Office of the CISO

Perspectives on Security for the Board

March 2025 – Edition 7

Google Cloud

March 2025

For more information, visit our Board of Directors Insights Hub

Table of contents

Foreword

We continue to see boards of directors facing increasing pressure to effectively oversee cybersecurity risks. As board members, we can help safeguard our organizations and our stakeholders. Our first report of 2025 offers insights and recommendations for boards seeking to enhance their cyber risk oversight. Specifically, we provide guidance on three crucial areas to help boards enhance their cybersecurity governance and maintain a strategic focus.

Optimizing Board Oversight	The New Insider Threat	Incident response plans and tabletop exercises
We examine committee structures for cybersecurity oversight, considering factors such as industry, regulations, and existing risk management frameworks. We explore the importance of clear responsibility lines and resource allocation to manage cyber risks effectively, and provide a comparative overview of different committee structures.	We address the evolving threat from North Korean IT workers operating covertly within organizations. We highlight key trends for boards to be aware of, such as the exploitation of remote work practices and the increasing use of AI in their operations. We also emphasize the importance of a collaborative approach to insider risk management, involving security, HR, legal, audit, and finance functions.	We explore the crucial role boards play in cyber resilience preparedness, focusing on incident response planning and tabletop exercises. We delve into the importance of proactive planning and training, even for those without deep cybersecurity expertise.

Phil Venables, CISO, Google Cloud

Optimizing Board Oversight: Why One Committee Structure Doesn't Fit All

Cybersecurity is a strategic investment that can drive innovation, business resilience, customer retention, and shareholder value. Boards structure effective oversight of cybersecurity in different ways, depending on factors such as sector, market segment, regulatory environment, and existing risk management frameworks. Regardless of the specific structure, the board plays a crucial role in establishing clear responsibility lines and ensuring the allocation of appropriate resources to manage cyber risks.

Emerging threats and regulatory changes are driving boards to refine how they integrate cybersecurity reporting into their committee structures. Should the Audit Committee, the Risk Committee, the Technology Committee, or the full board oversee this risk? Or might a combination be the best approach? The answer, as with most aspects of risk governance, is nuanced and depends on a variety of factors.

The chart below provides a comparative overview of the benefits and considerations of different committee structures in the context of cyber risk oversight.

Structure	Benefits	Considerations
Audit Committee	• Provides oversight of financial reporting, internal controls, and regulatory compliance • Aligns with common practice of delegating cyber risk oversight to the audit committee as seen in 71% of S&P 500 companies	• Sufficient cybersecurity expertise, whether through existing members or external advisors • Anticipation of future threats, investment in emerging technologies, and alignment of cybersecurity strategy with business objectives
Risk Committee	• Integrates cybersecurity strategy with organizational risk appetite • Evaluates the potential impact of cyber incidents on business operations, reputation, and customer trust • Aligns with common practices used in financial services industry	• Effective integration of cybersecurity into existing business risk oversight processes
Tech/Cyber Committee	• Possesses in-depth understanding of technology and associated risks	• Limited or siloed view of cybersecurity, potentially overlooking broader business implications
Multi-Committee Approach	• Offers diverse expertise and perspectives on cyber risk	• Clear communication and coordination to prevent duplicated efforts, confusion, and unclear responsibilities
Full Board	• Increases awareness and engagement on cybersecurity at the highest level	• May result in less focused discussions and limited in-depth analysis

Putting this into action

The company's decision on the committee structure depends on many aspects, but at a minimum boards should carefully consider the following factors when making this determination.

- **Expertise:** Does a specific committee or full board possess the necessary technical expertise to understand and assess cyber risks in business context?
- **Resources:** Does the chosen structure provide sufficient resources and support for effective oversight, considering the potential burden associated with covering different risk types, including cyber?
- **Integration:** How well does cybersecurity integrate with other risk management activities within the company?
- **Reporting:** Does the structure ensure timely and accurate reporting of cyber risks to the board?
- **Compliance:** Does the structure meet regulatory requirements for cybersecurity governance, which are becoming increasingly stringent?

By addressing these questions, boards can establish a robust cybersecurity oversight structure that protects the organization and its stakeholders. Effective cybersecurity governance is not a one-size-fits-all solution, but rather a continuous process of assessment, adaptation, and improvement.

Beyond the Firewall: Addressing Insider Risk

Most organizations' security posture prioritizes external cybersecurity threats, yet a growing danger comes from within.

The explosion of data stored on internal networks, in the cloud, and on increasingly large portable devices has significantly increased the potential impact of an insider threat. Employees with access can now easily acquire, store, and exfiltrate vast amounts of sensitive information.

For boards to effectively oversee insider risk, they must be aware of the diverse range of insider threats, including:

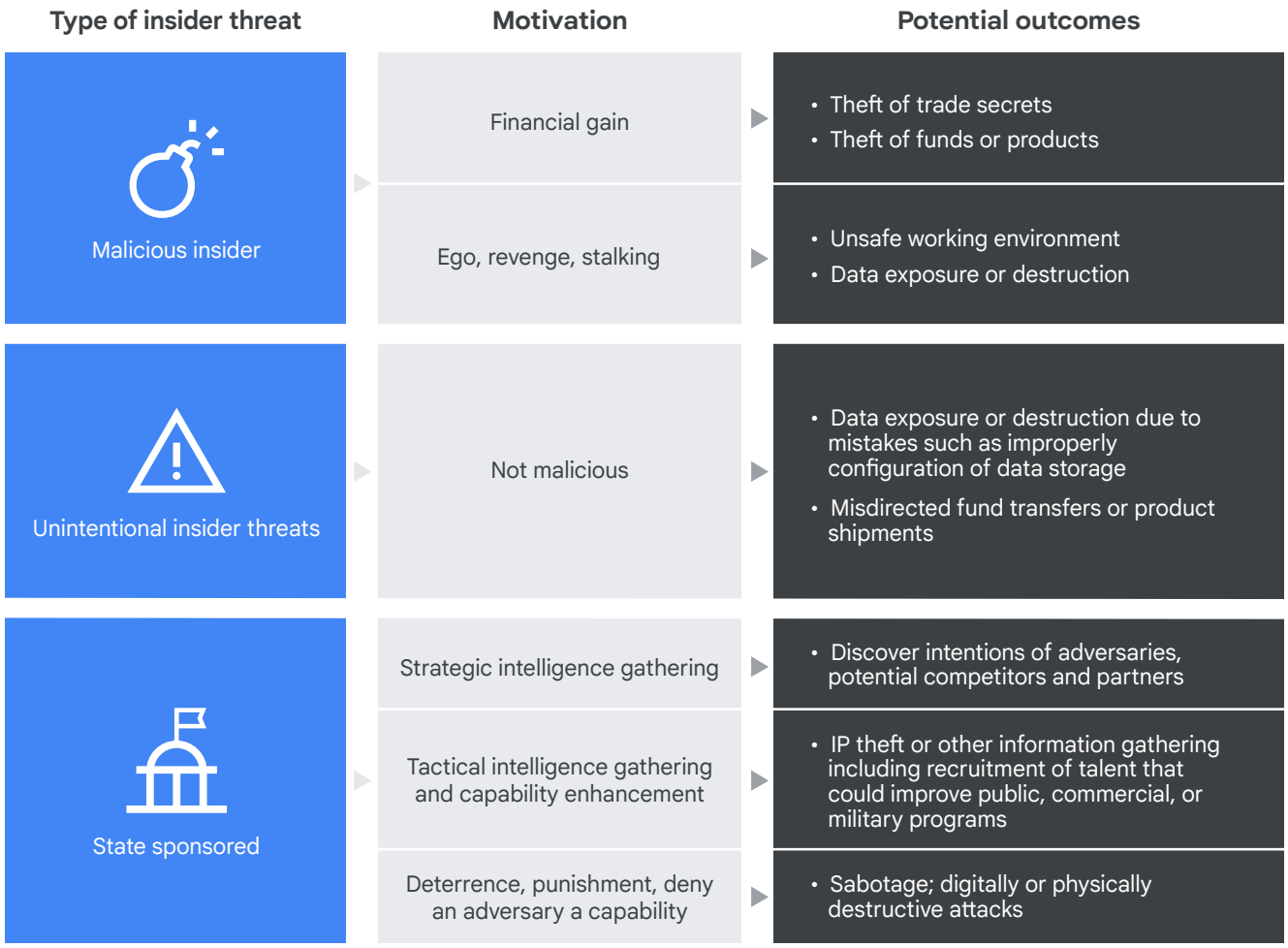
- **Malicious insiders:** Employees may steal or sabotage data for personal gain, revenge, or to benefit a competitor. For example, ransomware groups have offered employees money to help them gain access to a network and steal sensitive data.
- **Unintentional insider threats:** Unintentional insiders may accidentally expose data due to carelessness or a lack of training. These individuals are often tricked into assisting threat actors through social engineering campaigns.
- **State-sponsored insider threats:** Insiders have previously been used by government agencies to facilitate intelligence gathering operations and to conduct industrial sabotage.

The New Insider Threat: North Korean IT Workers

A prime example of the evolving nature of insider risk can be seen with the rise of the North Korean IT worker threat. These individuals seek employment across various sectors under the guise of legitimate remote workers, often using stolen or fabricated identities. Once hired, they use their access within an organization to generate revenue and conduct cyber espionage for the North Korean regime.

The Google Threat Intelligence Group has identified several important trends that boards should be aware of:

- **Capitalizing on modern working practices:** Organizations relying on remote hiring, work-from-home policies, and freelancers face heightened risk from North Korean IT workers. These individuals frequently create fake resumes and job applications, presenting themselves as skilled professionals.
- **Move to extortion and data leak operations:** Revenue streams for the North Korean regime, facilitated by its IT workers, include salaries, financial transfers, and occasional cryptocurrency theft, alongside "legitimate" work within the cryptocurrency industry. More recently we have observed an uptick in extortion operations against large organizations where IT workers will threaten to leak sensitive data unless a ransom is paid.



- **Experimenting with AI:** IT workers are experimenting with AI, including generating fake profile photos, using deepfakes during video interviews, using AI writing tools to get around language barriers, and even attempting to gain employment as AI developers.
- **National security considerations:** IT workers increasingly collaborate with North Korean Advanced Persistent Threat groups that specialize in espionage operations. IT workers have applied for roles with U.S. security clearances as well as organizations within the defense industrial bases globally and in European governments.
- **Global operations:** IT workers are encountering challenges in gaining and maintaining employment in the U.S. given increased public reporting, indictments, and visa challenges. IT workers have now been employed and actively seeking roles across a range of countries in Europe and Asia alongside the U.S.

Putting this into action

Tackling insider risk should be viewed as a joint responsibility. Various teams have a role in identifying and addressing insider risk, including security, HR, legal, audit, and finance functions. Boards should set clear expectations with these teams around:

- **Robust insider risk frameworks:** Conducting an insider risk assessment can help an organization identify weak points and audit their current controls.
- **Limit the blast radius:** To reduce the business impact of insider threats, organizations should introduce clear separation of duties with granular access controls. Limiting the amount of sensitive information or access any single insider can achieve is an effective way to reduce overall insider risk.
- **Monitoring and detection:** Security teams should have the appropriate visibility and logging capabilities to identify if employees have exfiltrated sensitive data or provided network access. While this is ideally detected and prevented before a significant incident occurs, organizations should also factor insider risk into their incident response plans.
- **A security-minded hiring process and culture:** Education and training can help employees to understand the various types of insider threats and their role in protecting the organization's assets. Stringent background checks, careful interview processes on-camera, and vigilant job vetting can all help mitigate the risk posed by North Korean IT workers.

From Good to Great: The Board's Cyber Resilience Game Plan

What distinguishes a good athlete from a truly great one isn't just natural ability, but the presence of a well-defined plan and the unwavering dedication to training against it. The same principle applies to cyber resilience preparedness for board members and executive leaders. In this section, we explore incident response plans and tabletop exercises, two critical areas where board members must be proactive in their planning and training, even if they don't have expertise in cybersecurity.

The Plan

A robust incident response plan is the cornerstone of any organization's risk management program. It outlines the steps to take in the event of a cyberattack, from initial detection and containment to recovery and post-incident analysis. It's important for board members and business leaders to have a clear understanding of the organization's cyber incident response capabilities and plans, especially concerning their own role in the process.

Putting this into action

Some key questions boards should be discussing with business leaders:

- Do we have a comprehensive incident response plan that is regularly updated and tested?
- Have we clearly defined roles and responsibilities for incident response, including communication protocols?
- What are the expectations for the board during an incident, and conversely, what expectations does the board have for the executive team during a live event?
- In the event of an incident, what is the protocol for communicating with the board, and what is the expected timeline?
- Who is responsible for determining materiality and what factors will be considered in making that determination?
- Do we have the necessary resources and expertise to effectively respond to a cyberattack?
- How are we leveraging third-party experts to aid our response and timeliness?
- Does your plan identify your key assets, systems, and data, including prioritization for restoration and recovery?
- How are we incorporating lessons learned from previous incidents and industry best practices into our plan?

Overall, boards are expected to have a clear understanding of the resources and processes that would be activated during an incident – ensuring these resources match the organization's risk profile, along with a clear understanding of the role the board will play during an incident.

Exercise the Plan

While it's important to know the plan, organizations should also simulate real-world cyberattacks with regular tabletop exercises. They provide a safe environment for your organization to test its incident response plan, identify gaps and weaknesses, and practice decision-making under pressure.

These tabletop exercises should be aimed at various responder levels including technical, executive, and board. Your third-party ecosystem may also be included, with representation from external incident responders, crisis communications, and your legal and insurance providers. These sessions should also provide an opportunity for the board to learn about current cyber threats and trends.

We recommend that external cybersecurity tabletop experts be used to design, facilitate, and generate a report that includes observations, areas of strength, and recommendations for improvement.

Putting this into action

- As board members, it is important to understand your role and exercise readiness when it comes to responding to suspected cyber incidents.
- To get the most out of tabletop exercises, actively participate and ask probing questions about how the team would respond to different scenarios, like ransomware attacks or data breaches. For example:
  - How would we handle a ransomware attack that encrypted our critical data?
  - What steps would we take to communicate with customers and stakeholders during a data breach?
  - How would we coordinate with law enforcement and other external partners?
- Be clear on communication protocols and when the board will be notified, and practice your activation and notification procedures.
- Use the exercise findings to drive continuous improvement in your organization's incident response.

To read previous Perspectives on Security for the Board reports, and to learn more about our guidance for boards of directors, please visit our Board of Directors Insights Hub and consider subscribing to Phil Venables' Cloud CISO Perspectives bimonthly newsletter.

Google Contributors

Michael Barnhart, Principal Analyst, Google Threat Intelligence Group

Jennifer Burnside, Practice Leader, Mandiant Crisis Communications

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

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

David Homovich, Solutions Consultant, Office of the CISO

Phil Venables, CISO, Google Cloud

Google Cloud