EXECUTIVE SUMMARY

CISO Insights on Closing the Cybersecurity Preparedness Gap

2024 Hybrid Cloud Security Survey

Today's evolving cyber threat landscape is a formidable one. Despite global information security spending expected to reach a projected $215 billion in 2024, organizations are losing ground in the security arms race to threat actors. Over half (54 percent) of Security and IT leaders claim to be strongly prepared to identify threats across their hybrid cloud infrastructure but continue failing to detect breaches.

In the last 12 months, more than **1 in 3** organizations **(37 percent)** failed to detect a breach using existing security tools, rising from **31 percent** in 2023. Ever-more complex hybrid cloud environments are increasing cyber risk by expanding the attack surface and introducing visibility challenges, and as hybrid cloud infrastructure continues to evolve, scale, and adapt to facilitate AI deployments, the danger will only continue to grow. **At this turning point in enterprise IT infrastructure, how can CISOs best approach closing their cybersecurity preparedness gap?**

We surveyed over 1,000 Security and IT professionals across Australia, France, Germany, Singapore, UK and USA to publish our 2024 Hybrid Cloud Security Report: Closing the Cybersecurity Preparedness Gap. You can read the full report [here] but this executive summary delves specifically into the insights of more than 230 CISOs globally to understand the key issues and priorities facing this critical role. The findings reveal:

Regulations are adding pressure

As cybersecurity posture catches the eye of legislators, the role of the CISO is evolving to encompass compliance and even legal risk. Cybersecurity has therefore caught the attention of boards around the world, giving CISOs much needed support—but do leaders really understand what CISOs need to achieve security success?

CISOs are keenly aware of visibility gaps

Today, nearly half **(46 percent)** of CISOs do not feel strongly prepared to identify threats across hybrid cloud infrastructure. These respondents show particular concern around East-West and encrypted traffic, which present threat actors with the ability to remain undetected in organizations' infrastructure. As a result, **7 in 10** don't believe they can detect breaches with existing security tools.

Tooling strategies are a top concern

Tool consolidation continues to dominate organizations' priorities, with both optimization and investing in new tools being **ranked #1 and #2,** respectively, among CISOs for identifying and remediating visibility gaps.

Zero Trust has become a must-have

Long understood to be important, the specter of Zero Trust mandates has become a reality for organizations around the world—with USA taking the lead. CISOs must now turn their hand to practical implementation, with **44 percent** listing "pressure from the board to achieve Zero Trust" as a top 3 concern.

Deep observability defined: The ability to efficiently deliver network-derived intelligence to cloud, security, and observability tools. This eliminates security blind spots and reduces tool costs, enabling better security and management of hybrid cloud infrastructure.

Engaging the Board

With cyberattacks routinely making headlines, industry leaders and governments around the world are making it clear that cyber risk is a business risk. From EU's DORA to the SEC's new disclosure rules, mandates around risk accountability and threat detection place the onus of security failings firmly onto the shoulders of business leaders. And it seems to be working—**85 percent** of CISOs report cloud security is now a priority for the board, as leaders work with CISOs to identify and manage their organization's cybersecurity-induced risks. On the surface, this is great news for CISOs, with **6 in 10** CISOs reporting that the most empowering factor in their work is cyber risk being a true boardroom priority.

But with increased attention comes added pressure. When asked about their key issues, almost half of CISOs **(44 percent)** identified pressure from the board to achieve Zero Trust as one of their top concerns. This pressure is keenly felt by CISOs, while just **29 percent** of total global respondents agree.

What are your top concerns?

CISO TOP 5 ANSWERS RANKED

1. **Pressure from the Board to achieve Zero Trust architecture, without the resources/skills to deliver**
2. **Having too many tools that are poorly integrated, leading to breaches**
3. **New, more focused, and consequential cybersecurity legislation and compliance mandates**
4. **Securing the exponential growth of IoT/OT devices**
5. **Blind spots being exploited that you didn't know were there**

As a modern CISO, your role is evolving. You have to speak in relation to the business and insulate it against negative implications, particularly in relation to legal and compliance risks. When we talk about risk, there is acceptable and unacceptable risk. As government dictates push business leaders to accept legal culpability for the amount of accepted risk, risk appetite is becoming clearly defined. The ability to accept risk without ramifications is a thing of the past.

CHAIM MAZAL
Chief Security Officer, Gigamon

The survey results illustrate an ongoing dilemma: CISOs need their boards to understand and prioritize cyber risk, but regulations alone will not solve their biggest challenges. Modern CISOs are increasingly tasked with addressing business and legal risk alongside technical needs, but they simply don't have the resources to prepare and protect their organizations against the next generation of cyber threats. Without the technical support, board-level pressure risks adding to CISO stress without improving security posture.

Understanding the Risks

Across surveyed CISOs, there is a general lack of confidence in their organization's threat detection capabilities. Just under half **(46 percent)** feel only somewhat or not at all prepared to detect threats across hybrid cloud infrastructure, and **48 percent** have similar doubts about their ability to respond quickly to unauthorized hybrid cloud access. Although not an optimistic picture, these numbers still suggest overconfidence: just 1 in 5 **(20 percent)** of CISOs report being able to detect and mitigate the damage of a breach in real time using their existing security tools. With cloud migration continuing to accelerate—and AI deployments promising even more cloud investment—improving visibility is an urgent priority for CISOs to truly be confident in their threat detection capabilities.

Detecting and preventing attacks is not the only element of security preparedness under the spotlight. Organizations are facing consequences for failing to quickly understand and disclose the extent of a breach: a weak point for many organizations. In the last 12 months, over half of CISOs **(53 percent)** admit that they were first alerted to a breach only when notified that users could not access applications, and **1 in 3** cite that they were unable to determine the root cause. A lack of post-breach intelligence carries serious consequences: **39 percent** of CISOs cite an extortion threat as the first indicator of a serious security breach, while **36 percent** only discovered the attack when data was leaked on the dark web.

How were you able to detect the data breach?

56% **Our IT team detected the threat using security and observability tools**

53% **Users were unable to access applications and digital resources**

43% **Users experienced slow application performance**

39% **We received an extortion threat from the adversary**

36% **Our organization's proprietary information was leaked on the dark web**

Respondents had the option to select multiple answers.

The stark number of attacks flying under the radar of security teams indicates that threat actors are aware of and exploit organizations' blind spots. Recent headlines would suggest the same, as intelligence agencies warn against a rise in nation-state backed Living off the Land attacks, in which threat actors hide out or dwell for lengthy time periods in breached networks, moving laterally to gather intelligence and increase the damage of their eventual attack.

Poor East-West visibility and a reliance on log-based security monitoring offers these hackers a helping hand. Logs are mutable records that bad actors can manipulate to evade detection. Similarly, cyber criminals are increasingly weaponizing organizations' use of encryption as a security measure—masking malware, movement, and data exfiltration in encrypted traffic. Overcoming these tactics requires a crackdown on implicit trust by CISOs and complete visibility into East-West and encrypted traffic. Currently, **7 in 10** CISOs report struggling to gain visibility into encrypted traffic, and yet **8 in 10** still perceive that encrypted traffic is secure. Until organizations address the risk posed by this persisting blind spot with sufficient resources, they cannot be confident in their overarching security posture.

Managing the Risk/Reward of AI

Existing tool stacks certainly seem to be falling short, but CISOs appear to be split on how to move forward. **Four out of five** CISOs describe their security teams as being overwhelmed by tool sprawl, and a tool overhaul tops CISOs' priorities for remediating blind spots over the coming 12 months. Almost two-thirds of CISOs listed tool consolidation and optimization as their number one priority **(62 percent),** closely followed by investing in additional tools **(54 percent).** While global respondents pin their hopes on security automation and AI, with **54 percent** selecting this in first place, CISOs are more skeptical. For this subsection of respondents, AI comes in fourth at **46 percent.**

Despite AI being named Gartner's top cybersecurity trend for 2024, those closest to security are more focused on getting their fundamentals in order: remediating blind spots, optimizing tooling, and preparing for upcoming mandates. AI-generated threats also loom large on their threat radar, with **83 percent** of CISOs expecting the technology to further the growth of the global ransomware threat. The dawn of AI availability presents organizations with as much risk as it does opportunity, and there is a clear disparity between how CISOs and their C-suite colleagues value its potential for reducing risk. Perhaps this is because CISOs are well-aware that they play a critical role in securing all AI deployments, as well as mitigating AI-enabled breaches.

This is indicative of a wider trend: the role of the CISO is expanding to cover more than just cybersecurity, touching on AI strategies, physical security, and general IT technology decisions. And yet, as the scope of this already-stretched function grows wider, CISOs don't currently have the tools and support to fully protect their organizations.

85 percent of CISOs agree that gaining deep observability into a hybrid cloud infrastructure is crucial for shifting to a proactive mindset and essential for preventing attacks.

Closing the Preparedness Gap

CISOs' dissatisfaction around existing tool stacks is matched by their boardrooms, that commonly pursue tool consolidation and platform offerings to reduce IT spend. But with both consolidation and investing in new tools making organizations' priority lists, it seems that a "rip and replace" strategy is not the way forward, nor is total consolidation behind just one vendor.

Instead, organizations should focus on ensuring that existing tools are working efficiently and are well integrated to eliminate security blind spots. This requires deep observability, powered by high-fidelity data and network telemetry, that goes beyond MELT (metrics, events, logs, and traces) data. This is something that CISOs are well aware of, with **83 percent** agreeing that deep observability is a foundational element of cloud security.

Achieving this level of deep observability will set CISOs and their organizations up for the IT strategies of the future. Successful AI deployments need to be fed high-fidelity data, and **65 percent** of CISOs recognize that visibility into all data is the number one priority for ensuring secure and successful AI investments. Hybrid cloud infrastructure will only continue to grow in complexity as organizations rightly embrace the benefits of new technologies and scale their operations. Proactive CISOs must look to employ infrastructure technologies that can efficiently deliver network telemetry to their existing tool stack and inform security teams in real-time, ensuring continued deep observability into hybrid cloud infrastructure.

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived intelligence to cloud, security, and observability tools. This helps eliminate security blind spots and reduce tool costs, enabling you to better secure and manage your hybrid cloud infrastructure. Gigamon has served more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

Download the full report to discover the insights from your region
gigamon.com/cloud-security-survey

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

05.24_01