Office of the CISO

Perspectives on Security for the Board

August 2025 – Edition 8

Google Cloud

August 2025
For more information, visit our Board of Directors Insights Hub

Table of contents

Foreword

The future of business resilience and growth hinges on strategic cybersecurity.

That's the pivotal truth we routinely hear from board members when they talk with our Office of the CISO.

Through our dedicated board insights efforts and hosted roundtable events, we've seen leading organizations move beyond reactive defense to a more proactive approach to strategic cybersecurity because they recognize that a robust security posture can be the ultimate enabler of innovation and trust.

Our commitment to empowering business transformation through security is why we curate Perspectives on Security for the Board, a forward-looking guide where we distill three key themes derived from our ongoing conversations with boards.

Ransomware's Evolving Front Lines

We delve into critical shifts in ransomware tactics, highlighting how threat actors exploit identity, and emphasizing what boards need to know about treating identity as a crucial security perimeter.

The Strategic Challenge of Cyber-Enabled Fraud

We explore the rapidly escalating threat of cyber-enabled fraud, including sophisticated schemes that can directly challenge a company's financial health, brand reputation, and core mission—and introduce a framework for boards to elevate fraud prevention to a strategic business priority.

Orchestrating Innovation with Robust Cybersecurity

We examine how boards can ensure that rapid digital transformation and innovation are pursued through a lens of informed cyber risk management. This includes fostering a risk-first culture, demanding agile reporting, and championing proactive security integration and engagement beyond compliance checkboxes.

For our eighth edition, we hope to encourage boards to embrace the principles outlined in this report—understanding the nuances of modern threats, proactively combating cyber-enabled fraud, and strategically aligning cybersecurity with innovation. This report is another step in our journey to build and share critical board insights, with a broader goal to help directors drive accountability, foster a culture of shared responsibility, and fulfill their fiduciary duties as we build together a more secure and innovative future for all.

Nick Godfrey, Senior Director, Office of the CISO, Google Cloud

Ransomware's New Front: Identity, Help Desks, and Modern Infrastructure

Ransomware has shifted from an IT nuisance to a major strategic risk for organizations worldwide. By locking up corporate systems and threatening to leak sensitive data, cybercriminals have been able to impose substantial costs on victims and demand hefty extortion fees.

In recent months, the cybercriminal actor UNC3944 (also known as Scattered Spider) has captured headlines and shot up risk registers following a devastating ransomware campaign. The campaign rapidly expanded from the U.K. retail sector to U.S. retailers, before widening to include insurance and aviation organizations.

The impact of their ransomware operations has been severe, causing system outages, operational disruption, customer data loss, and reputational damage. UNC3944's rampage serves as a critical reminder that ransomware remains the top cyber threat to most organizations.

Beyond the immediate impact to victims, this campaign also highlighted crucial evolutions in adversary tactics and the broader cyber risk environment. For boards of directors, these incidents and evolving tactics demand a proactive, informed strategic response to safeguard organizational resilience.

Ransomware on the move

UNC3944's recent campaign has illuminated important shifts in the ransomware threat landscape that impact cyber risk management. The following insights detail specific threat developments that boards should understand and consider.

- **Voice phishing (vishing) and help desk vulnerability**: UNC3944 operators frequently impersonate employees to trick help desk staff into resetting credentials or multifactor authentication (MFA) methods, often adding attacker-controlled devices for password resets. Social engineering bypasses IT network defenses by targeting the human element, and has proven highly effective against organizations with large and outsourced IT functions.

  As help desk processes often fall outside direct security team control, it is vital for boards and executives to foster a strong security culture across the organization—especially with large and outsourced teams. This empowers a cybersecurity team to protect these critical human processes. Read more on the high cost of vishing.

- **Targeting modern IT infrastructure**: As organizations embrace digital transformation and diverse supply chains, threat actors will follow and their modern IT infrastructure requires strategic risk oversight. UNC3944 has frequently targeted cloud providers, moving between cloud and on-premises systems. They also abuse single sign-on (SSO) solutions with compromised accounts to gain widespread application access, significantly expanding intrusions beyond traditional infrastructure.

- **Defending identity as the new center of gravity**: Identity is UNC3944's primary and most exploited initial access vector, so defending against identity abuses is paramount in stopping them. Their attacks heavily rely on compromising and abusing legitimate identity credentials to gain and expand access.

  These attacks should elevate robust Identity and Access Management as a foundational pillar of organizational resilience, if it hasn't been already. Organizations should ensure identity security is treated as a core business enabler. When security teams face pushback on critical controls like phishing-resistant MFA, boards are uniquely positioned to set the tone and ensure these vital safeguards are adopted organization-wide.

Actions for boards

Translating cyber threat developments into tangible protective measures requires deliberate action and appropriate oversight from boards. The following recommendations provide a roadmap for enhancing resilience against cybercriminals and ransomware.

- **Prioritizing rigorous identity controls**: Fostering a culture of rigorous, enterprise-wide identity security is a critical component of the board's oversight role in protecting the company. This includes: improving help desk identity verification processes that reset credentials, implementing phishing-resistant MFA methods (such as passkeys and USB security keys), securing MFA registration processes, and educating employees on social engineering tactics.
- **Building a proactive, threat intelligence-led security posture**: Countering ransomware begins with deeply understanding how these operations occur. Boards can play an important role in championing a threat intelligence-led security posture, ensuring security investments and controls precisely align to active, critical risks. Resources that exemplify this approach include Google Threat Intelligence's UNC3944 hardening guide and Mandiant's red team exercises.
- **Identifying and addressing risks associated with digital transformation**: While digitalization and cloud adoption can enhance overall security, boards play an important role in overseeing the identification and mitigation of cybersecurity risks associated with modern infrastructure. This includes ensuring that technology and cyber investments are appropriately aligned to protect organization's as they evolve their technology stack.

Board's Strategic Guide to Combating Cyber-Enabled Fraud

Cyber-enabled fraud is a rapidly-escalating threat that directly challenges a company's financial health, brand reputation, and core mission. It's crucial that boards of directors discuss fraud prevention with management, and help jumpstart cyber-enabled fraud detection programs.

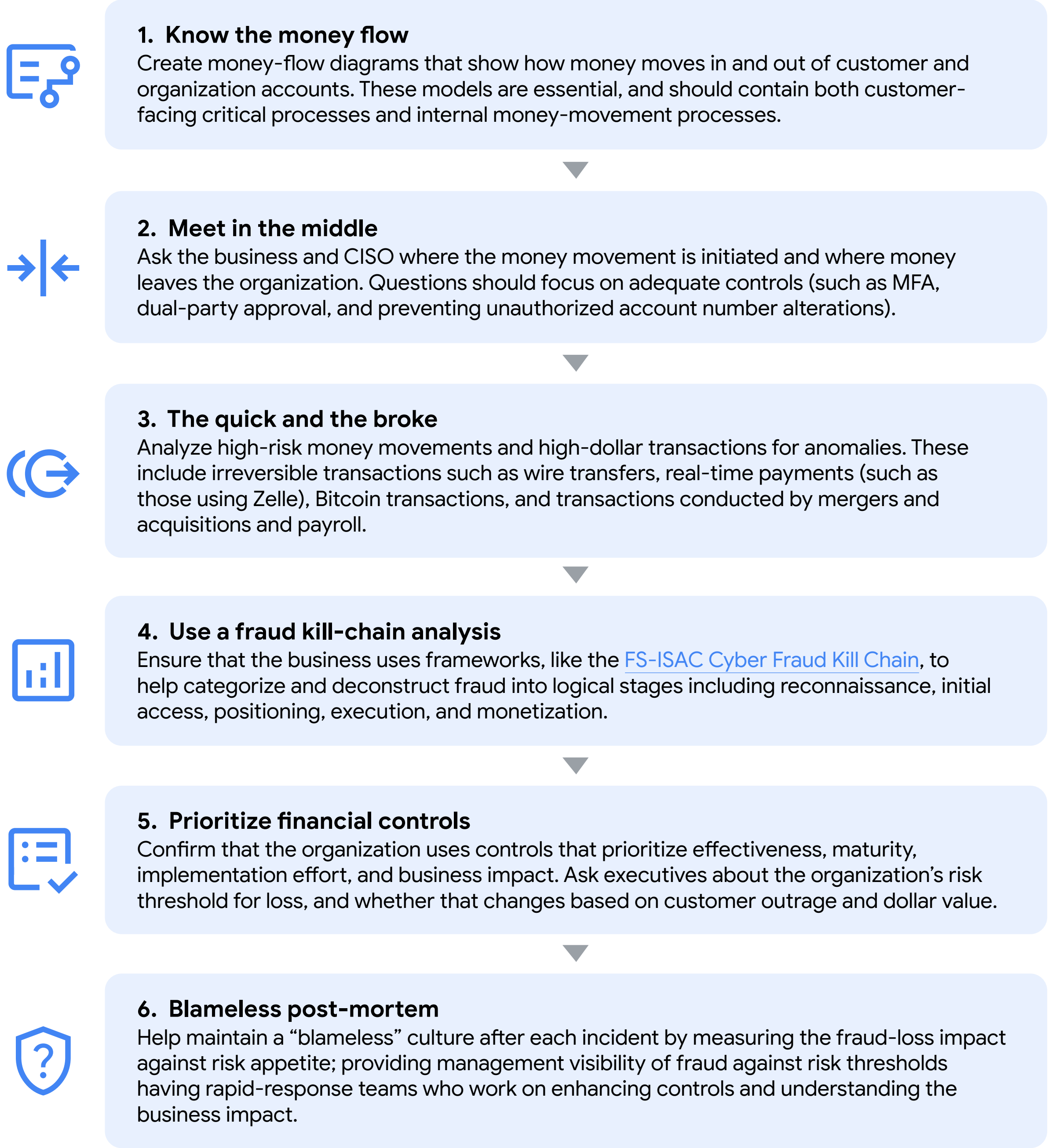
The financial toll of cyber-enabled fraud is staggering. The FBI said that the cost of cyber-enabled fraud was $13.7 billion in 2024, a nearly 10 percent increase from 2023, and represented 83 percent of all financial losses reported to the FBI in 2024. Funds obtained through fraudulent activity are often used to fuel transnational organized crime, including human trafficking, creating a vicious cycle.

Common Types of Cyber-Fraud

- **Smishing triad:** SMS phishing campaigns using fake texts (such as package deliveries and DMV notices) to trick customers into revealing credentials and installing malware.
- **Business email compromise (BEC):** Fraudsters impersonate executives and vendors via email to trick employees into making unauthorized payments.
- **Romance baiting:** A long-term romance and investment fraud scheme where victims are lured into fake cryptocurrency investments, often targeting executives.
- **Account takeover (ATO):** Unauthorized access to customer online retail accounts can lead to fraudulent purchases and data theft.

To help boards shift to a more proactive posture and talk with their organizations about fraud prevention and mitigation, we offer a model that might be useful for cyber-enabled fraud prevention conversations with key stakeholders.

How can boards help their organizations take a more active approach to mitigating cyber-enabled fraud? Here are six steps to help make that shift.



1. Know the money flow
Create money-flow diagrams that show how money moves in and out of customer and organization accounts. These models are essential, and should contain both customer-facing critical processes and internal money-movement processes.

2. Meet in the middle
Ask the business and CISO where the money movement is initiated and where money leaves the organization. Questions should focus on adequate controls (such as MFA, dual-party approval, and preventing unauthorized account number alterations).

3. The quick and the broke
Analyze high-risk money movements and high-dollar transactions for anomalies. These include irreversible transactions such as wire transfers, real-time payments (such as those using Zelle), Bitcoin transactions, and transactions conducted by mergers and acquisitions and payroll.

4. Use a fraud kill-chain analysis
Ensure that the business uses frameworks, like the FS-ISAC Cyber Fraud Kill Chain, to help categorize and deconstruct fraud into logical stages including reconnaissance, initial access, positioning, execution, and monetization.

5. Prioritize financial controls
Confirm that the organization uses controls that prioritize effectiveness, maturity, implementation effort, and business impact. Ask executives about the organization's risk threshold for loss, and whether that changes based on customer outrage and dollar value.

6. Blameless post-mortem
Help maintain a "blameless" culture after each incident by measuring the fraud-loss impact against risk appetite; providing management visibility of fraud against risk thresholds having rapid-response teams who work on enhancing controls and understanding the business impact.

Figure 1. Follow the Money—Cyber-Enabled Fraud Framework

Actions for boards

Based on the escalating threat of cyber-enabled fraud, boards of directors should take the following three critical actions:

1. **Elevate cyber-enabled fraud to a strategic business priority**: Boards should formally integrate cyber-enabled fraud into the enterprise risk management (ERM) framework, ensuring it's treated with the same gravity as financial and operational risks, and champion a proactive, organization-wide anti-fraud culture from the top down.
2. **Implement and oversee a proactive "follow the money" fraud prevention framework**: Directors should shift the organization from a reactive to a proactive fraud posture by mandating the development of comprehensive, end-to-end money-flow diagrams, scrutinizing and securing high-risk financial transactions, and ensuring robust, multi-layered controls are in place at all critical money-movement points.
3. **Drive continuous improvement through blameless post-mortems and clear risk thresholds**: Boards should ensure that management conducts thorough, blameless post-mortems after every fraud incident to identify control gaps, enhance defenses, and understand the full business impact. They should also establish clear, measurable risk appetites for fraud and regularly review the organization's performance against these defined thresholds.

By embedding these actions into regular board discussions and oversight, directors can elevate the conversation, drive accountability, and fulfill their organizational responsibilities to safely navigate the complex landscape of cyber-enabled fraud.

Orchestrating Innovation with Robust Cybersecurity

While meeting compliance requirements is a critical baseline, achieving robust cybersecurity requires a more comprehensive and proactive approach. Boards increasingly understand that a strong cybersecurity program can drive competitive advantage.

“Meeting compliance requirements isn’t the same as strong cybersecurity and privacy practices that create the culture and conditions required for us to innovate—and the potential to differentiate a brand,” said Grant Waterfall, Cybersecurty Partner, PwC, on our Cyber Savvy Boardroom podcast. “I would argue right now that a strong cybersecurity program can be the new competitive advantage in a digitally transformed and data-driven world.”

Rather than solely a cost center or compliance hurdle, robust cybersecurity directly enables business growth by fostering trust with customers and partners, safeguarding intellectual property, and providing a secure foundation for digital transformation and innovation. A strong security posture can reduce the risk of costly breaches and reputational damage, allowing organizations to confidently pursue new technologies and market opportunities.

Ultimately, it can allow businesses to innovate and operate with greater agility and resilience in an increasingly digital landscape.

Innovation is crucial for an organization’s survival and growth. To foster secure innovation, boards should encourage a risk-first mindset. The board should actively work with the CISO and business and risk functions to provide them with the necessary tools to comprehend cyber risks and allocate resources appropriately to manage them.

Critically, boards should insist that these same business, risk, and security functions collaborate on agile reporting, so that team members, managers, and executives provide timely, relevant, and transparent information to key stakeholders—including the board. Empowered by agile reporting, organizations can better support rapid responses to dynamic threat environments and be more flexible when allocating resources.

The concept of “shifting left” in security and compliance offers a powerful paradigm for boards to consider. Shifting left involves embedding security considerations early in the development lifecycle, integrating it seamlessly into business thinking from the top down.

This proactive approach ensures that security is an integral component of innovation. As security processes increasingly become automated, particularly through AI, even complex organizations can gain enhanced visibility and improved resilience.

Tools and approaches for balanced innovation

Successfully navigating the tension between innovation and compliance requires specific tools and proactive approaches. Boards should actively engage with their CISO, business leaders, and risk functions to champion the adoption of the following:

- **Proactive regulatory engagement:** Boards should move beyond passive compliance and support proactive engagement with regulators and policymakers. By participating in industry groups and trade associations, and facilitating direct meetings with regulators and supervisors, organizations can develop an early understanding of regulatory trends and also educate regulators about their concerns.
- **Using regulation as a catalyst:** Regulatory requirements can be transformed into opportunities for innovation. For example, boards can encourage their organizations to use regulatory requirements as an impetus to integrate security into core purpose and values, which can lead to improved risk reporting and even achieve compliance as a byproduct of a broader, more impactful transformation.
- **Regulatory sandboxes:** These controlled environments allow organizations to test cutting-edge cybersecurity and AI-driven innovations under an adapted regulatory process to facilitate innovation while managing oversight. Successful examples, such as the U.K.'s Financial Conduct Authority (FCA) can provide a safe space to assess risks, refine products, and demonstrate compliance feasibility before full market deployment.

Actions for boards

To truly drive secure growth and maintain a competitive edge, boards should take decisive steps to embed innovation with robust cybersecurity. To that end, here are three steps that boards can take today:

1. **Innovate with a risk-first mindset:** Boards can foster a culture where innovation is pursued through the lens of informed cyber risk management. They can encourage the CISO and business functions to provide the necessary tools and insights for effective capital allocation, making risk a core consideration from the very beginning of any new initiative, product development, or strategic decision, thereby fostering a deeper inquiry into the underlying risks and consumer harms that regulations aim to mitigate.
2. **Prioritize agile, decision-grade reporting:** Advocate for cybersecurity reports that are timely, business-focused, and provide clear, actionable intelligence for strategic decision-making and resource adjustment. Mandate agile reports that link security performance to clear business outcomes like reduced fraud, improved uptime, and faster time-to-market. These shared metrics align priorities and enable rapid, data-driven resource allocation. This agile reporting is also crucial for responding to dynamic threat environments.

3. **Champion proactive security integration and continuous engagement:** Encourage the organization to “shift left” by including security leaders, teams, and functions early in all new digital initiatives, product development, and strategic thinking. Concurrently, CISOs should commit to ongoing board education and proactive engagement with industry peers, regulators, and external experts.

How boards can learn more

To delve deeper into these critical discussions and explore all of our “Perspectives on Security for the Board” reports, including AI and cybersecurity, cyber risk oversight, cloud adoption risk mitigation, supply chain security, and insider risk, please visit our dedicated Board of Directors Insights hub.

Google Contributors

Alicja Cade, Director, Financial Services, Office of the CISO

Jamie Collier, Lead Threat Intelligence Advisor (Europe), Google Threat Intelligence Group

Nick Godfrey, Sr. Director and Head of Office of the CISO

David Homovich, Customer Advocacy Lead, Office of the CISO

Seth Rosenblatt, Cybersecurity Editor

David Stone, Financial Services, Office of the CISO