought of a companywide work from home edict, we sent the entire CSOC team home for a week to work. This was part of training and preparation. Members of the CSOC team were already working at home one day a week. That was a regular part of their training.

Because of the capabilities of our next generation CSOC, as well as the company's mobile-first initiative, and their regular experience working from anywhere, we were confident they could do the job remotely. And they did. So, when they were directed to work from home full time as a matter of corporate policy, they were fully prepared.

As for our employees, cybersecurity is part of our corporate culture. I consider every employee to be a cybersecurity sensor. We ask key people to take a cybersecurity test every year; if you don't pass this test, then you have limited privileges. We make sure that all of our people are trained in and aware of basic cyber hygiene.

Our processes also have built-in security protections. For example, all of our people at all locations connect to our network via a virtual private network. The VPN is always on. They can disconnect temporarily, but they can only do certain tasks. Constant communications are built into our processes; when working from home we organize virtual get-togethers to update all employees—and to listen to them.

Perhaps all of this attention to preparedness is a factor of having one of our headquarters in Houston; with the ever-present threat of hurricanes here, we have learned a lot about the benefits of being prepared.

Be Ready for the Unexpected

When we began implementing our cybersecurity modernization strategy several years ago, we didn't know there would be an event like COVID on the horizon. But by focusing on our people, processes, and technologies, we were prepared for virtually anything.

The investments we made in technologies such as next generation CSOC, cloud, and secure network transformation; the commitment to our people through training, awareness, and flexible work hours; the processes we installed to enable mobile-first and digital transformation, such as mandatory VPN—all of this allowed us to scale from 25,000 to 80,000 remote workers in just a few days, with no disruption of business operations.

As for the future, we don't know what it holds, particularly when it comes to the ever-changing world of cybersecurity and navigating the Digital Age. But we do know this: whatever happens, we are prepared to the best of our abilities.

7 TIPS FOR SECURING REMOTE WORK

1. Make remote working part of the business strategy.
2. Have policies and procedures in place detailing when and how working from home can be done securely.
3. Train the staff – cyber awareness, training, and preparation should be ongoing activities built into the corporate culture.
4. Protect remote access to business data, business assets, and business services/infrastructure.
5. Segment your work and implement Zero Trust.
6. Have a data-centric security strategy by implementing digital rights management and tokenization.
7. Teach your people about best practices in cyber hygiene and ensure that they comply with cybersecurity policies when working remotely.

15

Reacting to Cyber Attacks Doesn't Work: Why You Need a Proactive Approach

Dr. Yang Zhoulong — Vice President and Board Director, Yunda Group

The world of cybersecurity has never been more challenging, more complex, and more important than it is today. Hackers are smarter, better organized, and more committed than ever, and the attack vectors they seek to exploit are far more numerous than just a few years ago.

The futures of companies, industries, communities, and people depend upon smart cybersecurity defenses. But it is clear that we all must take a step back, rethink what we have been doing, and consider a new approach to cybersecurity to thwart the hackers who threaten us economically and operationally.

That approach needs to be built upon the core concept using intelligence to secure our networks, data, identities, and devices. But, as I will explain shortly, simply adding intelligence to our cybersecurity frameworks is not enough.

We must build and operate intelligent network security that protects our assets before, during, and after attacks. Because of the resourcefulness and persistence of our adversaries, it is not enough to use intelligence to detect threats before they happen, to prevent their intrusion during the attack, or to remediate problems after the attack.

Far too often, our organizations remain stuck in "react" mode. We scramble to lock out intruders after we detect them inside our digital walls, or when we clean up the havoc that hackers create after they have exfiltrated our data. In order to implement intelligent network security effectively, we must use that intelligence more proactively.

Three Elements of Intelligent Network Security

Computer networks have become just as essential as electrical power to all organizations, because they carry our most precious corporate asset: Data. Fortunately, our networks have become faster, more reliable, and more resilient than ever. However, they are often the number-one target of hackers looking to view, steal, manipulate, or compromise our data.

Business leaders have understandably stayed away from the "plumbing" issues of computer networks, but ensuring that networks are secure is now of prime concern to C-suite executives, and the board. That's due in part to compliance, legal issues, and data governance, of course. But network security is as much a business issue as it is a technical one, in large

part because of the often proprietary and competitively differentiated nature of the data that traffics the network.

Traditional network security was effective when hacking methods were less advanced than they are today. Now, hiring more security engineers or buying the right security tools—while certainly important—is no longer sufficient. We must adopt a mindset of intelligent network security using artificial intelligence, machine learning, deep learning, and other points of intelligence that augment human intelligence.

There are three major elements of intelligent network security:

- **Real-time detection.** Reacting to incursions puts our organizations in a catch-up position. Instead, intelligent network security must be utilized to close the gap between detection and preventative action before something takes place.
- **Collaboration.** This must take place on many levels—among security checkpoints, throughout internal business units, and with third parties such as partners, suppliers, industry groups, and law enforcement.
- **Automation.** The days of relying on growing numbers of security engineers manually monitoring network behavior and data movement are over. A premium must be placed on automated steps that learn from experienced, savvy humans, and can extrapolate extensive data points into a single set of actions to cut off threats before they make their way into our systems.

Only when we make intelligence the foundation of cybersecurity defense frameworks will we be able to counter the enemy's moves before, during, and after they attack us.

Why Cybersecurity Needs to be Intelligent

Obviously, security professionals have been aware for some time that the nature, magnitude, and impact of expanding threat vectors is becoming more and more problematic. The difference now is that business executives and board members are just as aware, and are just as concerned as the security operations team, about dealing with these problems proactively.

We've seen the clever, even at times brilliant, nature of hackers. They are resourceful, persistent, and collaborative to the point where they share "tips and tricks" about how to get into our systems. And they are in the forefront of using AI and machine learning algorithms to understand our weaknesses, and to plot their ideal points of attack.

This never-ending game of "cat-and-mouse" is going to be with us for quite some time, as hackers continue to evolve their methods. We need a way to actually predict or forecast what the hackers will do, when they will do it, how they will do it, and where they will attack.

It's time for us to become more intelligent than the hackers. Even if organizations could fill every one of their open job spots for security professionals—which we can't—we would still be highly dependent upon manual monitoring, detection and remediation. While our people are very smart and highly committed to our cyber defenses, we must use digital intelligence tools to act as a lever against these threats.

Our cybersecurity frameworks must be built upon AI algorithms at the platform level, not just within a few point products. Intelligent network security is our best bet to spot problems before they occur, defend against them as they are occurring, and mitigate their impact after they take place.

What We Learned and What We Did

The Yunda Group is a leading company that provides express delivery services. Our logistics businesses, combined with our cloud-based virtual stores, and other commercial enterprises, have served diverse needs of businesses and consumers for many years.

Of course, we have hardly been immune to the threats of hackers, and we believe we have been very diligent in securing our digital assets, such as our intellectual property, customer data and employee identities. As we detected the changing nature and frequency of cyberattacks, our management team committed to an accelerated time frame to modernize our defenses. At the heart of this effort was making our network security more intelligent.

We did a lot of the things any responsible organization would do, such as tightening up our security policies, hiring a lot of smart security professionals who understood both the business and technical issues, and assembling an array of world-class cybersecurity tools. Many of those tools leveraged AI and machine learning algorithms to address issues before, during, and after attacks. But we knew we had to do even more.

First, we wanted to take advantage of the power of collaboration in order to fortify our potential stress points. Fortunately, we benefit from a wide range of business partnerships, including a tight strategic relationship with Alibaba for e-commerce and as an equity partner. Those and other partnerships helped us build a culture and ecosystem of collaboration that allowed us access to more knowledge, insight into threats, and defenses, in the rapidly changing cybersecurity landscape. We also spoke to colleagues, and even competitors, at industry events to share our respective experiences about security incidents.

Second, we leveraged the relationships we already had in place with local and national law enforcement. These agencies have become increasingly adept at spotting potential cyberattacks and have the benefit of aggregating information from many different sources, including from other law enforcement bodies, private-sector companies, and their own intelligent network security.

Third, we took advantage of our long-standing relationships with leading technology vendors (including Palo Alto Networks), not just for their excellent technology, but also for the invaluable insights they have developed in using their own intelligent network security.

We also recognized that the cloud was a vital and strategic part of our cyber defense, and that it also needed to come under the intelligent network security umbrella. Yunda built a digital "middle desk" to accelerate our digital transformation efforts, and our cloud platform was the foundation of that middle desk. However, cloud brings new challenges to organizations, especially relating to cybersecurity. Many attackers are leveraging the cloud as the console for launching cyberattacks. So we put in place a hybrid solution that leverages the utility and efficiency of public cloud, with the added security and control of a private cloud.

The Always Evolving Security Operations Center

I do not know how many organizations see their security operations center (SOC) as a strategic asset, but we certainly do. We have always sought to constantly improve our SOC, based on new experiences and new learnings, much of which is fed by the increasing digital intelligence built into our SOC itself.

We see the modernized SOC having four critical components:

- **Data management.** Today's SOC must account for massive growth in both structured and unstructured data. In fact, it often is this huge amount of unstructured data that represents the richest targets for hackers. Your SOC must make data management a priority, or your organization will be deluged by data overload and escalating alerts that will eat up all your SOC engineers' time and effort.
- **Technology.** The underlying technical foundation remains vitally important at both the individual tools level and at the intelligent platform level.
- **Operations.** The SOC must operationalize cyber defense before, during, and after incidents, and it must do it faster and more efficiently than ever.
- **Governance.** This is an element of a SOC that many organizations tend to neglect. In fact, it is vitally important, and it must involve top leadership on everything from service-level agreements, incident response, internal and external communications, and process management.

An important aspect to making your SOC a vital part of your overall business success is to realize that the SOC must become more automated, more intelligent, and less dependent on manual processes. The much-discussed autonomous SOC depends heavily on having the right operational processes in place for both the near and long term. It must also be planned, deployed, and managed with key principles in mind, including flexibility, responsiveness, analytics, and data visualization. There are great tools available for building and running an autonomous SOC, and you can find very smart people to provide the human intelligence from which computers can learn, but having the right processes is mandatory.

The Essential Role of Business Leadership

No discussion of intelligent network security would be complete without talking about the essential role of business leaders that make daily, monthly, quarterly, annual, and longer-term decisions about business operations. As I mentioned earlier, business leaders must be intimately familiar with, and involved in, cybersecurity because of its impact on the business.

Top leadership engagement is very important, not just for pivoting to an intelligent network security model or building an autonomous SOC, but for the entire cybersecurity framework. Obviously, there are regulatory and legal implications to cybersecurity breaches that directly involve business leaders, and board members. This is particularly important because there are many other forms of security threats that businesses must consider in addition to network security. These centers of risk include data security, identity authentication, access control, physical device proliferation, mobility-centric workflows, the Internet of Things, and much more.

These add substantial complexity and impact to cybersecurity risks. Many of the principles of intelligent network security—AI and machine learning algorithms, automation, collaboration, and more—apply to these other centers of risk. Those risks also carry implications that go far beyond the financial and regulatory impact of data breaches, such as customer confidence and user experience.

The good news is that when an organization commits to a framework for intelligent network security, it is a short journey to building a comprehensive intelligent cybersecurity defense from the data center to the edge to the cloud. And this cannot be done solely by the

technology leadership; it must have the support, engagement, and active participation by the business leadership.

This certainly includes making important decisions on the levels of investment—in technology tools, services, personnel, and facilities—to defend the enterprise. Because the impact of cybersecurity breaches is greater than ever, those financial investment decisions carry greater weight, and are necessarily more complex and multi-dimensional. After all, when an incident occurs, the intangible costs often are even greater than the tangible ones.

Intelligent network security has the potential to improve the long-term sustainability and viability of the entire organization by dealing with cyber risk before, during, and after an event. But it can only be truly effective when it is viewed through the broader lens of business operations instead of through the traditionally narrow lens of the technologist.

In order to get the most from intelligent network security, organizations should:

- Visualize all assets and security vulnerabilities before the attack, in order to guarantee the effectiveness of various risk defenses.
- Analyze the entire attack chain during the attack, to facilitate a speedy and effective response.
- Review and summarize the process and impact after the attack to determine appropriate next steps, such as continuous automated and intelligent monitoring.

There is no magic wand we can wave in order to ensure full cybersecurity at all times. But that doesn't mean we shouldn't find new and more efficient ways to protect our most valuable digital assets: Intelligent network security is a must for any organization in today's rapidly changing threat landscape.

16

The Path to a Successful Cloud Transformation

Mike Towers — Chief Information Security Officer, Takeda Pharmaceuticals International

I first became a Chief Information Security Officer (CISO) in late 2008. Almost immediately, I began to ruffle feathers and raise eyebrows because I was a strong advocate that the cloud was the direction in which we all needed to move. My reasoning was that security in the cloud was more advanced, reliable, and resilient than anything we could do internally. The cloud, even at that time, offered the best way to collaborate safely.

Today, more than a decade later, in the midst of a global pandemic that has put enormous pressure on organizations of all types and sizes, I believe more than ever that the cloud is still the best way to go. In fact, I would argue that there are maybe 10 companies in the world that can secure and run their data centers as well as the large hyperscale cloud providers such as Amazon Web Services, Google, and Microsoft.

In many organizations, the skills and resources necessary to empower digital transformation and run IT and security on-premises are not aligned with targeted business outcomes. For example, in the pharmaceutical industry, we are building new channels for direct digital engagement with healthcare professionals and patients, yet must operate within rapidly evolving data privacy and regulatory parameters. Companies that try this with do-it-yourself approaches at scale are hard-pressed to match the capabilities of the cloud providers. A classic example is encryption-at-rest, which is a constant data center frustration. Yet, cloud providers have shown that they have the scale, platform, and resources to do it, and do it well.

The cloud is no longer a choice—it's a destination we have to get to. The question is not whether to embrace the cloud, but how can business and technology leaders choose the right path and timeline for their organizations.

Be Aware of the Pitfalls

Before you can discover the best route for your organization, you should be aware of some of the pitfalls that can delay you, or worse, stop you in your tracks completely. From the CISO's perspective, perhaps the biggest challenge is accepting the fact that you will not have direct control of your data and applications at all times.

Cloud is a shared responsibility model, meaning that the cloud provider is responsible for securing and managing the portion under its control; typically the

infrastructure, operating systems, virtualization layer, and security—virtual and physical—in which the service operates. Your organization, as a customer, is responsible for your operating systems and applications, including updates and security patches, as well as configuring firewalls, networks, identity, and other aspects of cloud access management.

In my experience, putting the stewardship of data in the hands of someone else is often the toughest pill to swallow for the CISO. However, it is important to remember that the hyperscale cloud providers are probably light years ahead of your organization in understanding and addressing the challenges of modern cybersecurity. Plus, their business models require that they stay ahead of the curve and embrace innovation as soon as it is available. They have far more experience, knowledge, skills, and people to devote to cybersecurity than all but the very largest of enterprise organizations. Rather than adding risk by moving some aspects of your security and IT operations to the cloud, you will actually reduce risk.

Once you overcome any trepidations about losing control, you will likely have a few more pitfalls to avoid before you can fully embrace the cloud. These may include:

- **Compliance and regulatory challenges:** Most regulators have built their models and inspection processes assuming that IT is still on premises. They are still learning the cloud and sometimes don't know what to look for. They want to see your ability to demonstrate control, but because of new models of application development, automation, and other factors, they are re-learning how to regulate in the cloud.
- **Skills:** Many of the skills that your people have developed internally will not be sufficient when moving to the cloud. They will not be able to leverage the full benefits of the cloud because they are not aware of or accustomed to what those benefits are and how they can be used by your organization. In many cases, it's like asking people to drive a Ferrari when the only experience they have is driving a minivan.
- **The financial model:** One of the benefits often touted by cloud suppliers is that cloud enables organizations to move from a Capex to an Opex model. However, most business decision-makers and CFOs are accustomed to Capex for IT; you spend the money up-front and then your ongoing costs go down. With the cloud, you pay for usage and you continue paying. In my experience, business leadership struggles with the idea of paying for IT every month.

Security Is About Trust

The most important advice I can share with my fellow CISOs is that we must all challenge ourselves to do a better job of thinking about the business impact of our decisions. For a long time, we've been lobbying for a seat in the boardroom and in the C-suite. Now that we have it, we must start thinking and acting like business leaders.

Our job is not about just protecting against breaches; it is about making our organizations more successful, responsive, and resilient. The cloud journey provides a perfect opportunity to do this. I remember listening to a keynote speaker at a conference, a couple of years ago, and her main message resonated strongly with me: "Security used to be about protection," she said. "Now it is about trust."

I take this to heart when I look at the role of cloud transformation in our organization, which is a leader in the pharmaceuticals industry. We are a values-driven company, with the goal of always making decisions based on patient trust, reputation, and business—in that order.

Patients have enough to worry about, without having to be concerned if their digital experience is safe and secure.

For a long time, pharmaceutical companies only dealt with doctors, and even then, it was not a deep relationship. But our model has changed for the better. The entire industry is focused on long-term health management. We want to establish long-term relationships with physicians and patients, across our entire ecosystem and supply chain. Instead of a work force on the order of 70,000, we are looking at a potential patient population in the millions.

For that level of scale, size, and trust, you have to use the cloud. Our business, and the overall business climate, move too quickly for anything but the cloud. We cannot wait a week, or even a day, for a new server. We need cloud agility, scale, and resilience. In our organization, we have gone from pockets of cloud to a board-level, CEO-sponsored full-on initiative to move virtually everything to the cloud in the next three years.

Taking the Cloud Journey

I have been a cloud advocate for a long time in my career as a CISO. Fortunately, I have been in the same industry, which I love, for that entire time. But I have also worked in different companies. I am aware of both the challenges in cloud transformation, as well as the opportunities. Here is some guidance I can offer from my own experience and as an active participant in the broader cybersecurity community.

1. **Tread lightly.** Cloud transformation is a journey. Do not expect to go home over the weekend and come back on Monday fully formed in the cloud. Start with areas that can deliver immediate and clear benefits, such as backup, recovery, and software development. Migrate more directly as you get more experience.
2. **Do not underestimate the challenge of living in both worlds.** Even for early adopters and companies seeking a cloud-first or cloud-only strategy, there will often be a need to reach back into the on-premises world for data. There are likely to be interdependencies with legacy applications, technologies, and processes that are not transferable.
3. **Consider the depth and breadth of your ecosystem and supply chains.** Most business models are no longer focused solely on internal operations. We are all dealing with external ecosystems. In the case of pharmaceuticals, it extends to patients, physicians, payers, and beyond. The cloud can help you scale as needed, which is essential because your external ecosystem is typically even larger than your workforce.
4. **Embrace security automation.** The cloud is about server builds, capacity extension, elastic infrastructure. In the past, we used to do many of those things manually. The value of the cloud is speed and agility, largely devolved from automation. In the shared security model, make sure you are automating your portion of the security responsibility, and do not just rely on the public cloud provider's automation. In the rush for speed, developers or line of business managers might want to avoid security. Don't let that happen. Build security automation into your processes and models.
5. **Build up new sets of skills and processes.** In the cloud era, software development is also in a period of rapid transformation. With cloud development, microservices, containers, Kubernetes orchestration, and API security, many companies and IT/security teams are finding themselves back in the application

development business. Organizations must have in-house skills in areas such as API security, DevOps, and SecDevOps.

6. **Modernize hiring, training, and talent acquisition.** Stop looking for the 10-to-15-year security pro. They barely exist. Change your talent acquisition and retention processes to focus on fresher, more agile talent that has experience in cloud, DevOps, API security, and other areas that are likely to hasten your cloud transformation. Manage your teams to keep them at your company using flexible approaches, high levels of automation, support for remote work, and more.
7. **Streamline security with a platform model.** One of the changes in the cybersecurity industry over the past few years has been the emergence of platform models. We have seen many instances where innovative start-ups have come out with solutions to specific cybersecurity challenges. However, a company like ours is hard-pressed to get the support we need from a 30- or 40-person company. There are larger security companies that have been able to stay close to security innovation by acquiring these start-ups and embracing a platform model. This provides a greater level of confidence in dealing with a company that truly understands the challenges of cybersecurity scale, support, service, and innovation—particularly in the cloud.

Reaping the Business Benefits

Cloud transformation has been of particular value to our organization in responding to COVID-19. We are on the front lines, working on treatments and partnering to deliver vaccines. With remote work and digital transformation, cloud transformation is allowing us to embrace new business models that will probably reshape our industry forever.

Why should our field sales teams continue to go door-to-door to physicians' offices? Why do treatment centers require sick people to come into a facility where they come into contact with other sick people? Why can't we use remote diagnostics for disease identification, research, and other functions?

COVID in some ways has been a rallying cry for digital transformation. I have had an internal joke running with our Head of Risk Management; every time someone would come to him with a problem, he would ask: "Doesn't Mike handle that?" The number of business operations and processes that are not related to the Digital Age is getting smaller every day. Every risk today is a digital risk.

For modern CISOs, the world has changed. Security must be viewed through a new lens, not as a technology risk, but as a business risk. One of the ways to think about cloud transformation is an investment in the most critical requirements of the business—resilience, availability, agility, and security.

The cloud provides a fundamental and inherent improvement, not just in security, but in your overall business operations and capabilities, much more so than you could ever build internally. As I said earlier: Cloud is no longer a choice, but a destination.

17

How to Build and Deploy an Autonomous SOC

John Paul Lonie — Head of Security Operations, Iress

One of my favorite sources of inspiration is the motivational speaker and author, Daniel Pink. I find him particularly interesting and an apt source of ideas because he is a motivational speaker on … motivation.

Now, you might not automatically equate theories on motivation with the benefits of an autonomous Security Operations Center (SOC). But there is a very clear and direct link, as we discovered when we embarked on our journey to the autonomous SOC. Trust me.

Dan's main point is that employees are motivated more by things like autonomy, purpose, and mastery than they are by money. Yes, of course money matters. But at some point, once employees feel they are not being short-changed financially, they will seek out more intrinsic goals to enrich them and satisfy their workplace needs.

The autonomous SOC is not only about helping to drive down costs, improve agility, and improve collaboration with business stakeholders. It also gives technically oriented teams working on cybersecurity a sense that they are making a bigger contribution to the organization's mission.

For us, the question quickly changed from "should we adopt the autonomous SOC model," to "how can we make that transition better and faster?" I will not spend much time in this chapter reciting the benefits of transitioning to an autonomous SOC (hint: flexibility, agility, better deployment of human resources, consistency, tight alignment with the corporate mission). Instead, I want to give you what I hope you will see as actionable advice that will not only improve your organization's cybersecurity risk profile, but will also make your employees more productive, more engaged, and more excited about the organization's mission and their role in it.

I knew SOC automation had the very real potential to positively impact what our employees did and how they did it. Dan Pink's advice, and seeing this phenomenon with my own eyes, taught me that our employees wanted their work lives to be more fulfilling, and doing rote administrative tasks wasn't delivering that. We wanted them to be excited to be here, not just view their job as a transit stop on the way to somewhere else. SOC automation allowed them to work on more impactful things, solving com-

plicated problems, and being viewed as more than an organizational cog.

Process Counts

We were extremely fortunate when we set out to build our autonomous SOC: Many of our senior executives had strong technical skills and appreciation for, the value of automation. Those of us on the security operations team benefitted from that, as well as the reality that we have a surprisingly flat organization for a company with more than 2,000 employees.

This helped immeasurably when we began our journey, because our goal for automation aligned very nicely with their business goal to use automation where possible to improve our efficiency and use our human resources more wisely.

Unfortunately, a lot of organizations don't have that kind of technical acumen and appreciation resident in the corner office, but they are very keen to improve their business, so you may have to become innovative in finding ways to achieve that alignment and buy-in.

One thing for CISOs to consider is to take a step back away from the cybersecurity issues and position what you want to do in business themes and an operational context. Talking the business executives' language, especially in giving your goals to them in a way that they could see you are all pulling in the same direction, is a real advantage in trying to get what you want. This is a huge benefit for business leaders because they see the SOC team as part of the same journey toward improved business outcomes.

Business leaders and SOC teams might want to consider something like a contest where teams are built to demonstrate real-world proofs of concept. Imagine your security specialists teaming up with the people in finance, manufacturing, marketing, or legal. It would be fairly easy, in fact, to identify problems that the SOC team could address, demonstrate how it would work, and attempt to quantify the benefits. You could even have some fun with it by creating videos of each project and turning it into a competition. At very least, your security and business teams will gain some recognition, and achieve the motivational goals of autonomy, purpose, and mastery. And, if you make good choices on the problems you seek to solve, you could come up with some big-impact programs that feed the organization's goals.

During the process it's important to keep in mind that soft skills really matter—often as much as, and sometimes more than, the harder technical skills. You have to have the kind of collaboration between the technical, and the business people that make the business side feel comfortable opening up about their problems, and require the technical side to listen, ask good questions, ensure they are hearing the same thing, and find ways to give not just what the business side wants, but also what they need.

Our Journey to the Autonomous SOC

So, how did this play out for us, as Iress set out on its ambitious journey toward the autonomous SOC? Well, if I'm being honest, pretty darn well.

It's not like it was simple; we never expected it would be. In fact, we were well aware of several potential pitfalls we'd have to address and overcome. First, we knew that training and skills development were essential, because change management can be very difficult for people especially when asking security professionals to act like software developers, who are comfortable with experimenting and iterating consistently. Second, we had to consider how to measure the maturity and value of automation; it's one thing to automate, but it's yet another thing to do it well. And third, we had to be honest in acknowledging the potential impact of mistakes. Auto-

mation, it turns out, is a fantastic way to destroy stuff at scale if you're not careful. You have to be honest and open about what might happen when you unleash this thing, and you must have a rigorous testing process. Start small and grow quickly.

Fortunately, we did a lot right, and we learned some things along the way.

- **You have to be brutally honest with all concerned about what you can realistically achieve.** That doesn't mean you shouldn't set big, tough goals, or give up too soon. But managing expectations among business stakeholders and the SOC team is essential. Like a lot of buzzwords, automation can be viewed as a magic word, and the expectations can become very unrealistic very fast. It won't solve all your problems, at least not right away. There is a maturity curve all organizations must anticipate it, experience it and learn from it. It is not overstatement to say that the "vision" will not be attained immediately, so don't oversell it.
- **You need to show the business value quickly.** That means agreeing on the right metrics and the right measurement methodology are very important. But in keeping with the spirit of our first point, it's better to do it iteratively rather than as a singular moon shot. Be sure you communicate—no, make that over-communicate—with business colleagues about what is happening, where the challenges are and what is being accomplished.
- **Show the C-suite and the board the return on investment.** That means that business leaders, while not exactly writing a blank check, need to be there to support the effort financially, and through other, less-tangible ways. Be sure to have senior executives on the planning committees and as part of the operational teams, not only to ensure that the money is being well spent, but that the progress is seen, acknowledged and rewarded.
- **You are never really done with SOC automation.** That's why I refer to this as a journey to SOC automation. There is no finish line, no triumphant cry of "we did it!" and time to sit back and bask in the glory of success. (Well, maybe a round at the local pub with the team would be nice.) One thing you will likely learn is that automation, done right, is going to uncover even more things that you could do better and more efficiently, tasks that should be brought under the banner of SOC Automation 2.0. But don't worry that this may seem like a long process; people are going to find what they are working on to be more important, more visible to the organization and more rewarding personally, and professionally.

Advice for CISOs and Business Executives

Whether you head up the SOC automation effort as a CISO or put your business leadership political capital behind it as a C-suite executive, there are some things you should be doing to make this journey more successful.

CISOs (and their cybersecurity teams) must build a sense of teamwork and empathy with the business teams. Talk to them, spend time with them, learn their language and feed your hopes and dreams back to them in their language. You may need to upskill yourself in order to speak that language, but when that is combined with your innate technical skills, you will be viewed as a well-rounded, diversified, and context-aware resource who can help them accomplish their goals.

Business leaders must also reach out, proactively, to the CISO and their SOC team, to get a sense of "the possible," where seemingly far-fetched ideas can morph into something actionable and very exciting. This also means that business leaders must learn the technology vocabulary of the cybersecurity guys, both to build rapport with the techs but also to get an idea that maybe you are not being given the full picture.

Ultimately, all sides must find new ways to work together to identify and achieve goals. If something goes wrong—and it inevitably will—it will be less likely that fingers will get pointed and blame will be cast around, and more likely that everyone will focus on how to learn from that experience and avoid similar outcomes.

After all, everyone—CEO, board member, CISO, security engineer or accounts payable clerk—wants to feel motivated by what they do and know they are getting more out of this than a paycheck.

Empowering Your People

Which brings me back to Dan Pink, and his comments on motivation.

At the end of your journey, I believe the most important lesson you will learn is that the key to a successful migration to your autonomous SOC is the motivation and emotional well-being of your people. Technologies, tools, and processes are certainly important, but it's your people who matter the most.

An autonomous SOC does not mean you get rid of your people—far from it. It can, in fact, empower your team to do things that matter the most for the organization. And it will liberate your people to accomplish personal and professional goals that matter most to themselves.

Now, in a time when our very concepts of work and workplace are in upheaval, it is essential that your people have every opportunity to do their best work and do so in a way that rewards them financially, professionally and personally. Think of your autonomous SOC as a powerful, efficient and self-reinforcing driver of personal motivation, and you won't go wrong.

Cybersecurity Awareness, Understanding, and Leadership

18

Security Transformation as a Business Imperative

John Scimone — Senior Vice President and Chief Security Officer, Dell Technologies

Despite everyone's best intentions and significant investments in budget, manpower, and corporate attention, organizations in every industry and geographical location are falling behind in the all-out-fight to protect their digital assets against cyber threats.

Why? While reasons vary for each organization, a few truths have quickly become self-evident. For instance:

- It takes much, much longer to detect sophisticated intrusions than it does for bad actors to carry them out.
- Hackers can try an indefinite number of times and only need to succeed once; defenders must be successful every hour of every day.
- The sheer volume of detected IT vulnerabilities is multiplying faster than ever—and those are just the ones we can actually detect.
- Businesses are rapidly digitizing their operations, building increased dependence on the same infrastructure that is becoming increasingly vulnerable.
- Hacking tools are more sophisticated and easier to access, and the financial barrier to "market entry" for hackers is dropping.
- The ability to confidently attribute cyberattacks remains elusive, creating an environment where criminality can exist without accountability.

The result: Cyberattacks may be the mostprominent"low-risk/high-reward" enterprise in the history of humankind.

Get Ready for Security Transformation

This narrative represents a grave risk to modern businesses and demands aggressive management. Clearly, whatever our organizations are doing is not enough. Not nearly enough. Traditional approaches are not even slowing the advance of cybercrime, never mind actually defeating it. No board member, CEO, or CISO should be willing to accept this status quo.

Instead, business leaders—not just the CISO and CIO—must enter a new era of security transformation. A radical rethinking of security—yes, a transformation—is essential. This approach, by the way, is not overly dependent on cutting-edge security tools, serious financial investments, or recruitment of experienced professionals—although all of those are certainly necessary.

Perhaps what is needed most is for board members and business executives—including CISOs and CIOs, by the way—to move beyond traditional approaches to cybersecurity threats. We must all enthusiastically embrace security transformation rooted in a realistic recognition that cyber threat actors can hit a business with devastating consequence at any moment, 24/7/365, and that this is no longer a black swan risk in terms of likelihood. This compels a level of aggression in attitude and activity that is currently missing from the dialogue.

Security Transformed—Resilience on an Equal Footing With Defense

As much as we are seeking to prevent a cyberattack, we are also preparing for a cyberattack. As you can imagine, there's a world of difference between the two approaches. A key element in preparing for a cyberattack is the notion of resilience. Of course, every business leader and board member understands that systems, applications, and technology investments don't deliver any value if they are not available or if the data they contain cannot be trusted. In fact, when systems are down or data integrity is in question, it's even worse: We lose economic value and business competitiveness because we're chasing our tails fixing problems, rather than creating value for our customers.

That said, CISOs have historically been charged with ensuring resilience primarily for regulatory compliance and to avoid lawsuits regarding service interruptions. But resilience is much more than simply passing audits or avoiding fines and contract claims for failing to demonstrate compliance. As business leaders, you want your security forces to be fixated with laser-sharp focus on ensuring availability of essential resources in order to avoid problems and assure business success—not simply on "being compliant."

When considering cyber risk management, we can break it down into three component parts:

1. Threat management
2. Vulnerability management
3. Consequence management

Unfortunately, there really is painfully little we can do on the threat management front. Unless you are part of a law enforcement or related government organization with investigatory and arrest powers, one's ability to impact the threats on the other end of the keyboard remains limited.

From a vulnerability management perspective, our adoption of pervasive mobility, cloud computing, personal applications, and the exciting world of the Internet of Things all increase our cyberattack surface and associated risk profile. As a result, the number of publicly reported vulnerabilities will almost double in 2020.[1] Now, these are risks well worth taking for most businesses—in fact, the decision to not digitally transform would be a death knell for most businesses today—but we also need to acknowledge that with this shifting business technology footprint comes substantially increased cyber risk.

As a result, the CISO spends much of his or her day focused on vulnerabilities—fixing them, mitigating them, and devising ways to avoid them in the first place. Not surprisingly, this has left scant resources for consequence management.

That's where a commitment to resilience becomes essential. Recognizing that in the current environment where threat actors and vulnerabilities remain pervasive and uninhibited and are likely to remain so for the foreseeable future, a greater focus and priority must be placed on how to manage the consequences that come during and after an attack. Organizations need to focus on developing the

capability to effectively fight through what is increasingly becoming the inevitability of an attack. In order to do this, businesses must focus as much on security-minded business process improvements and continuity planning as on the deployment of additional security tools.

Security Transformed—Custom- Tailored, Risk-Aligned Programs and Investments

Transforming the way security is planned, deployed, and managed must change with the reality that business conditions are constantly evolving, operational initiatives are always in flux, and—especially—the bad guys are forever evolving their own tactics.

Traditional approaches no longer work in an era marked by heavy reliance on digital assets that range from monolithic data centers and traditional applications to the "connected enterprise." For instance, the legacy approach—which does not necessarily mean it's been in place for decades, but more refers to an outdated approach—to security has mostly been binary: Either your organization is secure, or it's not.

But the lessons of past breaches have taught us that security is best measured as a scale of risk. Remember what I said earlier: We're not trying to completely prevent breaches, but rather anticipate and respond to them so we can effectively reduce their impact to an acceptable level. Since you can't stop everything in today's vastly complex and vulnerable technology landscape, you need to establish a clear sense of priorities and invest most meaningfully in both defending and preparing a resilient posture for those areas.

Another transformative way of looking at security is the shift away from standard "best practices." As comforting as it is for business executives to hear from their CISOs that they have aligned with well-established best practices on security, the harsh reality is that best practices are not actually effective in meeting the risk expectations of most modern enterprises. (If they were, we wouldn't be reading about the latest breach at a premier corporate brand so frequently.) In addition, the notion of best practices can also obscure the reality that security no longer can be a one-size-fits-all paradigm. CISOs have recognized that security strategy must look and behave differently for every organization, based on its business strategy, risk tolerance, and perceived value of the protected business assets.

Security Transformed—Structure Matters

Business leaders also should evolve their most basic assumptions about how structured security responsibility within the organization must change. Historically, the CISO most often has reported to the CIO or some other senior technical officer. That organizational structure makes sense if you assume that security is a corporate technology initiative rather than a business risk management function. However, remember what IT organizations are going through these days, with practices such as shadow IT, tech-savvy end users firing up their own virtual machines, affordable public cloud services used for business applications, and oceans of unmanaged endpoints, ranging from smartphones to wearable computers. In security transformation, the CISO is best able to defend the organization when he or she is positioned to look across all cyber risk, not just the risks created by the corporate IT organization. Further, beyond simply reactive risk management, CISOs should be leaning forward to focus on digital opportunities, a role best enabled when the CISO is positioned to have visibility across all of an organization's digital activities and in tight and direct alignment with other business executives.

Security Transformed—Perimeterless Security

Finally, security transformation mandates that cybersecurity defense go far beyond the traditional emphasis on keeping bad guys off the network and away from valuable data. Instead, a more enlightened, business-centric approach to cybersecurity should embrace and account for new digital models, including widespread mobility, cloud platforms, and increased third-party risk factors. This shifts the emphasis away from devices and platforms, and toward the protection and defense of digital identities and the data that is most important to the business.

Some examples of how organizations are embracing security transformation include: the idea that security is not a binary concept and should be measured on a scale of risk; or why security programs should not be driven primarily or exclusively by compliance mandates, but instead should be tailored based on business priorities, such as operational efficiency, brand reputation, or market competitiveness. We should begin to think of cybersecurity not as a component of IT risk, but rather, as a business function that addresses business risk across the entire enterprise. And we should ensure that our cybersecurity programs are following the data and identities that are so key to protect, regardless of where the evolving technology and third-party landscape takes them. In whole though, the most essential aspect of security transformation is fundamentally understanding and accepting that the current approach—level of attention, investment, tools, skills, business process tradeoffs—is woefully inadequate to effectively manage cyber risk, and then having the fortitude and commitment to implement the changes necessary to address this disparity.

Putting It Into Action: Questions Board Members and C-Level Executives Should Ask Their CISOs

If you're a CEO, COO, CFO, or board member, you need to be proactive and talk with your CISO about what they are doing to transform security protocols and processes. And that does not mean asking which new intrusion detection tool they've bought or which advanced persistent threat remediation program they've implemented. Instead, your conversations need to focus on ways to turn security transformation from a technical discussion to a business one, and you should seek to understand if the appropriate level of boldness and urgency is present in every aspect of the program.

I encourage you to ask your CISO such questions as:

- What is the likelihood that the breach that just hit Company Y will happen to us?
- If it does happen to us, what is our legal, operational, brand, and compliance exposure?
- How have you transformed our security protocols and practices to move beyond what isn't working at other peer companies like Y?
- Are you confident our overall business risk tolerance is clearly defined, and is our cybersecurity then properly aligned to it? If not, what do we need to do to achieve that definition and alignment?
- What is the most glaring vulnerability in our cyber defenses today, and what is it likely to be three years from now? What plans are in place to address both of these and against what timeline?

- Does a risk-governance structure exist that clearly defines corporate roles and responsibilities relating to cybersecurity-risk identification and management? Do your business stakeholders understand their roles, and have they effectively operationalized them? Is accountability being introduced where dependent stakeholders are not meeting expectations?

Hopefully, this discussion will demonstrate to you that your CISO understands and is committed to a transformed approach that is appropriate and necessary to support your business.

And, if you don't like the answers they give you, you should encourage them to reconsider their strategy—radically, if necessary. After all, if they are investing in legacy best practices that are benchmarks in most companies in your industry, your organization is just as likely to be the next victim of a major attack. That's because the status quo, for most organizations today, is an ineffective posture, as evidenced by the constant stream of public breach notifications. And for a modern business to survive and thrive, it must transform its security posture alongside the broader business and digital transformations that are already underway.

---

[1] CVSS Severity Distribution Over Time, National Vulnerability Database, NIST.

19

An Antidote to Stress in Cybersecurity

Gemma Garcia Godall — Founder, Instituto de Inteligencia Emocional

Stress is an unfortunate but unavoidable occupational hazard in cybersecurity. Think about it. Each time you go to work—or, in today's world, log on from home—you are facing thousands if not millions of potential attacks. If a single one is successful, it can cripple the business and leave permanent scars on your organization's credibility and goodwill. It can damage your own reputation and job security.

Whether you are the Chief Information Security Officer (CISO) at the top, or an analyst working in the Security Operations Center (SOC), the cumulative effects of constant stress can feel overwhelming. And that's just in normal times.

When your organization has been breached, the pressure ratchets up intensely, to the point where many cybersecurity leaders and professionals feel they can never log off. They risk the anxiety of being in reaction mode all the time, 24 hours a day, seven days a week, often for weeks or even months at a time.

The shift to work at home for employees and IT teams as a result of COVID-19 has piled even more challenges on cybersecurity teams that were already typically short-staffed and operating beyond their normal capacity. It is a vast understatement to point out that dealing with that amount of stress is unhealthy. The statistics offer sobering and scary testament to the emotional impact of stress in cybersecurity.

More than 90% of CISOs said they suffer from moderate to high stress and a third believe their jobs would be at risk if their organizations were breached, according to a survey of 408 CISOs in the U.S. and U.K. Even more worrisome: 26.5% said stress was impacting their mental or physical health; 23% said the job was eroding their personal relationships, and 17% said they turned to medication or alcohol to deal with job stress.[1]

This isn't just bad for these individuals and their teams; it's bad for business.

I am not here to tell you that you can eliminate stress from cybersecurity. As I said upfront, stress is an unavoidable occupational hazard. But I am here to tell you there is a proven way to deal with stress and alleviate the pressure so teams can work productively and collaboratively even under the most trying of circumstances.

Managing stress effectively in cybersecurity starts with focusing on emotional intelligence (EQ) and, subsequently, practicing intelligent emotional leadership. Frankly, I shudder with trepidation as I write these words. It is my experience that many hard-driving business leaders and computer professionals

are wary of the word "emotional." It is also my experience that this happens more often with men than women.

If you've gotten this far, I urge you to continue. If you take in even a little bit of what I have to share, it will help—and may even reshape some of your attitudes at a time when organizations are desperately craving leaders who can think creatively, innovatively, and empathically. When we can include emotions balanced with our rational thinking, we are more successful and even happier. When we are authentic to ourselves and our colleagues, we build closer and more powerful teams.

Transformative Power

I've come to believe in the transformative power of EQ and emotional leadership from two vantage points. First is the scientific evidence of its benefits; second is personal experience.

Let's start with science. In the Digital Age, it is a natural tendency to rely primarily on data, facts, and rational thought. However, we can never forget the human element, particularly in cybersecurity. Even with artificial intelligence and machine learning, many critical decisions will be made by humans, and everything that is impacted by people will have an emotional layer.

Scientists at UCLA[2] have demonstrated that expressing emotions reduces the emotional reaction in the amygdala, which is the component in the limbic system that is best known in the processing of fear. When we are exposed to a fearful stimulus, information about that stimulus is immediately sent to the amygdala, which then sends signals to the brain to trigger a reactive response, such as "fight, flight, or freeze."

Research suggests that information about potentially frightening things can reach the amygdala before we are consciously aware, meaning a fear reaction may be initiated before we even have time to think about what might be so frightening. The scientists at UCLA have proven that putting feelings into words is a positive way to reduce the pressure on the amygdala. So, I always encourage all leaders to speak about their own fears in a trust environment to avoid reactive responses.

Now the personal. I was one of those hard-charging business executives I mentioned earlier. I wasn't in cybersecurity, but I was the CEO of a midsized company. I worked insane hours, weekends, nights, constantly on the phone, online, on high alert, "on" all the time. I felt it in my body, pressure in my chest. My doctor warned I was headed for a stroke or heart attack. I needed to stop, relax. But I couldn't. I refused to listen to my doctor, or my body. I had headaches every day, constant pain in my chest.

My breaking point came when I saw myself through the eyes of my eight-year-old daughter. I promised her that I would spend more time with her and her younger brother and spend less time at work. "Mommy, I don't believe you," she replied, angrily. "You always say you are going to work less and you never do it. And the worst thing is, you are not okay. I can see it in your eyes."

This was a real turning point for me. I realized she was right: I was not okay at all. So I changed. I decided to get a coach to guide me to become aware of my emotions, accept, and manage them. I learned to share them with people I trusted. I learned that being open and vulnerable sometimes makes me stronger. I eventually left that job, and I am now devoted to training business and technical leaders on the value of EQ and emotional leadership. As I've experienced first-hand, emotional leadership can not only change your relationship with your teams and colleagues; it can also change your life.

Understanding Leadership Competencies

Everything we say and do is affected by our rational intelligence—but also our feelings. Emotions have an inevitable effect on all of our activity, and even more so if we are a leader.

In leadership, it is commonly accepted that interpersonal skills matter more than cognitive skills. Examples of interpersonal skills include the ability to communicate; show respect; express empathy; active listening; adapting to your environment; giving and receiving feedback. These are all competencies of emotional intelligence.

Because interpersonal skills are key to communicating and managing our relationships, EQ is a must for today's digital leader. But what does EQ actually mean? I use this simple definition:

Emotional intelligence means being able to identify, understand, and manage our own emotions and also the same applied to others' emotions.

To be able to connect with other peoples' emotions, we first need to be able to identify, accept, and manage our own emotions. The leader that reacts to pressure with angry screaming, who loses control and shows low capability to manage his or her own emotions, will have serious difficulties connecting, understanding, and managing emotions in others.

In a stressful cybersecurity environment, the results of this type of leadership can be disastrous. Emotions are highly contagious. If the leader reacts poorly to stress, the team reacts poorly to stress. In the work I do with CEOs all around the world, I see leaders who have what I call "emotional radar" and others who do not. To develop emotional radar and be able to perceive the emotions of those around you, you need to be in a state of internal calm. Without our own self balance, the emotional radar will never work.

Each of us has at least three types of intelligence: Rational, emotional, and intuitive. When a leader is emotionally intelligent, I say he or she is a balanced leader who has the ability to include and balance these three types of intelligence.

How to Lead With Emotional Intelligence

Talented individuals, particularly younger people, love this kind of leader. The next generation of people with high technical skills wants to be led with empathy and autonomy. In cybersecurity, where the skills shortage is pronounced and competition is fierce to hire, retain, and inspire talent, the difference in leadership can have long-term tangible benefits; and the risk of poor leadership can likewise have severe negative consequences.

As Fred Laloux wrote in his book *Reinventing Organizations:*

"The future will no longer be organized as in the Industrial Era, where the boss gave instructions, and humans worked as machines."

Modern organizations are more refined; decisions are made based on trust and collaboration instead of on ego-driven fears, ambitions, and desires. In the current Volatility, Uncertainty, Complexity, and Ambiguity (VUCA) world, where we need to face these issues all together, there is no super leader who has the capacity to decide on his own and find the way alone. Team power is vital, collaboration is essential to generate collective intelligence and overcome the challenges. So, the leader needs to have EQ to generate the right environment for the team.

Practical Steps to Take

Based on my experience working with dozens of leaders and teams, I have several practical recommendations on how to leverage emotional leadership to effectively manage cybersecurity teams

in today's environment—particularly in light of the uncertainty and disruption that has been caused by COVID.

- **Breathe:** Whenever you feel triggered by emotions, just stop six seconds and breathe. Take one to three deep breaths. Our breathing connects us immediately with our body and has the key to connect emotions with our rational thinking.
- **Share:** Working from home gives us the opportunity to share a little bit more of our private lives with our colleagues. This should be a good thing. I've heard leaders say that they have two separate lives, their work life and then their personal life. But that is not the real world. Each of us is one whole person, we cannot be split into two. We need to integrate both parts. We need to feel warmth and be authentic. It is important to be open, to talk about our personal ups and downs, and also our fears, concerns, triumphs, and losses. As the leader, create the space for sharing and team trust will increase. Ask your team directly: What is the worst-case scenario? As I said before, if we speak about our fears we can confront them. We can put light on the darkness.
- **Meetings:** Build into the work process informal spaces to connect. With people working from home, we run the risk of losing some of that personal connection that takes place in an office, at the coffee machine or during lunch breaks. Put aside 40 minutes each week to have a team call where you don't talk business, you just connect as human beings. Also, when you are conducting work meetings, create a space at the beginning and the end to talk. Check in as the meeting starts: How are you feeling today, are you ready to address today's challenges, is there anything worrying you? Check out before the meeting ends: What did you think of the meeting? Are you prepared to take the next step? Create the emotional energy for the team to work at their best.
- **Feedback:** This is a vital point for any team going through a crisis such as a cybersecurity breach. Every tech professional nowadays needs to learn and improve continuously to deal with today's rapidly changing environment. Talented professionals may be highly prepared for their jobs but face new challenges they have never before confronted. How can they evolve if they don't receive quality feedback? So prepare your team for that.

One of the keys to being an emotionally intelligent leader is the ability to give and receive feedback. Feedback triggers emotions, so it is important to pay attention to the emotional impact feedback may have on you and others. Feedback needs to be:

- Constant and integrated as a process for improving and learning.
- Bi-directional—it is just as effective to give as to receive.
- More positive than negative. A Harvard study talks about a ratio of feedback/performance in a work team, i.e., leaders should give six positive comments for each negative comment in order to keep people motivated.

Here is an effective formula in having a positive feedback conversation:

- Prepare the environment, the right place, the right time.
- Explain the situation (facts as specific as possible).
- Explain the behavior seen.
- Explain the impact of the behavior.
- Make your suggestion.

- Encourage the person to do it better the next time and focus on future possibilities.

Always check how the message has been received. How do you see it? Can we agree on my suggestion? Any alternatives? Assertive communications is a key skill for the emotional leader. Practice it.

As you would learn a new programming language, or sign language, or any other new form of communication, get ready to understand emotional language I can tell you it is much easier than all the technological or business knowledge you have learned. You only need to put a little bit of attention to it and ask for training if needed. You will be surprised at the amazing results you will get with relatively little, but focused, effort.

Being Flexible

COVID-19 has taught us that organizations need to be flexible to succeed in today's environment. We are not machines – why do we continue working as if we were? Taking care of our human part increases our productivity. For example, we don't need to all take breaks at the same time, or eat at the same time. Some people work better in the morning, others at night.

Young professionals want that flexibility. Flexibility and autonomy can lead to more productive and empathetic corporate cultures. I know of one company in the financial technology business where many of the employees love surfing, the water kind not the web kind. They have a completely open calendar. On rainy, dark days their part of the office is bustling, and amazing work gets done. On windy days, not so much. The result: High engagement and rotation near to zero. So apply your own formula and be creative!

The Best Leaders

To me the best leader is the one that role models what we want to see on the team. Leaders can be a role model of excellence by using mistakes to teach; share emotions, learning, and challenges; offer help and care to colleagues; and assist team members to find better solutions and become stronger.

We are never going to eliminate stress from cybersecurity unless we eliminate the human element, and it would be a sad day, indeed, if that were to ever happen. For the foreseeable future, at least, people will remain vital to successfully navigating the Digital Age. And, as long as we are managing people, we need to be able to manage stress.

Good leaders understand the value of emotional intelligence in inspiring, motivating, and empowering today's workforce. As the workplace continues to change in response to a global pandemic, good leadership in cybersecurity may mean the difference between avoiding breaches and protecting the organization, or risking being more vulnerable to successful attacks.

In today's era, cybersecurity leaders can't afford to ignore emotions and the power of intelligent emotional leadership. Emotions are part of our whole intelligence. In fact, I can assure you that the best leaders will be the ones that embrace and harness EQ.

As a computer needs electricity to work, we need emotions to give us energy. Emotions are the energy that move us into action. Emotions move teams to do amazing things. Emotions move the whole world.

---

[1] "Major Global Study of Senior Cybersecurity Professionals reveals increasing pressure, workload and budgetary deficits," Nominet, February 2019.

[2] "Putting Feelings Into Words: Affect Labeling Disrupts Amygdala Activity in Response to Stimuli," Psychological Science, May 2007.

10 MANTRAS FOR THE EMOTIONALLY INTELLIGENT LEADER

1. Recognize and master my own emotions.
2. Connect with the other from the same level – reason, body, emotion.
3. Be present, and observe body language.
4. Create environments – moments and spaces – for informal conversations.
5. Use mistakes to learn.
6. Create a routine for feedback and improvements on the team.
7. Generate a positive atmosphere.
8. Accept diversity in the team – different visions, personalities, etc.
9. Express appreciation, and gratitude.
10. Celebrate together.

20

The Importance of Cybersecurity Preparation and Leadership

Stephen Moore — Vice President and Chief Security Strategist, Exabeam

If your organization is like most, you probably have an incident response plan designed to help your teams work their way through a cybersecurity attack. It covers the technical and nontechnical steps the organization must take to respond. It has passed the muster of auditors and been reviewed countless times for the purpose of fulfilling regulatory compliance requirements. All in all, you are proud of this document and can point to it and say, "Yes, we are prepared."

And then a breach happens.

Guess what? You're not prepared. No matter how much time and effort your teams have put into their incident response plan, there is no way they could possibly foresee and prepare for the massive toll a major data breach will inflict upon your organization and your people.

Through my experiences, I've learned what to do if your organization has been breached, and what not to do. I've learned about the steps organizations can take to ensure they are better prepared to handle a breach, including some ideas I will share here. Most of all, I've done my best to learn what it takes to be a leader and what it takes to inspire confidence and comfort in times of crisis.

On the Frontlines

There's no way to synthesize everything that happens during a breach, the gravity of it. You might be a mid-level manager and all of a sudden find you are thrust into technical response, and also asked to communicate with senior-level executives, customers, and with people across the entire organization responsible for responding to the breach. Very few are prepared for this drastic change in pressures and responsibilities.

I must make the point that nothing can prepare you for what it is like to be in the vortex of a data breach, especially those of great depth and breadth. I'll give you one example: Time. Talk to people who've never been through a breach, and they'll tell you that the impact and implications will probably be mostly over in a matter of months. All I can say is, "No way." It is going to take years for the company to recover; and even then, there are likely to be lingering issues.

A breach will affect every aspect of your business: the retention and attraction of new clients; your personnel and corporate culture; whether people will even want to work at the company; your reputation. You will likely be dealing with multiple investigations, audits, regula-

tory groups, the press, and a retooling of your technology infrastructure. Not to mention litigation. All of this will go on for years and will be a huge and constant drain on resources. Going forward, every aspect of the business will be shaped by the breach.

The Human Impact

The toll this will take on your people is something that you can't measure, anticipate, or really appreciate until you're actually going through it. The pressure on your people is immense. Most organizations don't have the depth of management, the training, and the people with the right skill sets to adequately deal with a major breach—both immediately and over the vast span of time the circumstances require.

Even if you have adequate response and communication plans, you need people to execute them. In a breach, a communications funnel gets created and most of the information is communicated through a small group of people leading the investigation. It is up to those people to synthesize the information for the appropriate individuals—whether board members, senior-level executives, auditors, clients, the media, partners, or any other effected parties.

There is an art to this, and most people forced into these roles are not prepared to do them well. They must learn, and learn fast.

Steps to Being Better Prepared

Given the immense challenges and dramatic impact that a cybersecurity event will impose on your organization and its people, how do you prepare for something that is probably beyond any preconceived expectations you may have established? It sounds like an unsolvable riddle, but can you prepare for something that can't be prepared for?

Actually, you can. I've developed several ideas that I believe will help individuals and organizations do a better job of preparing their people to deal with the ramifications of a cyber breach, without forcing them to constantly strive to do hero work.

No. 1: Write Your Breach Notification Letter Before You Suffer a Breach

Lacking experience, organizations need to work backward, starting with the breach notification letter. Sit down at the highest levels possible within the organization—senior management, CISO, perhaps even including board members—and write the breach notification letter, under the direction of counsel and as a draft "working" document. Interestingly enough, doing this will uncover many of the key challenges you will face. This is the finest executive tabletop exercise known to me, due to the questions and outcomes. When you sit down and write a notification letter that the world may one day see, you're going to have to start asking the right questions:

- Who writes the letter?
- What is the tone?
- Whose names are on it? The CIO? CEO? CISO?
- Who will answer questions from the media?
- What are the ingredients that go into the letter?
- There are the staple talking points, such as "we've retained outside experts and contacted law enforcement." But do we have a pre-existing relationship with them? Shouldn't we?
- How well-prepared are the people inside the organization to do the work that will be required? Are they trained for this?

- What will it cost to pay an outside organization for public relations? What type of executive coaching do they provide?
- How do we securely share information and communicate if breached?
- Who meets with the press? Who coaches these people prior to meeting with the press?
- How do we contact clients? By letters? Phone calls? Email? Via the web site?
- Where do we host our breach information website? What happens if our site is part of the breach?
- Are we going to do credit monitoring? What does that cost? Is it worth it?
- Most importantly, who is the source of truth for investigative answers? Won't they already be a little busy? How often do we update these talking points? Are we able to answer these in-house today, or do we lack this ability?

I could go on with more questions, but I'm sure you get the point. These are typically not questions that organizations raise until they've suffered a breach, and at that point, it is too late. You've already gone from the frying pan into the fire.

No. 2: Conduct a Field Trip to the Source of Truth—the Security Operations Center (SOC)

If you have a breach, who would you call internally? Who would that person call next? Who would prepare executives for difficult interviews and questions from clients?

Work your way down to the unfiltered answer: those staff members normally ignored and probably working buried within your information security team—your security operations center (SOC). Without question, the reputation of your organization and your future professional comfort is in their hands. Have you even met them? Do you understand their workday, their challenges, and their pain? How well can they articulate their investigative processes?

Their problems and observable risks must be externally supported and prioritized. Seek their counsel *before* you have no choice but to seek it. Please do not underserve your SOC.

No. 3: Build a Better Type of Response Plan and Response Action

A plan untested, unshared, or created in a vacuum of experience is only good for those who can avoid the negative effects of its failure.

When I started this chapter, I was skeptical about the standard incidence response plans that most organizations use to satisfy executive management or outside auditors. Frankly, I've never seen a good one when it comes to actually responding to a breach. These response plans typically cover technical issues, but they don't discuss things like leadership or communications. And they don't address breaches as the multi-year events that they often are in the real world.

A more effective incidence response plan will address the pertinent questions raised by the breach notification letter. Who's in charge? What's the tenor and spirit of the organization? How do you sound? How large was the breach—how many records or systems were affected? How open do you want your plan to be—do you want to be cold, verbose, and succinct, or do you want to be open and share as much as you can? Do you share early before all the details are known, or wait to run out the clock? I recommend sharing early and honestly, knowing that additional updates will be made as the investigation unfolds.

No. 4: Plan to Deal With Issues Around Response Capabilities, Technology, Infrastructure, and Physical Space

Once you've suffered a breach, your entire technology infrastructure will likely be under investigation. Your IT teams will be buying new technology while they are still cleaning up the existing environment. Plus, you will likely be bringing in outside consultants, not just on the technology side, but across the board.

Along this line of thinking, remember that your multi-year plan, pilot projects, and pending budget requests will probably be green-lit. You will need three critical technical capabilities: visibility, analytics, and automated technical response. You can ensure you have these capabilities before a breach, or acquire them quickly post-breach. I'd suggest prioritizing these capabilities before a problem occurs; it's much less expensive.

Visibility removes technical blind spots, generally through data lakes to store event data and analytics to make sense of it all and create attacker timelines. And then response is your cleanup. Remember, without complete attacker timelines, you won't have complete response.

Logistically, do you have physical space for additional hardware while you remediate and clean existing infrastructure? Do you have enough rack space, cabling, and power to deal with all of the extra equipment? Ever think about allocating this ahead of time?

You also need to think about creating a landing zone to house all of the people you are going to bring on board to help. Where is the secure command center, and is it most convenient for the staff?

No. 5: Teach Your People Well

Your people, many of them technical mid-level managers, will be thrust into public-facing activities. Are they ready for it? Have you trained them? Do you feel comfortable having them speak to your most important customers? Do you have a backup plan and a backup plan for that?

You might need 25 more spokespeople. Have they been trained to speak in public, handle an interview, an auditor, or government official? This goes beyond what your corporate communications team can manage, because many interactions need to be technically oriented. You can use outside people to help, but they are most likely going to be speaking from a script. Is that the image you want to present to your customers, partners, and the general public? Crisis tends to burn through veneer.

The responsibilities are not just outside-facing. There are internal challenges as well. Mid-level technical managers, need to be articulate and clear when speaking to everyone, especially newly acquainted executive-leadership team members.

This is one of the hidden costs of dealing with a breach. It's natural to think about lost revenue, a declining stock price, damage to the brand's reputation. But there are a lot of people-oriented costs that must be addressed as well. If you can plan for some of these in advance, and spend the time training your people to handle a variety of roles, you stand a much better chance of mitigating some of the other challenges as they arise and threaten to cripple your organization once an attack takes place.

No. 6: Build Relevance with Your Sales Teams

This is advice aimed primarily at CISOs and other security leaders. Despite what we think, the board and executive leadership are often focused on one main goal, which is the retention and acquisition of customers. Everything else flows from that, beginning with the perception of the brand's reputation. In a breach, you will be asked: "Does our present situation put any pending deals on the bubble?" and

"Who might leave?"

Clients and prospects will have a ton of questions, and how you answer them will be critical. Again, it is essential that you encourage comfort and confidence. When I speak to CISOs, I often ask how many have presented at their sales quarterly business reviews or even know their sales teams. Curiously, I've never had a positive acknowledgement. Let's change this.

A breach creates ongoing challenges for those who make money for the company; understand the sales pain. You will be pleased to discover that doing this opens a wonderful door of relevance for your organization and even personal brand.

You may think your job is to keep the bad guys out, but it's also to facilitate the business. I've learned to develop a strong relationship with the sales team, and it has given me an incredible amount of clout. Once I took the time to build the trust of the sales team by putting them first, my career changed. It changed who I was talking to in the organization, how I was treated, and the types of conversations I was involved in.

No. 7: Don't Rely Solely on "Hero Work"

People are not superheroes, and if your plan is to rely on herculean efforts you will probably fail. On the other hand, you want to create space for people to do hero work, which is usually the result of the type of leadership you provide and the type of culture you create.

If someone is operating in fear, he or she will not innovate, will not do hero work, will not be the brand ambassador, contributor, or thinker you need. Fear creates indifference quickly, and the level of indifference is often directly tied back to bad management. Your leaders have to take the heat, so the people on their teams can take the chances that hero work requires. You have to keep morale up and shield your people from pain or fear of failure. Hire and promote servant leadership today.

Leaders have to be leaders, and often in times of crisis, you see them slip back into the technical. This acutely means the leader doesn't trust his or her staff. Once you get into a position of leadership, you can't afford to be that technical person anymore. If you're spending your time playing around on a console, you're not a leader.

Conclusion

The skills involved in responding to a breach are much different than those involved in attempting to prevent it, particularly for most members of your technology teams. The reality, however, is that you have to rely on these people to step up their game and provide a level of leadership.

You need your leaders and spokespeople to inspire comfort and confidence in all directions. You can get ahead of the game by preparing them beforehand and being aware of which people are likely to step up and provide leadership in a time of crisis.

You can ensure that the overall organization is prepared so there is less chance that the people responsible for responding will be overwhelmed. You can ensure that there is leadership depth. You can take the time to write your breach notification letter ahead of time, answer the questions, and align resources to support those capabilities into your corporate culture. You can visit your SOC.

As an organization, you will likely be judged less on whether you suffered a cyberattack, and more on how well you responded to it. The better prepared you and your teams are, the better able you will be to respond appropriately. You won't be able to anticipate every scenario—nobody can—but strong preparation and leadership will help you deal with the unexpected.

21

Data Manipulation, Law Enforcement, and Our Future: Seeking to Build Trust in Our Digitally Connected Systems

Dr. Philipp Amann — Head of Strategy,
Europol's European Cybercrime Centre (EC3)

While we have traditionally considered data manipulation as the practice of altering documents and other information, that definition is changing. When we think about data manipulation now, the alteration of documents and information done with a criminal or harmful intent has become a major concern, but not the only one. We also think about things like fake news, social engineering through the discrete mining of social media information, and the use of data as a tool—or a weapon—to shape people's thoughts, ideas, opinions, and, ultimately, their actions.

As highlighted in Europol's Annual Internet Organised Crime Threat Assessment, data remains a key commodity for cyber criminals. However, it is no longer just procured for immediate financial gain, but it is also increasingly used, manipulated, or encrypted to further more complex fraud, for ransom, or directly for extortion. The illegal acquisition of intellectual property or its manipulation can reflect the loss of years of research and substantial investment. Data manipulation in this context can also mean using hiding techniques such as steganography to exfiltrate data or hide command-and-control commands.[1]

Data manipulation has become a moving target for those of us in the business of combating criminal activity online, building trust, and protecting our way of life in the Digital Age. Adversaries who manipulate data with malicious intent are constantly developing new tactics and attack modes, seeking any edge in a world where all of us are increasingly dependent on digital connections. This includes activities by criminals who hide their identity, mask their location, and obfuscate their financial transactions.

The Evolving Role of Law Enforcement

What can we do about data manipulation? The first focus for law enforcement is on investigating criminal behavior and prosecuting those responsible for crimes. With certain aspects of data manipulation and the often related criminal abuse of information technology, we have made significant headway in investigating and prosecuting criminals and shutting down illegal activities. A few examples:

AlphaBay and Hansa: In July 2017, authorities in Europe and the U.S., including the FBI, the U.S. Drug Enforcement Agency, and the Dutch National Police, with the support of Europol and other partner agencies, announced that they had shut down AlphaBay, at the time the largest criminal marketplace on the Dark Web, and Hansa, the third-largest criminal marketplace on the Dark Web. Both AlphaBay and Hansa were enabling massive amounts of illegal drugs, stolen and fraudulent identification documents, access devices, malware, and fraudulent services to be traded amongst cyber adversaries, which were enabling future data-manipulation crimes to be committed.[2]

Operation Power Off: In April 2018, the administrators of the distributed denial-of-service (DDoS) marketplace *webstresser.org* were arrested as a result of Operation Power Off, a complex investigation led by the Dutch police and the U.K.'s National Crime Agency, with the support of Europol and a dozen law enforcement agencies from around the world. *Webstresser.org* was considered the world's largest marketplace for DDoS services. These services enabled cyber adversaries to use data manipulation to launch approximately four million attacks measured, aimed primarily at critical online services offered by banks, government institutions, and police forces.[3]

There are many more examples of successful law enforcement efforts that we can cite, but I am pointing to these because they have specific common characteristics:

1. **They involved a coordinated effort across law enforcement agencies all over the world, along with the support of governments, regulatory bodies, and private companies.** This is an absolute necessity if we are to successfully address criminal activity online, including today's data manipulation challenges.
2. **The crimes involved activities that were clearly illegal, and thus fit into the law enforcement model for investigating and prosecuting criminal activities.** But, as cybercrime and malicious data manipulation evolve, not every instance will be clearly defined by legislation or regulation, thus making it more challenging to prevent, defend, investigate, and successfully prosecute perpetrators.
3. **In each instance, law enforcement was in a position to be more reactive than preventative.** Our ultimate goal is to be both. Law enforcement needs to successfully leverage resources from all around the world, not only to *respond* to crimes, but also to *prevent and deter* the criminal activity from happening in the first place, and ultimately to become more proactive.

These examples also highlight the high degree of professionalism, collaboration, and industrialization of the underground economy, where services and tools supporting the entire "cybercrime value chain" are readily available online and to non-tech savvy individuals.

Disrupting, Deterring, Diverting, and Defending

In dealing with malicious data manipulation and cybercrime, the expectation is that law enforcement—together with all relevant partners and in accordance with its mandate—will take on a more expansive and complementary role in defending against, disrupting, and deterring illegal activities *before* they can do harm and cause losses. This is why prevention and raising awareness are key topics, particularly in relation to addressing high-volume and low-level criminality online.

Law enforcement is in a unique position. Not only do we understand specific modi operandi and techniques when it comes to cybercrime; we are also constantly monitoring trends and threats, while analyzing the evolving motivations impelling those who would do us harm.

However, when it comes to data manipulation, even when activities are motivated by malicious intent, we are sometimes unable to contribute as effectively as we would like. One reason is that not all of the forms of data manipulation we encounter are properly defined as criminal by legislation. In other words, the intent may be malicious, but that doesn't necessarily make it a crime. There is also a lack of a harmonized common legal framework or an underuse of existing legal frameworks and provisions, meaning the same activity might be criminalized in one jurisdiction, but not in another.

Access is another issue. Not every organization involves law enforcement when it first encounters a problem. There are many possible reasons for this. However, I would ask executives to preemptively think about how they work with law enforcement—*before* they have an issue. By building a proactive partnership with law enforcement, you will be better equipped to prevent an attack and enable a stronger and more impactful response should an attack occur.

Even in instances where access is possible, we face challenges in relation to loss of data and loss of location, which create substantial obstacles for investigations. There is also a need for standardized rules of engagement with private industry to establish a clear understanding of the extent to which private parties can engage with us and we with them.

When it comes to young people with strong information and communication technology (ICT) skills, we also support projects such as the "deterring youngsters initiative," which, together with industry and academia, aims to divert young people away from a potential pathway to cybercrime by offering positive alternatives.[4] We see this not only as an opportunity to divert such talent to positive activities, but also as a way of addressing the shortage of ICT skills.

Cooperating, Collaborating, and Connecting

If there is one thing we've learned about today's cyber environment, it is that we are all in it together. We can gather strength in numbers and in pooling our knowledge, experience, and resources. It is a truism of the Digital Age that we are all connected. Our adversaries try to take advantage of our uber-connectedness—we should do the same in fighting them.

This touches upon the question of safeguards against and regulation of data manipulation, as well as responsibilities. Should it be left to tech companies to self-regulate when it comes to issues around data mining, data privacy, and data manipulation, or should the discussion involve all stakeholders, including industry, law enforcement, and the public? I would argue for the latter approach.

Regulatory and legal frameworks are just one example. If you look across the cybersecurity spectrum, you will see that every facet involves some level of cooperation and collaboration—from technology platforms designed to work seamlessly together, to law enforcement agencies that work together to not only investigate crimes, but also to detect, deter, divert, and to help defend.

The No More Ransom initiative is a great example of a joint initiative between law enforcement and industry, aiming not only at prevention and awareness, but also victim mitigation.[5] The joint platform is currently available in more than 30 languages and supported by more than 120 partners, offering more than 50 decryption tools, free to victims of ransomware.

Building Transparency, Oversight, and Trust

In order to attain the levels of collaboration and cooperation necessary to address data manipulation, we must trust our people, processes, and technologies and build trust-based relationships between industry partners and law enforcement. This means we have to also address issues around transparency and oversight, which are becoming far more complex as technology innovation continues to accelerate and flourish.

The growth of big data analytics and automated decision-making creates new issues in terms of transparency and oversight, and therefore trust. This challenge could become exacerbated with the expansion of machine learning and artificial intelligence. When we allow automated decisions to be based on an algorithm, we may not have a clear way to determine if the data or the algorithm has been manipulated, which becomes further complicated if the algorithm has a built-in bias. This can add risk and make it difficult to audit and/or verify the outcome of such processing.

Trust is also an increasing issue in the area of fake news. It's not just that fake news is being created and real news is being manipulated; sometimes only partial information is shared, thus creating a narrative that seems plausible, but which is not based on all of the available information. It is designed to support a specific idea rather than provide an accurate depiction of events. The challenge is compounded because adversaries are not necessarily breaking the law; they are merely taking advantage of their deep knowledge of social media and search-engine algorithms to manipulate data.

Finally, trust is also a key ingredient to successful public-private partnerships.

Moving Forward

Data manipulation is on the verge of becoming one of the largest criminal industries. Today's reality is that law enforcement has a vital role to play in creating a more impactful and proactive response, not merely reacting to criminal activities. Everyone benefits from a holistic, adaptive, and complementary approach that involves all relevant partners, one where organizations can leverage the capabilities provided by law enforcement agencies. For example:

- **With prioritized and coordinated joint actions** against the key cyber threats—supported by adequate legislation—we can increase the risks for cybercriminals and impose real consequences.
- **With effective prevention and disruption activities,** we further tip the scales to the detriment of criminals by leveraging cooperation and partnerships across law enforcement, government, and private industry.
- **With advanced technologies and open platforms,** we can use shared threat intelligence, machine learning, and automated decision-making to reduce risk and improve responsiveness. This enables us to eliminate manual processes and use software to fight software while adhering to strict data protection regulations.
- **With greater collaboration and commitment to sharing,** we can band together as a community to use combined resources in the war against data manipulation. The cyber industry has made great progress in this area through the establishment of platforms such as the Cyber Threat Alliance (CTA), a not-for-profit organization that enables near real-time, high-quality cyber threat information sharing among companies and organizations in the cybersecurity field. Another great example for collaboration that includes law enforcement as a key partner is the Cyber Defence

Alliance. And we have also made significant headway together with the members of our own Advisory Groups.

Looking Ahead

How do we turn this vision of cooperation and collaboration into reality? Europol and its European Cybercrime Centre (EC3) and its many different partners in law enforcement, industry, and academia are a prime example of the power of a networked response to cybercrime at scale. However, we need to continue to improve and forge new alliances, further our cooperation with other partners, and continuously adapt our response. We also need to focus on areas such as regulations and technology to clarify criminal activity, improve our preparedness, and enhance our ability to coordinate a response:

Regulations: With General Data Protection Regulation (GDPR) in Europe, we are seeing the benefits of proactive regulation with a strong cybersecurity element. GDPR forces organizations to understand what data they have, where it is stored, who works on it, who can manipulate it, and how to protect these assets. That is linked to quality and information management, with organizations defining how they run their businesses in relation to cybersecurity risk. It also promotes the idea of designing security protections into products and services.

Taking a broader perspective, GDPR is about improving business and management practices, understanding core business processes, and identifying the assets of an organization, as well as its risk posture. While GDPR is an important piece of legislation, its impact on the WHOIS database going dark after May 25, 2018, had substantial cybersecurity implications, not only for law enforcement, but also for the internet security industry as a whole. This highlights the need to strike a balance between privacy and protection of fundamental rights on the one hand, and security and safety on the other.

Technology: Cyber criminals are adopting new approaches to increase their capacity to manipulate data and commit cybercrime. We must use current and emerging technologies to prevent them. This means the use of shared threat intelligence, open platforms, AI, machine learning, and more. It also means we must explore the benefits of innovations, such as blockchain technology, to create an environment that is more transparent, trustworthy, and resilient.

Big Data analytics, machine learning, and AI can improve cybersecurity through better threat detection and prediction, intelligence collection and analysis, and faster response. With effective use of information, the deployment of scarce operational resources can be better targeted to intervene precisely where issues, crimes, and threats can be expected. However, it is important that we use such tools carefully, proportionally, and in line with relevant legislation and regulations.

An example of using technology and information collaboratively and effectively can be found in the Adversary Playbooks program that has been developed by the CTA. CTA members leverage an automated platform to share actionable intelligence to create Adversary Playbooks that provide a consistent framework to identify broad threat indicators and adversary chokepoints. These playbooks typically incorporate several core elements: technical profiles, typical plays, recommended actions, and technical indicators.

Suggestions for Business Leaders and Executives

Beyond regulations and technology, business leaders and executives have a vital role to play in addressing the evolving challenge of data manipulation. They have a responsibility to set the cybersecurity agendas for their organizations

and decide on the appropriate investments in people, processes, and technologies. Suggestions on steps business leaders and board members can take:

Develop an understanding of the evolving adversarial mindset: Executives can look to sponsor initiatives that drive your organization to build a proactive trusted partnership with law enforcement agencies. In doing so, you can gain insights into the motivations, technologies, techniques, and business models of cybercriminals, which can help to define the steps your organization can take to be better enabled to prevent an attack. Also look to collaborate with organizations, such as the Cyber Security Information Sharing Partnership, which enable secure threat intelligence to be shared.

Require organization-wide training and education: We all must be educated about the risks of data manipulation and the need for improved cybersecurity. This often starts in the executive suite, where C-level executives must understand risks so they can make the proper investments and strategic decisions. It also extends to security personnel, who are in relatively short supply in comparison to the need. So inspire, incentivize, and reward your IT security personnel to keep vigilant and informed. And recognize that, as leaders, we must leverage education and training in our work and classroom settings so users are aware of how they can mitigate risk whenever they go online.

Insist on a holistic approach: Cybersecurity should be part of a holistic approach that should be part of all processes. Business leaders and board members need to establish a cybersecurity culture whereby everybody is aware of his or her responsibility, and security and privacy "by design" are guiding principles. Since humans are often the weakest link, ongoing training, education, and creating awareness are indispensable tools in protecting against cybercrime and data manipulation.

Conclusion

The world is changing before our very eyes. The threat to data encompasses all three principles of confidentiality, integrity, and availability. By gaining access to data and subsequently exposing such data, criminals undermine the confidentiality of information. By manipulating the data, they undermine the integrity, and by attacks such as ransomware, they make the data unavailable. While data is a commodity now, it is increasingly emerging as a cybercrime attack vector through means such as data manipulation, compromised processes, and the increased potential to shut down basic infrastructure services and other pillars of our societies.

The good news is that no one is alone. In fact, we are all connected, both literally and figuratively. Our connected networks give us the ability to coordinate and collaborate in the face of data manipulation and cybercrime. Will we be able to build the trust necessary among our people, processes, and technology to overcome these threats? We must, we can, and we will.

---

1 "Criminal Use of Information Hiding (CUIng) Initiative," http://cuing.org/

2 "Massive Blow to Criminal Dark Web Activities After Globally Coordinated Operation," Europol, July 20, 2017.

3 "World's Biggest Marketplace Selling Internet Paralysing DDOS Attacks Taken Down," Europol, April 25, 2018.

4 "CyberCrimevsCyberSecurity:Whatwillyouchoose?,"Europol,https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/cyber-crime-vs-cyber-security-what-will-you-choose

5 "No More Ransom project helps thousands of ransomware victims," ZDNet, July 27, 2017.

The Convergence and Divergence of Compliance and Cybersecurity

22

Why Secure Availability—Not Compliance—Should Be Every Business Leader's Goal

Danny McPherson — Executive Vice President and Chief Security Officer, Verisign

Compliance takes up an inordinate amount of an organization's time, budget, and manpower, particularly when it comes to ensuring that access to IT resources and vital information are safeguarded at all times.

And I'm here to tell you that C-suite executives and board members alike—and yes, even a lot of us chief security officers—are fretting, fussing, and fidgeting over the wrong thing. That is, given that most IT security resource allocation still focuses on accommodating inherently reactive compliance objectives rather than considering overall enterprise cyber risk management, we may not be adequately protecting what we care about most!

An organization's overall *cyber risk* can be calculated [in part] by considering *threats* posed by motivated capable adversaries (to include intentional or unintentional insiders), the organization's *vulnerability* to those threats, and the immediate and residual *consequences* that result (e.g., be they impacts on confidentiality, integrity, or availability). Furthermore, enumerating what you care most about, and what enables it, is a critical first step in a comprehensive cyber-risk management program.

Let me be clear: I'm not saying that compliance isn't important. No one wants to risk fines, sanctions, or damaging publicity over regulatory violations. And no one wants to see our executives do a digital "perp walk" for the compromise of sensitive information.

That's why cybersecurity challenges have made compliance a source of anxiety and angst for C-suite executives and board members. I don't need to do a roll call of data breaches in your industry—we don't have enough hours in the day for that. Let's just all agree that those breaches, data losses, and regulatory compliance missteps are exacting huge costs on all organizations' finances, operations, legal exposure, and brand reputation, not to mention the long-term residual effects on impacted parties.

$$\mathbf{RISK_{cyber} = Threat\ (Capability,\ Intent) \times Vulnerability \times Consequence}$$

I'm sure that just the simple thought of a banner headline with your organization's name linked to a data breach sends shivers down your spine. I know that's what it does to me.

But compliance is not—repeat, not—your goal. Or, at least, it should not be the key focus of your cybersecurity program. And let me tell you why:

Being compliant is not the same as being secure.

For that matter, being compliant does little or nothing to ensure that your critical systems are available at any point in time, which jeopardizes everything you do. That's why you need to focus on taking the right steps to enable secure availability of essential services and key resources in the face of broadening cyber threat vectors. If you do that—and only if you do that—you'll have a fighting chance to maintain operational integrity and achieve compliance in today's incredibly interconnected internet ecosystem. Let me explain why.

Why Availability Matters and Why It Must Be Secure

For as much attention, spending, and energy that goes into the process of demonstrating compliance, it's important to remember that compliance is a very limited way to look at the security of essential systems or data.

Compliance regulations tend to be inherently reactive and very targeted, either by industry, geography, or type of information that needs to be protected. These requirements often focus heavily on the confidentiality and then on the integrity of the data. Although these are certainly important issues, they do little or nothing to ensure overall resilience—that is, that mission-critical systems and data are available when employees, partners, and customers need them. Besides, demonstrating compliance is too often viewed by business leaders as an event, typically played out in this conversation:

CEO to CSO:
How did the HIPAA audit go?

CSO:
Great, we passed with flying colors.

What the CEO says:
Glad to hear it; nice work.

What the CEO thinks:
One less thing to worry about until next year.

Demonstrating compliance—either with an external regulatory body or an internal function—is usually a point-in-time status check. But no one should delude themselves into thinking that their ability to demonstrate compliance guarantees them another second of secure availability. And even a few minutes of interrupted systems availability can cost millions of dollars, compromise customer trust, and tarnish an organization's reputation.

That's because, at any point in time, a cyberattack can:

- Take down a city's water filtration system.
- Disrupt an internet service provider's wide-area network infrastructure.
- Circumvent a retailer's digital loss prevention system.
- Interrupt a manufacturing plant's robotics-based assembly line.
- Undermine a municipality's online voting system.

If any of those systems—or any other mission-critical application—is rendered literally or functionally unavailable because of cybersecurity attacks, the compliance status you proudly hail won't mean a pile of beans.

Fortunately, many executives are getting the message—a message that is

often delivered by an anxious and persistent CIO or CSO, or a business leader who realizes that the organization will not demonstrate compliance unless it focuses on the bigger picture of secure availability and resilience. With increasing frequency, executives and board members are buying in to the notion that secure availability is the very foundation of compliance. As such, there are more nuanced discussions with business leaders and in boardrooms that go far beyond compliance-centric issues, such as confidentiality and data integrity.

Not surprisingly, organizations with a culture built around collaboration among business and technical leaders are demonstrating real leadership in promoting secure availability first, with compliance being one result of that focus. And those where the CEO and board see cybersecurity as a technology problem best handled by the SecOps team or solely by doubling the infosec budget … well, let's just say they are setting themselves up to be the focus of the next banner headline.

A Sobering Thought: New Business Initiatives Often Expand Your Cyber Risk Footprint and Threaten Compliance

In this book, and in many other discussions, you'll undoubtedly read and hear a lot about the exciting business opportunities made possible by the integration of technologies into everyday business processes and common "things."

Trends such as the Internet of Things, cloud computing, enterprise mobility, and digital transformation are making organizations more efficient and better positioned to bring new products and services to market faster.

They also are making organizations—and their entire business ecosystems—more vulnerable.

Take IoT, arguably one of the most exciting and promising applications of technology in decades. But when billions of everyday items are connected via the internet—not only to each other, but often also to our core business systems and IT infrastructure—we dramatically increase risks that threaten secure availability and, in turn, compliance.

Another dual-edged sword is the increased use of technology to enable customer self-service, such as online banking, omnichannel shopping, or ordering and managing municipal services from a digital consumer device or through a public cloud service. Yes, it creates a boatload of new services and improved customer engagement. And yes, it also introduces a boatload of unmanaged endpoints and easily accessible points of entry into our digital infrastructure, where systems can be disabled or rendered ineffective if availability is interrupted.

Mobility, cloud, virtualization, and other technology also are driving new workforce models, such as distributed teams, virtual collaborations, and new models for when, where, and how people work and share information. Those provide flexibility and empowerment for our employees, but they also represent big security headaches as more things that organizations care about live in more places with fewer direct capabilities to protect them.

Each and every one of these new opportunities carries a substantial risk factor that can result in regulatory or internal policy compliance challenges. However, these challenges will pale in comparison when new products and services are rendered unavailable due to security lapses or even network connectivity issues anywhere along the digital ecosystem.

Lessons Learned: Using a Three-Tiered Approach to Secure Availability

As I've stressed in this chapter, compliance is best achieved with a more strategic focus on secure availability with consideration of overall cyber risk to the enterprise. But actually achieving secure availability takes patience, practice, and a process rooted in business goals, not in technology.

Over the years, I've worked with my business colleagues to identify and overcome cybersecurity challenges—and to help ensure compliance objectives are met along the way. I've come to think of this as a framework for delivering secure availability, comprised of three major components:

- Doing what you **have** to do.
- Doing what you said you were **going to do.**
- Continuously refining and adapting to what **"good" looks like.**

Every organization is likely to develop and deploy this framework in its own unique manner, depending upon its own business goals, risk appetite, organizational strengths, and enterprise vision. But the issues within each of these three pillars are applicable to all organizations looking to ensure secure availability.

Doing what you have to do. This is where everything starts. After all, your organization must comply with the laws and regulatory obligations of the different jurisdictions where business is conducted. These include issues revolving around custodianship of information and data privacy regulations, and ensuring that you are acting responsibly with the data that others have entrusted you to safeguard. I'm sure you're thinking these are pretty fundamental, and you're right. These are table stakes, essential requirements for ensuring secure availability and meeting compliance mandates. But without meeting these baseline requirements, you might as well get ready for a regulatory assault—and a costly and damaging security incident brought on by a security breach or data loss.

Doing what you said you were going to do. This is all about a rock-solid commitment to actually following through in all ways—contractually, regulatory, internal policies, and even morally. This should be part of your organization's governance framework, jointly worked out among business leadership, IT and security teams, and legal officers. Again, the goal here is to ensure secure availability; if done right, compliance will be the byproduct. This is why your governance programs must go beyond good policies and policy management to extend to enforcement in the same way organizations enforce human resources or financial policies. Reporting must be consistent, transparent, and designed to easily flow up the organization. And, of course, policies and enforcement processes need to be communicated throughout the organization in both security awareness and targeted training programs. If you have a data loss prevention policy, but you're not educating your employees about how to label, securely share, transfer, and store data, or for how long and where, you'll run into big problems and find it extremely difficult to achieve a state of continual compliance.

Continuously refining and adapting to what "good" looks like. Fortunately, there are a number of useful and well-regarded standards for the protection of systems and digital assets, especially when it travels to and from the internet. Your CSO and IT executives undoubtedly know about the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF), a voluntary framework that provides models based on the principles of "prioritization, flex-

ibility, and repeatability." And the Center for Internet Security publishes a list of the top 20 security controls, which presents a great opportunity to identify the best value for information security investments. Certainly, business leaders need to get behind these and other applicable frameworks that help identify key security and resilience objectives, as well as corresponding metrics their organizations should consider embracing. These can also help measure the organization's ability to ensure availability and to provide a foundation for compliance.

Until fairly recently, internet engineers tended to measure availability in terms of internet access and service level agreements (SLAs). We didn't necessarily work ourselves into a frenzy because we lost corporate or residential internet connectivity for a few hours or even a day. But we've evolved in very meaningful ways in terms of how we gauge the business impact of service availability interruptions. Today, if you can't deliver uninterrupted core services to your employees, customers, and partners, you're in deep, deep trouble. So, we can't let our organizations get to the point where systemic dependencies bring down our systems and restrict our access to critical data and services. We must collaborate in order to get a fuller and higher-definition picture of risks and their impact and longer-term consequences.

In the U.S., if an organization's security program is intelligence-driven, the Cyber Security Act of 2015 makes it much easier for them to ingest and share cybersecurity indicators without the threat of antitrust violations hanging over their heads. Because attackers exploit asymmetries in ways defenders don't have the luxury of doing, they are constantly adapting their tactics and techniques; without adequate information-sharing and community collaboration, organizations may be lured into thinking that their state of security readiness and secure availability is much higher than it really is.

Steps Business Leaders and Board Members Can Take Today

Once an organization understands that enabling secure availability—and, by extension, demonstrating compliance—is a business issue rather than a technical one, it has taken the first step toward achieving that goal. And there are efficient ways for business executives to learn from the lessons and experiences of others to support those efforts.

First, keep in mind that your organization should study high-profile and particularly relevant breaches and learn how they may relate to your own situation. What vulnerabilities did the breach expose that may be relevant to your organization and operations? How did other organizations respond to mitigate the damage, both technically and from a communications perspective? What is your plan if such an incident were to impact you? What was the impact on their business operations, and how exposed are you?

Second, you must—absolutely must—have a game plan for DDoS attacks and ransomware. This is vital, because more and more organizations are being hit with these attacks every day. Why wouldn't they be? They're cheap to implement, and the bad guys are smart enough to either extort their intended victims or ask for ransoms that are small enough to be considered "nuisances" by business leaders and boards. Furthermore, your preparedness here will also enable you to better identify, protect, detect, respond, and recover from whole classes of destructive malware and other attacks, as illustrated in Figure 1, on page 169.

But how you respond when you are hit needs to be carefully planned and meticulously carried out, and that's where the

business experience and acumen of your executive leadership and board comes in very handy. They'll also engage you in some very probing question-and-answer sessions, but don't fear those—embrace them. If you've done your homework, you'll have a vital opportunity to ensure that your defense strategies are aligned with business priorities.

Third, use regulatory and governance requirements as an opportunity for more internal dialogue and game-planning. I used to cringe at the thought of quarterly disclosure filings, internal risk reporting, compliance documentation and audits, and the like. Eventually, however, I began to embrace these and other opportunities to discuss cyber risks, impending threats, impact, and preventative steps with my business colleagues and board members—from a whole of business perspective. I saw them as my chance to sound warning bells and highlight key cyber risks before something bad happened. I also saw them as a chance to provide important updates to key stakeholders about the latest changes, what we've done to ensure that our key assets remain available, and, of course, that we're still in compliance with applicable obligations.

At the end of the day, we should be worried less about passing audits and demonstrating point-in-time compliance than about the fundamentals of cybersecurity: availability, confidentiality, and integrity.

Your chief compliance officer might blanch at such heresy, but your focus on secure availability will do more than keep the regulators off your back. It will ensure you still have a business tomorrow.

Figure 1: Five phases of NIST Cyber Security Framework (CSF) 1.1
Credit: N. Hanacek/NIST

23

Why Corporate Governance Matters So Much in Cybersecurity

Paul Jackson, GCFE — Managing Director, Asia-Pacific Leader, Cyber Risk, Kroll

In the high-pitched, relentless battle against cyberattacks, much of the attention and energy has been focused on technical solutions, regulatory compliance, and balancing risks with opportunities.

What about corporate governance? What role does executive and board-level oversight play in ensuring robust cybersecurity … and what role *should* it play?

When most of us think of corporate governance, we tend to associate it with such business functions as financial integrity, hiring practices, legal and regulatory assurance, and corporate strategy. But the increasingly critical and complex issues presented by cybersecurity now have risen to the point where it must be a core component of an overarching corporate governance framework.

And that is happening not a moment too soon.

For instance, there is increasing evidence that boards are playing catch-up when it comes to prioritizing cybersecurity as a vital governance issue. A 2018 global study of more than 1,000 board members conducted by McKinsey indicated that cybersecurity was a "potential business disruption" topic on the agendas of only 37% of boards. The good news is that figure represents a nearly 50% increase in just the past two years; the bad news is that cybersecurity remains a dangerously weak area of understanding for boards in assessing its potential impact on business operations. In fact, only 9% of board-member respondents said their boards had a "very good" understanding of cybersecurity's potential for impacting business operations.[1]

Let me give you a real-world example of this disconnect. A large, Asia-based supply chain company asked our firm to do a thorough penetration test of their networks as part of what they assumed would be a routine due diligence exercise. But we discovered that an expensive monitoring solution was not achieving its intended goals and was not being properly managed. It quickly became clear that an attacker could have gained full control of the network, including full access to the CEO's system and had the potential to badly damage business partners' systems. Leadership was shocked to learn this, prompting an urgent rethinking of how to restructure cyber governance and remove reliance on the internal IT team to solve security problems.

This is why leadership, both among C-level executives and in the boardroom, has to step up in making cybersecurity

a more prominent element in corporate governance. But how?

I believe there are four major areas where corporate governance needs to evolve when it comes to cybersecurity:

- Inverting the cybersecurity leadership responsibilities.
- Adopting and "living" the right cybersecurity framework.
- Addressing the organizational structure.
- Getting smarter so business leaders can ask the right questions.

Inverting the Cybersecurity Leadership Responsibilities

One of the biggest problems is that cybersecurity has traditionally been designed with a bottom-up approach. In that model, individuals tasked with securing IT systems identified technical solutions to protect the infrastructure, applications, and data. Organizations spent untold billions of dollars on technology, only to find that it wasn't enough to stem the impact of expanded threats, increased vulnerabilities, and innovative attackers.

This brings to mind a popular adage: When every problem looks like a nail, every solution must be a hammer.

This bottom-up mindset brought about cybersecurity defense, detection, and response policies that were developed around technical tools, without considering the business needs or operational implications. Metrics were developed that told the CSO how many attacks were blocked and from what sources, while the real focus needed to be "Which attacks weren't blocked; which parts of the business were impacted; and what were the financial, legal, regulatory, and reputational costs?"

Instead, the cybersecurity governance model needs to be inverted to a top-down approach. This is the essential definition of organizational leadership:

- Understand and identify the challenges and opportunities.
- Establish priorities.
- Promote collaboration and innovation around solutions.
- Lead by example.

Leadership needs a full, transparent, and real-time understanding of the risks faced and the measures in place to protect the organization. If that information is not being clearly communicated to the C suite and the board, then leadership needs to find ways to ensure the right information is provided, typically by the CISO or CIO in today's corporate frameworks—or find someone else who will.

If implemented correctly, a top-down governance framework will eliminate most threats and provide a mature, defensible, and flexible structure for protecting sensitive data. It will also help to ensure compliance, establish good legal protections, and encourage good cybersecurity hygiene among employees, partners, and suppliers.

Adopting and "Living" the Right Security Framework

Security frameworks are important because they embrace the full set of issues necessary for good cybersecurity: business operations, legal, regulatory, risk management, and technical processes.

While there are numerous good frameworks available for leadership to evaluate—and keep in mind that all frameworks should be adapted to each organization's unique business conditions, operating procedures, and priorities—the most relevant and actionable one comes from the U.S. National Institute of Standards and Technology (NIST). This voluntary framework is the most broadly accepted and most widely implemented around the world, and has its foundation in five pillars:

- Identify the assets to be protected.
- Protect those assets with the proper safeguards.
- Detect incidents quickly, reliably, and comprehensively.
- Respond to incidents in a way that minimizes their impact.
- Recover from incidents and restore business operations as soon and as completely as possible.

There are plenty of actionable steps and best practices organizations can and should deploy in their cybersecurity governance model, such as assuring that appropriate security patches have been applied, end-of-life systems have been deactivated, and strong encryption and access control tools have been put in place and are being used. Still, those are technical solutions, most typically handled by the security and IT organizations.

The real power of the NIST model from a governance standpoint is that it creates an opportunity—or, depending on your sense of urgency—it provides a flexible framework for executives and board members to internally mandate and be used to hold business units accountable. The importance of the NIST Framework as a tool of self-assessment is that it places cybersecurity objectives in the context of the organization's overall business objectives. The framework's inherent flexibility guides business leaders and the technical management responsible for cybersecurity to focus on actions that will best position their organizations to manage their unique cyber risk, and to direct resources to areas where they can be most impactful to the business.

Addressing the Organizational Structure

It has often been said that you can learn a lot about any organization's priorities by looking at their org chart. This is becoming more and more true every day in the realm of cybersecurity governance.

Increasingly, corporate leaders are driving change by rethinking and realigning who is responsible for cybersecurity and how the role is positioned within the enterprise. For instance, the idea that physical security, internal investigations, and cybersecurity should be merged into a single organization **reporting directly to the board** is gaining in popularity, and has many advantages. Independence is an important motivation for this approach, of course, but it also facilitates a more complete approach to security that takes into account people, business functions, priorities, and technical factors.

There is little question that announcements of changes in reporting structures make people sit up and take notice. Some of that is office politics, but much of it centers on the notion of what—and who—is gaining importance within the organization.

In edition 2 of this book, there were some excellent recommendations on how to identify and hire the best possible CSO in order to keep with a vigilant governance model for cybersecurity that ties business and technical requirements. In the chapter from executive search firm Heidrick & Struggles, the authors offered some clear-headed advice:

"Boards need to exercise even more diligence than ever when determining who to hire, how to structure their roles and responsibilities, where to look to recruit them, and which tradeoffs are appropriate to make in order to land the best possible candidate."

And then Adobe CSO Brad Arkin offered helpful advice to boards and C-suite executives: Listen closely to how your cybersecurity leader talks about problems and solutions. His pragmatic takeaway: If you're getting a lot of technical jargon instead of framing the discussion around business goals, you're talking to the wrong person.

Getting Smarter So Business Leaders Can Ask the Right Questions

As has been emphasized repeatedly throughout this book, security is a business issue, not a technical one. While we need the right technology tools to identify threats, protect against them, and remediate their impact, cybersecurity practices and policies must be planned, measured, and governed against business benchmarks.

Doing that requires strong, vocal, visible, and constant support from business leaders and the board. But it also necessitates that top management and board members put more energy and resources against expanding their own knowledge about cybersecurity's impact on their business.

Remember: You can't get the right answers if you ask the wrong questions. Or, in the context of this chapter, you can't govern if you don't know what you're supposed to be governing.

Now, no one is suggesting that the CFO or the head of marketing go back to school to get an advanced degree in cybersecurity, or that every board member have to pass a Security+ certification test. But the days of leaving cybersecurity responsibility to the technical people are long past. Regulations and legislation have changed the accountability quotient, and as we've seen too many times, an organization's very reputation—which has been carefully honed and crafted over decades with untold sums of money—can unravel after a cybersecurity glitch.

Some people have gone as far as to recommend that every board should have at least one member with extensive cybersecurity expertise in order to "keep the CSO honest." That concept may have some merit, but it still involves most board members and executive leaders turning to the "one wise man or woman in the room."

Business leaders and board members don't simply default to the CFO when a financial crisis hits, and they don't just assume the chief legal officer or outside counsel has everything covered when an embarrassing lawsuit pops up. In those and other scenarios, executives and board members jump in with both feet because, among other reasons, corporate governance demands that they do.

The same is now true with cybersecurity.

One of the important ways business leaders can get smarter and ask better questions is to have a commonly used prism of business issues through which cybersecurity issues can be analyzed, discussed, and acted on. For instance, discussions with the CSO on topics such as distributed denial-of-service attacks should be centered on how the business was impacted in areas such as downtime, lost productivity, revenue, and profit impact, and whether cybersecurity investment priorities should be re-examined.

Of course, this is a two-way street. Not only do board members and business leaders need to take steps to better educate them on cyber issues, but CSOs and other technical leaders need to re-imagine and re-engineer how and what they present to the business side. Things that have often been taken for granted, such as how a CSO's PowerPoint presentations look or why an organization is changing its policy for using public cloud services, must always be framed in a business perspective—ideally one that aligns with the organization's core values and business priorities.

What Boards Should Do Now

What should boards be doing in order to receive regular, appropriate security metrics around monitoring and detection?

First, the board needs to understand what cyber threats exist inside their organizations. A good starting point would be to obtain a report on current cyber threats

impacting their industry and some recommended safeguards. Importantly, a search of any data on the Dark Web—passwords, personal data, confidential documents, or financial documents—that have already been exposed should be conducted by a reliable third party, and mitigation controls put in place.

Second, keep in mind that employees are almost always targeted for attacks. Board members need to receive regular updates on the level of staff security awareness through steps like controlled phishing exercises. The board also must ask if management is fully committed to this kind of organizational cyber hygiene in order to emphasize the importance of good security habits.

Third, internal and external resources should be deployed to regularly hunt for threats already on the networks but undetected, rather than simply relying on metrics around detected security events. Experience has shown us that attackers are often already inside networks for many months before real damage takes place. These hunts should be based on actionable intelligence and real-world knowledge of current threats.

Conclusion

Corporate governance has changed a lot in recent years, driven by such issues as increased regulatory oversight, more active and involved board members, and a need to apply healthy doses of both skepticism and support in an increasingly complex business environment.

And cybersecurity may be the single biggest thing to reshape corporate governance in decades.

Unfortunately, we still don't have enough clarity for actionable advice that corporate leaders can implement from the word go to help ensure the security of their organization and its data. But taking a more business-centric, inclusive, top-down approach to cybersecurity corporate governance will take us a long way toward achieving our respective organizations' goals. When cybersecurity is considered as a business issue, rather than isolated as a technical problem that has to be solved by technical people using technical tools, we will have a much greater chance for success.

---

[1] "A time for boards to act," McKinsey, March 2018.

24

Compliance Is Not a Cybersecurity Strategy

Mark Gosling — Vice President, Internal Audit, Palo Alto Networks

In many boardrooms around the world, members are receiving serious presentations from their chief information security officers about the status of their efforts against a whole host of security and privacy regulatory mandates that have increasingly significant potential fines. Board members are undoubtedly taking their governance responsibilities seriously and are likely asking tough questions to determine how big of a regulatory risk their organizations may be facing and if they are on track to demonstrate compliance.

But while compliance is important, it should not overshadow the board's focus on the greater issue of managing cybersecurity risk.

Clearly, this is not an either/or scenario between risk and compliance. Organizations and their boards need to pay strict attention to both issues. The most successful organizations are the ones that understand the tight relationship between the two, even in the face of mounting cyber threats, and act accordingly regarding budgets, manpower, and executive focus.

Compliance and security are not mutually exclusive; far from it, in fact. Ideally, compliance can document and provide metrics that reflect an organization's cybersecurity risk management approach. If you take the necessary steps to safeguard your most critical data across your networks, cloud environment(s), and endpoints, and regularly train your employees to practice good security hygiene, your organization will be well-positioned for compliance.

That's why it's important to remember that, in an ideal scenario, compliance is a **floor** for your organization's cybersecurity efforts, not a **ceiling.**

As important as it is for organizations to demonstrate compliance with regulatory mandates, it's not the be-all and end-all for executives. And board members should not become distracted by the latest new thing in the regulatory game—nor should they view cybersecurity risk as an unsurmountable threat fueled by the latest breach headlines.

Instead, board members should help their organizations focus on the big picture of cybersecurity—reducing risk, increasing business opportunity, and using precious resources wisely and strategically.

Cyber risk discussions now take up more time, energy, and attention for board members. And, with a deluge of information about cyber risk and regulatory demands out there, it can be hard to

make sense of it all. However, the common goal and focus for all board members, organizations, employees, customers, partners, government agencies, and regulatory bodies should be straightforward: Reduce cyber risk. Reducing cyber risk is too often rooted in either the anecdotal lessons from public breaches or the penalties associated with compliance and legal issues. A sound approach is more about ensuring the long-term vitality, competitiveness, and solid financial footing of the organization—and perhaps using your organization's security as a competitive differentiator and a mechanism to ensure the trust of your customers.

In an Era of Hyper Compliance, Don't Get Distracted From the Real Goal

Around the globe, new regulations designed to address digital challenges—from protecting private information to ensuring that critical infrastructure is not compromised—are consuming an increasing amount of attention. Business and technical decision makers, with the support and guidance of their boards, have devoted significant financial and personnel resources to shape these policies, avoid unintended consequences, and demonstrate compliance.

But organizations that focus myopically on regulations, rather than on the bigger issue of cyber risk reduction, are going to be hard-pressed to align their security practices with their core business priorities.

While no one wants to be hit with fines or have to spend hours explaining and negotiating with regulators after a data breach, it is essential for organizations to remain true to their business priorities first. And that's a critical role played by board members.

Instead of asking, "Did we pass that PCI DSS audit?", board members should ask questions that emphasize whether critical business goals could be impacted by security problems.

- What types of data exfiltration could include our latest intellectual property?
- How are we ensuring that customer records are not stolen, tampered with, or erased?
- Can we be certain that our email messages with that potential acquisition partner do not appear on the screens of our top competitor?

Let's also keep in mind that even the best-intentioned compliance mandates can have very real, and very unattractive, consequences if not enveloped by a broader cyber risk reduction framework.

New regulations have the potential to result in confusion, conflict, and inefficiencies that actually may increase cyber risk, not reduce it, by diverting valuable resources from threat detection and prevention toward reporting and accounting. Take, for example, the lessons learned from the implementation of the original U.S. Federal Information Security Management Act of 2002. This regulation required U.S. federal agencies to produce hard-copy binders on the status of the security of their networks, essentially diverting scarce IT and security personnel and resources away from actually securing those networks, in favor of recordkeeping. This is really more of a "checkbox" regulation, rather than a way for organizations' networks to be truly secure—another example of being compliant, but not necessarily secure.

This is a vital lesson learned for more effectively identifying and implementing common goals in cyber risk reduction and threat prevention among all parties—boards, executives, customers, trading partners, industry groups, regulators, and governments. Because being "secure" is not a static end-state

that lends itself to inflexible compliance checklists. It requires a constant evaluation of risk, relative to a rapidly evolving cyber threat landscape.

As you read Part 2 of *Navigating the Digital Age*, we encourage you to pay attention to the words of Verisign Executive Vice President Danny McPherson. Danny has done a great job of putting an exclamation point on this issue:

> *"...compliance is not—repeat, not—your goal. Or, at least it should not be the key focus of your cybersecurity program. And let me tell you why:*
>
> *Being compliant is not the same as being secure. "*

Major Board Implications

Certainly, board members must continue to ask tough questions of all their senior executives, including but not exclusively, their CISO and CIO. Specifically, board members' questions on cybersecurity must rapidly swing from, "Are we compliant?" to "What is our risk profile?"

This means that board members need to move from a somewhat passive, detached approach to security oversight to one that is more proactive. Take the results from a recent study conducted by the National Association of Corporate Directors (NACD) about cyber risk. Following were the top four answers board members gave to the question, "Which of the following cyber risk oversight practices has the board performed over the last 12 months?"

- Reviewed the company's current approach to protecting its most critical data assets (82%)
- Reviewed the technology infrastructure used to protect the company's most critical data assets (74%)
- Communicated with management about the types of cyber risk information the board requires (70%)
- Reviewed the company's response plan in the case of a breach (61%)

"Review" and "communicate," as important as they are, do not go far enough to identify and act on the best ways to reduce cyber risk, especially with a prevention-first strategy. Instead, boards need to become both more intimately knowledgeable in how executives charged with reducing cyber risk are identifying threats before they do damage and in becoming true partners in helping those executives fortify their defense plans.

This also means that board members need to accelerate their own education on cyber risks—both in general and as it specifically pertains to their organization. For instance, in the NACD survey of directors, 73% of respondents said their boards had "some knowledge" of cyber security risks. Clearly, in order to fulfill both their fiduciary responsibility as directors and to make good on their requirement to understand and support their executives' risk prevention, they need to become even more conversant on cyber risks and in identifying the right solution specifically tailored for the unique requirements of their organization.

Whether that means utilizing outside cyber security consultants as board advisors, putting a cyber risk specialist on the board, or taking some other steps, is obviously the board's call. But it's a call that needs to be made. After all, a study conducted by NASDAQ pointed out that 91% of board members are unable to interpret a cybersecurity report.[1]

And that is a big problem.

Board Oversight Questions

To facilitate a more robust and effective strategic plan for reducing cyber risk, board members need to ask a new set of questions designed to provide a deeper understanding of current and potential risk levels and a stronger basis for tak-

ing action to protect against current and emerging threats.

- **Which people, processes, and technologies are currently being used to defend your network?** Your CIO and CISO also must be able to tell you what your organization is already doing about spotting risks before they are weaponized, and where they believe the next attacks are likely to occur. This information needs to be aligned with a thoughtful, open discussion on how, where, and when resources are being deployed against the threat identification and protection processes.
- **What additional resources are needed in people, processes, and technologies in order to limit risk?** Of course, no one is going to give the CISO a blank check, so ask tough questions to determine where the greatest financial efficiencies can be gained by making smarter—and not necessarily bigger—investments.
- **Which threat intelligence services is the organization using, and how are they performing?** It's vitally important to know what demonstrable impact those services are making to help the organization spot risks and protect against them before they pierce its defenses.
- **How do our organization's security training programs need to change to reflect the new realities of cyber risk?** Should existing education programs for users, partners, and even customers be modernized, overhauled, or scrapped entirely in favor of approaches that better reflect the coming threats?
- **Can your legal and compliance officers identify all existing regulations that apply to cyber and information security, and do they understand which new mandates are under consideration or in development?** How will those emerging requirements impact your organization's threat profile? And, should your representatives become more involved in the process of framing those mandates in order to ensure that they really do help reduce risk and not become just another checkmark on the compliance "to do" list?
- **Are representatives from the security team included in every business planning meeting that's being held?** This is an extremely important mindset shift for organizations: Boards need to be in front of this transformation and move from "security as an afterthought" to "secure by design." This means everything from new product development and supply chain management to marketing programs and customer retention—not just compliance or data governance.
- **What is your plan to keep up with the pace of change?** Ultimately this is one of the most important questions. By anticipating change, you will be better prepared to understand the impact on your organization, infrastructure, and the associated risks, which will directly affect your ability to safely and quickly adapt to change.

Conclusion

One of the biggest things board members can do to ensure that their organizations' cybersecurity resources are deployed in the most effective and efficient manner is to remember that unyielding, relentless attention to aligning cyber risk reduction with business priorities will go a long way toward achieving compliance goals.

Board members who help their executives focus on reducing vulnerabilities

and properly balancing risk with opportunity will have the biggest impact on their organizations' successes—but only if they remember that compliance is a byproduct of that effort, not the ultimate goal.

This chapter was adapted from "How Can Board Members Help Turn Cyber Risk Reduction from a Goal into a Reality," published in January 2018 in NACD Directorship, the official publication of the National Association of Corporate Directors.

---

[1] "Grading global boards of directors on cybersecurity," Harvard Law School Forum on Corporate Governance and Financial Regulation, 2016.

PART 3
Make Sure You're Covered Today

Part 3 – Introductions

25

Welcome to the Frontlines of Business and Cybersecurity

Pablo Emilio Tamez López — Chief Information Security Officer, Tecnológico de Monterrey

Digital transformation. The Internet of Things. Big data analytics. Cloud computing. Artificial intelligence. Machine learning. Somehow, we have come to think of these innovations as the future, the defining technologies of the next iteration of business, and the foundation for what the World Economic Forum aptly describes as the Fourth Industrial Revolution.

Guess what? The future is now.

Every one of those technologies is in practical use today. Type a search on Google, and you'll immediately see ads related to that search. It happens automatically—you might even say surreptitiously. All of the underlying technologies and business models that are transforming our world act like an invisible hand guiding almost everything we do in the Digital Age.

But take a second to look at it from the other side. From the perspective of our adversaries, those who would harm us for profit, geopolitical warfare, ego, or even just to create mischief. For them, digital transformation, the IoT, and big data analytics mean a greater attack surface. For them, cloud computing, AI, and machine learning are simply more weapons to use against us—and more sophisticated ones at that.

The situation has the potential to become more precarious in the near future, unless we act now, as leaders, to address it. Consumers and enterprises are spending more and more on IoT and mobile devices. The growth is exponential—with all of these connected devices generating information and, on the other hand, adding incremental attack surfaces. CISOs must understand this evolving risk environment, how to handle this data, and how to protect their assets. So, it is very important to implement adaptive and scalable technologies for this growing attack surface, either in the cloud or in the physical data center.

Now's the Time to Act

I share this viewpoint not to create fear or cause alarm, but to make sure we are all aware of today's reality and urgency. The audience for this book, *Navigating the Digital Age, Third Edition*, represents leaders in business, academia, and government who are not only directly affected by cybercrime, but are empowered to do something about it.

In Part 1 of this treatise, we focused on the future. In Part 2, we focused on lessons learned from the recent past and today's world. In Part 3, we focus on

applying those lessons—what is happening now, how we can address today's rapidly evolving threat landscape, and, perhaps most importantly, how we can prepare for what is coming next.

Business leaders and board members are in a unique position, approving investments, guiding the vision for digital transformation, striving to build environments where innovation and opportunity can flourish. That also means being at the frontlines of cybersecurity.

You don't have to be a technology wizard to understand the vital role that cybersecurity plays in business today—or to provide leadership for your organization. In fact, as many of our authors express, you *must* provide leadership. If not you, then who?

For too long, it seems, our adversaries have been one step ahead of us. Now is the time to reverse that trend and put *them* on the defensive, make it more difficult, costly, and risky for *them* to attack *our* data, privacy, elections, infrastructure, business operations, or wherever else they may seek to expose vulnerabilities.

Making Sure We Are Covered Today—and Tomorrow

How do we do that? What can we do now to make sure we're covered today and also build the right foundations—in people, processes, and technologies—to give us the best chance of protecting our future and fulfilling the promise of the Fourth Industrial Revolution?

Many of the answers to these profound, provocative, and paramount questions are contained in the chapters ahead. In Part 3 of *Navigating the Digital Age, Third Edition,* we hear from leaders across the cybersecurity spectrum—business executives, government officials, legal experts, technologists, chief information security officers, and others.

Each author shares his or her individual experiences to collectively create a compelling guide designed to spur action, communication, and innovation. The hope is that organizations of all sizes, locations, and industries can leverage the wisdom and practical advice contained in Part 3 to become better prepared to successfully navigate the challenges of the Digital Age. Some of the ideas that are sure to resonate include:

- **Trust:** How do we ensure that trust is no longer an issue for users?
- **Communications:** How do we get business and cybersecurity leaders on the same page, speaking the same language?
- **Regulations:** How do businesses work cohesively with regulators?
- **Technology:** How can the good guys leverage technology innovation to thwart the bad guys?
- **Preparation:** How can we prepare for attacks and limit the damage if a successful attack takes place?
- **Business enablement:** How can we transform cybersecurity from business risk to business advantage?

Conclusion

We've come a long way in a short period of time to reach the critical juncture in the Digital Age that is now before us. Many of the organizations that are using connected digital technologies to redefine industries weren't even in business as recently as 10 years ago. Now some have valuations in the billions of dollars.

At a time when our world is moving so quickly, when digital technology is transforming our lives and work, we must ensure that cybersecurity does not stop our progress. That's why today, this moment, is a critical time in our journey. If we are to move forward safely in the Digital Age, we must make sure we are covered today. When it comes to addressing the challenges of cybersecurity, *our* future is now.

26

Preparing for the Coming Technology Tsunami

William Dixon — Head of Centre for Cybersecurity, World Economic Forum

Greg Day — Vice President and Chief Security Officer, EMEA, Palo Alto Networks

The Digital Age is on the precipice of dramatic new horizons. Just ahead, we can visualize the impact of technologies such as quantum computing, 5G, artificial intelligence (AI), edge computing, and the Internet of Things (IoT). In some cases, like IoT and AI, we already feel their presence in our everyday lives.

Business leaders need to prepare for these new technological marvels, because when they do arrive in full force their impact will be immediate, transformative, and irreversible. It's not just that the Digital Age will never be the same; the world will never be the same.

How do we prepare for something that we know will be profound, yet the precise details of how, when, and why will not be fully evident until we are actually living through the experience?

In a paradoxical way, COVID-19 may be providing a sense of what might be in store as far as unanticipated—yet urgent—pressures being suddenly thrust upon business, IT, and cybersecurity leaders.

Lessons From COVID

With COVID, no one knew that there would be a worldwide pandemic in the early spring of 2020. Yet some companies were better prepared than others, particularly when it came to adjusting to remote work and providing secure, productive connections at unprecedented speed and scale.

While these companies didn't plan for a pandemic, they planned for something. They leveraged modern technologies such as cloud computing, software-defined wide-area networks (SD-WAN), machine learning, AI, Zero Trust, and shared threat intelligence.

They modernized their Security Operations Centers (SOCs) with extensive automation, machine learning, and artificial intelligence. They invested in their people, with cyber training, awareness, and practice. The most progressive companies-built cybersecurity into their cultures so when the unexpected arrived, they could more easily and fluidly adapt to changing work forces, supply chains, and business models.

Why were these companies better prepared? They recognized just how dependent they were becoming on digital processes, both directly and through their supply chains. They saw the need to build much stronger resilience strategies around this.

As we brace for the next wave of paradigm-shifting technology advances, we can take at least one critical lesson from COVID: During a time of rapid change, cybersecurity is one of our most potentially disruptive and dangerous vulnerabilities, and one we must address before the ground beneath us begins to quiver and shift.

The Next Technological Wave

Fortunately, unlike with COVID, we can look to the horizon and see the potential impact of quantum computing, 5G, AI, edge computing, and the like. When they fully arrive, no one can claim that there hasn't been proper advance warning.

The critical questions are: How can we prepare for exponential change? How can we embrace innovation and potential business disruption? And, perhaps most relevant to those of us responsible for navigating the Digital Age, how can we make cybersecurity a facilitator rather than an inhibitor?

Just to set the stage on what is coming:

- **Quantum computing** represents a quantum leap forward in computing power and performance. It is still relatively early in its development, yet McKinsey has predicted its market value could reach $1 trillion by 2035.[1] New quantum computing security models promote the safe adoption of the technology and also ensure that issues over security don't act as a blocker to unlocking its value.[2]
- **5G** is critical to realizing the full potential of the Fourth Industrial Revolution because it offers five key functional drivers: superfast broadband; ultra-reliable low latency communication; massive machine-type communications; high reliability/availability, and efficient energy usage. Together, these defining features will transform many sectors, such as manufacturing, transportation, public services, and health, as described by the World Economic Forum (WEF).[3]
- **AI** investments are expected to double between 2020 and 2024, surpassing $110 billion, according to IDC.[4] Corporate leaders will be required to identify the specific benefits AI can bring to their businesses, as well as the concerns about the need to design, develop, and deploy it responsibly. "Striking the right balance will lead to sustainable businesses in the Fourth Industrial Revolution, but failing to design, develop, and use AI responsibly can bring damage to brand value and risk customer backlash," per the WEF.[5]

There's more. The Internet of Things is projected to reach 35 billion connected devices in 2021.[6] By 2022, edge computing will account for more than 50% of enterprise-generated data.[7] All of these technology waves are simultaneous, interconnected, and coming quickly on top of an environment that has already been forever altered by COVID.

The impact on areas such as supply chain, digital transformation, and cybersecurity will be dramatic. For all of the advances they offer, quantum computers also create challenges in our ability to encrypt information and exchange it securely. 5G allows for incredibly complex supply chains, challenging the level of visibility needed to understand and manage risk. We are already seeing businesses struggle to define who is accountable for what. With AI, businesses will be challenged to understand enough of the AI algorithms to have confidence in using them. It is likely that many will not

even develop their own AI algorithms and instead will rely on third parties.

Perhaps you see why we compared these challenges to a tsunami.

Start Asking Questions

Let's start with a simple premise. No business leader can afford to ignore a single one of these technologies. They are in your future, whether you like it or not, otherwise you have no future. Given the changes in the global economy, and the increased dependency on connected digital technologies, organizations must embrace digital transformation to remain viable in the near term and beyond.

But just because these technologies are inevitable, doesn't mean they are predictable, nor will every organization in every industry embrace them at the same time, or to the same degree. To prepare your company, it is important to not just understand the benefits of these technologies, but to also understand their potential risks—of which cybersecurity may be the most profound and ultimately challenging.

Technology is moving quickly and powerfully, it is scaling exponentially, all while there is a skills gap within IT and especially within cybersecurity. Given these challenges, there is growing potential for security to slip between the cracks when it comes to critical areas such as visibility, responsibility, scale, and governance.

For example: With IoT, there will be sensors virtually everywhere. Some may cost a dollar or two and come with no cybersecurity protections. But they may connect to a 5G network that may be connected to thousands of other devices, home, and business. Who is responsible for security? Is it the provider of the $1 device? The telecom service provider? Ultimately, if one of these devices causes a security breach, it doesn't matter who is at fault; if it impacts your company, then you will pay the price.

Business leaders and board members are starting to ask these types of questions, particularly now, with so many so many connected things in the home today; refrigerators, smart heating, smart home alarms, smart EDA, all potentially on the same corporate networks as business-critical servers and applications.

5G will represent a dramatic expansion of innovative use cases, many of which will have more real-world impact and criticality than current business processes. But this new level of powerful, fast, ubiquitous connectivity can also heighten risk, thereby raising the stakes on the importance of security.

For instance, think about issues around national security, or tele-surgery, or other life-or-death use cases. Business leaders are already thinking about issues like these, and they are concerned: An IoT survey by Palo Alto Networks revealed that more than 40% of IT business decision-makers said they need to make a lot of improvements in how they handle IoT security, and an additional 17% said a complete overhaul is required.[8]

Here's another real-world example: Self-driving cars and their impact on their broader ecosystems, such as insurance. In addition to the operational security challenges inherent in a self-driving vehicle, there are related issues to consider. If there is an accident, who is responsible? Is it the manufacturer of the car? After all, there was no driver. Or, perhaps the owner of the car didn't maintain it properly. And, does owning a self-driving car mean that individuals will have to acquire more personal liability insurance?

With technology platforms and supply chains as complex as the ones for self-driving cars, proving fault or transferring liability becomes increasingly difficult due to the number of data points and sensors, as well as issues with data processing, connectivity, latency, and cyber-

security. Will the interrelated industries get together to the point where they can define who owns which challenges—the manufacturer of the car, the owner, the service provider—and thus the responsibility if something goes wrong?

Steps to Take

What actions can business and technology leaders take now, individually, and collectively as a community, to make sure we are not looking back five years from now and wishing we had been more prescient and action-oriented?

One important step is to take the time to understand the potential new use cases, such as the example of self-driving cars, or the risk of billions of $1 sensors connected to data and systems that desperately need protection. Within each of these new use cases, try to identify what the ecosystem looks like and how the supply chain will work. Where can businesses take individual action? Where is collective action required? Where do regulatory bodies and government agencies fit in? How about industry coalitions, or regulators, such as in healthcare, retail, or financial services?

Another key step is to recognize that the sharing of information is essential to empowering innovation. The cybersecurity industry has been progressive in this area, with initiatives such as the Cyber Threat Alliance, as well as the World Economic Forum's Centre for Cybersecurity. As a community, we do a good job of sharing threats, threat indicators, and mitigations.

Where industry and governments need to improve is in sharing information across country borders at government levels and across industries. With more complex supply chains that interact at many more points, with a much larger and diverse attack surface, this kind of collaboration and sharing needs to happen more often. Business enterprises have shared values and, in an environment of multi-stakeholder capitalism, the ability to deliver safe and secure services must be placed above the tactical concerns of getting a leg up on the competition.

What else? Here are a few ideas:

- **Assess Your Cybersecurity Posture:** Take the time to identify operational deficiencies in your own organization's cybersecurity postures. At the very least start with an understanding of the potential risks before you embrace any new technology or any digitally transformative initiative. Does your organization have access to the right tools, governance, technologies, processes, and people? Are you taking advantage of cloud, automation, AI, and machine learning? Most organizations have processes in place to do this, but they don't do it often enough, especially with the move to the cloud. Organizations should begin thinking about real-time assessments, rather than annual or bi-annual, assessments. Also, focus on quantifying and measuring how technical risks impact business risks.
- **Emphasize Visibility:** If you don't know where sensors are located, what they do, or the business value they can deliver, you may not connect them to risk, or worse, you may not understand or evaluate the risk. 5G, IoT, the Industrial Internet of Things, and operational technology add complexity around the volume and diversity of what is connected and, importantly, who is responsible for what. To understand the boundaries of responsibilities for any new 5G-enabled business process, you need to visualize that process from end-to-end. Visibility is key for effective governance and risk management. Challenge your IT and cybersecurity teams to provide

regular updates on what is connecting to your network and who is responsible for securing it.

- **Participate in the Ecosystem:** Each organization should commit to widely sharing information—not just information about threats, but successful means of stopping and defending against threats. This includes participating in organizations such as the National Institute of Standards and Technology (NIST), the WEF, and others. One of the key initiatives of the WEF is to promote the concept of a "multi-stakeholder ecosystem," which includes working with peers/competitors. It also means working closely with government and law environment agencies on prevention, education, and regulation. Business leaders need to encourage your organization and supply chain to be an active participant in the broader cybersecurity ecosystem, or your organization will risk being an island, difficult to protect, and defend.
- **Transform Cybersecurity Governance:** As a community, build in more cybersecurity capability and assurance wherever possible, but with the recognition that in some areas there may be no guarantees within your control. For each organization, whether a government agency, service provider, or enterprise, there will always be parts of the ecosystem you can control and parts you can't. The key is being able to define exactly who is accountable for what risks both inside and outside the company, and across the broader supply chain and ecosystem. It may require new ways of defining and managing governance. For example, does it mean you have to get a license to participate, based on a mutually agreed-upon set of ground rules? Does it mean new types of governance models that offer some level of security assurance for your part in the broader ecosystem? Tough questions, but it is incumbent to start addressing them now.
- **Plan Time to Ensure Security by Design:** The pressure to adopt new technology will be intense. Time is a great driver for change; however, you must consider how you do it safely, otherwise you may transform digitally at the cost of prosperity. We've seen projects move quickly from skunk works to production without proper security vetting, sometimes to disastrous results. As a business, there is pressure to move at the speed of your market. To do so, security must be involved from day one. In the European Union, we refer to this as "security by design." The point is that in competitive markets, slowing down the process for cybersecurity is unlikely to happen—but if security is engaged from Day One it shouldn't need extra time—it's just included during the main go-to-market process. Not planning the time to include security by design adds unnecessary risks. If you launch a product or service without the proper security protections, you start behind the curve and it becomes very hard to catch up. You must also include planning for the skills gap across IT and in cybersecurity. You will need tech-savvy people, but you also have to take the time to figure out where you can leverage technology for automation to fill the skills gaps.

In the Digital Age, the march of progress is inevitable. It is also fast and furious, particularly now, with a coming confluence of interconnected technology innovations piling on top of an unex-

pected transformation of the workforce.

It may feel overwhelming. The opportunity, however, is to not be overwhelmed but to be strategic. By building a cybersecurity foundation that can respond to and withstand change, your organization can leverage cybersecurity as a facilitator for innovation and transformation. Now is the time to get moving.

---

1 "McKinsey Forecasts Quantum Computing Market Could Reach $1 trillion by 2035," The Quantum Daily, 2020.

2 "We Need to Build a Quantum Security Coalition. Here's Why," World Economic Forum, 2020.

3 "The Impact of 5G: Creating New Value across Industries and Society," World Economic Forum, 2020.

4 "Worldwide Spending on Artificial Intelligence Is Expected to Double in Four Years, Reaching $110 Billion in 2024, According to New IDC Spending Guide," IDC, 2020.

5 "Empowering AI Leadership," World Economic Forum, 2020.

6 "How Many IoT Devices Are There in 2020? [All You Need To Know]," TechJury, 2020.

7 "How to Overcome Four Major Challenges in Edge Computing," Stratus, 2020.

8 "How Connected Teddy Bears, Coffee Makers and Connected Cars are Challenging Security Teams," Palo Alto Networks, 2020.

Language

27

How to Articulate the Business Value of Cybersecurity

Mark Rasch — Cybersecurity and Privacy Attorney

Every aspect of business today has an IT security component. Every business relationship, product, hiring decision, and marketing program. Every customer interaction, communication, product design, and executive decision. Keep going: supply chain management, manufacturing, distribution, customer service. And more: finance, human resources, insurance, product safety, worker safety, and employee collaboration.

In fact, anyone reading this book would be hard-pressed to come up with a single business activity that is not, in some vital way, connected to a computer or computer network—and, therefore, to cybersecurity.

Yet, in far too many cases, we think of cybersecurity the same way a compliance officer sees cybersecurity—as a necessary evil. General counsel sees it as a cost associated with contractual or other compliance. Chief risk officers may take a risk-based approach to cybersecurity spending. Those involved in insurance or loss prevention may see cybersecurity and its related concepts of data protection and privacy protection as a potential loss to be managed.

All of these approaches lead to inadequate attention to resources and management for cybersecurity. If the goal of cybersecurity is simply to prevent a reportable breach of personal data, then a company will only likely do the bare minimum to prevent or mitigate such a breach. If the goal is merely to comply with a legal or regulatory standard, then we will do no more than necessary to say that we have, in good faith, complied.

In the competition for scarce corporate or government resources—money, technology, people, and attention—we still fail to think of cybersecurity in terms of how we can use it to empower and differentiate the business. And we still tend to judge our chief information security officers (CISOs) and other security professionals based not on how well they've propelled the business forward, but on how many phishing attacks they've deflected.

Something's got to give. We have to shift our perspective and make sure we are talking and thinking about cybersecurity in a language that ties into the goals of the business: profitability, customer retention, corporate culture, brand reputation, and product innovation. And we have to create new ways of measuring the effectiveness of our cybersecurity teams. When you look at the concept

of cybersecurity strictly through the lens of preventing harm, it will only get you so far. It's not that risk mitigation is a bad thing. But when it comes to cybersecurity, it can't be the only thing.

What can we do to change the language, adapt the cybersecurity culture, and shift our perspective? How can we modernize the way we look at cybersecurity to appropriately address today's rapidly changing world? I thought you would never ask.

Where We've Come from; Where We're Going

Compare the workplace of the 1960s with that of the 2010s. Think *Mad Men,* the U.S. television series that faithfully depicts the former era. Lots of low-wage, moderately trained workers moving mail, typing, filing, taking stenography. Pools of secretaries, rows of clerks, people in the mailroom. Fast forward to today. Those jobs are all gone.

You now have IT and security professionals who have, in effect, replaced those people. IT director, CISO, CIO; these are all jobs that didn't exist in the 1960s. Instead of 20 secretaries and 30 clerks making low wages, we now have a handful of people making higher wages. Only, we're far more heavily dependent on them—and the technologies they provide for us.

But this progress has resulted in what could be called "tyranny of the technologists," wherein technology becomes our greatest asset and our greatest potential liability. The goal of computer security is not to secure computers; securing computers is easy—unplug them and lock them up. The goal of security is information security as part of overall information management. And the goal of information management is business enablement.

If you manufacture widgets, you need IT for everything, from payroll and internal communications to business process flow, supply chain management, manufacturing automation, marketing, sales, HR, recruiting, and customer interface. Rather than asking how infosec can ensure compliance, CISOs need to ask how responsible security practices can enable new efficiencies, products, services, and customers.

The CISO needs to align metrics and goals with those of the core business. Thus, the CISO can show how an effective VPN solution empowers telecommuting, which reduces downtime and promotes efficiency and—guess what—sells more widgets. A secure virtualization platform enables the mobile workforce and customers to access their data, which promotes customer satisfaction and—wait for it—sells widgets. A secure payment system permits online ordering and—you guessed it—sells widgets. Security empowers sales, promotes efficiencies, and enables business processes that enhance products, cut costs, and, oh yeah, also ensures compliance and risk reduction. But mostly, it sells widgets.

With technology embedded in your business, you can adopt new business models. You can have a third of your workforce working from home and still maintain a critical mass of workers, social engagement, and collaboration. You can provide dedicated service to customers at any time from any location in the world. You can connect your supply chains in a constant loop of real-time information and advanced analytics. You can do virtually anything you can imagine, as we've seen with companies such as Uber and Airbnb, which have leveraged connected technologies to disrupt decades-old business models.

In reality, however, you can only do those things if the connections and flow of data are secure. That means cybersecurity becomes an enabler—of collaboration, efficiency, productivity, agility, cost

reduction, product development, innovation. Security enables the organization to drive revenue and profits through the exploitation of data in new ways. Back in the *Mad Men* days, once you made the sale, the hard work was done. Now, the sale is just the start of the relationship. Data collection, storage, and analytics become critically important—as does security.

Aligning Cybersecurity With Business Objectives

If the end game is to align cybersecurity strategies and investments with business objectives, most companies are still discovering how to make the leap. Part of the challenge has to do with the metrics we use to measure CISO performance.

This becomes a problem when we build our budgets based on hardware as opposed to value; when we measure cybersecurity performance on criteria that has nothing to do with the actual risk mitigated or the overall value provided to the business. Have we done a good job if we prevent 98% of the attacks, but the 2% we miss are devastating? If we stop 90%, but the 10% have zero impact, have we done a bad job?

When it comes to budgeting and metrics for cybersecurity, we often fail to place the right value on the things we value most highly as a business. Part of the problem here is the "stovepiping" of data security: too many, or more accurately, too many different, chiefs. We have a chief privacy officer, chief information officer, chief information security officer, chief risk officer, chief executive officer, etc. Each "chief" has his or her own domain to protect—often with overlapping responsibilities. Each chief believes that her problems or solutions are the most critical for the company.

The CEO—and ultimately the board of directors—has to balance these competing concerns. Recent SEC guidance in the U.S. has suggested that cybersecurity needs to be a primary concern of the board of directors of a company, and that those responsible for cybersecurity should report directly (or more directly) to the CEO and the board, who should be periodically briefed on the company's security status.

But before such briefings are going to be effective, the CISO and security personnel need to learn how to speak the language of the CEO and board—or educate them on speaking the language of the security personnel.

As a community, we still haven't figured out how to value certain essential aspects of our businesses, particularly when it comes to cybersecurity. I would suggest that most organizations are comfortable placing a value on tasks such as data collection, processing, and analytics, but struggle to place a value on something more esoteric, such as privacy.

We don't value privacy because we don't place a value on privacy. Sure, we can assess the cost of a data breach. We can say a breach will cost $15 per record, that we have 100,000 records, and that therefore a breach will cost $1.5 million. This helps, but it is imperfect.

We need to develop the right metrics for valuing privacy, because if we don't put a dollar value on it, it means we don't value protecting it. We measure privacy based on the cost of not protecting it, rather than the value of it intrinsically. Privacy protection—real and abiding privacy protection—promotes confidence. Confidence promotes trust. Trust promotes sales. And sales promotes the CISO.

Focusing on Business Enablement

Outside the cybersecurity realm, business enablement is typically a factor in just about every decision. Say the company is considering opening a plant in a country where it has never before done busi-

ness. Management will address a series of questions: What are the risks? Is the government stable? Is there sufficient electricity and transportation? Is there a large enough pool of workers? How will this decision affect our profitability, revenue growth, customer relationships, and partner relationships?

Cybersecurity must be included in each of those discussions. Does the country have cybersecurity laws? Does it prosecute cybercriminals? What are the data retention requirements? Can we safely do business on the internet? Can we hire cybersecurity professionals in the region? Is there a legal structure that will protect the confidentiality of our data? Will law enforcement work with us if we are attacked? Can we get appropriate insurance? Are our partners reliable, and will they protect our data?

We should go a step further and attach a cybersecurity component to *everything* that gives the company value. When we develop a new product, we have to embed decisions about what data is collected, how that data flows through the service, how it is secured and monitored, how we will manage secure payments, and what the risks are associated with data loss.

The same is true with privacy. We treat security and privacy as separate concerns at our own peril. While you can be secure without protecting privacy, (you can securely violate privacy rights) you cannot protect privacy without security. This is the principle behind "privacy by design" requirements in government contracting and in data privacy laws.

It means looking at products, services, solutions, and new technologies and asking: What data is being collected? How is it being collected? What is the impact of collecting, storing, and processing this data? How is the data to be used? How long will this data live? From a security standpoint, does it mean asking who has access to the data? How do I audit access to the data? Is the data encrypted or secured, either in whole or in part? How do I protect data confidentiality, integrity, and availability?

If business enablement is the goal, then we have to use the language of business. Security reduces costs because it increases the efficiency of moving data and enabling collaboration. Security accelerates speed to market, which means we can make more profit. Security empowers us to do things routinely today that we couldn't have done a few years ago. Security enables us to hire the best people because we are not limited by geographic constraints. Security allows sales and marketing to leverage analytics and be more responsive to customer needs.

The Language of Business Enablement

We shouldn't *stop* talking about risk mitigation and regulatory compliance. These will always be critical to the success of our cybersecurity teams. But if CISOs *start* talking about reducing the overall risk to the company, they will be far more effective in speaking the language of business.

How do we change the conversation? Here are some suggestions for IT security professionals:

1. **Closely examine the overall objectives of the business.** Determine how the security function fits with what the business does and how it operates. Develop a framework for articulating the role cybersecurity plays in key business functions—hiring, operations, sales, marketing, distribution, etc.
2. **Look ahead.** Where is the company going, and how can cybersecurity be a business enabler? Is the company looking to leverage robotics, the IoT, artificial intelligence, big data analytics? Is it looking to break into new global markets? Perhaps there is a

new security technology that will enable the company to do something it couldn't before. *Let security drive the conversation.*

3. **Take a more expansive view of the regulatory environment.** Perhaps your organization is not operating in the European Union now, so there's a sense you don't have to worry about GDPR. But you may have business partners doing business in Europe; you might decide to open offices there; you may collect data there. Be aware, be comprehensive, be expansive. Don't look at privacy as a separate discussion, but embed it in your security posture.
4. **Talk business.** Focus on sales, profits, innovation, corporate culture. If the security team does a great job and there are no breaches, what will motivate corporate management to invest more in security? The selling point shouldn't be that nothing happened; it should be that security enabled and empowered the business to achieve these specific quantifiable and measurable results.
5. **Quantify the value of risk reduction.** At some point, the conversation will inevitably turn to risk. When a CISO can effectively quantify the value of risk mitigation, he or she can be more articulate and insightful in explaining overall return on investment. You truly change the conversation when you attach real numbers to risk mitigation and combine that with values associated with profits, sales, speed to market, hiring, product development, and improved operational efficiencies.

Conclusion

Business enablement through cybersecurity is not an option in the Digital Age. It is a fact of life in doing business. If you are involved with other companies, they will demand that you have a comprehensive cybersecurity program. Failure to have one means you won't be able to do business, period. However, if you merely place cybersecurity in the bucket of either "cost of doing business" or "risk mitigation," you may be missing the real opportunity at hand.

Cybersecurity can and should be about driving revenue, achieving greater profitability, attracting and retaining new customers, operating more efficiently, empowering innovation, hiring the best people, transforming the workplace. Only when we think of cybersecurity in those terms, can we truly leverage the power of the Digital Age.

If the only thing we're trying to do is not fail, that doesn't necessarily mean we're going to succeed. It's time to transform our language, mindset, and perspective. When it comes to cybersecurity, whether we are on the board, in the C-suite, or on the frontlines, we should all be speaking the language of business enablement.

28

Language, Please: How You Talk to Boards and Executives Can Make or Break Your Cybersecurity

James Shira

It's 4 a.m. on a quiet Sunday, and your Hong Kong office is suddenly offline. A fringe political group has hacked the local electrical grid, cutting off power to fans and cooling systems in the local data center. All production systems are down.

The result: Your global banking operations are not available. Dead. Not functioning. And the organization is bleeding money by the second.

As your organization's CISO, you get that panicky, middle-of-the-night call you often have nightmares about, and the cybersecurity playbook that was so neatly designed and prepared six months ago goes into effect. With good planning and tight execution, the disaster recovery and business continuity plans are enabled—hopefully automatically—and everyone jumps to attention to find the source of the problem, remediate it, and stanch the damage.

As you contact your boss to let them know what's happened and that a catastrophe has been averted, remember this: What you say next may be the most important step toward ensuring the organization is secure—as well as your career.

What you say to the business leaders of your organization—and how you deliver the message—must give them confidence that you:

- Know what happened.
- Know how it happened.
- Can determine and measure the impact on the business.
- Have a clear, defensible recommendation to ensure it doesn't happen again.

And you can't do that with a litany of technical terms, jargon, and "Don't worry, I've got this covered."

Cybersecurity Is Not a Technology. Don't Talk About It That Way.

Unfortunately, the scenario sketched out above is occurring far too frequently—and often with an unhappy ending. Too many organizations treat cybersecurity as a technical problem, one that is ideally addressed by technical people applying technical solutions to technical threats. And too many CISOs talk about cybersecurity with a technical voice, not with one of a respected business operator.

Cybersecurity isn't about firewalls, intrusion detection, authentication, malware prevention, or even threat intelligence. Oh, those are all important components of a good cybersecurity framework. But CISOs often fail—and their organizations suffer as a result—when they look at cybersecurity solely through a technology lens and talk about it that way to business leaders.

Instead, I strongly urge—no, I implore—you to rethink how you, as your organization's firewall against cyber risk, talk to C-suite business executives and boards about cybersecurity. Your language has to help bridge the gap between the technical underpinnings and the business implications. And the first thing you need to know is that it is not the responsibility of the CEO or the board to come to you and tell you what they want to know.

It's on you.

You must take the first step—and the second, third and however many it takes—to close that gap of knowledge for the non-technical executives. And you can't do that without arriving at a common language for communication.

For instance, let's go back to our nightmare scenario at the beginning of this chapter. When the CEO or a board member asks you, "What happened?" it's important not to talk about unanticipated data exfiltration, buffer overloads, or IRC-controlled botnets. Instead, your reply should focus on the business implications of operational missteps or technical failures, such as loss of online banking services for two hours, which resulted in spikes to our call centers and a 4% loss of revenue.

As a CISO, you must operationalize cybersecurity from a business perspective, rather than through a technical lens. You must describe the problems the organization is confronting in plain language that is rooted in business outcomes. You must be able to monitor, measure, and improve those outcomes, and it is up to you to turn cybersecurity into a strategic discussion, rather than a technical reaction to a problem none of them truly understand.

The words you choose, and how you communicate with the board and other business leaders, will be some of the most important steps you can take toward becoming viewed as a business operator in the same way the heads of functional areas, such as finance, operations, marketing, legal, and others, are regarded. If you don't use the right language, you will not be successful as a CISO.

Preparing Your Audience

In working with many CISOs in both the private and public sectors, I've learned that good communication, based on the most appropriate language, is aided significantly by following a familiar refrain: Know your audience.

As a CISO, you have to talk to a lot of different decision makers, colleagues, and influencers throughout the organization. So it helps to understand how best to get through to your audiences. One important way is to ask yourself if you are talking to someone who is a "reader" or a "listener."

A reader is someone who takes in information visually, reading position papers, case studies, situational analyses, and status updates before a board meeting or a gathering of executive staff. The reader comes prepared for the meeting by arming themselves with pertinent facts, opinions, options beforehand, and is armed to discuss options and consequences.

By comparison, a listener likes personalized discussions, often one-on-one, with the CISO so they can hear from you directly and ask questions as they are processing what you are telling them. With listeners, it's a good idea to have private pre-meetings, so they are prepared for the broader discussion with their peers.

You know the saying, "All politics is local?" Well, a good CISO should remember that "all communication is personal." So be prepared to tailor your language to the needs of the person who is processing what you're telling them.

The Power of Language

Interestingly, one place where cyber professionals and non-technical leaders have understood this requirement and have taken important steps to operationalize cybersecurity through language is the U.S. military. Security has been pulled into the normal chain of command so it's part of the core set of functions undertaken by the U.S. military branch. It's not an IT activity that resides on the edge of the operational framework; instead of talking about "information assurance," everyone speaks the language of "mission assurance."

How else can the CISO use the right language in the right context to be viewed as a true business operator, rather than as a technical guru?

First, don't give in to many business executives' stereotype of the CISO as a technical kingpin, perhaps a little eccentric, and probably biased toward technology solutions that fail to account for business realities. This means you should minimize acronyms, avoid hyperbole, steer clear of run-on sentences, and focus on how cyber risk affects business operations.

Second, understand your organization's business environment as well as the heads of any business function. Become knowledgeable and articulate in issues, such as competitive strengths and weaknesses, customer behavior, sales and profit trends, distribution channels, and branding considerations.

Third, build professional ties with colleagues based on personal empathy. Learn your colleagues' business challenges and frame your cybersecurity discussions and recommendations in their terms. Talk about how an investment you recommend will increase e-commerce application availability by 20%, ensuring that the organization won't bleed revenue like its competitor did last week when its ordering platform went down for two hours. Or talk about how a modernized data protection approach will make it easier and faster for the legal department to produce documents during the discovery phase of a lawsuit.

Finally, remember that you must back up your words and "own the fix." When you talk to your board about a recommendation for a cybersecurity investment or new policy, take ownership of implementation and accountability: "With your support, I am prepared to do the following." You can't be the person who opines on what to do but isn't prepared to own it.

Language Skills Will Be a Prime Requirement for the CISO of the Future

It's natural for us to play to our strengths as we conduct ourselves in business every day. After all, our strengths are what got us to this place. If a CISO sees himself or herself as the cybersecurity technical guru, they will talk that talk and walk that walk.

But I'm seeing important new trends in how CISOs are being put in place. For instance, I fully expect that more and more CISOs will come from top MBA programs, rather than from computer science programs. I also expect the CISO to be trained, mentored, and recruited internally, within organizations from non-technical disciplines such as finance, operations, and even sales and marketing.

That's because the CISO of the future is going to need to have stronger business skills and, especially, greater communications skills to build the coalitions

and collaborations necessary to have the technical and non-technical disciplines work together. Without them, organizations will struggle to properly and proactively identify sources of risk, weigh the possible solutions, evaluate their impact on the business operations, and make difficult decisions on factors other than the best technical fix.

The communications skills are going to be particularly important as the CISO acts as a "translator" between the technical and business sides, as well as communicates up to the CEO and the board about balancing business opportunity with business risk. To make knowledge power, you have to make it understandable. In security, too often we've made it less understandable. The lack of technical knowledge of your audience such as the CEO and the board means they have to trust the person presenting the technical issues to them, which often means they miss the opportunity to ask the right questions that could avert a disaster down the road.

In the context of cybersecurity, great communication skills are required to promote better, faster, and more impactful decision making. The most specific things a CISO needs to communicate, clearly and compellingly, revolve around the need for appropriate investment, the requirement for shared ownership of cyber issues, and a bias for action in a time of crisis. Raising your game in communications is essential in order to move cybersecurity from a reactive mode to a proactive, strategic discipline.

Ultimately, the CISO needs to be the general manager of the full spectrum of security—not only information security, but physical security as well. Again, this is where having a CISO with strong business skills—communications, prioritization, political acumen, delegation, and collaboration—comes in handy. As CISO, you need to demonstrate managerial DNA, which highlights a comfort level with assuming operational responsibility for security.

And here's something else to keep in mind—something potentially controversial: Many current CISOs, as well as candidates for that job, don't want operational ownership.

Many CISOs still see their role as providing technical leadership in the areas related to information security. For them, it's about firewalls and advanced persistent threats and identity management. Too many "traditional" CISOs learned their craft at a different time, when security threats were often well known and their business impact limited.

No longer. And any CISO who dodges operational responsibility and the tight integration with all business functions within the organization does so at their own peril.

To be a successful CISO from this day on, you can't cringe before power. You must hold the organization accountable for a smarter, more effective balance between risk and innovation. And, you can't act like you're the only one in the room who understands the bits and bytes. You don't want to be seen as a CISO who is so comfortable lapsing into the next hype cycle.

Finally, remember that the most successful CISO is "prepared for why." Sitting in a boardroom, or having lunch with the CEO, you may be prepared to argue for new investments in tools, training, or staff. You may have compelling data to highlight a problem or anticipate the next threat. As important as those are, you will not succeed unless, and until, you are able to articulate the reasons *why* your recommendation makes sense. And the people who make those decisions are going to demand that you can defend your recommendations; they are not in the habit of giving you what you want because you dazzled them with your technical brilliance.

Elsewhere in this book, USAA Chief Security Officer Gary McAlum uses a particularly apt way of describing how to close the gap between what a CSO says and what the business executive or board member hears. He calls it "So what?" and he explains that everyone must be ready to explain the business significance of any problem, recommendation, or course of action to ensure rock-solid cybersecurity.

Your "why" must be concise, sober, and grounded in business benefits that are in lockstep with the organization's strategic goals. If not, freshen up that resumé.

Conclusion

In Part 1 of this book, Justin Somaini told a very important story about how he set out to build strong relationships—and foster credibility—with business colleagues by asking to join the sales organization.

Justin's rationale was brilliant: "Protecting the company from security breaches and ensuring compliance is actually not a very good description of my job, nor the job of my peers and colleagues around the globe ... How could I enable sales if I didn't understand sales?"

As a CISO, it's important to step back and acknowledge that, at the end of the day, your job is to ensure that your organization achieves its most important goals. You may do that by reducing and managing cybersecurity risk, just as the head of sales may do that by creating new sales channels or the head of logistics streamlines global supply chains. It's a means to an end—not an end itself.

Strategy

29

To Get Ahead of Cybersecurity Threats, Focus on Preparedness and Sustainability

Heather King — Former Acting Senior Director for Cybersecurity Policy, White House, National Security Council Staff

Megan Stifel — Executive Director, Americas, Global Cyber Alliance

Everyone understands natural disasters are inevitable. Hurricanes, tornados, flash floods, wildfires, and other extreme weather conditions happen frequently and at different levels of severity, and the economic, human, and social impacts can be enormous, if not deadly. So it's imperative that representatives from all parts of the community share the responsibility to prepare for the onslaught of any threat or hazard.

Ultimately, greater individual and organizational preparedness contributes to a stronger, more resilient community. Doing that means everyone has to get out ahead of the problem, prepare for a wide range of potential challenges, and ensure that protective actions and defensive measures can be sustained in wave after wave of potential disasters.

Wave after wave of potential disasters: Sounds like the current state of cybersecurity, doesn't it?

We all have to rethink our strategies to ensure our organizations and our communities can achieve and maintain a stronger state of cybersecurity. And, those strategies must be built on resiliency, and subsequently, the twin pillars of preparedness and sustainability. Unless leaders move toward a mindset that emphasizes long-term planning and sustainable cyber-resilience, informed by the lessons learned from any given event, we will continue to fall further and further behind.

In no other institutional function would we accept such a downward trend without meaningful change. If company sales and profits were trending down, we'd find a way to plan and execute a sustainable path to financial health. If our house was repeatedly robbed, we'd either get an alarm system or we'd move. And if a country's economic and social position deteriorated, we'd look at things like job training, educational opportunities, import/export strategies, and an entire array of policies and programs.

But far too many organizations realize too late that they are behind the curve when it comes to cybersecurity, and yet they continue to cling to outdated, inefficient, reactionary, and ultimately unsuccessful approaches. Since all organizations experience incidents or intrusions, it's not surprising that many chief information security officers often feel over-

whelmed by the sheer volume of actions necessary to better prepare.

It's time for a change.

Preparedness and Sustainability

Many organizations still view cybersecurity through a perimeter security lens, where the focus is on securing the network against intruders—an outdated castle-and-moat approach. Too many organizations have built cybersecurity defenses focused on addressing individual problems or reacting to specific threats. Unfortunately, that has created numerous cybersecurity silos and stovepipes—a solution for advanced persistent threats, another for mobile malware, another for phishing, and still others for threats in specific geographies or vertical industries. Intruders and malicious insiders exploit the seams and gaps this approach creates. Thus, it is inefficient, ineffective, and not sustainable.

Today, we must dramatically expand the focus of cybersecurity, so we can not only secure our networks but also secure our products and services used by other businesses, organizations, and individuals. And we're not just talking about the influx of tens of billions of connected things—it's nearly every aspect of how we work and interact using technology. Moreover, in order to change our strategies, it's a transformation/shift in how we think and approach doing business. For instance, instead of "first to market," think of it as "secure to market," putting a premium on providing the most secure products and services. At the heart of our recommendations on how to improve cyber resilience are the concepts of preparedness and sustainability.

By preparedness, we mean getting out in front not only of today's cyber risks, but also to anticipate what may be coming next. Together, these steps help organizations determine the potential business impact of cyber risks, and enable them to put in place heightened business continuity plans and incident response plans that are tested through training and exercises and updated regularly—not just after the latest incident.

The concept of sustainability is intricately tied to preparedness because it also recognizes the need to engage today in order to ensure the same or better opportunities tomorrow. Sustainability management expands the aperture of a company's product—whether hardware, software, or service—from the moment just before it goes to market to the point at which the company expends resources toward the product. Companies adopting sustainability management practices work across business lines to assess supply chains, interoperability and scale, consumer engagement, and regulatory compliance to ensure what goes to market today will withstand tomorrow's challenges and that the product's lifecycle is fully understood.

An organization's cybersecurity preparation must be sustained over time in the face of new threat vectors and rapidly changing business requirements. It's like shifting thinking of your business processes that support the enterprise from the view of IT acquisition, to extending supply chain risk management to your entire business operations—truly knowing who your vendors are, who they rely on, knowing your product's lifecycle, and how you will support it throughout, including managing vulnerabilities and patching to data collection, retention, and use.

The harsh reality is that our business leaders are far too optimistic about their organizations' current state of cybersecurity resilience. As a result, they often fail to see the upside of developing cybersecurity strategies in the same way they develop long-term product roadmaps or multi-year market development programs. Ultimately, organizations should

be integrating cybersecurity into these and other business operations. Leaders still too often see cybersecurity as a cost of doing business rather than as a step toward improving customer experience, enhancing workforce productivity, maintaining trust with customers, or protecting the organization's brand.

To counter this mindset, business leaders and board members need to discard the all-too-prevalent, "what is this going to cost us?" reaction to cybersecurity measures to "how can cybersecurity investments improve our business competitiveness and deliver a better ROI."

To support such a shift, we need a more holistic approach to cybersecurity, which is informed by successful approaches from other disciplines, including preparedness and sustainability. When our organizations are prepared for as many eventualities as we can imagine, and when we take the long view about securing the organization and its digital assets, we begin to reassert control over the challenges confronting us.

Moreover, adopting sustainable business management practices has helped organizations achieve higher profits, in addition to improved environmental, social, and governance ratings. It stands to reason that organizations that adopt a broader vision toward sustainable cybersecurity practices can do things like anticipate and adapt to changing threat vectors more quickly and effectively, because their cybersecurity framework is built on holistic preparation, agility, and an ability to scale their programs as conditions change. A sustainability-framed approach to cybersecurity enables these resilient characteristics because it is shaped not only by lifecycle, enterprise, and supply chain risk management, but also by user interaction and anticipated experience.

Rethinking and Re-architecting the Approach to Cybersecurity

Experience has taught us all that information sharing is fundamental to an organization's ability to build a new cybersecurity strategy upon the concepts of preparedness and sustainability. No sole organization can spot, react to, and remediate the impact of risks in real time on their own. Without a commitment by organizational leadership to collaborate with colleagues, partners, and even competitors to share relevant threat information, we will continue to fall behind malicious actors.

At the Cyber Threat Alliance, we recognize that information sharing supports an organization's preparedness efforts, and ultimately, its resilience. In fact, information sharing—whether human-to-human or near real-time automated machine-to-machine—demonstrates an organization's confidence in its own products and services. Moreover, it's no longer how much data an organization has access to, but it's what their products can do with the data. Furthermore, it communicates a realization that the threat is growing exponentially, and organizations can no longer tackle these threats individually, but that we have a shared responsibility to share information from our different perspectives and confront the challenges facing the digital ecosystem.

For instance, through its members, CTA enables near-real-time actionable cyber threat and incident information sharing among highly competitive cybersecurity providers. These competitors have voluntarily come together to improve the cybersecurity of the digital ecosystem in an effort to better prepare and protect customers, and ideally, achieve a more digital resilient world. They all believe this collaboration will improve their profitability, not weaken

it. Further, CTA's information sharing facilitates analysis aimed at disrupting malicious actors, enabling more effective and collective defense actions, and forcing adversaries to invest time and money in new infrastructure and how they do business.

A good application of information sharing as a preparedness action is VPNFilter in May 2018. Cisco's Talos Group, one of CTA's founding members along with Palo Alto Networks, Fortinet, Check Point, McAfee, and Symantec, notified CTA of the VPNFilter threat that was targeting network equipment all over the world, and shared their analysis and malware samples with CTA members. As a result of the incident information sharing done through CTA, all of CTA's members were able to rapidly develop protections and mitigations for their customers and quickly counter the threat.

Moreover, as Megan wrote in "Securing the Modern Economy: Transforming Cybersecurity Through Sustainability," reliance on technology to do both mission-critical and everyday tasks in business, at home, and in our communities will only accelerate. Without a commitment to organizational preparedness and sustainability, organizations and individuals and the internet ecosystem will be put at greater risk as we are exposed to more and more public instances of information security problems: "Maintaining public trust in technology relies, in significant part, on all stakeholders maintaining cybersecurity."[1]

As organizations commit to a cybersecurity mindset based on preparedness and sustainability, executives and boards must challenge each other to rethink their most basic assumptions about technology usage and cybersecurity resilience. For instance, they must:

1. **Make cybersecurity a C-suite priority with their active participation.** A number of chapters have talked about why cybersecurity should be a C-suite priority. But their active participation is critical. This starts with conveying in management meetings, employee all-hands, and even your reports for publicly traded companies how serious you regard the cybersecurity threats facing your organization and ultimately, what you're doing to prepare and sustain your organization, both when an incident or breach occurs and when you take products— services or devices—to market. As we all know on any management topic, when executive leadership prioritizes and actively engages on an issue, it delivers a sense of urgency.
2. **Make cybersecurity intuitive in your day-to-day business operations.** Organizations should maximize opportunities for educating and raising awareness within the workplace, so that employees better protect the organization while "on the job" and understand how they can reduce their own digital risks "off the job." Software vendors should be required to demonstrate that they have secure development processes, supported by a software bill of materials. Next, organizations should communicate what is expected of employees by requiring best practices in the enterprise environment and following product deployment, and encouraging their adoption at home. Organizations can develop "cyber civics" programs that emphasize using two-factor authentication and password managers, thinking before clicking on suspicious links, and being cautious about what they post online about themselves and their families' status and activities (e.g., limiting communications about travel).

3. **Recognize that cybersecurity underpins all business operations.** As Siân John of Microsoft points out in this book, security is a business problem, not an IT problem. Therefore, it's important to remember that a great risk management framework integrates technical solutions with business goals. Putting security first in all business operations enhances confidence in the processes that develop products and services, which results in better products and services that support the brand and ultimately leads to increased profits. Failing to incorporate security throughout the organization risks the confidentiality, integrity, accuracy, and authenticity not only of information within the enterprise, but also of the very products the organization depends upon to earn a profit.
4. **Inform your approach to cybersecurity planning with worst-case scenario consequences.** Consider not just the enterprise network, but also everything it depends upon (vendors, employees, power, physical structures) and attaches to it when assessing cybersecurity risk. In addition to adopting the Cybersecurity Framework promulgated by the National Institute for Standards and Technology to manage enterprise risk, get incident response and continuity plans in order, practice them regularly, and update plans, policies, and processes appropriately. Acquisition and plans must be collaboratively developed by all business functions within the organization, not just by the CISO. And don't forget to include product and service security upgradability and patching in these "dooms day" scenarios.
5. **Actively participate in an information-sharing organization … or two.** Business leaders often struggle to get past their innate discomfort at sharing information with others. But as indicated earlier in this chapter, in the rapidly evolving cybersecurity landscape, this reluctance can no longer be tolerated. Invest now in learning some best practices about what, when, where, and how to share information, because going it alone is no longer an option. Sherri Ramsay says it clearly in her chapter of this book: The bad guys are collaborating; why aren't we doing the same?

As you undoubtedly imagine, this kind of holistic, integrated, comprehensive, and deliberate change in the way an organization thinks and approaches its business demands the support and active participation by every organization's executive team, from the corner office to the boardroom. We've not only tried to raise awareness about the need to confront threats in a more proactive, end-to-end manner, but we've also offered tangible ways organizations can challenge their own assumptions and create more cybersecurity resilient organizations based on the underlying pillars of preparedness and sustainability. And, it's essential for executives and board members to embrace this mindset; otherwise you risk leaving your organization to expend countless resources on a defensive posture that's always going to be playing catch up to the bad guys.

Conclusion

Too often, business leaders continue to take the castle-and-moat approach to enterprise cybersecurity. But modernizing that philosophy by adopting the preparedness and sustainability principles we've talked about in this chapter is essential because it enables executives to look around the corner and anticipate the impact of existing and emerging threats on business operations.

As we institutionalize this kind of mindset and reinforce it in our discussions and interactions with customers, investors, employees, vendors, and third parties, we take major steps toward a more resilient cybersecurity posture that is proactive, analytical, and self-reinforcing. It's like preparing for extreme weather conditions. The more you plan, and the more you put measures in place—not just for a point-in-time event but for the long term—the more routine this will all become and the more successful your organizations will ultimately be in managing cyber risk and, as a result, achieving their mission.

---

[1] "Securing the Modern Economy," Public Knowledge, April 2018.

30

Learning and Leveraging the Wisdom of "So What?"

Gary McAlum — Chief Security Officer and Senior Vice President for Enterprise Security, United Services Automobile Association

As cyber threats become more frequent, more sophisticated, and more impactful on business operations, organizations need to adopt a practical approach if they are to make sense out of what promises to be an uncertain and confusing future.

Yes, many business executives and board members will convene meetings with their chief information security officers and other senior IT executives to consider financial investments and changes to business processes. And many of those discussions will be riddled with technical buzzwords and talk of things like intrusion detection systems, UEBA, multi-factor authentication, next generation firewalls, network segmentation, and machine learning, just to name a few. Your top IT and security experts will undoubtedly impress you with their depth of technical knowledge and give you an array of solutions to "defend the perimeter" and establish "multi-layer security frameworks." And every vendor has "the last piece of the puzzle that you need" in your security technology stack to solve all your problems.

And when those buzzwords start flying and the acronyms dominate discussions, your reaction and response should be simple:

"So what?"

I don't mean you should ignore or belittle the technical expertise of your CISO or CIO, or disregard their requests for smart and even potentially large increases in security budgets. "So what?" is just the lead-in for a series of questions that need to be properly addressed. As important as technology solutions are in establishing stronger cybersecurity, it's essential that business leaders and board members focus on the operational implications of cybersecurity challenges and keep the technical issues rooted in a business context.

- How is this threat impacting or how could it impact our business?
- How are our customers and partners going to be affected?
- What are the financial, operational, regulatory, legal, and brand implications of the threats?
- What is our risk exposure? What is our residual risk?
- How will we know if we are succeeding in defending our most valuable assets?
- How can we look around the corner at what's next?

- And the hardest question of all: How are we measuring success? In other words: So what?

How USAA Learned the Lesson of "So What?"

Several years ago, the financial services industry was attacked—not by masked thieves breaking into our vaults under the cover of darkness or by smash-and-grab robberies of our branch offices. It was a cyberattack—a distributed denial-of-service (DDoS) attack, to be precise, targeting the U.S. financial services sector. And it was a real mess.

Seemingly, no financial services organization was immune—and that includes where I worked at that time. In fact, we were hit twice. Believe me, the fact that we had plenty of company did not make it any easier for us.

As the first wave of attacks hit organizations throughout our industry, we could see the writing on the wall. The media started picking up on the attacks, so there was a daily dose of reporting and an increasing tone of fear, uncertainty, and doubt (FUD). We knew it was going to be a board-level issue, that they'd want clear answers, and they'd want them fast. So we began to prepare our presentation.

I sat down with my SecOps team, and posed an open-ended directive to them: "Give me a short presentation for the board, no more than three slides." I knew this was a challenging request, and I felt it was a good teaching moment for my team to gather information they felt was relevant for senior leaders and to give them an opportunity to develop strategic communication skills.

I wasn't surprised when the team came back with a technical presentation on botnets, how they occur, what they do, and all the technical considerations. There was a great deal of detail on the types of DDoS attacks that were occurring: UDP Flood, Ping of Death, NTP Amplification, HTTP Flood, etc. What the brief didn't include was an answer to the fundamental question: So what? In essence, we were telling the board how the watch worked, but not what time it was.

It would have been easier for me to give them more explicit instructions—especially considering the sense of urgency of the moment—but I felt it was crucial for our team to see and "feel" the impact of not providing the right information in the right context. I challenged some of the leaders within my group to go out and talk to business teams, to understand the financial, operational, and reputational impact of being offline, let's say, for eight hours. In fact, I suggested that the Business Continuation team would be a great place to start, since their annual Business Impact Analysis would be an authoritative source of valuable data.

They learned their lessons well. They came back with a tight, business-oriented presentation that was short on technical minutiae and long on business impact.

By the way, it was a single slide. They boiled down the "so what" to its essence, and that's what we presented to the board. Essentially, they answered the question, "So what if our customers can't get to their online accounts for eight hours?" There were very definite answers pertaining to lost business, inability to service customers, impact to money movement transactions, etc. Any downtime due to the DDOS, regardless of type, was going to be a big deal. They got it.

We know they got it because we were able to easily demonstrate the business impact of not taking action in dollars and cents, and what it would mean in terms of pain for our customers if we didn't take stronger steps. More importantly, it allowed the conversation to change to "Are we ready to deal with this? And if not, what resources are needed?"

Creating a Culture of Cybersecurity Using a "So What" Approach

In the Second Edition of this book, Patric Versteeg writes compellingly about the importance of setting a strong "culture of cybersecurity" throughout an organization. I think he has hit on an important requirement, and our "so what" discussion can be applied in the area of cybersecurity culture, as well.

Using our "so what" yardstick, how can business leaders and CISOs build and nurture a culture of cybersecurity? I have a few suggestions that may work for your organization.

- **Demonstrate that it is a top-down strategic initiative.** Sending out memos and approving policies on good cyber hygiene are fine, but they lack "so what" impact. Your organization needs to see its leaders "walking the walk" by doing things like engaging security team members on new-product development teams from the start, rather than simply having them eyeball your new IoT initiative as it's about to be released to the market.
- **Real leadership goes beyond writing checks.** Again, having business leaders and board members approve important cybersecurity investments is essential. But it fails to deliver the "so what" impact of steps like having your CISO report to a senior executive outside the typical CIO chain or having regular interactions with the board.
- **Making the right personnel decisions means everything.** It may sound counter-intuitive, but I believe we are all often better served by having fewer, rather than more, FTEs devoted to cybersecurity—as long as they are the cream of the crop. Maybe this is a vestige of my days in the military, but I always want an elite team rather than a large number of average performers simply to have enough eyeballs to monitor and manage security events. Business leaders have every right to ask "So what?" of the CISO who puts in a request to expand his or her team. So, what will this expansion do to decrease risk, improve business operations, or enhance products and services?
- **The executive team and board members need to commit to continuous security education.** Regularly scheduled presentations to the board and continuous conversations with business executives are good, but self-initiative on the part of the board and C-suite executives is better. Don't just sit back and ask your CISO for a briefing; take the lead and get educated on your own. Visit with the security team on-site and ask questions. Spend some time reviewing threat intelligence reports with your CISO. Attend conferences and listen to podcasts. Professional organizations like the National Association of Corporate Directors offer an increasing number of training and awareness events around cybersecurity. Your board and executives won't know how to evaluate the answers to "so what" questions if they are not committed to going beyond becoming cyber-aware and actually becoming cyber-centric. It's that important.
- **Adopt a "secure-by-design" approach.** This should be applied to everything from new-product development to how you use technology for everyday operations. Policies like changing passwords quarterly are annoying to your employees, in large part because they don't hear their "so what" pleas answered. The same is true with your system engineers and

application developers. They will push back on your well-intentioned edicts, for example, to strengthen authentication for that new online loan approval application, unless you make them understand the implications when security defenses are breached or customer accounts are compromised.

Framing "So What" Questions for the Best Results

As is true in nearly every type of relationship, your ability to get everyone on the "so what" bandwagon is influenced heavily by how you send your messages. Different people on the receiving end of a "so what" missive can interpret that in different ways, and the results can range from instant learning and embracing the spirit of "so what" to hostility, confusion, and fear.

What you say matters. But how you say it may matter more.

- Is your "so what" message motivational, challenging, instructive, and benefits-oriented, or is it threatening?
- Is it framed in business implications, such as financial impact, operational efficiency, company risk, or brand reputation?
- Do we need to shore up our defenses by increasing financial and manpower investments, or maybe re-prioritize the use of existing resources?

At the end of the day, "so what" is really a metaphor for an operational methodology that frames three key points:

- What is the business impact of this security situation?
- What are the risk implications?
- What are we doing about it?

For C-suite executives and board members, what you don't want or need is a growing cascade of reports, dashboards, and metrics. CISOs already have a vast amount of information that they are sending to business stakeholders about vulnerabilities and risk; just dumping more data on the desks of decision makers isn't going to work. Board members and executives have to walk that fine line between getting "so what" answers and wallowing in tactical details. And, time is always a limited commodity.

One way to help is for business executives and boards to train the technical presenter—the CISO, CIO, or anyone providing security information to the business side—not to pull the crowd into tactical, technical discussions. Board members, in particular, have a limited amount of time, and they need to have confidence and trust in the people accountable for ensuring the organization and its assets are secure. Coach your CISO and their team on how to deliver strategic answers to the "so what" question.

Moving Ahead with Your "So What" Methodology

Taking a "so what" approach to cybersecurity isn't about downplaying risk or minimizing the importance of smart technology investments. Instead, it's a pragmatic way to prioritize how, where, and when to utilize key resources (money, time, people, technology) to spot and prevent problems before they impact business operations.

When I was first exposed to "so what" in my Air Force career, I'll admit it was a little uncomfortable and occasionally disconcerting when my superiors challenged me in this way. If you're technically focused, you tend to think and respond in what you know best—technical terms. But CISOs and their teams have to force themselves to think and present information differently, even if it's not easy for them. I know it wasn't always easy for me. When you are sitting in front

of a 4-star general and having to explain why it's really important that computers supporting a major weapon system have to get patched (which means risk), you very quickly learn to cut through the technical details and answer the "so what" questions.

Ultimately, business leaders and board members should use the "so what" methodology—wisely, strategically, and non-judgmentally—to help CISOs and other security professionals sift through all the technical details and present only the information needed to make smart, fast decisions. For business leaders asking "So what?" may not be an easy process. Your technical leaders have a tendency to want to give you the whole story, to tell you everything. You have to help them pare that down.

After all, a DDoS attack may be right around the corner, and no one wants to hear about the history of botnets and how an ICMP flood attack works.

31

How to Optimize Cybersecurity Using Measurement

Richard Seiersen — Chief Executive Officer, Soluble.ai

"The winners are usually the guys who get 5% fewer of their planes shot down, or use 5% less fuel, or get 5% more nutrition into their infantry at 95% of the cost."

—How Not To Be Wrong
By Jordon Ellenberg

Digital transformation exposes more value, to more people, through more channels, at higher velocities. The capabilities behind this transformation are software-defined. The people who are making it happen are software developers. It's an all-encompassing evolution in enterprise strategy, and technology, that demands a change for security.

Digital transformation requires the role of security to evolve. Tactically, it requires security to be developer executed. That means enabling development teams to fulfill security requirements, while not impacting their velocity. Security's work shifts to optimizing processes and ensuring that requirements are working.

The new questions for the digitally transformed security team include:

- "Are security capabilities scaling as software accelerates?"
- "Is the software-defined attack surface shrinking fast and affordable enough?"
- "Is my risk surface growing beyond my risk tolerance and do I need to make a change?"

Measurement is the key to answering these questions. Once you can measure, you can work on optimization, which is the future of digitally transformed security work.

The Motivation for Measurement

Small cracks in the security status quo appeared about 10 years ago. The emergence of public clouds and DevOps were the early causes. Operational roles began to morph as infrastructure became more software defined. APIs took the place of boxes, networks, and the people who supported them. In the process, the speed with which developers could expose value and risk to customers was increasing exponentially.

More recently, cloud-native development—with containerized microservices, Kubernetes, and serverless architectures—added rocket fuel to the speed of digital change. Today, COVID-19 is

another factor pressuring global organizations to rapidly adopt these new technologies to better compete. Now in full force, digital transformation is requiring security to adapt to meet the needs of a software-defined world.

Digital Transformation Is a Security Disrupter

Digital transformation optimizes the way we do business, getting value directly to customers as quickly and conveniently as possible. For most consumers, this materializes as a one-click transaction on a mobile device. There is immediacy of satisfaction as the goods we ordered, or the transaction we authorized, occur with little to no impact to our lifestyle. This very same digital convenience is also being applied to business-to-business transactions. In any configuration, it's a focus on rapid fulfillment.

If you look under the covers of digital transformation, you will see what is truly being optimized – the means of digital value production. Moving to the cloud is a big part of it, but dig a little deeper, and you will see a massive evolution in software development. Teams that once produced a hundred software releases a year can now scale to many thousands of releases, with largely the same amount of resources. The cause of this efficiency includes, but is not limited to, DevOps practices, and cloud native-technologies such as containers, Kubernetes, serverless computing, and more.

Traditional operations teams (including security) and the technologies they use, are being disintermediated by DevOps practices and cloud-native technologies. Infrastructure has been turned into software in the form of infrastructure as code (IAC). Developers can now declare infrastructure, and get it instantiated with near immediacy of satisfaction—with no middle—people and processes. The pauses and gaps in processes that previously allowed security to insert itself have been compressed to practical non-existence. Even the concepts of pre-production to production are eroding. It's a shift in both the timeframes, and nature of the infrastructure security. It's leaving security on the ropes, or as an afterthought.

Security Responsibilities Are Shifting Left

Even before digital transformation, security professionals were getting outnumbered. According to the most recent Building Security In Maturity Model (BSIMM) survey there are roughly two security engineers per 100 developers across established enterprises.[1] Add DevOps practices, and cloud-native technologies to the mix, and your security-to-engineer ratio becomes meaningless. You're effectively comparing a moped to a Ferrari if not a rocket. Security can't keep pace. If security is going to make a difference, it requires a different approach.

We must shift more security responsibility onto development teams. When I say development teams, I mean DevOps, Site Reliability Engineers (SRE), Developers, and the like. It is security's job to enable development teams to take on more security responsibility.

The rationale is that there is no outside "insertion point" for security. Software moves too fast, and any outside influence will slow velocity. This means security will need to move from the one who "does security" to the ones who govern, analyze, and optimize the system, while enabling others to be responsible for security execution. Security's role shifts to being accountable and making sure the system is protected while it maintains velocity.

Reduce Drag and Augment Accountability

From a sheer resource and technology perspective, security is outgunned in

comparison to development teams. Not only are security teams outnumbered; they are typically uninformed about the particulars of the specific applications they theoretically protect. What is, and isn't, a security issue is context dependent. Expecting a security practitioner to have enough context across dozens—if not hundreds or thousands, of microservices—doesn't scale. When security tries to be responsible and stand in the middle of the flow of software, there is really only one outcome: Drag.

Drag is orthogonal to the velocity goals of digital transformation. As already stated, digital transformation exists to optimize the delivery of value with more speed. That is why security must be in the optimization game. One of the chief ways it does this is by getting out of the way and enabling security responsibilities (execution) to shift to those creating value. Remove the middle-person, remove the extra steps, remove the weakest link, process-wise, and you remove drag.

So where does that leave security? Security is accountable to the system as a whole. That means governing security capabilities executed by others. It means ensuring those capabilities are scaling with the increased velocity of development. And it means responding to meaningful degradations in capability performance. It's a natural evolution and response to a maturing ecosystem.

The Methods of Measurement

The methods of security measurement fall into two related classes; cybersecurity risk management, and metrics. Cybersecurity risk management makes forecasts about the likelihood, and impact of risk. It works at the portfolio, or enterprise level, and it combines subject matter expert (SME) judgments with relevant data. Think of it as the method for measuring and controlling for "risk surface." Metrics measure operations for the purpose of capability optimization. Metrics can work with small, and big data alike, and can also incorporate SME input in the more advanced applications. Metrics in this context measure capability effectiveness at controlling "attack surface."

Managing Risk Surface

"All models are wrong, but some are useful...and some are measurably more useful than others."

– George Box with some sauce from Doug Hubbard[2]

Cybersecurity risk management is measurement at the enterprise risk level. An example (see Figure 1.) might be forecasting the likelihood, and impact of having one or more breaches over a three-year period. This could be applied to a business unit, portfolio, or some crown jewel set of applications. The various forecasts can also be combined to provide an enterprise view of risk, as seen on the graphic. Since mathematically sound methods of measurement underpin these approaches, adding portfolios of risk together for a unified view is simple.

Using modern cybersecurity risk management methods, leaders determine what investments best reduce risk with the best return on investment (ROI). Results specifically help leaders make decisions about investing in capabilities (people, process, and technologies) and risk transfer (cyber insurance). Priority is given to investments that "reduce the risk curve" to a tolerable level with the least spend.

Determining risk ROI in its most simple form is quite easy. Assume your models forecast that based on the current risk surface you are expected to lose on average $10 million over the next three years. An investment of $2 million over that time frame in capabilities will reduce the expected losses to $5 million. I.e. (10 - 5) / 2 = 2.5 and 2.5 * 100 = 250% giving an ROI of 250%. All of your possible investments

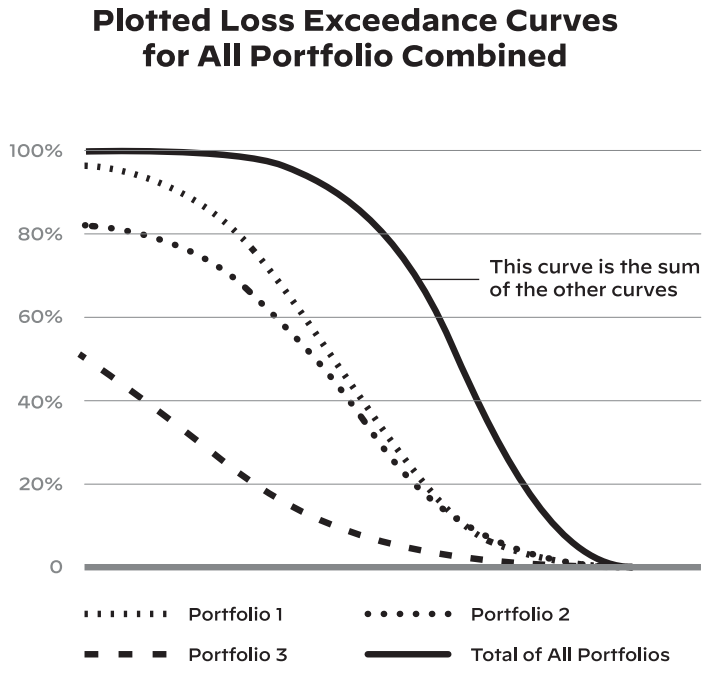


Figure 1: Plotted Loss Exceedance Curves
Credit: R. Seiersen

would be rank ordered by ROI in the same way. Given the budget constraints you have, you would then use this information to help inform your decision making.

Cybersecurity Risk Management Operationalized

Fully operationalized cybersecurity risk models alert on important changes in risk surface. Real-time data flows in from security systems, infrastructure, software, and SME inputs. Given that input, imagine finding out that due to the acquisition of say a new business there is a 30% chance of losing $50 million one or more times over the next three years. You were alerted because the likelihood of loss increased by 20% and impact by $40 million. This pushes you way over your enterprise risk tolerance. While it's only a model (see quote above), it should drive you, as a security leader, to do the research to determine if action needs to be taken.

The "risk surface" modeling process includes considerations for the state of security controls, the value of the environments being protected, and the likelihood of loss given the various permutations of those elements over time. While it sounds complex, that is NOT the goal. The goal is rapid forecasting to maximize security ROI. Models should be fully operationalized, as web services, with near real-time output. A security team can have any number of such models running to help measure and manage that risk surface.

Security Metrics: Managing Attack Surface

"A problem well-stated is half-solved."
— Charles Kettering

What would you see occurring specifically (empirically, mathematically unambiguously) that would let you know your security capabilities are getting better over time? This is my favorite evidence-based elicitation question. Wrestling with it will get you to the heart of the quote above. Not answering it will lead to no metrics or even worse – vanity metrics.

Metrics will tell us if our capabilities are scaling, accelerating, or slowing. Scaling simply means that security capabilities are keeping up with the speed of digital transformation. Accelerating means the rate of control is improving. And slowing means capabilities are degrading.

Scaling, accelerating, and slowing have value in relationship to objectives. An objective is a goal for your capability. Achieving an objective requires making changes to capabilities. You know those changes are working, if you see acceleration toward your goal. But we aren't always sure what we need to change to achieve our goals. When we are uncertain, we need to figure out what is the strongest predictor, or set of predictors, of success. What should we alter in our capability that best achieves our goal, with the least cost and disruption? The process of analyzing metrics in relationship to an outcome, is optimization.

An Intro to BOOM Metrics: Baseline Objectives and Optimization Measurements

BOOM3 is a metrics framework (see Figure 2) for measuring and optimizing capabilities. I designed it as a simple and modular approach that is not overly prescriptive.

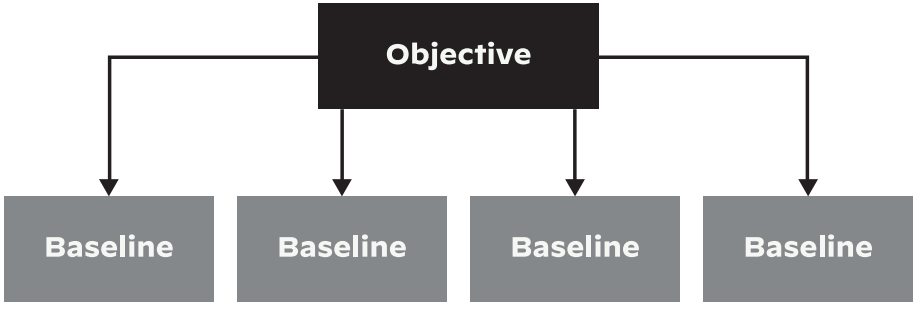


Figure 2: Baseline Objectives and Optimization Measurements
Credit: R. Seiersen

The baseline portion of BOOM has six fundamental metric building blocks. They are: Basic Counts, Burndown Ratios, Arrival Rates, Departure Rates, Survival Rates, and Escape Rates. I will explain each briefly:

- **Basic Counts** are the most atomic measures. They consist of hits and misses, ons and offs, ins and outs etc. For example, "There are 500 critical vulnerabilities over 50 days of age."
- **Burndown Ratios** are a cumulative measure of security work efficiency. You can think of it as tickets closed over tickets created. You might say, "Critical vulnerability remediation burndown for Q2 was 90%, this was a 5% improvement on Q1."
- **Arrival Rates** measure how much security risk materializes in a given time frame. This could be threats, or vulnerabilities. It is designed to be a predictive metric. You might say, "Based on the last two quarters, we expect 20 critical incidents a month on average. Given the rate and volume of software releases expected, we forecast this to expand to 50 a month on average over the next quarter."
- **Departure Rates** are essentially the same as arrivals rates. The former measures how many we expect to appear in a given time frame, and departures measures how much we should expect to disappear. In a digitally transformed environment things come, and go rapidly. It is important to measure both arrivals and departures to determine if capabilities will continue to scale, accelerate, or slow.
- **Survival Rates** measure how long threats, and vulnerabilities live. It uses methods coming from survival analysis. In its simplest form, you can say things like, "50% of critical vulnerabilities live for 5 days or longer, 10% for 30 days, and 1% for 365 days."
- **Escape Rates** measure the frequency with which risks change state over a time period. Change includes movement in location like pre-production to production, or north to south, or internal to external etc. You might say something like, "Over the last quarter 10% of known critical vulnerabilities escaped into production. This is a 5% improvement on the last quarter."

One or more baselines are assembled in various configurations under a measurement objective. Objectives are simply goals not dissimilar in concept to the now popular Objectives and Key Results (OKRs). A general objective might be, "Reduce the time to discover publicly exposed services that don't adhere to least privilege policy." Maybe there was an incident associated with a service that was wide open for several months, and it was compromised. If you decide to focus on this capability, the first step is assembling the correct baselines measures. Once baselined, you set a goal for the objective. From there, you determine what needs optimization. (More advanced optimization methods, like advanced quantitative data science methods, are beyond the scope of this paper.)

The Future of Security Measurement

A digitally transformed security measurement system will consist of descriptive, predictive, and prescriptive analytics capabilities. It answers, "what happened, what will happen, and what should I do now?"

Descriptive analytics is the real-time visibility and history of what happened operationally. Predictive analytics forecasts what will happen given what has transpired (input from descriptive analytics). From there, we analytically weigh the various factors involved in prediction to understand what will give us the best security ROI to control both attack and risk surfaces. We call that last step "prescriptive analytics."

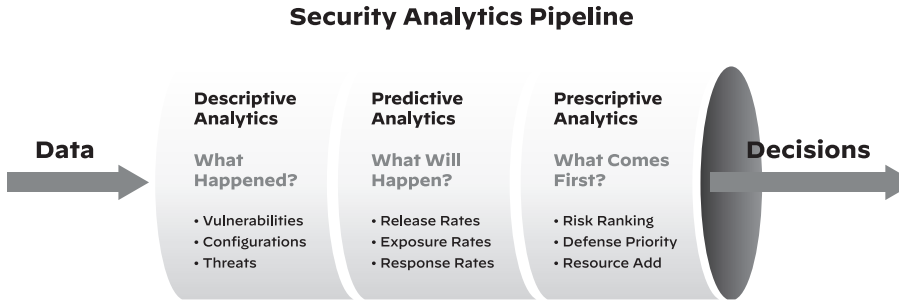


Figure 3: Security Analytics Pipeline
Credit: R. Seiersen

In Figure 3, we have raw data ingestion on the left. It's telemetry coming in from security solutions, infrastructure, software, SME input, and the like. It goes through analytic stages, and emerges as information for augmented decision making, or as input for security process automation.

It is not magic decision making. It's data aggregation, and analytics as a service, targeted toward a security user. Making meaningful models from data is context (enterprise) dependent. But the phases, and types of analytics, are standardized enough to function as a service pipeline that reduces, both the cost, and the effort of operationalizing security analytics.

Clearly, the descriptive analytics phase calls for data warehousing. Assembling predictive, and prescriptive, models at the risk surface, and attack surface levels requires localized data science skill sets, which, if you wish to acquire them, falls into the domain of probabilistic programming.

Once models are created, they can be turned into callable web services, or made available to end users as "no code" solutions. For example, it should be easy for a security analyst to configure the model based on her, subject matter expertise, and localized contextual knowledge. Analysts can set models to alert in real-time on:

- Changes from metric baselines regarding acceleration, scale, and slowness.
- Growth in attack surface based on forecasted software velocity rates.
- Exceeding risk tolerance given risk surface changes.

SMEs are in the best position to qualify model outputs, and determine their value in optimizing capabilities – for both risk and attack surface. There simply is no substitute for local expertise. The goal is not to automate expertise away, but to make the cost in modeling, and using that expertise exponentially more efficient.

Digitally transformed security shifts the responsibility for executing security capabilities to development teams. Now the role of security becomes accountability for assuring those capabilities are scaling (if not accelerating). The soul of accountability is measurement.

Ultimately, measurement enables both security process automation, and enterprise risk decision making. It gives

security a meaningful role in a digitally transforming organization, and gives them parity with the velocity of change without getting in the way. This is the future of digitally transformed security.

---

[1] "Building Security In Maturity Model (BSIMM) - Version 11," BSIMM, 2020.

[2] "How To Measure Anything In Cybersecurity Risk," Doug Hubbard and Richard Seiersen, 2016.

[3] "BOOM for DevSecOps," Soluble, 2020.

32

Making Cybersecurity the Smart Investment in an Era of Economic Uncertainty

Matt Gyde — President and Chief Executive Officer, Security Division, NTT

Due to COVID-19, business leaders have had to juggle budgets, re-prioritize spending and make hard decisions in walking that fine line between what the organization needs and what it can really afford. This has been a brutally tough challenge, with no easy calls—just sober, analytical thinking that often results in no one being satisfied, and a nagging fear that you just haven't done enough.

I'm not here to tell you it's going to get any easier. It's not.

But what I'm going to try to do is help you retain a reasonable level of cybersecurity spending. I also want to give you some rationale on how chief information security officers (CISOs) should make their case in the C-suite or the boardroom, and why business leaders should get out in front of this.

First, let me acknowledge the obvious: Yes, as President and Chief Executive Officer (CEO) of one of the world's largest and most successful managed security services providers, I do come to this discussion as a less-than-fully-impartial observer. But, as I often like to tell my colleagues, "Just because I have a vested interest in this discussion doesn't mean I'm not right."

What Have We Learned? Plenty

COVID's impact has been devastating. On a personal level, most of us know someone who has been directly affected by it. For organizations, many are faced with declining revenues and profits, workforce furloughs, customer upheaval, project delays, supply chain disruptions and more.

Our dealings with the pandemic have, however, taught us a few things. First, work from home is not a fad or a short-term accommodation; it is the way more and more people will work in the future. Second, there are very important security implications to work from home, and these are going to entail conversations about budgets and resources. And third, those conversations are not going to be easy ones. Not for cybersecurity executives, CEOs, board members or chief finance officers (CFOs)—not when so many organization's business opportunities have been severely constrained, or in many cases see their businesses hanging by a thread.

The good news is that we are seeing indications that organizations seem to understand the increasingly strategic role of cybersecurity in this era of the

so-called "New Normal." Even as overall IT spending faces severe cuts, cybersecurity budgets have remained largely intact. A survey by PriceWaterhouseCoopers1 indicated that only 2% of CFOs said they are considering cutting their organization's cybersecurity budget.[1]

Since the pandemic erupted, I have not had a single executive tell me that their organization's cybersecurity budget has been cut. Although, I assume that people are being honest with me, I'm not naïve enough to think that apparent commitment to holding the line on cybersecurity budget cuts will hold unless a few important steps take place.

Let's Talk: The Right Way and the Wrong Way

Anyone reading this chapter is aware that cybersecurity investments must be meaningful, have executive support up to and including the board, and be tightly aligned with business goals.

Frankly, those are table stakes. And the stakes just got a lot higher, thanks to COVID and the relentless march toward new ways for us to work, live and interact in our communities. In order to keep our organizations, our employees, our customers' data and our most valuable digital assets secure, we must rethink the way we all talk about cybersecurity. That's because without the right conversations, CISOs, CEOs, and board members will struggle to find the optimal spending levels that straddle the line between fiscal responsibility and optimizing security as a business enabler.

After having conversations with hundreds of CISOs and business executives about the disruptions this year, I've learned valuable lessons about the right and wrong way for those groups to talk to each other about security spending.

First, the wrong way: Talking about doom and gloom, FUD (fear, uncertainty and doubt) and avoiding disaster caused by draconian cuts to the cybersecurity budget. Board members and CEOs occasionally take a perverse interest in the data breach stories of their competitors and in other industries, and CISOs often fan the flames of those fears in hopes of landing more funding. But those talks rarely, if ever, result in maintaining necessary spending levels for cybersecurity. That's because cybersecurity is cast as insurance, as disaster avoidance, as a moat around the castle keeping out the bad guys. That's a mindset that is still too prevalent in many business meetings, and it marginalizes both the cybersecurity function and the role of the CISO.

Then, there's the right way: Talking about cybersecurity as not just a technology—but as a business enabler. When it comes to cybersecurity budget and cost reduction, engagement must happen at inception. Making security an afterthought, after products or services are rolled out, or equating it with insurance, actually costs money ... and not just in the long run. Fixing security issues that arise late in the process, because that team wasn't clued in earlier, often results in quick fixes designed to address only the most essential potential glitches in order not to hold up new releases. You have to demonstrate the strong value of cybersecurity to the business, rather than treat it as piecemeal solutions where costs add up. This is especially effective when you are able to measure cyber risk. I would urge all CISOs to read Richard Seiersen's chapter which gives examples on how to achieve this.

Is Cybersecurity Your "No Team" or "Yes Team?"

When your organization fails to include the CISO and their team in the loop from the very start of business conversations, you put them in an unenviable spot: You make them the "No Team." And I don't know of many people who relish being on the "No Team":

- No, you can't let employees use their same passwords at home as they use at work.
- No, you can't extend access privileges to part-time workers.
- No, you can't release the new smart-home product because the security footprint is too big for that sensor.

Instead, think of how to position cybersecurity as the "Yes Team." Think of the sense of empowerment to your business when the cybersecurity team adds value to the business, and makes it more agile:

- Yes, you can expand work from home policies to all employees.
- Yes, you can enable customer self-service on account transfers from mobile devices.
- Yes, you can roll out that sensor-based inventory management system.

Whether the CISO and their team is positioned and acts as the "No" or "Yes Team" depends upon a lot of factors. These include the relationship the CISO enjoys with the CEO and the board, the trust developed among the parties, the extent to which the CISO takes a business view of issues rather than a technology-centric perspective, and many more.

But if the CISO has the foresight, discipline and cultural awareness (read: political savvy) to be an enabler, a problem-solver, a facilitator and a business visionary, he or she will take the key step toward building the perception of their organization as being the "Yes Team."

And when you become a "Yes Team," your budget discussions become a lot more strategic, and a lot more fruitful.

Of course, becoming a "Yes Team" is a lot easier when the technology teams and the business units rally around a common goal—or, in this case, a common enemy—to support a more digitally secure organization. Take the WFM paradigm. People had been working from home to varying degrees for a while, but COVID made that the new reality. And what we all found out very fast is that WFM could become a snake pit for employees, suppliers, partners and contractors if the right cybersecurity frameworks were not in place.

The same thing has become evident in cloud services, which are experiencing stratospheric growth across the board in businesses—including, interestingly enough, the development, deployment and support for cybersecurity services. The cloud's potential for delivering cybersecurity has been understood for some time, and now it is becoming a reality.

COVID may have accelerated these trends, but the collaboration throughout the organization in response to the pandemic has helped remake cybersecurity into the "Yes Team."

Changing Rules, Changing Roles

For all of us, our organizational roles and priorities have undoubtedly evolved as the pandemic has lingered and its impact expanded and deepened. Some of us are doing some of the same things, but—less traditional activities, while others may find themselves in completely new territory.

Take the CISO, for instance. With security budgets increasingly moving away from the centralized control of the CISO and residing at least in part now with business units, CISOs have been moving to build tighter relationships with business executives for some time. COVID has accelerated that to the points where the CISO now is acting more as a trusted advisor to the business, creating a security framework that the business units adopt and align with.

The CEO, of course, still is singularly focused on big picture issues and strategy. But now corporate strategy neces-

sarily includes cybersecurity, done in concert with the CISO and others. CEOs who have seen their organizations grapple with data breaches during the pandemic, and walk a tightrope of financial viability, have had to embrace a new skill set, new vocabulary and a new perspective on where cybersecurity fits into the budget picture.

CFOs unquestionably care more deeply than ever about cash management (cash preservation, actually) and driving operating profit amid increasing market uncertainty. But the CFO has often been tasked with being on the cybersecurity team, especially as it relates to the essential risk management functions of compliance, legal and governance. And has there ever been a risk management challenge as meaningful as COVID? The risk of a data breach during such potentially perilous times carries a lot of downside for everyone, not just the CFO. After all, an epic data breach might push the CISO out the door before anyone, but I'll bet that the CFO won't be far behind them in many cases.

We all have to find a way to work together to identify, protect against, and remediate the impact of cybersecurity risk. Many business leaders recognize that cybersecurity is more important than ever in an era of remote work. But with an uncertain economic landscape, it is critical to get alignment to the dramatic shift businesses have to make, earlier rather than later. Don't wait. Don't procrastinate. Don't delay having the occasional hard conversations. You may be surprised. At the end of the day, you want to build out your "Yes Team" to drive the organization toward safety and security, and having the proper investment and budget is absolutely essential. So go for it.

---

[1] "PwC CFO Pulse Survey," PricewaterhouseCoopers, April 2020.

33

Zero Trust: The Strategic Approach to Stop Data Breaches

John Kindervag — Field Chief Technology Officer, Palo Alto Networks

Addressing today's cybersecurity challenges requires a new approach, one that is focused more on strategy and less on tactics. At a high level, strategic thinkers agree that there are four basic levels of engagement:

1. **Grand strategy:** This is the ultimate goal of any entity. The grand strategic direction of an entity—whether it is a corporation or a nation-state—is determined at the highest levels. For nations, it's done by presidents and prime ministers; in corporations, it is done by CEOs and members of the board of directors. A grand strategy provides the vision and direction of the entity.
2. **Strategy:** This is the big idea that is used to achieve the ultimate goal, as defined in the grand strategic objective. It is done at the next level down in the entity. For nation-states, it's done by agency heads, legislatures, or generals. In companies, vice presidents and line of business leaders provide strategic vision. Strategy provides the ideas that give tangible momentum to the grand strategic vision. More importantly, to be strategic, the idea must resonate with the highest levels of the organization while being fully implementable at the levels below.
3. **Tactics:** These are the things we use to execute on the big idea, so that we are able to achieve the ultimate goal. Most people confuse strategy and tactics: They think they are strategic when, in fact, they are tactical. Tactics are implemented in the organization at the next lower levels in the organization.
4. **Operations:** This is the way in which we use the resources we have. The operational aspects are often overlooked because we are focused on tactics without understanding the importance of operational integration. Tactics align with operations to execute the strategic ideas so that the grand strategic goals can be achieved.

So, what can those of us in the cybersecurity community do to align with the grand strategic initiatives of the entities we are duty-bound to protect?

First, we must articulate a grand strategic objective for cybersecurity in the Digital Age; and it must be this: **to stop data breaches.**

To stop breaches, we must update what we think a breach is. Often, we cling to the old-school castle/moat analogy:

"Someone breached the castle walls and they are inside!" This is actually an intrusion, not a breach.

The term "breach" is now a term of art in the legal and regulatory professions. Think GDPR. The breach happens when data is exfiltrated from an organization's network or systems and placed into the hands of unauthorized entities, especially malicious actors. Therefore, to be successful in cybersecurity, we must prevent sensitive or regulated data from falling into the wrong hands. To do this we need a strategy.

That strategy is Zero Trust.

The Broken Trust Model

There exists in our industry a broken trust model for security, built on the axiom, "Trust but verify." This model of anthropomorphizing the network and giving it attributes of trust is the fundamental problem we have in cybersecurity today. Trust is a vulnerability. It serves no purpose for your organization. Trust is not necessary to move packets across a network.

The only users who benefit from trust in our systems are the malicious actors who exploit it for nefarious purposes. We must eliminate the idea of trust from our digital systems if we have any hope of protecting sensitive data and assets from exploitation and breaches by malicious actors. To do this, we must adopt the Zero Trust model.

I will describe the concepts behind Zero Trust in further detail. First let me discuss why it is essential connective tissue for the chapters on transforming cybersecurity from a cost center into a business enabler. To achieve this transformation, business and technology leaders need to rethink their approach to security in several important ways, including:

1. Security must align with the business function.
2. Security must be embedded in the design of networks and applications.
3. Security must be agile and dynamic, with the flexibility to design for change.

We can achieve each of these goals, and others, with the Zero Trust model. With Zero Trust, organizations can position themselves for a future in which they are not in constant reactive mode to threats, but instead have cybersecurity built into their technologies, cultures, and operations.

Why Zero Trust, Why Now?

Today, business-level decision-makers must be on top of the challenges facing their IT and security teams, particularly this important paradigm shift: When it comes to cybersecurity, the biggest issue facing practitioners is the breakdown of their traditional trust model, which is based on the "trust-but-verify" approach to cybersecurity.

In this model, the network was broken into two sides, an external side—the "untrusted" network that connected the organization to the public internet—and the "trusted" side, where all internal users had access to sensitive resources. This is best illustrated by the labeling of the interfaces of early firewalls. They generally had two interfaces: One interface was labeled "trusted," and the other was labeled "untrusted."

This pervasive model means that almost all negative security events—including data breaches—are an exploitation of that trust model. External attackers know that if they can get their packets of code past the "trust" boundary, they will be given privileges—trust—based upon the location of the packets as they traverse the network.

Additionally, threats from malicious insiders are a really big deal, but cybersecurity professionals are conditioned to think of the internal network as "safe"

and the internet as "evil." Users of internal network resources are even called "trusted" users. But some of the most highly visible incidents of our time—including the Chelsea Manning[1] and Edward Snowden[2] data breaches—happened by so-called "trusted" users on a so-called "trusted" internal network.

Zero Trust is built upon the idea that security must become ubiquitous throughout the infrastructure. The model is designed to be strategically resonant at the highest levels of any organization, and yet be tactically implementable by practitioners using commercial off-the-shelf technology. The concepts of Zero Trust are simple:

- All resources are accessed in a secure manner, regardless of location.
- Access control is on a "need-to-know" basis and is strictly enforced.
- All traffic is inspected and logged.
- The network is designed from the inside out.
- The network is designed to verify everything and never trust anything.

Zero Trust is designed to stop data breaches. Stopping data breaches must be the grand strategic objective of cybersecurity because a data breach is the only IT event that can get a CEO or company president fired. Therefore, Zero Trust is the only cybersecurity strategy. Everything else is just tactics.

Transforming the Security Model

Rebuilding security from the inside out means that the Zero Trust model replaces traditional perimeter defense with ubiquitous treatment of security throughout the organization. When assessing how to best redesign the network, companies often choose the Zero Trust framework because:

- **Security needs to align with the business function.** The working environment needs security to align with the business function. Most organizations are split into different departments and not all teams require the same amount of privileges. Enforcing strict access privileges where necessary and doing so efficiently is a priority for those adopting Zero Trust.
- **Modern organizations require elasticity and the ability to design for change.** Different SLAs, admins, audit requirements, regulations, and certifications necessitate flexibility and transparency for auditors and management. Infrastructure and security teams need an architecture that allows for quick changes and optimizations unhindered by controls and complexity.
- **Zero Trust is not rigid.** Another important aspect of Zero Trust is that it doesn't have one single approach. It is not cookie cutter and can be designed specifically around the data, applications, assets, or services that an organization needs to have protected.

Business Drivers

Today, companies are looking to leverage technology to position their internal technology management toward better security and manageability. Many organizations are trying to reimagine security outside of traditional parameters and redefine their security practices to meet both current threats and dynamically changing business needs.

But to get from here to there, organizations must rethink legacy network security to make it simpler and more efficient. When businesses attempt these types of transformational projects, they typically face onerous challenges. Zero Trust initiatives help address these challenges in the following ways:

- **Cost management:** Security teams often face significant restraints on financial, budgetary, and organizational resources. Zero Trust initiatives help maximize resources. Many companies adopt a startup mode when beginning the Zero Trust journey. Therefore, they handle their money very carefully, making sure spending is in line with the team's core competencies, in terms of manageability, maintainability, and scalability.
- **Personnel resources:** Working teams are already lean. Companies face staffing issues and most of the staff is already strained by daily operational needs. Zero Trust teams must start small and leverage the existing architecture and technology to address the environment in a new way.
- **Legacy architectures:** Traditional IT is inefficient. Most existing networks have grown organically and are not designed to be agile and efficient enough to meet business needs. New innovations, such as cloud computing and user mobility, mean that organizations can no longer stay within the bounds of old IT's capabilities. Zero Trust uses technology and architecture to its advantage to make IT a business enabler instead of a business inhibitor.
- **Cloud enablement:** Server virtualization and cloud services change the rules of the game. Most organizations want to collapse the network infrastructure to reduce the number of servers by leveraging virtualization and public cloud infrastructure. The security aspects of these technological shifts remain challenging. How do you put security controls in a virtual environment? How is traffic going to be managed? What happens when applications and data are in multiple clouds? How do you maintain visibility and control? Zero Trust network architecture is virtualized and cloud-friendly.

Conclusion

One of the keystones of protecting our digital way of life is preventing the breach of sensitive data. It is a core of every business strategy that relies upon connected digital technologies. To do this, incorporate a Zero Trust model to ensure that all resources are accessed in a secure manner and all traffic is logged and inspected. With Zero Trust, we can take the next step forward in trusting that cybersecurity can be a true enabler of business success and differentiation.

---

[1] "Everything you need to know about Chelsea Manning," ABC News, May 16, 2017.

[2] "This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks," Business Insider UK, September 16, 2016.

THE CASE FOR THE ZERO TRUST MODEL

- A broken trust model is the most urgent issue facing cybersecurity today.
- All users are effectively "untrusted."
- Security must be embedded throughout the network, not just on the perimeter.
- Networks must be designed from the inside-out, based upon the elements in the network that need to be protected.
- Networks must be designed with compliance in mind.
- All resources must be accessed securely.
- All traffic traversing the network must be inspected and logged.
- Zero Trust is the future of cybersecurity.

THE BUSINESS VALUE OF THE ZERO TRUST MODEL

- **Visibility and security:** The new infrastructure allows network administrators tremendous visibility into users and systems. With enhanced visibility, the environment is more lenient in terms of monitoring and allocating resources. Along with better visibility, Zero Trust forces the application, systems, and security teams to work together more effectively. Zero Trust encourages interdepartmental communication and breaks down silos that inhibit innovation.
- **Cost-effectiveness:** Companies that deploy Zero Trust typically see tangible capital and operational cost benefits. Zero Trust networks require fewer people to manage large, complex, and more secure deployments. Companies experience reductions in people and equipment costs, as well as improvements in uptime and failure rates.
- **Assessment and compliance:** Implementing Zero Trust makes auditing much more straightforward, simple, and quick. Zero Trust networks often have fewer audit findings because auditors can understand and conceptualize them more easily. Many compliance items are built into a Zero Trust network by default, and many current audit requirements were designed to uplift legacy networks and are not applicable in Zero Trust environments.

People

34

Making Boardroom Changes Today to Ensure a Cyber-Secure Tomorrow

Kal Bittianda — Head of North America Technology Practice, Egon Zehnder

William Houston — Advisor, Technology and Communications & Industrial Practices, Egon Zehnder

Go to our firm's website and click the "What We Do" link. The first three words you'll read describe the key drivers that frame our scope of work as management consultants and executive search experts:

Globalization. Convergence. Disruption.

We could just as easily apply those words to the tumultuous state of cybersecurity—and, in particular, the unique demands now faced by and debated in every boardroom. In fact, it would not be an overstatement to say that cybersecurity is reshaping how boards assess risk, practice governance, advise management, and ensure the very long-term viability and prosperity of their organizations. In cybersecurity, global risks are being accelerated by technology convergence at a rate never before seen, causing untold disruption in our work, our lives, and our communities.

And, as is typically true of all forms of dramatic change, board members face critical questions that will determine if the board—and the overall organization—is going to thrive in an era of intensified cybersecurity risk, or be steamrolled by it.

As boards typically do, sorting out the issues, debating the options, and arriving at the most appropriate recommendations involves asking and getting answers to high-impact questions. But instead of simply posing those questions to management, now boards have to look inward and ask those questions of themselves.

And one thing we have learned during our collective years of experience at advising the C-suite and board members is this: Not every board member is going to embrace this kind of change easily. And in some cases, not at all. Get ready.

Why Changes Are Necessary at the Board Level

Aligning your board with the dramatic changes going on in cybersecurity risk is a strategic issue, one requiring a lot of thought, deliberation, debate, cajoling, and even a little good luck. Making the right moves in how the board oper-

ates is a *facilitator in risk management.* The technology shaping cybersecurity issues is undergoing dramatic change—AI, machine learning, blockchain, Internet of Things, and more. The technology risks are getting more complex and dynamic, but at the same time, they reflect important new business opportunities that cannot be shunted aside simply because of new/greater risk.

The right board composition, coupled with setting the right mandate for leadership and action, is the best way for board members to make the greatest impact. It's about making the *right* choice, not the *safe* choice.

After all, nothing comes with zero risk. Boards have always had to deal with geopolitical, financial, regulatory, and product risks, and cybersecurity is the latest addition to the mix. The experience, expertise, mindset, and attitude of your board is critical to juggling the classic risk/reward equation.

There's another important factor—one that is a bit "delicate," to say the least. Although the pace of technology change in the past 20 to 30 years has been dramatic, this is nothing compared to what we will experience over the next few years. That's extraordinarily difficult for anyone to manage, even experienced people. The reality is that the mean age of board members is creeping up in many organizations and industries, and it is becoming harder and harder for some to stay on top of the changes. Yet as the threats grow in number and sophistication, with new types of bad actors and threat vectors, people with current operating experience, fresh ideas, and greater comfort with technology will be needed to help guide policy and priorities.

Although many boards understand the need to come armed with fresh perspectives, not enough board members actually know what to do. This is likely to become more and more urgent as cyberattacks have material impact on an organization's financial performance, regulatory standing, legal exposure, and customer confidence. The next shoe to drop may be successful lawsuits aimed directly at board members for failing to meet their fiduciary responsibilities in a cyber breach situation. If you're a board member, that will undoubtedly make you sit up and take notice.

This is where board dynamics become very important. If you have a board whose members are honest, open, and willing to listen to "different" ideas, it's far easier to deal with the uncertainty and magnitude of cyber risk. Board members need to be fearless in proposing ideas that may seem unconventional, or even radical. That can be a very powerful force for debate and change, even when your board is properly composed.

How You Know You Are Succeeding

Truth be told, a very small minority of companies proactively come to us and ask for help in defining their board composition with an eye toward the future. An initial step we believe bodes well for a board readying itself for the impact of cybersecurity risk is recognizing the need for an orderly board succession plan and then laying out a methodical execution plan over a two-to-five-year period. Savvy board chairs will meet their evolving needs, such as in cybersecurity risk evaluation and governance, by thoughtfully planning around upcoming retirements and departures.

A successful board transition begins with a documented strategic plan that defines the board member archetypes who will be recruited to the board over the period, and sometimes even identifies specific/aspirational people to approach. Unfortunately, too few organizations actually think this through and invest the time and energy to map it. Often boards realize, "Oops, this person

is retiring next year, we need to find an audit committee chair." Or they may have been dinged with a poor diversity score from ISS or Glass Lewis that triggers a search for a female board member.

Experience has also shown us that successful transition plans involve creating and maintaining synergies and strong working relationships in the boardroom. While it doesn't mean everyone has to spend quality time together outside the boardroom, it does mean avoiding adversarial, confrontational meetings where personalities and perceived slights get in the way of doing productive work. Give a lot of thought to the intellectual, personal, and political dynamics of your board.

After all, the days when board members spent 20 years in their seats and then retired gracefully are quickly passing us by. These are ground-shaking times, requiring a more proactive board willing to explore new ideas and new ways to achieve success.

Remember: We're not recommending overhauling your board by orchestrating a palace coup in the boardroom. We've all seen examples of how messy those can get and the kind of unproductive, even hostile, environments they can create. The evolution of the board needs to be designed with its future desired state in mind, in conjunction with managing affected board members in a thoughtful, respectful, and personal manner.

Make no mistake: It has to be done. The very future of your organization and its success depends upon it.

ESSENTIAL QUESTIONS FOR THE BOARD ... ABOUT THE BOARD

We've often seen that boards that are most successful at anticipating and coping with sea changes of the magnitude in cybersecurity risk are willing to look inward and ask very tough, often uncomfortable, questions. Four come to mind:

Are the right people on our board? A successful board starts with having the right people around the boardroom table. However, the answers to the question, "Do you have the right people—and if not, who should they be?" will vary widely depending on the type of organization you have and the current mix of experience on your board.

- If you decide to bring a cyber expert onto the board, unless you are actually expanding the board, that's a board seat you're giving up to a specialist. If having that kind of expertise is a strategic differentiator in your industry (e.g., technology, financial services), or if you want to dramatically shift the cyber posture of your company, that may be a smart decision.
- But if your organization believes it has less cyber risk, you may not want to devote that seat to a cyber expert. Instead, you may decide to focus on ensuring the company has a world-class organization with strong cybersecurity credentials (and the business acumen to match), including strong leaders who will regularly meet with and brief the board.

ESSENTIAL QUESTIONS FOR THE BOARD (CONTD.)

Do you have the right committee structure for evaluating and governing cybersecurity risk? Committees and sub-committees are important to give weight and light to such functions as audit, HR, regulatory, strategic planning, risk, and cybersecurity.

- If you're in an industry where the risk of a cyber breach could have a devastating impact on the company, you'll probably need a technology committee.
- It may be harder for boards in industries that have traditionally not relied as heavily on technology, such as retail and trucking, to justify a dedicated technology committee. Ironically, they could be the ones that need it most, as they probably don't possess sufficient technical talent in their organizations.
- Cybersecurity could also be incorporated into an existing committee, such as the risk or audit committees.

What should board members talk about? Board discussions around cybersecurity must be proactive and center on such issues as:

a. **Organization structure:** Have the CEO and CISO properly structured the organization to address information security? Do we have the optimal reporting structure and the right people in the right roles?

b. **Investment:** Are we allocating the right budgetary resources for our current and future risk profile? Are we making the right budget allocation, and do we know what we get from/for this investment? (Hint: Setting security spending levels is not a mathematical exercise.)

c. **Accountability:** Do we have the right person in the CISO role? Do they have the right goals, and are they properly incented for the desired outcomes?

d. **Improvement:** How do we know that our "non-mitigated" risk footprint is shrinking? What metrics are we using to determine this, and are they still appropriate? (For example: What portion of issues are resolved once and for all? Are the resolution times decreasing over time?)

Of course, the board also needs answers to forward-looking questions: Which threats are imminent that we have yet to address? What would happen to our bottom line if we lost our ability to take orders online for an hour? A day? A week?

What are the responsibilities for the rest of the board? Even if you're not the board's resident cyber expert or you don't sit on a relevant committee responsible for cybersecurity oversight and governance, you have a critical role to play.

- Every board member needs to be involved in the discussions and deliberations around cybersecurity.
- You may decide to let your colleagues take the lead on the issues, but you still can and must ask good questions.
- And don't assume that because a fellow board member experienced zero-day attacks at their own company, they are the only one qualified to ask questions about the organization's threat detection, prevention, and remediation practices.
- One smart practice we've seen some boards take is to have the less-technical board members spend a day, at least once a year, with the cyber team to watch what they do, ask questions, and get a practical education from people on the frontlines.

35

Recognizing, Developing, and Deploying Good Cybersecurity Habits

George Finney — Chief Security Officer, Southern Methodist University

I'm a Chief Security Officer for a major United States university. I love my job, even with its frenetic, unpredictable twists and turns. I thank my lucky stars every day that I don't have a boring job where I know what to expect when I show up at the office or log in to my email.

And that's not all I do. I'm a writer—seriously. I've written books, short stories, crime novels, and screenplays. But since they tell me that writers should write about the things they know best, my last four books have been about cybersecurity. In my most recent book, *No More Magic Wands: Transformative Cybersecurity Change for Everyone*, I introduced the topic with something I knew would become more and more important as we continued to battle with cyber adversaries:

"If security is everyone's job, everyone needs to have the right tools to actually do the job. Not *some* of the tools. Not a *little* bit of the tools. All of it."

And one of the most important tools anyone can have—whether you're a CSO, a CEO, a board member, or anyone who uses technology to do nearly anything—is good habits. Yes, next generation firewalls, automated monitoring, and threat intelligent services all are must-haves in any organization's cybersecurity arsenal. But it's not enough. You also need everyone in the organization—and everyone the organization deals with outside the firewalls—to have well-honed and expertly deployed cybersecurity habits.

That's because cybersecurity is not a skill to be learned, nor is it a competency. How do I know this? Simple: Because we've always assumed that making employees undergo training sessions for good cyber hygiene will yield improved results. And that isn't happening, not in any way, shape, or form.

Cybersecurity is a habit, like getting up in the morning to exercise, showing affection to your children, and adjusting your car's mirrors before you back out of the driveway. And when you look at cybersecurity through that lens, it's not surprising at all that making your employees watch a short video on security doesn't change their behavior. It's like reading a manual about using a treadmill. It's not going to make you any healthier.

Getting Started: Identifying Good Habits

I didn't come up with this epiphany early in my cybersecurity career. Like pretty much everything else, I had to learn it through trial and error. Years ago, we were doing what everyone else did, delivering online cybersecurity training videos, brownbag sessions, and simulated

phishing messages. But we continued to encounter cybersecurity events—just like everyone else, of course—so we knew we were missing something.

Two things stood out in my mind. First, I remembered my childhood experience of learning *tae kwon do*, especially the realization that simply learning the moves didn't really translate into success. I eventually figured out that the drills are what made the difference, and that I had to put in the time and diligence to see real progress.

Second, my HR colleagues and I decided to model our cybersecurity training around something that we knew had succeeded: wellness programs. These days, most HR departments have established health and wellness programs as employee benefits—partly because many employees like the idea of trying to take charge of their health, but more because they actually work. Wellness training succeeds in large part because we can educate and influence people about the benefits of eating healthier or working out, but also how to actually make it habitual. And they use incentives like free vacation days to give employees even more motivation to build new routines. These programs succeed because they force people to confront, acknowledge, and act upon the notion that wellness is a habit, not a skill.

To make wellness work in cybersecurity, we had to focus on identifying good cybersecurity habits and then doing drills with people. These habits need to be institutionalized, starting with top management and board members, not just the CSO having a monthly lunch-and-learn session. If senior executives don't buy into this and send strong signals that cybersecurity is a potential threat not only to organizations but also to employees, we will have to confront a major challenge.

What are some good cybersecurity habits?

Don't react. Don't just look at something and start acting. Try to "see" what is happening by taking your time and noticing the details. If this sounds like "can't see the forest for the trees," you're right. Chances are you are not just seeing an isolated incident or two, but rather data points in a pattern that can be viewed in ultra-high-definition, if you take the time to see the big picture. Automated network monitoring has done great things to help identify abnormal data movement patterns in and out of your systems, but we still need to rely on smart, discerning, curious people to review the information before we allow that very large file transfer to the Ukraine to go through.

Trust your gut. Instincts are powerful defense mechanisms—if we pay attention to them. I'm not suggesting that you overthink everything, and fall into the "paralysis by analysis" mode. But if that email from the CFO seems slightly different from past communications, don't just assume it's legitimate. Reply with a question, or, better yet, pick up the phone or walk down the hall.

Rely on community. One of the big mistakes we often make, both in business and at home, is that we are afraid to ask for help—or even just validation. We don't want people to see us as less than confident in our knowledge, or we may feel that by bringing others into our thought process we are giving away some kind of "competitive advantage" as we seek to advance in our careers. We're not alone, and when it comes to cybersecurity, it's far better to get another point of view. For instance, organizations should consider joining a cyber-intelligence-sharing consortium. Don't worry, you won't be giving up the company secrets, but you may be learning something you didn't know.

Slow down. Because so many factors—including the pace of technol-

ogy change—are accelerating the decision-making process, we too often feel the need to "ready, fire, aim." We often make decisions based on the "bias for action" philosophy espoused by business leaders. A bias for action is great, except when it results in bad decisions that were based on incomplete information and made just to be the first to market. Think about that when your product development team wants to roll out the industry's first IoT-enabled widget and they haven't baked in the security protocols.

Nothing is random; make planning a habit. When bad things happen—property crimes, shootings, motor vehicle accidents, and more—we ask ourselves, "What could we have done differently?" That kind of introspection is good, but only if it results in making scenario planning a systematic, thoughtful process. For instance, our employees and third parties accessing our proprietary data have to log on to Wi-Fi networks securely and with the right permissions. Everyone also must change their passwords in a thoughtful and sincere manner and avoid leaving those passwords on Post-It Notes on our screens. Good planning—and repeating good habits—is essential.

Let me give you a real-world example of what I'm talking about. I recently met a business journalist who had written about cybersecurity. We got to talking about the subject and my focus on good habits, and she excitedly told me a story about what had happened the night before.

Her husband received a text from PayPal, alerting him that a $1,000 transaction had been made in his account. He was initially confused and then immediately irate, convinced that someone at PayPal had made an error. He told his wife, sitting across the dinner table, what had happened, and said, "I'm going to see what they're talking about." Just before he could click the PayPal link in the text, the wife screamed, "Wait!" and grabbed the phone from his hand. As you can now imagine, her good cybersecurity habits warned her that something was amiss, and that her husband was a nanosecond away from enabling a phishing attempt.

This kind of thing undoubtedly happens all the time in our organizations, from the largest governments and multi-national corporations to small retail stores using technology to manage their finances, track inventory, and pay employees. We have become so dependent upon technology for everything in our business and personal lives that we sometimes let down our guard—often with catastrophic results.

What Can and Should Business Leaders Do?

While good cybersecurity habits are developed and honed by individuals, the C-suite and the board play outsized roles in promoting this kind of good behavior.

First, keep in mind Patric Versteeg's thoughts in the Second Edition of this book about creating a culture of cybersecurity. Patric notes that culture is shaped by management and then is embodied in the organization's people and processes. It's very trendy to talk about a bottom-up approach to problem-solving, and it often makes a lot of sense. But don't kid yourselves; we still are very prone to hierarchical organizations, and executives remain the most powerful and influential force in the enterprise. Executives need to exhibit "intentionality," based on the things they do, what they say, how they ask questions, and so on.

Second, it's unfortunate to say that too many executives display an air of entitlement when it comes to cybersecurity habits. It is often personified by that frightening word: Exceptions. Picture the stereotypical CEO. He or she may urgently need something done, so they demand action. Of course, they may feel they don't need to go through the proper

cybersecurity protocols to request that large payment to a strategic vendor that is trying to deliver a critical part. When that email comes through to the treasurer or CFO, everyone jumps to attention, only to find out that the request is really from a hacker mimicking the CEO's email account.

Third, executives need to support the CSO and the HR director in institutionalizing training programs for good cybersecurity habit development—and they need to participate in them, as well. If executives are going to be taken seriously in promoting the importance of good cybersecurity habits, it must become a leadership mandate. In my book, *No More Magic Wands,* the main character of the book isn't the CSO, it's the business executive who champions and pushes for change. It is incredibly important for business leaders to be seen as the agents of transformation for good cybersecurity habits, not seen as just sitting back and directing the CSO to lead the way. Nobody wants the CEO to be a micromanager on cybersecurity, but a CEO who abdicates their leadership role in this area is a big, red warning light for board members.

Conclusion

Aristotle once said, "We are what we repeatedly do. Excellence, therefore, is not an act, but a habit." Today, he'd either be a $1,000-an-hour management consultant or a CSO.

Leaders must take big steps toward institutionalizing good cybersecurity habits throughout their organizations; without it becoming part of the corporate culture, it will never be actualized by employees at the office, on the road, or at home.

So, keep investing in cutting-edge technologies, sophisticated analytics, and innovative cybersecurity tools. Make sure your SOC is properly staffed, your business units have embedded security professionals, and your CSO is as well-versed on inventory turns and competitive differentiation as they are on botnets and spear phishing.

But also remember to put in place the steps covered earlier in this chapter:

Don't react.

Trust your gut.

Rely on community.

Slow down.

Make planning a habit.

Then, please give me a call to share your experiences. We can write a book about it.

36

Social Engineering Attacks: We're All Targets

Yorck O.A. Reuber — Chief Information Technology Officer, Allianz Malaysia

In today's environment, professional attackers know how to avoid your security technology by using social engineering and picking out human victims within your company. In fact, human targets have moved ahead of machines as the top target for cyber criminals. As noted by IDG's publication, CSO, "Hackers smell blood now, not silicon."[1]

Your employees can be difficult to protect. Adversaries will use people's emotions and their readiness to be helpful to obtain information that helps launch a highly targeted and often believable attack. Process and technology alone will not address this. Raising awareness and increasing vigilance will help you protect your employees and your organization. More importantly, it will help you build a culture of cybersecurity.

Cyberattack Calling and Other Modes of Attack

Targets of a social engineering attack need not be executive staff or members of the research department working on a secret project. More often, criminals target a random employee they spied in advance to ensure the attack is formulated in a maximally convincing way. They use social media to discover details about projects, names, dependencies between departments and individuals, and friendships between colleagues. Once they have the baseline information, it's simple to approach an employee, appear legitimate, and obtain corporate information or access to corporate networks. Here are some examples of approaches used:

Cyberattack calling: A call via the switchboard results in what appears to be an internal call. In this call, an urgently required support activity will be referenced: "Our colleague, Mrs. X, has not given me the data I urgently need to finish the report for board member Y. She is now on holiday; I am sure I will be fired if I do not send it immediately. Please help me … I can't afford to lose my job." Far too often, financial, corporate, or personal information is then disclosed in an attempt to help the caller do their job.

Corporate network access: An employee receives an email from someone who appears to be working in the same company. The mail signature is correct, and the content fits with the daily routine of the recipient. The inhibition threshold to open the malware-infected attachment or to click the malicious link is very low. In 95% of all cases, this click will then result in a successful malware infection. This is the entry point

for a far more sophisticated campaign, which gives the attacker backdoor access to the corporate network that may only transpire several months later.

CEO fraud: The cybercriminal pretends to be a general manager, CEO, CFO, or other high-ranking employee. The email might read as follows: "A secret company takeover is coming and only *you* have the trust of senior management. Further information will be transmitted to you from (pretend) Bank Clerk X from (corrupt) Bank Y." The follow-up email will contain bank account details of an account controlled by the fraud organization and an amount to be paid.

The consistent theme, regardless of approach, is that the cybercriminals will have used social engineering to make their approach appear as legitimate as possible. Unless employee's awareness is raised to be vigilant at all times, these attacks can be treated as a normal communication from a colleague or manager.

Defeating Social Engineering Through Training

Cyberattacks via social engineering are nothing more than old-school acquisition of information through hands-on research. Many attackers and social engineers try to take advantage of people's emotions and readiness to help others. And their successes come from the ways in which their attacks appear absolutely believable. Little hints can help the attacker move forward, such as:

- Colleague X is on vacation
- This is done by Department A
- Yes, our CFO is usually very impatient
- No, we use antivirus from vendor Z

Every name mentioned, every connection from day-to-day business, will help the attackers prepare the next call so it's even more efficient or targets a more fitting contact person.

Train your employees and yourself to always stay critical and never divulge anything to unknown parties on the phone. Managers, especially, tend to underestimate this type of attack as they consider themselves unlikely to ever reveal anything. This can be a very dangerous mistake.

Raising employee awareness to suspicious phone and email communications is key. Some of the triggers employees should be trained to look for include:

- Subtle errors or differences in URLs or email addresses that on first look seem normal. Sometimes the sender's name is correct, but when you look at the address, it's subtly different.
- Most attacks will be focused on getting you to click something within an email. If you are being asked to provide personal or corporate information via a link, or if the actual address you're directed to go to doesn't look legitimate, call to check its legitimacy first.
- While many emails and phone calls are well-created, look for language mistakes, as adversaries may not be using their first language.
- Use of corporate graphics or images to make their emails seem genuine.
- Use of language in the email that is designed to make you take action.

If there's any doubt, it's best to call and verify if it is real or not, even if it seems the email has come from within the company. IT security teams should continuously train and inform employees and colleagues. This can happen via employee meetings or via automated penetration tests that check password quality.

Especially effective are self-designed phishing emails. These are created by your cybersecurity team and used to increase employee awareness of potential phishing emails. You can use a vari-

ety of incentives to mislead the recipient to click a contaminated link—different people will respond to different stimuli. You might try to tap into an emotional response or offer a tablet or smartphone as a prize. A phone call after a click explaining how to avoid the mistake in the future will not only reduce risk that the employee will make the same mistake again, it will also encourage people to come forward and report a similar situation in the future. This type of targeted education is far more efficient than generic training and preaching the same doctrine to all employees in a sterile environment.

Every email the IT department can identify directly after—or even before—the first click lowers the chance of a successful phishing attack. As soon as the attack path is known, the IT team can block access to malicious web addresses, prevent the execution of the malware, and reset potentially phished passwords.

For these tests and training to be effective, it is critical that there be a no-blame culture. Employees must understand how to report a situation in the future. And you need a way of monitoring people who do not report when they have clicked a contaminated link so you can work with them to ensure they do report it in the future.

The combination of deploying different activities and repeating them regularly is key to success. However, don't go overboard or you will achieve the opposite effect. A tool that checks the quality of passwords, is too old, or is poorly configured is not only expensive, it can also frustrate employees to the point where they start writing down their keys again. In this case, the company would have to spend a lot of money while decreasing the level of security. With a much less expensive employee event, the company might have achieved far more. Events that thrill the employees with concrete examples help generate awareness of cybersecurity challenges.

It also helps to recognize behavioral changes of employees and colleagues as early as possible. Anomalies can be logins from unknown places or data accessed from previously inactive seats. Modern protective tools and processes can help by recognizing anomalies and automatically alert IT and security personnel to proactively shut security gaps and contain and limit the damage of a successful attack.

It makes more sense to watch the critical data with this type of process than to establish stronger barriers around the data center. These days, intrusions into the company network are hard to prevent; it is crucial to notice manipulations and data loss immediately in order to limit them.

Posing Critical Questions

To get a feel for the organization's vulnerability to social engineering, and the type of training that would be most effective, the IT team can pose specific questions to managers and employees, including senior-level executives and board members. Questions to ask include:

- What percentage of individuals have a general security awareness?
- What is the common understanding of cybersecurity across the people in your department? How does that change across the company?
- How well are the organization's security experts understood, or do the IT and security teams speak a different language than the business people?
- What obstacles have data security concerns created at work?
- Has the security situation produced concerns, and what overreactions has it created?
- Who are the in-house, social engineering or forensics experts, and how do they keep themselves updated?

The answers to these questions will be different, depending on the business unit. Executives at a regulated company handling health data might exhibit greater awareness than those at an unregulated company. The reality, however, is that every company is vulnerable, and every organization has data that needs to be protected.

The potential for harm is endless. The organization must be aware of the risk. To reduce this risk, it is important to prevent an overreaction, which complicates interactions with customers and reduces your employees' ability to work.

In addition to posing questions to employees, organizations can benefit when senior-level executives pose specific questions to their cybersecurity leaders. These questions can help determine what intentions and goals they are trying to achieve with their cybersecurity investments:

- What is your intent with this investment? In other words, what are you protecting?
- What is the business impact of doing so?
- What is the business impact of not doing it?
- What is the risk of delaying the investment—can we delay it six months, or can we speed it up?
- Do we have anything similar already in place? Why is this not already sufficient?

Raising Awareness for Every Single Employee

Top executive management needs to be willing to bear the consequences of cyberattacks and ensure appropriate and balanced communications to all employees. There are some basic points I would urge all executives to look at within their departments and across their organizations.

Employees must be aware that information, such as, "Who is working where and with whom?" is extremely interesting for industrial spies and the people supplying them with background information. This is the same as it is in private life, where burglars are notified by Facebook when a house is empty due to a long-distance trip and where the house is located. This example can easily be transferred to work life. Pictures from the last company party deliver information regarding which employee knows which colleague and what their names are. This might already be enough information to tune a spear-phishing email with personalized information and provoke the fatal click.

Obviously, you can't prevent employees from using social media, but you can ask them not to post work-related information, i.e., people's roles, names of projects, etc. These days, every comment on the web can manipulate public opinion regarding the employer or provide important information that adversaries can use to start an attack against IT or other departments.

Conclusion: We Are All United

Every employee on every level of the organization must be actively aware that he or she is personally responsible for data security and the image of the company. Only with continuous and engaging communication can security awareness be established and a culture of cybersecurity be developed. Only by making employees aware of the risks and consequences can carelessness be prevented and sensibility raised. Only through constant vigilance can organizations ensure that security risks are identified and, even more importantly, reported.

It is also important that in-house security experts—and other leaders—network effectively and empower the right culture. By sharing information with colleagues from other companies, your IT and security teams will know what questions to ask internally. Leaders can learn from the failures of others, and also from their successes. In the war against cybercriminals, all companies must be united.

---

[1] "Top 5 cybersecurity facts, figures and statistics for 2018," CSO from IDG, Jan. 23, 2018.

Process

37

How to Manage a Data Breach

Lisa J. Sotto — Partner and Chair of the Global Privacy and Cybersecurity Practice, Hunton Andrews Kurth LLP

Every organization is vulnerable to cyberattack. But being aware that an entity is vulnerable is not the same as being prepared to manage such an event. The number of data breaches annually continues to skyrocket. According to the most recent data breach report by Verizon, there were 2,216 data breaches in 2017, across 65 countries. More than three quarters of those breaches were financially motivated.[1]

Managing a data breach is a major undertaking that can quickly overwhelm an organization in the throes of an attack. Depending on the size and scope of the incident, it could monopolize virtually all of management's time and energy for months. Worse, it could expose the organization to enormous risk—financial, legal, and reputational—if the appropriate steps are not taken from the beginning to help ensure a proper investigation, reporting, notification, and communication.

Among the most effective ways to prepare for a data breach is to have a clear understanding of the process involved in responding to an intrusion. There are many lessons to be learned from best practices that have evolved over the years and enabled organizations to successfully navigate global data breaches.

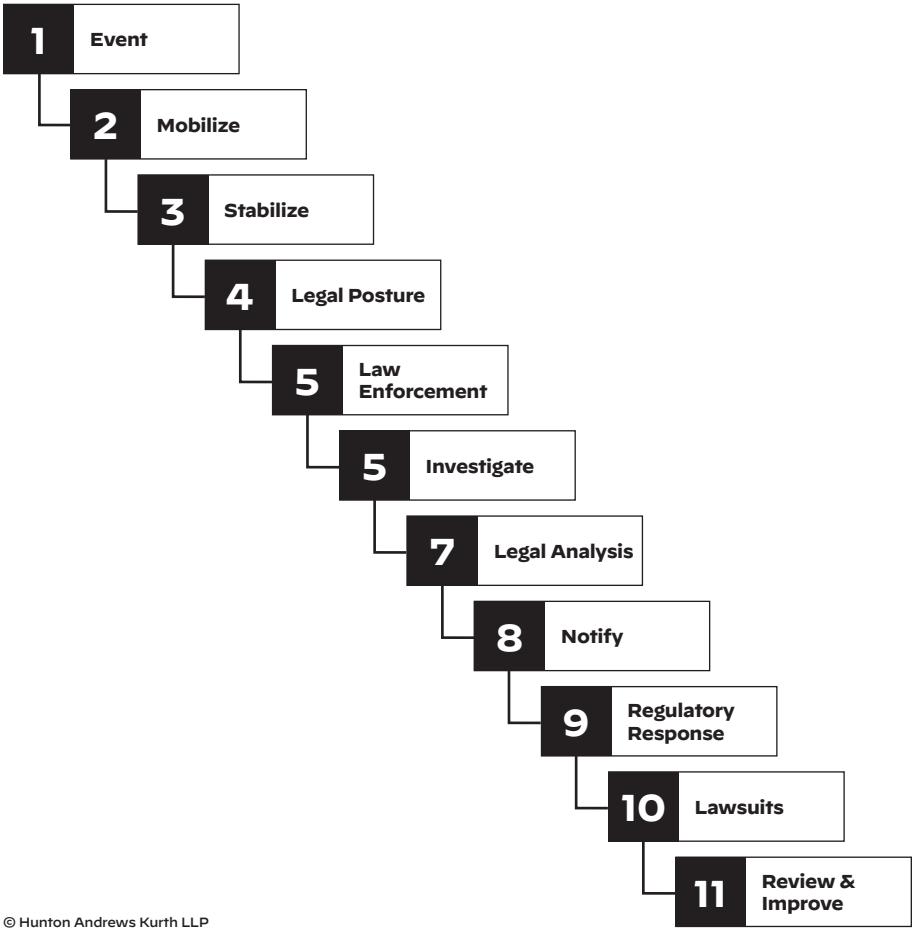
Event and Mobilization

To understand the arc of a data breach, it is important to consider each step in the timeline on the next page. Regardless of industry sector, every organization experiencing a cyber event generally will experience the stages set out in this timeline.

The response effort commences immediately following identification of an attack. The organization must quickly mobilize the proper resources for a coordinated response.

Businesses may learn about a cybersecurity event through a variety of channels. For example, the information security function of an organization may find an anomaly in the company's systems, signaling a breach of the system. Or the entity might be contacted by law enforcement officials who identified data linked to the company on the Dark Web. Alternatively, a company's customer service center might receive a sudden barrage of customer calls suggesting that fraud has occurred. The media also is active in identifying cyber events and notifying companies before they find the issue in their own systems. Although there are many different avenues by which an organization might identify an issue, the key is to respond immediately and start putting the right plan in place.

Data Breach Response Timeline



Once aware of an issue, the organization's chief information security officer and her team generally will take the lead, along with the company's general counsel. Outside counsel frequently is brought into the fray in an effort to preserve the company's legal posture, including protecting privilege—to the extent possible—around the investigation. If the breach appears significant, counsel likely will advise the organization to implement a legal hold, requiring that relevant records be preserved. Counsel also may raise the possibility that the breach constitutes a material event requiring disclosure under the securities laws. Finally, counsel may suggest notifying the relevant insurer.

Counsel will work with the organization to determine whether to retain an outside forensic investigator. For a major breach, several different investigative teams might be brought in, each with different areas of expertise. For example,

some external experts have deep technical knowledge in finding and following the footprints of an attacker. Others may be adept at gathering intel and determining the attribution of a threat actor. Still others, such as certified PCI forensic investigators, may focus exclusively on the payment card aspects of a breach.

In addition to hiring forensics experts, it also may be appropriate to contact law enforcement authorities during the early stages of awareness and investigation. Depending on the circumstances, the company might choose to contact either a federal or a local law enforcement agency.

It is important that the group handling the incident be limited to need-to-know personnel. Keeping the circle of breach responders small can help to prevent leaks and speculation.

Notification

As the forensic investigation is proceeding, the relevant legal analysis is occurring simultaneously. Among the questions at this stage are the following: What type of data is involved? Is the affected information considered personal data? If so, what data elements are affected? What are the jurisdictions of the individuals whose data may have been impacted? How many people's data is at risk? Over what time period did the attack occur? Is the intruder still in the system? Myriad questions will need to be answered at this stage.

With respect to breach notification, in the U.S. alone, it may be necessary to analyze the laws of each of the 50 states (and a number of other jurisdictions with breach notification requirements, such as Guam, Puerto Rico, the U.S. Virgin Islands, and Washington, D.C.). In the EU, with the enactment of the General Data Protection Regulation (GDPR), companies are required to notify government authorities of a personal data breach within 72 hours of becoming aware of such an incident.

Given the aggressive timing requirements of certain breach notification laws, organizations often are in the unenviable position of having to issue notification while the forensic investigation is taking place. The difficulty of this position is that the findings from a forensic investigation frequently change as the investigation proceeds; entities would be wise to avoid relying on their first instincts when trying to scope the issue. The forensic investigation will need to unfold before the nature and scope of the breach can be properly understood and assessed.

In these early stages, counsel typically begins working to craft the appropriate documents, which could take the form of notifications to regulatory authorities; letters or emails to affected individuals; and notices to a variety of other stakeholders, such as business partners, enterprise customers, service providers, media, employees, and relevant government entities (in addition to regulators).

There may be many parties to consider and numerous stakeholders to manage. Crafting a communication strategy can be challenging, and external PR experts may provide sorely needed assistance. Adding to the pressure, this strategy often must be crafted within a tight time frame when the facts are not clear. As mentioned above, in the EU, there is a 72-hour-notice requirement for notification to the appropriate government regulator. In certain industries, such as the energy sector, notification to the regulator could be required in as little as one hour.

It is also important to understand that the evolving narrative may not be in the company's control. Social media plays a significant role in today's information environment. News of a data breach will go viral quickly, even before an affected organization has had an opportunity to coordinate a communication strategy. A third-party public relations firm may be able to provide assistance in helping to

manage the message and craft the right PR framework.

The notification generally should be sent directly to the affected individuals. Alternatively, if the impacted organization does not have contact information for the relevant individuals, or the cost of mailing a notice to the affected population would result in expenses exceeding an amount specified by law, "substitute" notification is available. This enables the affected organization to provide the public with information regarding the data breach. The substitute notification rules require the affected entity to post information about the breach on its website, provide notification to statewide media (which is most commonly accomplished via a press release), and send an email to the relevant individuals if email addresses are known.

Sending the notification in a timely manner is essential. To assist with the mailing, companies often retain external mail houses. In addition, the services of third-party call centers are frequently invoked to assist with the inevitable barrage of calls following notification of a data breach. It is helpful to use skilled customer service agents, particularly those in specialty call centers that routinely handle data breaches.

Going Live

Once the event has been announced publicly, the affected company can expect an immediate barrage of inquiries—from federal regulators to state attorneys general to foreign data protection authorities. The company will be faced with myriad questions about the data breach, as well as the organization's overall security posture. Business leaders should anticipate a multi-month, or even a multi-year, exchange of information and dialogue with regulators.

With respect to regulator activity following a data breach, most government inquiries result only in an investigation, not enforcement. Should an investigation culminate in an enforcement action, fines may be imposed by some regulators (such as state attorneys general and some overseas data protection authorities). Other regulators, such as the U.S. Federal Trade Commission (FTC), have limited authority to impose monetary penalties and instead often seek equitable relief. In actions involving the FTC, enforcement associated with data breaches typically results in a settlement in the form of a consent order. The FTC could impose significant financial penalties for violation of a consent order.

In addition to regulatory activity, lawsuits are likely to follow most significant data breaches. These actions may be brought by affected individuals, issuing banks, shareholders, and other parties directly or indirectly impacted by the breach. Lawsuits resulting from data breaches can take years to resolve. Between litigation and regulatory action, organizations will be dealing with the ramifications of a breach long after the actual event.

Being Prepared

In addition to understanding the processes involved in managing a data breach, there are steps organizations can take to be better prepared before they suffer a breach and are thrust into response mode. Although some cyberattacks are inevitable and cannot readily be prevented, being prepared to identify intruders quickly and manage the fallout is critical in today's pernicious cyber environment.

One key readiness step is to build relationships in advance with cybersecurity experts. The better-prepared companies know which forensic firm, counsel, PR firm, call center, credit monitoring service, and mail house they will retain in the event of a breach. These breach response

providers may be listed, for example, in the company's incident response plan.

Purchasing cybersecurity insurance also is a key cyber preparedness step. The organization's cyber insurer can play a significant role in helping to assemble a breach response team. Cyber insurers often have significant experience managing breaches; compromised companies can leverage that experience to help accelerate and coordinate the response.

Other key cyber preparedness steps include maintaining a state-of-the-art incident response plan. This plan typically is a dynamic document that should be revisited frequently to reflect the rapidly evolving threat landscape. It is also important to establish a relationship with relevant law enforcement authorities before experiencing an attack. Get to know local cyber law enforcement teams in advance, and begin building a collaborative relationship before an incident occurs.

Many organizations conduct tabletop exercises to practice their incident response plans and help ensure that the members of their incident response team understand their respective roles and responsibilities in the event of a cyberattack. Tabletop exercises help build institutional muscle memory and will serve to streamline an entity's breach response, mitigating harm associated with an actual event. Although cyber incidents are inevitable, practicing managing such an event through a tabletop exercise can serve to reduce inefficiencies and organizational stress associated with real events.

Conclusion

The threat of cyberattacks continues to grow. Whether criminal hackers, nation-states, or hacktivists, cyber intruders are often technically savvy, well-funded, and highly organized. Because of the potential havoc cyber attackers can bring, it is incumbent upon all companies, regardless of industry sector, to take appropriate steps to prevent successful attacks.

In today's precarious cyber environment, organizations need to be aware that the increased scrutiny that could result from a data breach could have a profound impact on a business's operations, financial position, and reputation. How an organization responds to a data breach is often a bigger test than the breach itself. By knowing what it takes to respond, business leaders can be better prepared to provide the leadership and guidance necessary to successfully steer their organization through a cyberattack.

---

[1] "2018 Data Breach Investigations Report," Verizon, March 2018.

38

Incident Response: How to Deal with a Cyberattack

Dr. Andreas Rohr — Chief Technology Officer,
Deutsche Cyber-Sicherheitsorganisation GmbH (DCSO)

Compromised networks are the new normal. It does not matter which sector a company operates in or how large or small it is: Professional attackers find data in every organization that can later be turned into economic advantage or cash on the black markets. For some time, the question—from the criminals' perspective—has not been *whether* an organization can be successfully attacked; it has been only a matter of *when.*

While it may be uncomfortable to acknowledge this new reality, it is necessary. By recognizing that total protection is not economically feasible, leaders in business, IT, and security can focus on the real task at hand—minimizing the chance and impact of a data leak and getting back to the work agenda.

Of course, even in a world where successful attacks are a part of daily business, your organization cannot get by without security mechanisms such as firewalls, virus scanners, ID and access management, etc. These components generally ward off attackers that are not operating in a targeted fashion; adopting the watering-can principle (one of the sprays of water is bound to hit the target), these attackers search across wide areas for vulnerable infrastructures.

By contrast, professionals with a targeted approach can generally overcome these hygiene security mechanisms. In most cases, they do this by selecting one or more employees in the target organization and turning them into unknowing accomplices for the leap over the firewall, via social engineering. Another common mechanism is to use less-secure entry points at a subsidiary or supplier location that are connected to the corporate network.

Allow the Attacker to Have Their Moment

In such cases, attackers initially have one objective: remaining undiscovered for as long as possible in order to tap into company secrets. If data thieves have compromised your network, managers should take time to reflect on the situation. They should not act on their instinctive response to take the affected systems offline and delete or even dispose of them in order to keep the loss as small as possible.

Modern, smart attackers set up several back doors, allowing them to regain access to the network. In today's complex IT infrastructures, often distributed across countries, it is easy to set up vari-

ous hidden access routes. So, if the company deletes parts of the criminal's toolkit or footprint, it does not take out the data thief's full arsenal of weaponry.

This takes the company into a more dangerous phase because people think they can relax. But that relaxation is, at best, deceptive. Think about it this way: If you discover an intruder in a bedroom in your home because his flashlight has given him away, your instinctive response is to drive him off. But in doing so, you may have overlooked an accomplice lurking in the darkened kitchen.

Waiting has the additional advantage of allowing your team to learn about possible additional back doors by observing the behavior and tools used. Moreover, by gathering information, it is possible for your team to gain insights into what is motivating the intruders, possibly even discovering their identity.

Plan Countermeasures in Secret

Naturally, you cannot allow the intrusion to progress to the point where data thieves are clearing out the company silverware under the gaze of company management. If criminals are starting to work on databases, design drawings, confidential contracts, or the entire customer base, you must disable the ability of the attacker to act, and cut connection immediately.

But shutting systems or connections down is not enough. In order to avoid data being copied again once the connection is switched back on, the data needs to be completely removed from the compromised network and a transitional structure created.

Nearly all attackers have the patience to wait until a company shuts down parts of its network, so a shutdown without rebuilding is insufficient. As long as the intruders are only creeping through the network by lateral movements, cybersecurity specialists can track their movements, making it quicker to identify the entry points and tools used.

In an extended organization, this process of illumination and tracking can take anywhere from eight weeks to six months. Admittedly, a waiting period such as this can be hard to tolerate. For that reason, if an incident does occur, company management needs to be united in its response, in advance of the attack. If the discussion starts when you learn about the intrusion, valuable time is being lost—especially since the outcome of the discussion could well be of questionable quality, due to the massive pressure from the crisis situation.

Who Turns the Tap Off, and When?

It needs to be clear who in the company is allowed to do what in the event of an attack being detected. Which committee or which employee is empowered to decide that the connection gets cut? Who releases what information to outside parties, lawyers, supervisory authorities, the stock exchange supervisory authority, customers, and the press?

It does no good getting together for the first time to thrash this all out as the intrusion is actually happening. Being prepared also means developing as detailed a scenario as possible for "pulling the plug," i.e., determining which data is not permitted to be transferred outside the company by thieves under any circumstances, and how the shutdown of the affected systems is to be carried out.

In most cases, you will bring on an external incident-response service provider to handle illuminating the network and the hoped-for detection of the attackers. This service provider should be tied in to the company under contract at an earlier stage, and should not be brought on board in a frantic rush as the damage is being done.

At the same time, it is the service provider's duty to protect the customer from misuse by overly curious employees. Confidentiality clauses are therefore essential.

In order to enable the inspection of systems, networks, and services operated by external service providers, these rights need to be firmly anchored contractually in advance under outsourcing arrangements.

Set Out Responsibilities and Get All Stakeholders on Board

It is necessary to decide who will be making decisions in the event of a crisis, because no matter how good the preparation, unique situations will always arise. In bigger companies, it is probably the CIO, unless the CISO reports directly to the executive board. In that case, preference goes to the CISO, since the CISO's area of expertise relates directly to the technical issues involved. If neither post exists, then probably the only option is the CEO or managing director, due to the significance of the decisions.

In all instances, it is important that the security specialists and experts running the IT systems act as a unit. Trust-based collaboration during times of peace is vital. Without it, when the crisis hits it triggers superfluous, time-consuming discussions and turf wars that detract from the actual objective.

You also need to determine how the crisis manager or the service provider entrusted with monitoring the environment can gain access to areas of the organization for which separate administrator rights are required: network infrastructure, applications such as SAP, databases, etc. It is possible that specific areas are being operated by external partners. Advance clarification is needed with all these parties as to which rights are to be granted in the crisis situation.

Empowering a Crisis Team

Prior to a crisis, the organization should have an ad-hoc committee in place that has a clearly defined path for decision-making and can meet as soon as a crisis occurs. The chair of the committee—probably the CIO or CISO—must be empowered to make decisions even against the votes of committee members.

The crisis committee should comprise representatives of individual corporate functions, i.e. legal, IT, IT security/group security, finance, HR, communications, etc. The committee should meet regularly for sessions lasting a maximum of 15 minutes, delegating the matters discussed to the relevant departments for implementation. The decisions should not be discussed with the company's top management, but only within the committee.

Conversely, the organization should not spend too much time preparing for a crisis situation by devising various crisis scenarios. No matter how many employees take part in these planning games, they will still be surprised by the creativity shown and routines adopted by attackers. Accordingly, it should be sufficient to list the five or 10 most plausible attack scenarios (threat modeling) and play these through. Employees can rehearse some of these scenarios in a war game. It is more important to plan for response capabilities such as gaining visibility, given certain trigger information.

Steps for Dealing with the Crisis Situation

Preparing for the crisis situation includes defining the necessary steps and recording them so that no valuable time is lost if you are faced with the threat of data loss. It is true that every crisis involves something different, and every organization brings a different set of conditions to the table. Nevertheless, you can map out a viable plan in advance. Here are some key considerations that may not be apparent if you've never been through a cybersecurity crisis:

1. Never switch off the computers affected; instead, monitor the attackers by creating (real-time) visibility.

2. Do not waste time trying to elaborate on the root cause or assigning blame. This slows down your ability to deal with the crisis, because the people potentially affected will not be open about the situation, and they won't collaborate. Likewise, it is pointless to assign blame. Ultimately, it is the job of the audit team to answer this question during its follow-up.
3. Top management should sit down with the ad-hoc crisis committee at the start and then allow the team to get on with its work. That includes making all required resources available to the committee. It is as simple as it sounds: Give them two suitable rooms, a budget for catering, and release them from filling out irritating forms; tasks involving too much organizational detail should be handled by others.
4. The chair of the committee and his/her respective authorizations must be identified to the whole organization in advance.
5. It is not only IT security experts who need to work in shifts in a crisis situation; IT personnel running applications also need to ensure they can be contacted around the clock. Attackers often favor moving through networks at times outside their victims' normal office hours. If a monitoring sensor is triggered, an applications specialist may need to be brought on board to minimize the consequences.
6. Even if it is difficult for top management, the reporting that would normally happen needs to become a lower priority during the first two weeks after becoming aware that the network has been compromised. Perhaps a committee member can be available once a day for 10 minutes to bring management up to speed on the latest developments. One typical nail in the coffin in responding to an attack is when management wants individual reporting, which can require a great deal of time and effort. While it is an understandable stress reaction, it is a disastrous diversion from the work that is really essential.
7. Once you are past the first two weeks, a central control body should coordinate all further measures and, above all, obtain the necessary resources because, in most cases, there are no budgets for such situations. The employee entrusted with this role should have sufficient experience in having budget discussions with top management and in issuing instructions to the specialist departments involved. This normally rules out external consultants.
8. Another critical question is: Who pays for needed software or external experts? It is clear that the tendering process that would ordinarily be used has to be set aside, otherwise the organization will not be able to act in a timely manner in the event of a crisis. It is possible for a written power of attorney to be deposited in advance or, in the best-case scenario, even for a budget to be allocated. Alternatively, corresponding framework agreements can be put in place for possible support, which can then be called on as the process dictates.
9. A secure communications platform should be made available for communicating with everyone involved—the ad-hoc committee, employees in specialist departments, top management, external consultants, and auditors. The systems otherwise used for email or instant messaging should generally be considered as compromised, and therefore should be ruled out as a channel for exchanging confidential

information. Suitable arrangements include internet data rooms and email SaaS platforms with two-factor authentication that are independent of the company infrastructure.

Conclusion

The time has come to acknowledge that complete protection against cyberattacks has become uneconomical and unrealistic. Instead of spending the entire cybersecurity budget on prevention, a good portion of the money should be invested in mechanisms for identifying successful attacks (detection) and after-care measures (response capabilities).

It is also important to remember that technology is only one part of the solution. People will determine your success in minimizing the damage of a cyberattack, so make sure you make budgets available for raising their awareness. Without the knowledge of what a social engineering campaign conducted by criminals looks like, employees can quickly fall victim to an attack.

In the face of an attack, standard processes within the company and otherwise customary methods of risk management come up against their limits. It may sound crazy and counterintuitive to allow cybercriminals to continue their work once they have been discovered, but that is often an important way to minimize damage.

If we are indeed at a time when complete protection is unrealistic, we must take the time and make the proper investments to ensure that we can respond quickly and appropriately if an attack takes place. In this case, it is an ounce of preparation that is worth a pound of cure.

39

Don't Wait for a Breach to Build Your Communications Strategy

Robert Boyce — Managing Director, Accenture Security, Accenture

Justin Harvey — Managing Director, Accenture Security, Accenture

When it comes to cybersecurity breaches, there are two types of organizations: those who've been breached and those who don't know they've been breached.

So, let's assume the inevitable: Your organization has been breached. An unknown quantity of data has been stolen, records have been compromised, potentially damaging information may now be on a Wikipedia page, and your customers' personally identifiable information is floating around the internet. It's time to plot your communications strategy. Oh, wait. Too late.

Unfortunately, no matter how many smart steps you've taken to shore up your cyber defenses—girding your networks, and protecting your data with sophisticated tools and services—it's important to plan for a breach, especially considering that data breaches are occurring more frequently and with increasingly insidious intent and impact.

Equally important, data breaches aren't one-time-only events. Successful compromises beget more hacking attempts and, thus, it's in every organization's best interest to assume it will be hit—likely again and again—and have a detailed, actionable, and well-rehearsed communications plan already in place when a breach happens.

The Fundamentals of Breach Communications

Breach communications is more than sending letters to customers, talking to the media, or engaging lawyers. It is a comprehensive system of gathering, vetting, and sharing information with all relevant internal and external audiences. It also is designed to help ensure an organization's ability to recover and restore operations after a data breach, regardless of data loss or financial and brand damage.

In our many client engagements, we've seen a fair share of data breaches. We've seen smart, disciplined, well-planned, and meticulously executed communications strategies. But unfortunately, we've also seen some regrettable, unstructured, and poorly executed efforts. In assessing both the successes and failures, we can offer actionable advice in two main areas: components of a breach communications plan and potential landmines to avoid.

Please forgive the cliché, but we know that "hope is not a strategy." So, as you build out your breach communications

plan or modernize an existing one, we encourage you to begin with a few fundamentals:

1. **Stay calm.** The first few hours following the discovery of a potentially damaging breach are critical, and you can undermine your organization's well-intentioned efforts to minimize the internal and external damage if you allow yourself to be overcome by adrenaline, fear, or a misplaced need to seem bold and aggressive. The ability to remain calm and proceed in an orderly fashion will instill confidence in your employees, customers, trading partners, suppliers, opinion shapers, and regulators. It also can help minimize the potential for shooting from the hip with incomplete or inaccurate information, which could cause even greater damage.
2. **Be prepared.** It is an egregious failure of an executive's or a board member's fiduciary responsibility to not take the time and energy to prepare an action plan that includes steps to take before, during, and after a breach. Earlier in this book, Exabeam Chief Security Strategist Stephen Moore laid out some sound advice about cybersecurity preparation, including a smart idea to write your breach notification letter *before* you suffer a breach.
3. **Engage *all* key players well in advance.** When a breach occurs, everyone must know his or her role—which requires that the right people are recruited for input on the plan's development, for involvement in game planning the response, and for assigning the proper roles and responsibilities. Every functional group in the organization must be engaged, and the right external resources—lawyers, forensic analysts, crisis management communications firms—must be identified and recruited. Waiting until a breach happens to start communications planning is much too late, and if you're missing even one key contributor to the breach communications team, you risk leaving out critical elements from your plan.

Key Components of a Breach Communications Plan

At the heart of every breach communications plan is what you do before, during, and after a breach hits. Being prepared is a critical component of your breach communications strategy, but what are the actual steps you should put in place?

Assign roles and responsibilities. Once you've engaged all key players from all key functional groups, you need to decide who is doing what. At this point, don't worry about "committee creep" by including too many people. Some people and functions may participate in the overall communications planning, others may focus on customer outreach. Some may concentrate on governance, risk, and compliance-related matters, and a few may be involved in every element of the plan's development and deployment. The key is crystallizing everyone's role so that when a breach happens and time is of the essence, there's no ambiguity around who does what when.

Take a broad view of your communications targets. It's natural for organizations—especially large, well-known brands with global recognition—to put media outlets at the top of the list for post-breach communications. Obviously, consumer, business, and trade media are important, but they are far from the only people and groups with whom you need to communicate. Regulators will also be keenly interested in the status of your efforts, the extent of the breach, and your plan to stanch the damage. If you're a

publicly traded company, stock analysts will be asking you questions while also answering others from the media about any potential impact to your stock price or competitive position. And don't forget law enforcement organizations, who may see your data breach as part of an organized digital crime ring or another data point in an ongoing pattern of cybercrime they are investigating.

Identify and engage experienced third parties. Crisis communications firms, outside legal counsel, investor relations firms, and cybersecurity consultants all provide valuable perspectives from different areas of expertise. Undoubtedly, they've all been involved in similar incidents with other firms in the recent past, so they will be able to share advice based on real-world perspectives.

Pressure-test your plan. Okay, you've done everything listed above. You've got a comprehensive plan and everyone knows their role. Now what? Do you just sit around and wait? Well, does the military wait for their country to be attacked? Do police forces wait for a crime wave to hit? Of course not. They all practice, practice, practice. They stage rehearsals under as close to real-world settings as they can manage—and so, too, should you. Pressure-testing your plan is one of the most important things your organization can do before a breach hits. It could involve something as simple as tabletop exercises, where a pseudo-breach is assumed and everyone talks about what they are going to do. Or, it could be something more realistic, such as a full-on simulation where participants are not told it's a drill and might do everything short of notifying law enforcement.

Determine how you will communicate. Depending upon the type and severity of the breach, your normal communications media—email, internet, even phones—may not be available to you, either because they have been damaged or their security has been compromised. Have a plan to utilize out-of-band communications and, even, engage in face-to-face discussions. And be careful what you put in writing. While we certainly don't advocate doing anything illegal or improper, it's crucial to understand that written communications may become essential in legal discovery well after a breach has been resolved.

Keep the board informed. You're not necessarily asking for their permission on any aspect of your plan, but there's a good chance that some, if not most, of your board members have dealt with similar situations in their own organizations. Listen to their experiences and heed their advice about steps to take in developing a more effective breach communications plan.

Engage law enforcement. Depending on the nature of your breach and the expertise of the law enforcement jurisdiction, this step can be tricky. Not surprisingly, the increasing incidence of cybercrime has driven law enforcement agencies to treat digital crimes on the same level as crimes of the physical world—robbery, assault, and others. A local sheriff's department, for example, is not going to have the same capabilities—or maybe even the same interest—around data breaches as the U.S. Federal Bureau of Investigation or Interpol. While schools of thought are divided on how proactive organizations need to be in involving local law enforcement when a breach occurs, it's a smart practice to build relationships with law enforcement as part of your pre-breach planning. This way, you have a familiar voice on the other end of the line when you suspect your data breach may be part of something bigger.

Potential Landmines to Avoid

While it's unlikely that your planning will anticipate every potential twist and turn

leading up to and following a data breach, there are some clear problem areas you should anticipate and plan to avoid when developing and implementing your breach communications program.

Fight the urge to overcommunicate. This recommendation may run counter to what executives are used to doing in their day-to-day business roles, but we've seen numerous instances of organizations saying too much, too soon after a breach. Let's say Company A has a breach and loses data on 100,000 accounts; they release a statement talking about those numbers only to discover two days later that 500,000 accounts were compromised. While companies may need to keep regulators well informed on a regular and timely basis, it's good to not have escalating data breach numbers played out in headlines, day after day.

Don't overlook the need to test your communications plan. We've covered this in greater depth above, but one of the biggest mistakes you can make is to develop a comprehensive plan and let it collect dust on a shelf until the inevitable breach occurs. It's important to update your plan on a regular basis; after all, people come and go, business processes change, regulatory requirements evolve. Don't assume the plan you developed last year will still work next year.

Manage and control your employees' use of social media. It's astonishing to think that your employees would go on Facebook, LinkedIn, or Twitter to post updates on their efforts to "help" in mitigating the impact of a data breach. Sadly, we've seen this happen more than once. Most often, employees are simply trying to be good ambassadors of the organization to customers and visitors. To avoid any potential issues, make sure employees know that all social media communications related to a breach must be authorized by a designated functional group.

In her chapter on managing a data breach, Hunter & Williams partner Lisa Sotto provides important advice on the right way to use social media as an integral part of a coordinated breach communications strategy. Her key point rings loudly: "News of a data breach will go viral quickly, even before an affected organization has had an opportunity to coordinate a communications strategy."

Take executive responsibility. Remember the actions of Johnson & Johnson in the immediate aftermath of the 1982 Tylenol tampering scandal? The company's CEO was front and center, embracing responsibility and even advising the public not to take Tylenol; his leadership gained the organization much-needed credibility and leeway in re-establishing consumer trust.[1] Contrast that with the ill-advised comments of a BP executive after the tragic Gulf of Mexico oil spill and fire, where he complained, "I want my life back."[2]

Don't Become a Cautionary Tale

We cannot stress enough how vital it is to have an honest, open, and brutally candid discussion among your executive colleagues about your breach communications plan. As so many authors in this book have emphasized, cybersecurity is a leadership test—not a technology glitch. It demands the full attention and resolute commitment of both business executives and the board, and extends to their involvement in the development of a comprehensive and actionable breach communications plan, which is too important and complex to be left to a single individual to architect.

Cybersecurity isn't a static state; your technology solutions are always evolving to meet the changing nature of threats and vulnerabilities. Your breach communications plan must be every bit as flexible, dynamic, and modernized as your

technology infrastructure. If it's not, fix it—and fast. It's not an overstatement to say that your organization's very viability depends on it. Thoughtful planning, regular testing, and meticulous execution of a breach communications plan will separate the industry leaders from those that become cautionary tales in the wake of a breach.

---

[1] "How Poisoned Tylenol Became a Crisis-Management Teaching Model," Time, September 2014.

[2] "BP CEO Apologizes For 'Thoughtless' Oil Spill Comment," Reuters, June 2010.

40

Making Cyber Insurance a Strategic Tool in Reducing Risk and Improving Resilience

Robert Parisi — Managing Director and U.S. Cyber Product Leader, Marsh

If you magically found a spare $2 million to spend on cybersecurity, what would you do?

If your CISO was asked, their reaction would be immediate and decisive. "We'll expand our headquarters' security operations center (SOC) and those in our core international facilities. Then we'll install next-gen endpoint protection, institute biometric access controls to our data centers, harden our critical infrastructure, and expand our threat intelligence subscription services."

Those and similar technology investments *are* a smart way to go. But it approaches security as a problem to be solved rather than as a risk that needs to be managed. Managing any operational risk needs to be more nuanced. So let's look at it from a different perspective.

Now, what if your CFO and Chief Risk Officer were told that $2 million spent on a bespoke cyber insurance policy could take $100 million of risk off their books and, at the same time, improve the organization's operational resilience? In other words, you would not only be financially protected in case of a costly data breach but also ensure that the organization can withstand the financial impact of a disruption to business operations for a material period of time.

That's not a hypothetical scenario. More and more organizations are facing the harsh reality that their technology will fail, a vendor will not be there when needed, or they will be attacked—if it hasn't happened already—in the future, with potentially grave financial, operational, legal, regulatory, and reputational consequences. Certainly, having the right technology tools, services and protocols in place is essential to fortifying cybersecurity in the face of expanding threats. But the cold, hard truth is that bigger technology spending, in and of itself, isn't going to stop the problem. It may slow it overall, and it may even relegate certain specific threats to irrelevance. But that's not enough to keep your business humming after a supply chain meltdown, data breach, malware campaign, ransomware demand, or distributed denial-of-service (DDoS) attack. Cyber risks are not simply problems that can be spent away. These are operational risks that need to be managed with the same level of attention and diligence as any traditional risk that could potentially put you out of business.

Cyber risk has now overtaken other, more traditional risks and become the number-one nightmare for business leaders and board members. And that risk

has now evolved beyond privacy breaches and lost credit cards. The modern commercial entity is now so heavily dependent upon technology—their own and others'—that the board's biggest concern is whether or not their organization is truly cyber resilient and up to the challenge from the myriad threats out there.

It wasn't that long ago that the C-suite's primary worries about ensuring continuous operations dealt with things like natural disasters and political risk, particularly for multinational conglomerates. And those things are certainly still material considerations, but they are no longer likely to be either the most probable or the most severe disruption a company faces. The Business Continuity Institute, which assesses factors that shape business continuity and their impact on organizations, recently concluded that unplanned technology and telecommunications outages now outpace natural disasters and political risks in disrupting local, national, and even global supply chains. And as severe as the impact may be when an organization is in a geography hit by a flood, hurricane, or tornado, the potential impact of something like a ransomware attack—as the 2017 NotPetya malware attack demonstrated—is likely to be even greater.[1] Not only that, but a ransomware attack is far more difficult to predict and defend against because its source is rarely known until after it hits. Imagine if the hurricane could pick and choose where it made landfall based upon where it could cause the most damage. Now you have an idea of why cyber risk is scarier than weather. But companies manage their risk across a spectrum, with technology, protocol, and procedures being the primary risk mitigation tools. At some point along that spectrum, those risk tools no longer prove effective. It is at that point—for the residual risk—that insurance comes into play. You need a cyber insurance policy that aligns with your risk profile and that is integrated into your overall risk management framework. Cyber insurance is no more an alternative to sound risk management principles than technology is a silver bullet against every threat or exploit.

Cyber Insuranceas a Resilience Play

We all know the traditional insurance model. An event occurs that has financial impact on a person, a community, or an organization. The insurance coverage pays the affected party a sum of money in accordance with the terms of its policies, coverage limits, and so on.

But traditional property and casualty insurance has left a vacuum by not evolving its breadth of coverage along with the changing risk profile of its customers. This is where cyber insurance plays a critical role. Cyber insurance anticipates and accounts for the need for operational and financial resilience. There are massive hard- and soft-dollar costs associated with running your business in the Digital Age. Even very small companies depend heavily—and will depend even more heavily in the coming years—on the integrity and availability of the technology underpinning their day-to-day operations.

It is a lack of resilience, even more than security, compliance, and the threat of lawsuits, that makes organizations increasingly vulnerable to cyber risk. And that's why cyber insurance must be considered part of an integrated risk management strategy.

Recognizing, Acknowledging, and Acting on the Threat

The good news is that cyber insurance is increasingly being viewed that way—as part of a holistic approach to risk management on par with traditional governance, risk management, and compliance functions. Interestingly, research conducted by Marsh, with Microsoft, indicates that cyber insurance "take up" rates—the percentage of organizations in a particular sector that purchased stand-

alone cyber insurance—have been trending strongly upward in recent years.[2]

In virtually every major industry, take-up rates have moved higher in each of the past three years, with manufacturing, education, and hospitality/gaming demonstrating the highest rates of increase. Healthcare, meanwhile, remains the industry with the highest take-up rates. There's a qualifier to this good news, however. The fact is, most organizations have yet to move to dedicated cyber insurance policies. In fact, only about one in three organizations have done so.

What Should You Do First?

Of course, acknowledging the risk and the need to close the risk gaps that even great technology, and incredibly dedicated and innovative CISOs, can't fully plug is the first step. This is truly a case in which denial is not an effective strategy.

Making smart and strategic decisions on how, where, and when to use cyber insurance to mitigate risk starts with some key learnings and actions:

Cyber risk has to be part of the board's normal operational risk discussions. It is business risk, plain and simple. Too often, executives and boards fall victim to a kind of cyber mysticism when confronted with cyber risk, throwing up their hands because they don't feel confident they understand the technology. But at the end of the day, it's about looking at the potential impact of a cyber event, and working backwards from that to plot out how all the defenses and responses, including cyber insurance, mitigate that. It's not only about "How do we stop that DDoS attack that's going around our industry?" but it also has to cover "What is the financial and operational impact to our business if our global supply chain is cut off?"

Get help in assessing organizational risk. Cyber insurance is still a fairly young line of business, and as such, it lacks the rich actuarial data associated with fixed-asset valuation like cars and plants. But there are a lot of helpful assessment tools to evaluate risk, from both inside and outside the firewall. Cyber-risk modeling companies run non-invasive scans and scrapes, and knock on your virtual doors to see if ports are left open. They can give you susceptibility metric to estimate attack vulnerability, without being disruptive to day-to-day business operations. Think of it as CCTV cameras on your virtual world that can see where information is flowing in and out, and that help you determine what that means. For instance, if you learn that you've got a lot of data flowing from a particular port to Kazakhstan—and you don't do business with anyone in that country—it's a pretty good clue something's amiss.

Take the time to understand relevant cyber insurance trends on coverages, premiums, and services, and compare your organization with others. Examining your peer group, however you define it, is a good way to put your assumptions into context, and to frame decisions about how to work with your broker to create a customized solution. But that analysis should not be limited to just what cyber insurance your peers are buying. Some of the assessment tools mentioned above can benchmark your threat vulnerability against a peer group.

Do a thorough, ongoing evaluation of the organization's at-risk asset values. And be sure to stretch your imagination when identifying those assets. Do you have a lot of personally identifiable information of employees, customers, prospects, and trading partners? Do you have trading algorithms? What is your inventory of intellectual property? And be sure to reassess those assets' value regularly, especially when corporate "events" like mergers or the introduction of new products and services take place. In addi-

tion, NotPetya made it clear that physical assets are also at risk from cyber perils, with millions of dollars of smart phones, tablets, PCs, and servers "bricked" by the malware. Being able to understand the value of at risk assets and the potential financial impact of a cyber event are critical first steps in determining the right level of insurance.

Be honest about your pain threshold when it comes to cyber risk. Executives and boards need to be on the same page when it comes to evaluating how much cyber risk they are willing to accept and how much they want insurance to cover. One organization may decide to hold the first $25 million in losses as their pain threshold and expect insurance to step in above that, while others may feel uncomfortable waiting for a digital catastrophe before receiving relief through insurance. Regardless, waiting until the disaster hits is not a good way to make that determination; have that discussion now, and revisit it regularly.

Make sure all the key players are at the table to discuss cyber insurance issues and to make the critical decisions. Of course, insurance decisions traditionally have rested in the CFO's domain, but smart CFOs, CROs, and compliance officers are bringing CISOs to the table to get a better handle on identifying current and future sources of cyber risk, and to collectively assess the impact of that risk on their operations. And CEOs should do more than just stick their heads into the room when these discussions are taking place; they need to have skin in the game, too. And the same thing goes for board members. In another chapter in this book, Paul Jackson of Kroll talks powerfully about heightened levels of board-level corporate governance brought on by cyber risk. Ask a director at any organization that has suffered a debilitating and embarrassing cyberattack if they wished they had asked more probing questions about what their insurance policies did and didn't cover when it came to cyber risk.

Conclusion

Does anyone reading this book honestly believe that their organization's use of technology will do anything except skyrocket in the coming years? Of course not. So it's reasonable to assume that since the bad actors aren't sitting still, your cyber risk profile is going to expand and deepen.

Cyber risk is not a problem you can solve with quick technology fixes. You need to have a smart, sober, responsible plan for mitigating cyber risk that integrates technology, process, and cyber insurance. Evaluating cyber risk on an ROI basis is, of course, smart and necessary. But be sure you consider the full impact of a cyber event on business resilience when deciding what role cyber insurance plays in your enterprise-wide risk mitigation and management strategy.

---

[1] "NotPetya tops list of worst ransomware attacks," ComputerWeekly.com, October 31, 2017.

[2] Marsh Microsoft Global Cyber Risk Perception Survey, 2018.

WHAT YOUR CYBER INSURANCE SHOULD COVER

Cyber insurance is the yin to traditional insurance's yang. The latter enables a company to transfer the risk associated with physical perils, while cyber insurance responds to risk from non-physical perils arising from the ever-evolving nature of technology. Born during the dot.com bubble, cyber insurance now extends to cover a wide spectrum of liability and direct loss and has at its core the premise that all of a company's technology risk should be insurable.

Liability
The heart of liability insurance is coverage for harm that a company causes third parties. In the case of cyber insurance, the harm is caused by either a failure of the insured's computer security or a data or privacy breach, including things like wrongful collection or unauthorized access to confidential data, be it personal or commercial. If such allegations are made against an insured, the insurance will provide a defense of the claim as well as indemnifying the insured for any damages it may be legally liable for.

Regulatory
With the abundance of privacy and data breach regulations, including the recent coming online of GDPR, the insured will likely face a regulator or the obligations imposed by statute before they face a civil plaintiff. Cyber insurance provides legal counsel to assist in responding to a regulator's inquiry and in determining the extent of any obligation under the statute. Insurance can also cover fines and penalties assessed against the insured. The underlying thought here is to avoid a misstep that could come back to bite you later in any civil legal action.

Direct Loss
Cyber insurance indemnifies an insured for loss or damage to its digital assets, as well as loss of revenue and extra expenses incurred because of a computer security failure, or any technology failure not caused by a physical event. Loss of revenue can also be insured if the cause is a security or technology failure at a business that the insured depends upon in its operations, such as technology infrastructure vendors and an insured's supply chain. This aspect of coverage has been evolving the fastest lately, with some insurers now offering coverage for loss of revenue due to either a voluntary shutdown or the failing reputation in the wake of a cyber event impacting the insured. In addition, insurers have added coverage that touches upon the "physical" with indemnification for bricking losses.

WHAT YOUR CYBER INSURANCE SHOULD COVER (CONTD.)

Event Response Expenses
Cyber insurance is unique in that it assists the insured almost from the moment an event is discovered or suspected. An organization will incur significant out-of-pocket expenses investigating the cause and nature of a breach or failure, responding to the various regulatory obligations such as breach notification statutes, and addressing the associated reputational noise. The cyber insurance market has developed two approaches in this area. The first and more traditional being to provide indemnification for incurred expenses, with the insurers also providing an insured access to a panel of expert service providers. The second approach, more popular with smaller companies, is to essentially have the carrier's panel step in to manage the event for the insured, with the insurer dictating which providers are to be used.

Miscellany
In addition, cyber insurance indemnifies the insured if it is the victim of an extortion threat to cause an otherwise covered loss or liability. Cyber insurance also is adept at filling the vacuum created as traditional insurance lags behind or fails to keep pace with the evolving risk profile of the economy. Two recent examples are the extension of coverage for liability arising from a company's use of IoT technology and the risk associated with blockchain technology. Finally, cyber insurance also has expressly adapted to align with traditional insurance as losses become more nuanced, where a physical injury has some cyber aspect lurking in its chain of causation, to ensure that an insured can achieve the maximum recovery for the loss.

Technology

41

How You Should Use Cybersecurity Technology to Improve Business Outcomes

Naveen Zutshi — Senior Vice President and Chief Information Officer, Palo Alto Networks

Throughout this book, you've read great advice from smart people about cybersecurity, with a recurring theme: Cybersecurity is a business issue, not a technical one.

That's correct, of course. But it doesn't tell the entire story.

There's no longer any debate that cybersecurity must be addressed strategically and in a business context by executives and board members, in close concert with their CISO, CIO, and security operations (SecOps) teams. But when it comes to cybersecurity, technology does matter—a lot.

The right cybersecurity technology can prevent a vast majority of attacks, detect vulnerabilities quickly, mitigate cybersecurity risks, and enable security of strategic business initiatives like digital transformation. If done right, these business outcomes can be achieved without impeding the speed of delivery. Of course, that's not to say that wasting investment dollars on yet another point product, or hiring mediocre security operations personnel to manually monitor networks for aberrant data movement, is the way to go. Security threats are dynamic, fast moving, and can be highly unpredictable for legacy and manual approaches to keep up with. With an increasingly machine-based adversary, cybersecurity approaches that are manual, highly fragmented, and point-product-based are doomed to fail.

Instead, we need to take a different approach—one that embraces a comprehensive view of security architecture, with new technology assumptions to make our organizations more secure, even as we use technology to surface new business opportunities. While I won't subject you to a chapter riddled with terms like containerization, micro segmentation, serverless compute, or service provisioning, I do feel it is important for business leaders to understand that there are some critical technology shifts underway that can help us create a more agile, scalable, and modernized cybersecurity layer.

With the workforce changing drastically due to COVID-19—an unfortunate crisis of massive proportion—the need for hybrid or completely distributed workforce management and capabilities takes on heightened importance. As more

employees work remotely using BYOD devices, the attack surface expands.

If we don't make some important technology shifts, we will:

- Not be able to build a strong global organization.
- Waste money.
- Divert badly needed manpower to perform manual tasks.
- Fail to keep up with the breakneck pace of new security risks.

Without a commitment to a new cybersecurity technology paradigm, we will put our organizations in peril, causing irreparable damage to our brands and destroying our customers' confidence in our ability to protect them.

Let me explain why and how.

Delivering Speed and Agility—Securely

In the digital world, success requires organizational speed and agility—more than ever before, in fact. Every organization wants, and needs, to move faster and become nimbler in spotting and taking advantage of new business opportunities. Technology plays a key role in making that goal attainable, as many of us learned over the past few decades.

But for a long time, technology needed a large footprint in order to deliver business benefits. Big iron. Big applications. Big data centers. Big staff to monitor and manage networks. These big capital expenditure (Capex) investments and large IT/security workforces were often considered competitive differentiators for companies. Unfortunately, this legacy of "big technology and large workforce" has become a boat anchor, weighing down our organizations and restricting our ability to achieve speed and agility.

Fortunately, we have seen an acceleration in the adoption of cloud computing, Software as a Service, and anywhere/anytime connectivity. These paradigms enabled organizations to seamlessly adjust to remote work. The impact of COVID on many industries has been devastating; it would have been exacerbated if not for these shifts that have taken place. Additionally, software-based automation has laid to waste traditional approaches to tackling threats and is significantly reducing the need for massive security operations centers (SOCs).

But with the adoption of any new technology comes risk—specifically, cybersecurity risk. Take the cloud, for instance. It has dramatically altered the way we work, and we've only begun to scratch the surface. With cloud adoption, most companies are benefiting from the speed, scale and flexibility that the cloud provides. In our case, when COVID struck, we were able to provide connectivity and secure access to all of our employees who started working remotely—without any change. This was due to the fact that we had switched from on premise based secure access to using our own company's cloud based secure solutions.

With public cloud, however, there is a risky underbelly that can impact companies in profound ways. There is risk in assuming that, because you are using someone else's infrastructure, you don't have to secure it. This is a false, and potentially dangerous, notion. Public cloud requires a shared security model. This typically means that customers are responsible for security above the operating system, including all customer data and IP, and the public cloud provider provides security of the underlying hardware and infrastructure.

Additionally, in using public cloud, access control API keys can be easily discovered and used to compromise vast amounts of compute resources in minutes, since hackers have automated tools looking for those vulnerabilities within systems. They can then exploit

them in ways ranging from bitcoin mining to much more nefarious means, such as stealing intellectual property or customer/employee data.

Like the public cloud, other ascendant technologies like SaaS, big data, machine learning, and connected Internet of Things devices, are today's double-edged sword: big benefits with big risks. This, in turn, has put great pressure on IT and security professionals to move quickly and embrace agility, while at the same time provide critical security safeguards. It's not easy. But it can be done.

Reject the Shiny Tool Syndrome

One of the big challenges in addressing these technologies is how quickly they are being implemented and how fast they are growing. Keeping up with the pace of innovation is becoming nearly impossible. Public-cloud feature development is a good example. In the first eight months of 2020, AWS released so many features that it would take nearly 450 pages of hard copy if you wanted to print them. And that's just one cloud provider.

Some security and IT professionals suffer from what I call the "shiny tool syndrome," while having a fear of missing out (FOMO) on all the new tools/features being developed. Unfortunately, the dirty little secret is that major cyberattacks happen due to poor cyber hygiene. Having legacy security architecture that is good on paper but doesn't prevent attacks, porous access control, and poor implementation of security controls will result in a broad attack surface that no new shiny tool will solve. Focusing first on basic blocking and tackling, like patch management, access control, service account rotation, certificate management, network segmentation, and others—while "uncool"—is a must. A strong, disciplined security process, coupled with an automated, software-based approach to security, one that is focused on solving for the right security outcomes will enable a stronger security posture and better position the company for today's and tomorrow's cybersecurity requirements.

Welcome to the Age of Software-Defined Security

Taking an automated, software-based approach to security is in keeping with one of the important trends rippling across the technology spectrum today, which is the shift to "software-defined" models. Software-defined is typically embodied as an algorithm or application programming interface. What we now call the "software economy," as well as traditional industries, is being disrupted by software-based approaches.

Industries thought to be untouchable, such as printing, taxi operations, hospitality, brick-and-mortar retail, and energy are being disrupted by the software economy. Traditional silicon-based approaches to security are being attacked as well. Having a software approach enables our two favorite requirements: speed and agility. Software-defined solutions can be deployed faster and provide organizations with the ability to deliver new business solutions in a more agile manner. And they provide additional important benefits, such as reduced reliance on Capex and a "light" management profile that doesn't require armies of technicians.

Today's cybersecurity solutions are machine learning powered software-defined solutions. Thanks to the development of powerful and adaptable machine learning tools based on the enormous amount of data being collected, cybersecurity defenses are increasingly shaped by software and the concepts of automation, integration, and cloud optimization. Software-defined security is designed and implemented with the understanding that automated, scalable, cloud-deliv-

ered security software now enables issues to be discovered and remediated in near real time. And as the incidences of zero-day attacks continue to increase, "real time" carries a whole new meaning and business impact. In addition, machine learning–based solutions are complementing rule-based software to further shorten the detection lifecycle of zero-day attacks and prevent them from causing havoc to our critical infrastructure. The futuristic vision of machines fighting machines may be a few years away, but it is increasingly advisable to choose a purely software-defined approach to security.

Software-defined security enables embedding security into the software lifecycle through automated security tests so development lifecycles can be iterative and fast. Additionally, Software-defined security empowers our employees to take more proactive roles in rooting out vulnerabilities and reducing risk. Our SOC team can do penetration testing to hunt for issues before they become problems and set up "honeypots" to attract threats and nip them in the bud. This is an entirely new model for cybersecurity—proactive, automated, and predictive, instead of reactive, manual, and based on "best estimates."

Another aspect of software-defined security is to buy security platforms that enable reinforced integrations (each integration improves the overall security posture), are scalable as companies grow, are consistent across cloud and on-premise implementation, and automate implementation, ongoing upgrade, and policy management.

By using software-defined security platform principles—which are going to be implemented in an agile, enterprise-wide platform, rather than a variety of point solutions for individual threats—organizations can scale security defenses in lockstep with the development of new environments for things like testing new business services or modeling assumptions on customer behavior or supply chain interruptions.

There's that speed and agility we talked about earlier. And that's what makes software-defined security a business issue, not just a technical issue. But it *is* really cool technology.

How Business Leaders Should Talk About Technology to the CISO

It's easy to equate business executives talking to technical leaders with what happens when we go to the doctor for a problem. When we experience sharp pain in our shoulder when working out at the gym, we don't want the orthopedist to give us the intimate details of the composition of the rotator cuff. We want to know how we can stop the pain and maintain our active lifestyles.

Business leaders obviously don't need to know—and certainly most of them don't want to know—about the technical underpinnings of their organizations' cyber defenses. They do want to know whether the CISO has taken the right defenses for known and anticipated risks, has the appropriate funding to ensure success, and has calibrated their cybersecurity with their risk/reward profile for new business opportunities.

When business executives talk with the CISO or CIO about cybersecurity technology, they shouldn't worry about which tools are being used as much as why and how those tools are delivering improved security outcomes. After all, business leaders understand risk, and they have all come around to the understanding that the right cybersecurity technology is an enabler to reduce risk while achieving strategic outcomes safely.

They also now know that the more manual your security processes are, it becomes exponentially harder to prevent new threat vectors from impacting the business, and it adds cost and complexity.

So, business leaders' conversations with CISOs—whether in the boardroom or impromptu in the hallway—should

focus on issues like technical risk and technology process, rather than on trying to learn the language of bits, bytes, and bots.

For instance, business executives and board members should ask questions like:

- Do you believe you have the right security architecture in place for threats that have not yet impacted our business?
- Are your security teams embedded in the business and technology units, or are they sitting in ivory towers monitoring event logs?
- How are you quantifying risk, in terms of our core business assets? What is the financial impact of an hour of downtime after a hack?
- How are you minimizing the attack surfaces and points of compromise?
- What business service or product of ours are you most concerned about from a cybersecurity perspective (our crown jewels), and what are you doing about it?
- When we expand our corporate footprint through acquisition or market expansion, can we scale our existing security infrastructure without having to make huge new investments in Capex and staff?
- What is our optimal approach to adopting a new set of cybersecurity technologies—crawl, walk, or run? What are the trade-offs of each?
- Does our current security technology adequately protect us against potential problems with our cloud service providers or other third parties we connect with?

Conclusion

As I mentioned earlier in this chapter, organizations face an important challenge: how to achieve the goals of speed and agility, but in a safe and consistently secure manner. We all know that technology has become a critical catalyst for delivering speed and agility, as it has for ensuring rock-solid cybersecurity.

But can we use technology to achieve it all at the same time? Can we have our digital cake and eat it, too?

I believe we must. And, fortunately, I'm confident that we can. In fact, it's already happening at many enterprises around the world—enterprises whose business leaders and CISOs have modernized their approaches to cybersecurity technology in a software-defined, platform-driven model that prizes speed, agility, automation, and analytics.

Traditional approaches to cybersecurity—encounter a problem, buy some technology, plug the gap, then repeat—no longer work. They don't scale with the massive expansion of threats and vulnerabilities, and the resultant "security sprawl" is expensive, inefficient, and leaves too many gaps.

Organizations can move quicker and more securely than ever by re-imagining cybersecurity around software-based platforms that are easily deployed, cloud-powered for easy scalability and simple maintenance, and well-integrated into the core business processes.

And when they get to that state, they may even have gotten over the shiny object syndrome.

42

When It Comes to Shadow IT, What You Don't Know—and Don't Prepare for—Can Hurt You

Alice Cooper — Global Head of Derivative Trade Processing IT, BNP Paribas CIB

In a fast-paced and dynamic business environment, organizations depend more than ever on their IT teams as a source of growth, innovation, and competitive differentiation. With those escalating demands have come a tricky supply-and-demand balancing act: how to provide the IT services and resources needed by everyone, from business users all the way up to the corner office.

Many business users have grown frustrated and impatient because of a perceived inability of IT departments to meet their business needs with new systems, applications, and services in a timely, affordable manner. But the harsh truth is that everyone is clamoring for more support and collaboration from the IT organization at a time when IT budgets are not growing fast enough—and sometimes not at all—to keep up with skyrocketing and increasingly sophisticated user demands.

Perhaps even more important is the fact that IT hiring has flatlined in many industries, despite repeated requests for more programmers, application developers, systems analysts, data scientists, help-desk technicians—and yes, more security professionals. So, since necessity is the mother of invention, the business users have come up with a simple solution: *"We'll do it ourselves."*

Why and How Shadow IT Took Hold

This trend, widely known as shadow IT, has become increasingly prevalent in enterprises of all sizes, industries, and geographies. Some organizations tacitly support the practice, while others are blithely unaware of its existence. Regardless, shadow IT has serious cybersecurity ramifications.

What exactly is shadow IT? Global IT consulting and research firm Gartner puts it succinctly:

> *"Shadow IT refers to IT devices, software, and services outside the ownership or control of IT organizations."*[1]

Not that long ago, the notion of a shadow IT organization was preposterous. IT was a complicated discipline built upon in-depth, often arcane technical knowledge and access to expensive computing infrastructure. But that's changed dramatically. Today's workforce—and not just the millennials who were born

seemingly tethered to their numerous Wi-Fi devices—is far more technologically adept and more comfortable writing applets, setting up wireless networks, deploying virtual machines, and putting in place digital sandboxes for short-term projects.

Then there's the cloud. Affordable, easily accessed cloud services have helped business users launch their own systems and procure IT services with a simple credit card transaction, all without the notice, review, approval, and control of the traditional IT organization.

As a result, shadow IT has not just become a big factor in how IT services are developed and deployed, but it also is an often-hidden development escaping the vision of IT and business executives. One study noted that 72% of companies don't know the scope of shadow IT at their organizations, *but want to.*[2] Another study pointed out a key reason for this disconnect: CIOs, on average, dramatically underestimate the number of cloud services running within their organizations. How dramatically? By a factor of more than 14 to 1.[3]

To many business executives and board members, the shadow IT movement seems like a smart, even necessary, workaround to a problem: the growing chasm between demand (for more IT services and solutions) and supply (of IT resources to get it all done). Initially, business leaders who were aware of this complaint from their business teams often applauded their creativity and innovation in finding organic, affordable solutions to their problem. This predisposition for "a bias for action" is, of course, widely supported and even encouraged by business leaders on their teams.

CIOs, CISOs, and other technical executives have been working feverishly to meet the growing demand for IT services and tools to help their organizations solve strategic problems, ranging from identifying new competitive threats and reducing global supply chain costs to mining troves of new data to make smarter, faster decisions. They want to help the organization succeed by leveraging technology for business benefit, and they want to collaborate with business colleagues to do that.

However, what once may have seemed like a creative way to bypass the IT bottleneck in the quest for digital transformation is now a problem. A big problem.

Shadow IT's Impact on Cybersecurity

Shadow IT dramatically expands an organization's cybersecurity threats in many ways and for many reasons. It's typically being done innocently enough, certainly without malevolent intent. But the impact can be really bad.

The reasons why shadow IT is so commonplace and so problematic today include:

- The dramatic growth of "bring your own device" policies (formal and otherwise), which have introduced a slew of unmanaged and either unprotected or under-protected devices on the wrong side of your firewalls.
- A lack of visibility into, and control of, inbound/outbound data traffic, often resulting in compromised data integrity and extensive data loss.
- The growing popularity of the Internet of Things, which manifests itself both in terms of new types of equipment that is often security-deficient and in "rogue" projects that, while exciting and full of business potential, can leak sensitive data like a sieve.
- An increasingly mobile/virtual workforce, where employees—as well as customers, suppliers, and partners—often access sensitive data over open networks that can easily be hacked.

As I mentioned earlier in this chapter, shadow IT often lurks under the radar of corporate IT, and thus is shielded from business executives and board members who ultimately bear responsibility for all cybersecurity problems.

Just how bad is the problem? I'll give you one example to let your imaginations run wild. A research study pointed out that 80% of IT professionals said their end users have gone around them to set up unapproved cloud services.[4] And do you want to know the really scary part? That data is five years old, taken at a time when cloud services were still in their infancy. You can only imagine how pervasive the problem is today—and will be in the future. The question is: What should you do about it?

Addressing the Cybersecurity Challenges of Shadow IT

Fortunately, there are some common-sense steps organizations can and should take to minimize the potential negative cybersecurity impact of shadow IT. While I don't think organizations should be taking draconian steps to curtail initiative and self-sufficiency of technically astute employees, there are some reasonable, collaborative approaches that can create stronger partnerships between enterprising business users and the security and IT professionals whose job it is to keep the organization's data and IT assets safe.

Of course, this also means that business leaders and boards must (A) acknowledge that the problem exists and that it has potentially devastating impact, and (B) lead the way in encouraging smart answers to the problem. Denial is not a solution.

But first, let's keep an important fact in mind: The end users themselves—your employees, primarily—are incredibly naïve as to the extent they are putting your organization at risk. They're not connecting the dots, despite the fact that this is a topic that is increasingly covered in news reports and is being talked about by others. Even though today's workers are very tech-savvy—especially the new generation of employees—they don't have a clue what happens when they open a gateway in any direction. It gives the bad guys the key to the house.

So, what is the best way to address this problem? Education? Audits? Penalties? Yes.

In my organization, we conduct mandatory cybersecurity training. That training has been extended to topics like shadow IT, so everyone knows when bad security hygiene is taking place and what its impact will be. Explain to your employees who are acting as "citizen developers" and are commissioning applications to be built what can happen.

I know that everyone will groan about adding training into employees' busy days, but those sessions don't have to be long. You can give people reading materials they can go through on their own time, but you have to have formal training programs on this, especially for new employees joining the organization. Testing is also a good step to ensure that users are fully conversant in policy goals and objectives.

There are times when penalties—such as shutting down rogue applications or access to certain cloud services—may be necessary. Your very clever people may know how to get around access controls or authentication, but do they know which actions are likely to open up the organization to bribery or blackmail threats? Do they realize the reputational damage that can result?

While we don't want to stifle innovation or discourage creative problem solving, organizations should send a zero-tolerance message. Your business units may be demonstrating initiative and even doing some very exciting work on their own, but if they are inviting in security risks, the downside can be

much larger than the upside. Organizations can't afford to be naïve either about the incidence of shadow IT or its potentially catastrophic impact.

This should be part of every organization's risk tolerance profile: How much are we willing to let our employees do in order to get the work done?

Of course, that opens up another issue: The growing imbalance between what business units need in IT services and support, and what the IT organization is able to deliver. This is likely to raise some very challenging, yet important, discussions on budgets, manpower, use of outside contractors, and how to assess opportunity versus risk.

But we all have to understand and admit that until we address the root causes of shadow IT, we will never be able to solve the problem.

Conclusion

Despite many organizations' discomfort with shadow IT, I do not think executives should issue orders to outlaw the shadow IT. I know most organizations—if they are able to have very honest and open conversations with their teams—can highlight instances where enterprising employees working outside the sphere of the IT organization have done some things that resulted in a competitive advantage because they moved quickly and flexibly to take advantage of an opportunity.

Still, that doesn't mean you allow or look the other way on reckless behavior. You don't know for sure if it's reckless unless you understand what is happening and what the risk-to-reward ratio looks like. If you think you haven't been bitten by this problem yet, you either haven't been paying attention or you've been lucky. But I can promise you that your luck will not protect you from a data breach, a service interruption, a compliance violation, or a lawsuit.

As with so many things in today's business environment, it requires a real give-and-take among business users, IT, security, and business leaders. Once someone in your organization goes rogue and starts their own IT solution or service, it can lead to a lot of trouble if there is no discussion on the impact.

While it's true that talk is cheap, the cost of a cybersecurity problem is not.

---

1 Gartner IT Glossary, Shadow IT https://www.gartner.com/it-glossary/shadow

2 "Cloud Adoption Practices and Priorities," Cloud Security Alliance, 2015.

3 "CIOs Vastly Underestimate Extent of Shadow IT," CIO magazine, 2015.

4 "Security, Privacy, and the Shadowy Risks of Bypassing IT," Spiceworks, 2016.

43

Unlocking Productivity with Security

Siân John, MBE — Chief Security Advisor, Microsoft

Mobile working has changed how organizations conduct business, from the development labs and the factory floor of the global supply chain all the way to the end customer. Mobile working and its facilitators—cloud computing, Internet of Things, and IT consumerization—have unleashed new waves of innovation that have resulted in new products and services, an empowered workforce, a streamlined global supply chain, and an engaged customer base.

But these and other mobile-centric developments have done something else: They've significantly expanded cybersecurity threat vectors and, in some cases, opened up vulnerabilities that are threatening to undermine our aspirations for agility, efficiency, and productivity. This is a common side effect of the move to a more digital and mobile world; we just need to be aware of and manage this risk if we are going to achieve our aspirations.

By now, you've undoubtedly picked up on the fact that I'm talking about "mobile working" rather than the more common "mobility" term. That's because I believe mobility has become synonymous with devices, and getting work done when away from a traditional fixed-point setting like an office is about much more than mobile devices.

For instance, so much of the flexibility, freedom, and balance now available to us in our work lives is driven not as much by small, lightweight devices as it is by the cloud. I'm sure that many of you reading this chapter were early adopters of tablets because they enabled you to leave your laptops at home when out and about while still remaining connected to business services. You could access your corporate email, search enterprise databases, or work on presentations or documents—thanks to the cloud.

So, as important as devices are in the overall process of mobile working, we must look at this trend as an ecosystem of devices, applications, workflows, and services.

Unfortunately, mobile working brings with it a host of new security threats that too many of our organizations have yet to confront, let alone overcome. It should surprise no C-level executive or board member to learn that Wi-Fi networks at the airport, sporting arena, or your local coffee shop are easy and frequent targets for cyber criminals.

Unless we commit to integrated security functionalities in our products, services, and workflows from the start, we will fail to achieve many of our most essential business goals. Conversely, if we pay attention to security from the start and design effective and efficient security safeguards into everything, we will unlock and unleash a wave of productivity never seen before.

Let me be clear about what I'm saying.

- Security is not an IT issue. It's a business issue, and it demands the support and leadership of business executives, IT and security professionals, board members, and end-user stakeholders.
- The financial cost of designing security into products, services, and workflows is far, far outweighed by both its long-term economic benefits and the resultant costs of remediating problems after the fact.
- Native security breeds confidence by all users, which in turn promotes productivity and delivers economic value.

We need to ensure we are living up to our own expectations of managing these issues.

What Secure Mobile Working Can Do for Productivity

It's important to understand and embrace the notion that you can't have productivity in mobile work without security—specifically, security integrated from the very beginning of product development or business-process creation.

Before mobile working became the accepted standard, employees were doing it any way they could to get the job done. But they did it by using personal email on personal devices, which do not have the same security levels as their work accounts. They could access sensitive data sent through email accounts or through personal subscriptions to public cloud services, for example looking at patient records over Gmail or searching intellectual property drawings downloaded to a personal Dropbox account.

The ability to work anywhere at any time, to access data and applications from home or on the road, is central to worker productivity. We're now firmly entrenched in the era of non-traditional work hours, driven by such factors as a desire to juggle work and personal commitments, the realities of the global economy, and a need for many so-called knowledge workers to react instantaneously to a germ of an idea, to a spark of brilliance.

To do that, we must have native security in our devices, applications, and business processes. And if our organizations don't enact steps to bake in security from the start, the regulators will come knocking on our doors. The new Global Data Protection Regulation demands that we automatically do the things we should have been doing all along, in terms of protecting and managing personal information.

When it comes to secure mobile working, GDPR and other data protection mandates have simply increased the cost of doing nothing—which, in my view, is a very good thing.

Why You Can't Have Digital Transformation Without the Right Security for Mobile Work

If there's any term being bandied about by business executives more than "digital transformation," then I haven't heard it. By now, every business leader and board member has embraced the notion of using technology to further business goals, especially in retasking our bright, creative employees away from rote, repeatable activities that can easily be done by technology.

To further the goals of digital transformation, organizations should focus on three areas:

- More use of cloud platforms to accelerate the delivery of IT services for business aims.
- Customized, personalized computing built around mobile platforms to drive greater employee engagement.
- Improved productivity through the paradigm shift that is mobile working.

And to accomplish all of that, organizations must acknowledge that traditional security controls and procedures were not built in anticipation of digital transformation and all its components.

Too many organizations still cling to the concepts of strong physical boundaries that promote routing back through the physical network, rather than extending the perimeter to the cloud. By embracing the cloud as a tenet of mobile working, organizations optimize security risk management by leveraging the investments, knowledge, and ability to experiment—safely—of cloud service providers.

Done properly, digital transformation is more easily attained when security issues are anticipated and integrated in advance, rather than after a security problem arises. And it's important to keep in mind that organizations are only going to embrace digital transformation if their customers truly trust it. For this reason, the cybersecurity office should be considered an essential part of any digital transformation team; too often, they are left to the end of the process.

Enabling Security Professionals to Think About Mobile Work Outcomes, Not Security Outcomes

When security is baked into products, services, or business processes to support mobile working, everything starts with the consideration of how security affects business outcomes. Although we are fast moving away from old practices of "bolting on" security after the fact, it still happens far too often.

This is a crucial role for business leaders—to whom the CISO typically reports—and board members who naturally want to empower their employees to work in a way that engages them. And it all starts with analyzing business risk, though doing so can't be the sole domain of the business teams; it must include security professionals.

Business leaders need to consider the following steps (which your security team can definitely help accomplish):

- **Assess the possible threats that your industry and organization are exposed to.** A number of possible threats will already be known. However, executive support is needed to enable the security team to gain additional knowledge from cyber threat intelligence-sharing organizations (such as UK Cyber Information Sharing Partners and TruSTAR), as well as collaborating with law enforcement agencies.
- **Understand how identified threats could impact your intended business outcomes.** These could include flexible working arrangements, data analytics, global collaboration, productivity, employee empowerment, or more. It's essential to support your security teams' efforts in understanding how your business works; and in turn, how business units are affected by cyber risk, not just from a technical perspective but also from a user or operational standpoint.
- **Define how you can address the threats you are exposed to, whilst still achieving the business outcomes.** Ensure this happens from a people, process, and technology perspective and is articulated so all areas of the business can understand what they would need to do differently, and why.
- **Determine what type of digital transformation is needed for your security procedures so that your organization is protected as you change approaches.** If the suggestion is to buy more security products, ensure that you ask what impact they will have on your employees. Will it make it easier for them to follow procedures intuitive-

ly—has this been tested with users? Is there a cloud solution that can be deployed very quickly and easily maintained, rather than the protracted route of traditional software?

- **Ask how you can keep yourself up to date about the latest risks and threats and ensure that you are able to respond to them in a timely manner.** Make sure the previous four steps are a continuous loop to ensure that decisions are always being made to maintain security and risk management, as well as productivity.

Improving the Mobile User Experience with Security—Without Compromising Your Defenses

Striking the delicate balance between airtight security and worker flexibility and engagement is harder than ever in the era of mobile working. Users will look for the path of least resistance and for shortcuts to bypass what they consider to be cumbersome, annoying, and invasive procedures for authentication and access management. And they won't hold back in sharing that with their colleagues.

There are questions that board members and executives can ask to understand what can be done to strike the right balance between airtight security and mobile working within their own organization:

- **How easy is it for a user to access applications, services, and data?** You should find that by making user access simple and intuitive, you improve your security posture. More than likely, your CISO has deployed multifactor authentication (MFA) to reduce the risk of identity theft and ensure proper access to data. One key change could be to eliminate passwords as the authentication method of choice. While passwords may continue to be used in some MFA protocols, look at other approaches, such as biometrics or single sign-on using mechanisms such as Apple FaceID and Windows Hello.
- **What reasonable controls do we have in place to detect unusual and unusually high data movement?** This pattern could indicate that users are working outside of security controls. What type of data is it affecting and does that increase our risk exposure? Are there patterns in the type of data moved or applications being accessed that indicate users are working around security controls? What actions have we taken to mitigate that?
- **How do we enable collaboration while protecting information?** This is particularly important—given the widespread use of third-party relationships in daily business activities—in order to ensure that only the right people can access sensitive data.
- **Are we able to detect and respond to threats across the full enterprise ecosystem?** Devices, identities, cloud services, data, and more all must be protected in order to enable operational efficiencies and productivity, without introducing unacceptable levels of risk.
- **What security outcomes do we need to see?** Do we need to adjust our existing controls to enable productivity and mobile working, but still maintain our risk management levels?
- **What about our cloud service providers' risk management and security procedures?** With the continued uptick in cloud services adoption, organizations need to ensure that those providers have put in place the proper risk safeguards and strong controls to enable and protect identity, information, and the entire organization's digital profile.

Finally, ask your security team: Have you fully considered how cloud services and mobile working affects our risk and threat management models? Be sure your security team has tested its controls for usability on mobile devices and cloud services, and ask if they have taken all necessary steps to achieve the visibility and control needed for those environments, without impacting productivity.

In short, good security and a positive user experience are not mutually exclusive—not unless you make them so. Please don't.

Conclusion

We have only scratched the surface when it comes to the benefits of mobile working, and integrated, native security is a big reason why this trend will only accelerate. As we increasingly adopt over-the-top communications services, security will be assumed by users from the start. This will make mobile work a natural extension of the entire work experience and dramatically increase technology.

We must rapidly and zealously continue to move past the old paradigm when security—often in the form of frequent logins, repetitive identity verifications, and clunky passwords changed far too often—inhibits productivity. And adopting the right security practices and solutions for mobile working can prevent the need to lock down and route traffic in ways that result in unacceptable latency and deployment issues.

Instead, built-in security will make users—employees, customers, and all participants in the digital ecosystem—more confident in using technology for mobile working. And while this is great for our workers, it will undoubtedly be our enterprises that will benefit to the greatest extent.

Conclusion

44

How We Can Change Our Approach to Cybersecurity Today

Nir Zuk – Founder and Chief Technology Officer, Palo Alto Networks

One of the main goals of this book, *Navigating the Digital Age, Third Edition,* has been to foster a deeper understanding about cybersecurity between technical and non-technical executives. As the founder of several cybersecurity technology companies, including Palo Alto Networks, I have had the opportunity to straddle both worlds, coming from a background as a technologist and subsequently dealing with the challenges involved in building a successful business and creating a dynamic corporate culture.

When it comes to cybersecurity, I see the world from both the technology and business sides. From either perspective, I see challenges—and opportunities—when I look at the approach that most organizations take to cybersecurity today. The fundamental challenge is that our approach to cybersecurity is too reactive and the mechanisms we have in place are typically too slow and inefficient to react.

As our adversaries innovate faster, we fall behind, coming up with fixes for individual threats, but failing to create a sustainable platform to consume innovation quickly and efficiently. Our adversaries are innovating constantly, and it takes us months, if not years, to choose, procure, and deploy a new reactive response. Our slowness and inefficiencies come from other directions, too. Often, we maintain a mind-set of using humans to fight machines, when we should have long since transitioned to a model of fighting machines with machines.

Traditional cybersecurity approaches have been struggling to deal with rising cyberattacks, a shift to cloud, and explosive growth in the Internet of Things. Then came the COVID-19 pandemic and all the changes that were fomenting for years accelerated, with remote work becoming the norm and digital transformation taking on urgency. New levels of complexity are piling on top of an environment that was already too overwhelming for most organizations.

If we don't address these challenges now, they will only get worse as our adversaries up the ante by using technology advances such as automation, machine learning, and artificial intelligence.

That's the bad news. The good news is that we can fix this. We can build cybersecurity into our technologies, products, services, and corporate cultures. We can make cybersecurity a business enabler. We can create a model of cybersecurity

innovation that goes a long way toward addressing the relentless challenges.

We can fix it, and we will fix it. Here's how.

Challenge No. 1: Inefficient Consumption

The way cybersecurity has worked, thus far, is a vicious cycle that keeps adversaries one step ahead: Cybercriminals innovate quickly and come up with new mechanisms to cause more damage and make more money. Then cybersecurity companies, often led by innovative startups, develop solutions to stop those specific attack mechanisms. These new solutions usually take months to evaluate and deploy and, when they are finally deployed, they add to cybersecurity complexity.

As this cycle has evolved, our defense mechanisms have become cumbersome and inefficient. Companies now typically have dozens and sometimes hundreds of different cybersecurity solutions, which don't necessarily work in concert but rather in silos. The organization is paying to support and maintain these solutions, incurring costs to upgrade and replace them. Most importantly, a lot of time and energy goes into integrating products rather than operating them.

Challenge No. 2: Humans vs. Machines

Not only are we consuming cybersecurity innovation inefficiently; we continue to approach cybersecurity from the wrong mindset. In today's era, with automation, machine learning, and AI, if the battle is man against machine, machine will have the upper hand almost every time. We can't bring humans to that fight and expect to win.

Machines scale much quicker than humans. Whatever the human capacity may be—whether each person can deal with five security events, or 50 or 500—when the adversary is automated, it can always overcome that number simply by throwing more computing resources at the problem.

From the adversary's perspective, success is a function of compute, efficiency, automation, and ultimately money. As a defender, if you are relying on people to fight this battle, then you have to scale with people. So every time the adversaries add more compute power, you may need to increase the size of your team. Of course, then the adversaries just go out and spend a few more dollars to get more compute power.

There's no possible way to keep up, either logistically or financially. On the adversary side, growth is becoming exponential because of the easy availability of compute resources. Not only can they go to the public cloud to get compute resources; they are also stealing them from their victims, taking over our end-user machines, servers, or anything else they can use on the cheap and on the sly.

Today, we have humans in our security operations centers (SOCs), fighting machines with the help of machines. We have to shift the paradigm and have machines fighting against machines, with humans to help the machines. Whenever a machine can't do something, it can use a human.

The Opportunity: A Better Approach to Consuming Innovation

The technology to address these challenges is available today. There are between 2,000 and 3,000 cybersecurity vendors out there, each delivering their innovation as a product that needs to be evaluated, procured, deployed, and operationalized.

What we need is a better approach to *consuming* that innovation. And we need you, as a business executive, to demand it. *Now!* If your CISO or security team seeks to buy a cybersecurity solution that

will be deployed in a few months or a year, you have to challenge their basic premise. Here's what CEOs, CIOs, and board members should demand:

1. Any new cybersecurity solution must be deployed in a day—preferably less than a day—across the entire infrastructure globally.
2. Any new cybersecurity solution cannot come with the requirement to hire more people.
3. Our entire cybersecurity team must demonstrate an accelerated rate of deploying innovation. The bad guys are moving fast; we must be moving just as fast.

At first, your CISO and security teams may be flustered because these demands fall so far out of the paradigm of how they've been doing things for so many years. That's okay, because the old paradigm is broken. Your cybersecurity professionals need to go to their vendors with the same demands: Find us a way to respond to this challenge, to deploy cybersecurity innovation quickly, efficiently, openly, and comprehensively.

Cybersecurity Innovation Through SaaS

What constitutes a better approach to consuming cybersecurity innovation? In today's world, software-as-a-service (SaaS) is the most efficient way to consume IT resources and innovation. We've seen the SaaS model work across many business functions: customer relationship management (CRM); salesforce management; human resources; enterprise resource planning; email; file sharing; and instant messaging.

All of these activities have either moved to a SaaS model or are moving quickly in that direction. That's because SaaS enables innovation to be consumed easily and quickly. Thus, the answer to the earlier question about addressing the challenges to our cybersecurity approach is the same for cybersecurity as it is for all of these other business activities: We transform cybersecurity to a SaaS model.

If you look at most SaaS solutions, all you need to consume them is a web browser, and your access to innovation is immediate. Cybersecurity needs to be consumed just as easily. However, cybersecurity poses a different challenge than most of those other business activities because of the necessary evil of having the technology deployed within the infrastructure. The only way to get information from the infrastructure and to act on it, is to be part of the infrastructure. This goes for data centers, public clouds, and even end user-devices. So, given that a software "agent" is needed in all these locations, it would be useful to deliver many SaaS cybersecurity solutions over each of these agents.

Cybersecurity as a Platform

The answer to that challenge is actually quite simple: Cybersecurity as a platform. Look at some of the most successful IT platforms: Apple, Windows, Facebook, Salesforce.com They provide a simple way to both provide and consume innovation by having an open platform that basically allows anyone with a good idea to come in and sell it. With a platform, the ability to deliver value and innovation becomes near instantaneous.

A platform is when the economic value of everybody that uses it exceeds the value of the company that creates it. Then, it's a platform. — Bill Gates

As our adversaries become better funded, more sophisticated, and more adept at leveraging automation, machine learning, and IT, we must fix the fundamental flaws in our security approach, and we must do it now. We must be able to consume cybersecurity in a way that enables us to deploy innovation quickly and fight machines with machines.

Cybersecurity has to become a set of services that you consume, rather than a set of technologies you deploy in networks, on endpoints, and in data centers. As we continue our journey in navigating the Digital Age, a platform is the path to get from here to there, to change forever the model for consuming cybersecurity services and innovation. It is the future of cybersecurity. And, as Pablo Emilio Tamez Lopez said so well at the beginning of this section: The future is now.

Looking Ahead

I am going to refrain from getting into the technical details of how a cybersecurity SaaS platform model can work. Your cybersecurity professionals should be able to explain the details to you. I will say this: Think about this with a sense of urgency. Your adversaries aren't waiting, so you can't afford to wait either.

We are now at the end of our book and, if you've read all, most, or even some of the preceding chapters, you can't help but conclude that cybersecurity is one of the defining issues of our time, not just in business, but in the world at large.

You are on the frontlines. You are in a position to *take action:* whether it is setting the tone in your organization, pushing your teams to deploy a SaaS cybersecurity model, creating training and awareness programs, participating with government officials on regulation, or advocating for cybersecurity innovation.

There's much work to be done. Now is the time to act. In some ways, it seems like the Digital Age has been with us forever. In other ways, it seems all brand new, as many of us experienced firsthand when we had to respond suddenly and strategically to COVID. For all of us involved in shaping and navigating the Digital Age, there is still within our grasp the time and the opportunity to help build a better world. Let the journey continue.

Contributor Profiles

Contributor Profiles

Dr. Philipp Amann — Netherlands
Head of Strategy
Europol's European Cybercrime Centre (EC3)

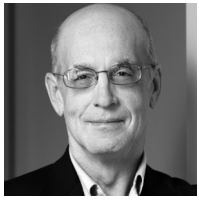
Dr. Philipp Amann is Head of Strategy of Europol's European Cybercrime Centre (EC3), which is responsible for the delivery of strategic, situational, and tactical cyber-related products such as the Internet Organised Crime Threat Assessment. Prior to EC3, Philipp held management positions with the Organisation for Security and Cooperation in Europe, the Organisation for the Prohibition of Chemical Weapons, and the International Criminal Court.

Nikesh Arora – United States of America
Chief Executive Officer and Chairman
Palo Alto Networks

Nikesh Arora is Chief Executive Officer and Chairman of Palo Alto Networks. Previously, he was President and Chief Operating Officer of SoftBank Group Corp., and Senior Vice President and Chief Business Officer at Google.

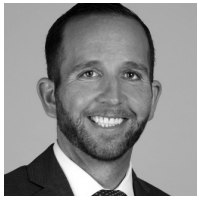
Kal Bittianda — United States of America
Head of North America Technology Practice
Egon Zehnder

Kal Bittianda heads Egon Zehnder's North American Technology Practice, where he works with companies in the mobility, communications, systems, software, and technology-enabled services sectors. Previously, he led business units at Kyriba, EXL, and Inductis.



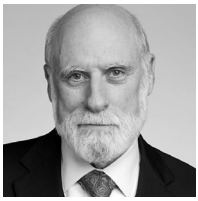
Gary A. Bolles — United States of America
Chair for the Future of Work
Singularity University

Gary A. Bolles is the Chair for the Future of Work at the Singularity University. He lectures to, and consults with, organizations around the world to embrace a human-centric vision of work, learning, and organizational growth. He is the former editorial director of publications such as Inter@ctive Week and Network Computing.



Robert Boyce — United States of America
Managing Director, Accenture Security
Accenture

Robert Boyce is Managing Director of Accenture Security. Robert is responsible for the growth and development of Accenture's Cyber Threat Operations capabilities. He also provides hands-on consulting services to the Global 2000 in the areas of advanced security operations, crisis preparedness and response, and cyber defense and protection strategies.



Vint Cerf — United States
Vice President and Chief Internet Evangelist
Google

Vinton G. Cerf is Vice President and Chief Internet Evangelist at Google. Known as a "Father of the Internet," Cerf is co-designer of the TCP/IP protocols and architecture of the Internet. He has received numerous awards, including the U.S. National Medal of Technology, ACM Alan M. Turing award and the Presidential Medal of Freedom.

Mario Chiock — United States of America
Schlumberger Fellow and Former Chief Information Security Officer Emeritus
Schlumberger

Mario Chiock is a Schlumberger Fellow and former Chief Information Security Officer at Schlumberger, where he was responsible for developing Schlumberger's worldwide cybersecurity strategy. Mario served on the advisory boards of Palo Alto Networks, Onapsis, and Qualys.

Alice Cooper — United Kingdom
Global Head of Derivative Trade Processing IT
BNP Paribas CIB

Alice Cooper is Global Head of Derivative Trade Processing IT at BNP Paribas CIB. She has held a wide range of responsibilities at BNP Paribas across a number of IT functions for trades processing, credit, and equity. Previously, she worked at Mitsubishi Bank and Citibank.

Lieutenant General Bruce T. Crawford — United States
Retired Chief Information Officer
U.S. Army, Department of Defense

Lieutenant General Bruce T. Crawford recently culminated 34 years of service as the Army Chief Information Officer, serving as the senior government official responsible for policy and oversight of the Army's $12.B IT portfolio. Other key assignments include senior cybersecurity and enterprise IT positions in every major theater of operations at the strategic, operational, and tactical levels. Bruce now serves on the advisory boards of Rubrick Inc, and CyberArk.

Greg Day — United Kingdom
Vice President and Chief Security Officer, EMEA
Palo Alto Networks

Greg Day is Vice President and Chief Security Officer for EMEA at Palo Alto Networks. He is also Chair for the global CSO community I-4 members advisory committee, Chair TechUK Cybersecurity AI Working Group, and member of the World Economic Forum's Centre for Cyber Security. He previously held leadership roles at FireEye, Symantec and McAfee.

William Dixon — Switzerland
Head of Centre for Cybersecurity
World Economic Forum
William Dixon is the Head of the Centre for Cybersecurity at the World Economic Forum, focusing on the impact of next generation technology on the security, and risk landscape. Previously, he was Global Head of Intelligence at Barclays, and held leadership roles in the UK Civil Service.

George Finney — United States of America
Chief Security Officer
Southern Methodist University

George Finney is the Chief Security Officer for Southern Methodist University and the author of *No More Magic Wands: Transformative Cybersecurity Change for Everyone.* He previously worked with several startups and global telecommunications firms. George is a member of the Texas CISO Council, a governing body member of the Evanta CISO Coalition, a board member of the Palo Alto Networks FUEL User Group, and an advisory board member for SecureWorld.

Ryan Gillis — United States of America
Vice President for Cybersecurity Strategy and Global Policy
Palo Alto Networks

Ryan Gillis is Vice President for Cybersecurity Strategy and Global Policy at Palo Alto Networks. He has also held leadership positions in cybersecurity at the U.S. National Security Council and the Department of Homeland Security.

Gemma Garcia Godall — Spain
Founder
Instituto de Inteligencia Emocional

Gemma Garcia Godall is the Founder of Instituto de Inteligencia Emocional, where she guides leaders, teams and organizations to shine through cultural transformation projects. Previously, she was the Chief Executive Officer of a leading player in the financial services industry.

Marc Goodman — United States of America
Author and Global Security Advisor

Marc Goodman is the author of *Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It.* He is a leading speaker, author, and global strategist on the impact of technology on all aspects of our society. He also is a former law enforcement official and has consulted for such organizations as the FBI, Interpol, and NATO.

Mark Gosling — United States of America
Vice President, Internal Audit
Palo Alto Networks

Mark Gosling is Vice President of Internal Audit at Palo Alto Networks. He has previously held internal audit, compliance, and risk and controls leadership roles at Pricewaterhouse Coopers, Verisign, and NetApp.

Matt Gyde — United States of America
President and Chief Executive Officer, Security Division, NTT

Matt Gyde is President and Chief Executive Officer at NTT's Security Division, where he is also the representative director on NTT Security's board of directors. In his nearly 25 years in the cybersecurity industry, he has held leadership positions at Dimension Data, Datacraft, Surf Control and Secure Computing.

Justin Harvey — United States of America
Managing Director, Accenture Security
Accenture

Justin Harvey is Managing Director of Accenture Security, with responsibilities for Global Incident Response and the Cyber Fusion Center Consulting Practice. In his role, he provides security thought leadership as a strategic advisor on cyber espionage, cyber war, and cybercrime. Justin previously held senior positions at Fidelis Cybersecurity, HP/ArcSight, CPSG Partners Consulting, and Mandiant/FireEye.

William Houston — United States of America
Advisor, Technology and Communications & Industrial Practices
Egon Zehnder

William Houston is an Advisor in Egon Zehnder's Technology and Communications & Industrial Practices. He previously worked in Google's Emerging Business Development Group and has held senior positions at the U.S. Department of Homeland Security and in U.S. Cyber Command.

Salim Ismail — Canada
Founder, ExO Foundation; Board Member, XPRIZE

Salim Ismail is the best-selling author of *Exponential Organizations*; he is also a sought-after business strategist and renowned entrepreneur with ties to Yahoo, Google, and Singularity University. Salim founded ExO Works in 2016 to transform global business by catapulting organizations into the world of exponential thinking.

Paul Jackson, GCFE — Hong Kong
Managing Director, Asia-Pacific Leader, Cyber Risk
Kroll

Paul Jackson is Managing Director and Asia-Pacific Leader for Cyber Risk at Kroll. He has worked in close concert with such leading organizations as Interpol, the U.S. Secret Service Electronic Crimes Task Forces, and Microsoft's Digital Crimes Consortium. Paul spent 22 years with the Hong Kong Police Force, eventually becoming Chief Inspector and Head of the IT Forensics Practice. He also has held leadership posts at J.P. Morgan Chase bank.

Siân John, MBE — United Kingdom
Chief Security Advisor
Microsoft

Siân John is Chief Security Advisor for the UK in the Enterprise Cybersecurity Group at Microsoft. She previously held a number of senior roles at the Houses of Parliament, Ubizen, and Symantec. She is the Chair of the Digital Economy Program Advisory Board for the Engineering and Physical Sciences Research Council and is Chair of the TechUK Cybersecurity Management Committee. Siân was made a Member of the Most Excellent Order of the British Empire (MBE) for Services to Cyber Security in the New Year's Honours List for 2018.

Ann Johnson — United States of America
Corporate Vice President, Cybersecurity Solutions
Microsoft

Ann Johnson is Corporate Vice President, Cybersecurity Solutions at Microsoft. She previously was CEO at Boundless, an open-source geospatial solutions company, and COO at Qualys, a leading supplier of cloud security and compliance solutions. She also has held executive positions at RSA and EMC.

John Kindervag — United States of America
Field Chief Technology Officer
Palo Alto Networks

John Kindervag is Field Chief Technology Officer at Palo Alto Networks. Previously, he was Vice President and Principal Analyst on the Security and Risk Team at Forrester Research. John is considered one of the world's foremost cybersecurity experts, and is best known for creating the revolutionary Zero Trust Model of Cybersecurity. John holds numerous industry certifications and a Bachelor of Arts degree in Communications from The University of Iowa.

Heather King — United States of America
Former Acting Senior Director for Cybersecurity Policy, White House, National Security Council Staff

Heather King was formerly Acting Senior Director for Cybersecurity Policy for the White House, National Security Council Staff. Previous to that she was Chief Operating Officer at Cyber Threat Alliance. She has also held senior roles in cybersecurity policy at the U.S. National Security Council and other federal agencies.

Gerd Leonhard — Switzerland
Author; Executive "Future Trainer;" Strategist;
Chief Executive Officer, The Futures Agency

Gerd Leonhard is an influential and best-selling author of *Technology vs. Humanity* and several other books. He is a sought-after executive "future trainer," a trusted strategic advisor to Fortune 1000 companies and government officials around the globe, and the CEO of The Futures Agency, a global network of over 30 leading futurists.

Dr. Yang Zhoulong — China
Vice President and Chief Technology Officer
Yunda Group

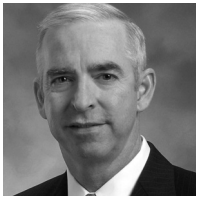
Dr. Yang Zhoulong is Vice President and Chief Technology Officer of Yunda Group. He is also the Deputy Chairman of China E-Commerce Logistic Industry Alliance, and the Logistics Information Expert of China Federation of Logistics and Purchasing. He has been working as an IT professional in the financial service industry and e-commerce logistics for 20 years.

John Paul Lonie — Australia
Head of Security Operations
Iress

John Paul Lonie is the Head of Security Operations at Iress. He has spent the past 25 years in financial services starting in development and IT operations and the last 12 years in a variety of information security roles.

Pablo Emilio Tamez López — Mexico
Chief Information Security Officer
Tecnológico de Monterrey

As Chief Information Security Officer of Tecnológico de Monterrey, Pablo Tamez Lopez is responsible for the security of all its institutions, which includes Higher Education and Healthcare. Pablo has designed and led the organization's cybersecurity strategy, which includes workforce consolidation, security technologies and services, security operation center, and incident response.



Gary McAlum — United States of America
Chief Security Officer and Senior Vice President
for Enterprise Security
United Services Automobile Association

Gary McAlum is Chief Security Officer and Senior Vice President for Enterprise Security at United Services Automobile Association. He previously spent 25 years in the United States Air Force, where he held various staff and leadership positions in cybersecurity, information technology, telecommunications, and network operations.

Danny McPherson — United States of America
Executive Vice President and Chief Security Officer
Verisign

Danny McPherson is Executive Vice President and Chief Security Officer at Verisign. Previously, he was Chief Security Officer at Arbor Networks, and he has held technical leadership positions at organizations such as Qwest Communications, MCI Communications, and the U.S. Army Signal Corps.

Stephen Moore — United States of America
Vice President and Chief Security Strategist
Exabeam

Stephen Moore is the Vice President and Chief Security Strategist at Exabeam, focused on driving solutions for threat detection/response and advising customers on breach response. Prior to joining Exabeam, Stephen has held a variety of cybersecurity practitioner and leadership roles. He spends his free time advising industry-leading organizations, mentoring, and helping those in need.

Sean Morgan — United States of America
Director, Cybersecurity Policy and Partnerships
Palo Alto Networks

Sean Morgan is Director for Cybersecurity Policy and Partnerships at Palo Alto Networks. He has also held positions in cybersecurity at the U.S. National Security Council and the Department of Defense.

Robert Parisi — United States of America
Managing Director and U.S. Cyber Product Leader
Marsh

Robert Parisi is Managing Director and U.S. Cyber Product Leader for Marsh. Previously, he was Senior Vice President and Chief Underwriting Officer of eBusiness risk solutions at AIG, and was legal counsel for several Lloyds of London syndicates.

Sherri Ramsay — United States of America
Cybersecurity Consultant; Former Director of the U.S. National Security Agency / Central Security Service Threat Operations Center

Sherri Ramsay is the former Director of the U.S. National Security Agency / Central Security Service Threat Operations Center. She currently works as a consultant, engaged in strategy development and planning and development of security operations centers. She is a member of the Board of Advisors for the Hume Research Center at Virginia Tech and a member of the Board of Advisors for TruSTAR Technology.

Mark Rasch — United States of America
Cybersecurity and Privacy Attorney

Mark Rasch is a cybersecurity and privacy attorney with more than 25 years of experience in corporate and government cybersecurity, computer privacy, regulatory compliance, probabilistic risk assessment, resilience, computer forensics, and incident response. Earlier in his career, Mark was with the U.S. Department of Justice, where he led the department's efforts to investigate and prosecute cyber and high-technology crime, starting the computer crime unit within the Criminal Division's Fraud Section.

Yorck O.A. Reuber — Germany
Chief Information Technology Officer
Allianz Malaysia

Yorck O.A. Reuber is Chief Information Technology Officer at Allianz Malaysia. Previously he was Chief Technology Officer for AXA IT. A certified Navy Chief Engineering Officer, Yorck formerly held senior-level positions at IBM, Verizon, and T-Systems.

Dr. Andreas Rohr — Germany
Chief Technology Officer
Deutsche Cyber-Sicherheitsorganisation GmbH (DCSO)

Dr. Andreas Rohr is Founding Manager and Chief Technology Officer at the Deutsche Cyber-Sicherheitsorganisation GmbH (DCSO). In this role, he leads cyber defense services and security engineering for the operative business. Previously, he worked in management positions at RWE, Volkswagen, and the German Federal Ministry of Defence.

John Scimone — United States of America
Senior Vice President and Chief Security Officer
Dell Technologies

John Scimone is Senior Vice President and Chief Security Officer at Dell Technologies. Previously, he was Senior Vice President and Chief Information Security Officer at Sony and Director of Security Operations at the U.S. Secretary of Defense Communications Office.

Richard Seiersen — United States of America
Chief Executive Officer
Soluble.ai

Richard Seiersen is Chief Executive Officer at Soluble.ai. He is a retired Chief Information Security Officer, and co-author of "How To Measure Anything In Cybersecurity Risk" (Wiley 2016) and "The Metrics Manifesto: Confronting Security With Data" (Wiley 2021).

James Shira — United States of America
Principle, Global, and U.S. Chief Information and Technology Officer
PricewaterhouseCoopers

James Shira is Principle, Global, and U.S. Chief Information and Technology Officer at PricewaterhouseCoopers, where he has led an organization-wide information security transformation. Previously, he held executive positions at Zurich Insurance Group, including group CISO, and at American General Financial Services, where he was Chief Security Officer.

Justin Somaini — United States of America
Chief Security Officer
Unity Technologies

Justin Somaini is Chief Security Officer at Unity Technologies. Prior to joining Unity, he was Chief Security Officer at SAP, Chief Trust Officer at Box, and held the role of Chief Information Security Officer at Yahoo, Symantec, Verisign, and Charles Scwab.

Lisa J. Sotto — United States of America
Partner and Chair of the Global Privacy and Cybersecurity Practice
Hunton Andrews Kurth LLP

Lisa Sotto chairs the top-ranked Global Privacy and Cybersecurity practice at Hunton Andrews Kurth. She is the managing partner of the firm's New York office and serves on the firm's Executive Committee. Lisa has received widespread recognition for her work in the areas of privacy and cybersecurity and was named among the *National Law Journal's* "100 Most Influential Lawyers." She also serves as Chairperson of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee.

Jennifer Steffens — United States of America
Chief Executive Officer
IOActive

Jennifer Sunshine Steffens is the Chief Executive Officer of IOActive, a global consulting firm dedicated to making the world a safer place. She has received numerous industry awards for her leadership in the cybersecurity industry, including *CV Magazine*'s IT Security CEO of the Year award for 2018. Previously, she held leadership positions at groundbreaking cybersecurity companies such as Sourcefire and NFR Security.

Megan Stifel — United States of America
Executive Director, Americas
Global Cyber Alliance

Megan Stifel is Executive Director, Americas, Global Cyber Alliance. She has previously held cybersecurity leadership posts at the U.S. National Security Council and the U.S. Department of Justice.

Mike Towers — United States of America
Chief Information Security Officer
Takeda Pharmaceuticals International

Mike Towers is the Chief Information Security Officer at Takeda Pharmaceuticals International. He has worked in life sciences technology for over 25 years, leading global security functions since 2008. He is a regular speaker on digital trust, information risk and cybersecurity. He has received four Information Security Executive of the Year awards within the healthcare industry and serves on the board of the Health Information Security and Analysis Center.

James C. Trainor — United States of America
Senior Vice President, Cyber Solutions Group
Aon

James C. Trainor is Senior Vice President within the Cyber Solutions Group at Aon, responsible for helping to shape the organization's overall cyber strategy. He previously led the Cyber Division at the Federal Bureau of Investigation, where he led agents and analytics in every major high-profile cyber investigation involving the FBI.

Rama Vedashree — India
Chief Executive Officer
Data Security Council of India

Rama Vedashree is Chief Executive Officer of the Data Security Council of India. She previously was Vice-President at NASSCOM, overseeing a wide range of initiatives, including domestic IT, eGovernance, smart cities, and healthcare. She also has held executive positions at Microsoft and General Electric.

Nir Zuk — United States of America
Founder and Chief Technology Officer
Palo Alto Networks

Nir Zuk is Founder and Chief Technology Officer at Palo Alto Networks. Earlier in his career, Nir was CTO at NetScreen Technologies, which was acquired by Juniper Networks in 2004. Prior to NetScreen, Nir was co-founder and CTO at OneSecure, principal engineer at Check Point Software Technologies, and was one of the developers of stateful inspection technology.

Naveen Zutshi — United States of America
Senior Vice President and Chief Information Officer
Palo Alto Networks

Naveen Zutshi is Senior Vice President and Chief Information Officer at Palo Alto Networks, where he oversees the organization's IT solutions and strategy. Previously, he was Senior Vice President for Technology at Gap Inc., as well as Vice President for Technology and Operations at Encover, a SaaS-based CRM company. He also held senior technology positions at Cisco and Wal-Mart.

Navigating the Digital Age | Third Edition

The world did not need a global pandemic to recognize the unlimited power of digital technologies. But, early in 2020, that's just what happened. Overnight, nearly every organization faced the daunting challenges of securing their people, scaling remote work, protecting critical assets, and ensuring business continuity. There was precious little room for gaps in cybersecurity.

During this unprecedented time—what does it mean to navigate the Digital Age? How can business and technology leaders ensure the security of their organizations, while keeping pace with accelerated digital transformation such as the shift to cloud, the rise of machine learning, and the growth of Internet of Things?

This book, the third edition of *Navigating the Digital Age*, is designed to help executives understand what it takes to prepare for the unexpected, and stay vigilant in maintaining modern cybersecurity best practices.

Inside these pages, 50 thought leaders from around the world share their ideas on a range of vital topics, from addressing disruptions caused by COVID-19, to driving business transformation through innovation, to safeguarding our digital way of life. Individually, the chapters are practical and illuminating. Collectively, they point the way to a more secure, safe, and exciting digital future.

www.navigatingthedigitalage.com

paloalto® NETWORKS