paloalto NETWORKS | UNIT 42

Five Security Concerns for CISOs and How to Address Them

Attack Trends and Strategies for Proactive Defense

Table of Contents

Introduction 3

Trend 1: Intentional Operational Disruption 4

Trend 2: Increasing Impact of Software Supply Chain and Cloud Attacks 6

Trend 3: Acceleration of Intrusions 8

Trend 4: Nation-State Insider Threats 10

Trend 5: AI-Assisted Attacks 12

Shifting from Reactive to Proactive Security: A CISO's Imperative 14

As the attack surface expands and threat actors leverage AI, the ability to rapidly detect, contain, and remediate breaches is paramount.

A proactive and robust cybersecurity approach is essential to safeguard critical assets, preserve business continuity, and maintain resilience.

We are now experiencing a "third wave" of extortion: intentional operational disruption. Attackers are moving beyond data theft or encryption to prioritize sabotaging systems and forcing prolonged downtime. Attacks are accelerating at unprecedented speed, with nearly one in five exfiltrations occurring within the first hour, assisted by automation and generative AI.

This e-book distills five key trends from the 2025 Unit 42 Global Incident Response Report, based on our direct experience responding to over 500 real-world cyberattacks across 38 countries in 2024.

We'll give CISOs and their teams actionable recommendations to navigate this complex landscape with confidence.

As always, Unit 42 is your strategic partner – providing incident response, threat intelligence, and proactive and managed services to help you build and maintain a secure ecosystem where your business can thrive.

SAM RUBIN

Senior Vice President,
Unit 42 Consulting and Threat Intelligence
Palo Alto Networks

TREND 1

Intentional Operational Disruption

In 2024, we observed threat actors augmenting traditional ransomware attacks with tactics specifically to disrupt business operations. This marks a new wave of extortion and goes beyond typical encryption and data exfiltration tactics. By disrupting systems, locking customers out, and forcing prolonged downtime, attackers sought to maximize their leverage in negotiating a ransomware payment.

Incidents that disrupted business operations saw a big jump in the median initial extortion demand. It went up 80% from the previous year, from $695,000 in 2023 to $1.25 million in 2024.

Victims in industries like healthcare, hospitality, manufacturing, and critical infrastructure suffered massive impacts that rippled beyond the target organization to affect their partners and customers, as well.

86%

of incidents caused operational downtime, reputational damage or both

Recommended CISO Actions

CISOs must prioritize **operational resilience**. "Resilience" in this context means the ability for critical systems to continue functioning, at least minimally, in the face of a compromise. Building resilience keeps an attack from affecting the course of the business and the experience of your customers and partners.

To build resilience, identify which systems and assets are essential to maintain, as well as the systems needed to support them. Use disaster recovery metrics like recovery time objective (RTO) and recovery point objective (RPO) to inform a ransomware-resilient strategy and guide your backup processes.

Regular **testing and incident simulations** are crucial to validate technical controls, train response teams, and assess the organization's capacity to maintain essential services during an attack. It is also vital to ensure that partners are made aware and prepared to adapt to new systems in the event of an attack.

TREND 2

Increasing Impact of Software Supply Chain and Cloud Attacks

Nearly one-third of cases (29%) we investigated in 2024 were cloud-related, with 21% of cases seeing threat actors adversely impact cloud environments or assets.

Issues with identity and access management (IAM), such as excessive policy access, overpermissioned accounts, and password issues remain prevalent contributing factors but weren't the only factors. Attackers leverage misconfigurations and exposed credentials to embed within cloud environments, scanning vast networks for sensitive data or commandeering resources for large-scale attacks against other organizations. Supply chain vulnerabilities, like the critical XZ Utils library, highlight the potential for widespread damage through third-party software.

The cloud is complicated. 60% of organizations are running over half of their workloads in the cloud and 54% will move their workloads to the public cloud in the next 12 months, according to a CloudZero report. Research in 2024 found that on average, 20% of an organization's attack surface is replaced each month with new or updated services, which contributed to nearly half of new critical exposures than the previous year.

21%

of cases seeing threat actors adversely impact cloud environments or assets

Recommended CISO Actions

For a truly proactive defense, CISOs must extend their focus to the entire cloud and application lifecycle. This involves **limiting credential abuse** through robust **IAM** controls like multi-factor authentication and frequent credential rotations, while also ensuring **centralized logging and auditing** of cloud resources for comprehensive visibility.

Securing the software supply chain requires **prompt patching** of all components and implementing **rate limiting and strong scanning tools** to prevent vulnerabilities from reaching production. Ultimately, the goal is to **secure applications and cloud environments from development to runtime**, swiftly addressing misconfigurations and vulnerabilities at every stage.

TREND 3

Acceleration of Intrusions

Cyberattacks are accelerating due to attackers' increasing adoption of automation, ransomware-as-a-service (RaaS) models, and generative AI (GenAI), which streamline campaigns and give defenders minimal time to detect and respond.

The speed of attacks forces global organizations to reassess their response capabilities and prioritize early detection. In 2024, the median time to data exfiltration was about two days, but in 19% of cases, exfiltration occurred within the first hour of compromise. Unit 42's internal simulations showed AI-assisted attacks reduced time to exfiltration from a median of two days to just 25 minutes. Meanwhile, dwell time (attacker presence before detection) has decreased to seven days in 2024 from 13 days in 2023, showing an acceleration of the actual attack progression.

In nearly one in five cases, data exfiltration took place within the first hour of compromise.[1]

1. Global Incident Response Report 2025, Unit 42, February 25, 2025.

SPEED OF ATTACKS IN AN AI-ASSISTED SIMULATION

Recommended CISO Actions

For CISOs, **rapid cyberthreat detection and response** is non-negotiable. It means constantly improving how quickly you **spot and neutralize threats**. Harness **AI-driven analytics** to centralize data, identify real-time anomalies, and surface critical alerts at speed. Implement **automated playbooks** for immediate containment, isolating compromised systems in minutes. Regular **drills and red-team exercises** ensure seamless pivots from detection to response, prioritizing **high-risk assets** for swift action. Ultimately, **empowering your SOC** with consolidated visibility and automation is key to transforming potential crises into manageable incidents.

TREND 4

Nation-State Insider Threats

Insider threats are no longer limited to the typical disgruntled employee. As an example, North Korean nation-state actors are using synthetic or stolen identities to legitimately get hired at international organizations as IT staff and technical engineers. Once on the payroll, they perform their duties to at least the bare minimum, while systematically exfiltrating data, deploying unauthorized tools, altering source code, referring additional fraudulent workers, and more.

These North Korean nation-state groups, such as Wagemole ("IT Workers") have transformed development and engineering departments into an attack surface. Rogue assets in IT positions have legitimate permissions, credentials, and technical skills. They know how to cover their tracks and evade detection for long periods of time.

> **All of a sudden, people are asking, *'What is my hiring process?'* They find the hiring process is outsourced to an outsourcer. They say they vet candidates, but what does that really mean?**
>
> - Michael Sikorski | CTO & VP of Engineering - Unit 42

INSIDER TACTICS

Data exfiltration

Unauthorized tool deployments

Altering source code

Extortion

Malicious referrals

The New Face of Insider Threats Executive Insights from the 2025 Global Incident Response Report, Unit 42, June 2025.

Recommended CISO Actions

Addressing insider threats requires more than just technical controls; it demands a **culture of security awareness** and **active monitoring of user activities**, particularly for those with elevated privileges. CISOs should implement **least privilege policies** and conduct thorough background checks, recognizing that staffing firms can be unwitting facilitators anymore. It is crucial to pay close attention to **behavioral indicators**, such as unusual data transfers, which might seem innocuous on their own but, when correlated, could signal malicious activity. Ultimately, organizations must **balance trust with verification** by fortifying internal processes, monitoring privileged access, and emphasizing security at every level.

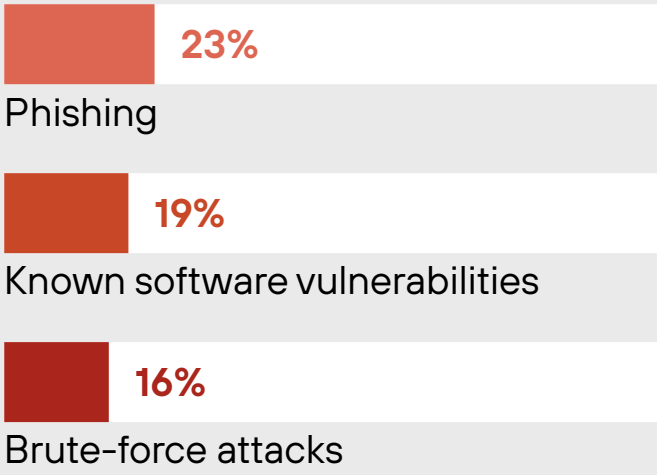
TREND 5

AI-Assisted Attacks

While still in the early stages, AI is helping attackers amplify the scale and speed of attacks. Attackers leverage AI to craft more convincing phishing campaigns, automate malware iteration and deployment, and accelerate the attack chain. Large language models (LLMs) can create highly accurate phishing emails and generate/obfuscate malicious code, lowering technical barriers for less-skilled threat actors.

As stated before, simulated attacks integrating GenAI showed a dramatic reduction in time to exfiltration, demonstrating how AI can significantly shorten the "time-to-impact".

TOP THREAT VECTORS



Aided by AI, phishing was the top initial access vector followed by software vulnerabilities and brute-force.

Recommended CISO Actions

To defend against AI-assisted attacks, CISOs must invest in **defensive AI**, especially to detect malicious patterns across numerous data sources. **Automated response workflows** are essential for proactively positioning the Security Operations Center (SOC) to contain threats before attackers can pivot or exfiltrate data.

CISOs must also **train staff** to recognize AI-generated phishing techniques, deep fakes, and highly targeted social engineering attempts. **Incorporating adversarial simulations** using AI-based tactics into tabletop exercises can prepare teams to defend against rapid large-scale attacks.

Shifting from Reactive to Proactive Security: A CISO's Imperative

Cybersecurity is a critical business imperative, impacting revenue, reputation, and operations. So, the CISO mandate is clear: rethink cyber risk and move from constantly reacting to breaches to a proactive, predictive defense that stops threats before they cause damage.

1 Embrace Zero Trust as a core principle.

Eliminate implicit trust, enforce least privilege access, and continuously verify every user and device to minimize the attack surface and limit lateral movement for adversaries.

2 Enhance cloud and identity security.

Implement robust multi-factor authentication (MFA) and secure non-human identities as well. Continuously monitor cloud configurations and user behavior to reduce attack surfaces and remediate risks quickly.

3 Address insider threats, whether malicious or unintentional.

Conduct rigorous vetting of all personnel, especially IT contractors. Continuously monitor privileged access and correlate identity, network, and behavioral data for early detection and swift intervention.

4 Accelerate detection and automate response.

Leverage AI-driven automation to cut response times from hours to minutes. Automate the analysis of security logs to surface high-priority threats faster, reducing attacker dwell time and minimizing damage.

5 Transform your SOC into a strategic hub.

Provide holistic visibility to identify the true signal in the noise to shift from reactive firefighting to proactive defense.

Embrace proactive strategies, to build a robust, adaptive security posture that not only defends against current threats but anticipates future challenges. Unit 42's proactive assessment and incident response services help organizations make this critical transition, moving beyond reaction into a state of continuous, threat-informed defense.

About Unit 42

Palo Alto Networks Unit 42® brings together world-renowned threat researchers, elite incident responders, and expert security consultants to create an intelligence-driven, response-ready organization that's passionate about helping you proactively manage cyber risk. Together, our team serves as your trusted advisor to help assess and test your security controls against the right threats, transform your security strategy with a threat-informed approach, and respond to incidents in record time so that you get back to business faster.

Visit paloaltonetworks.com/unit42.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

Five Security Concerns in 2025 for CISOs and How to Address Them
August 2025