Google Cloud

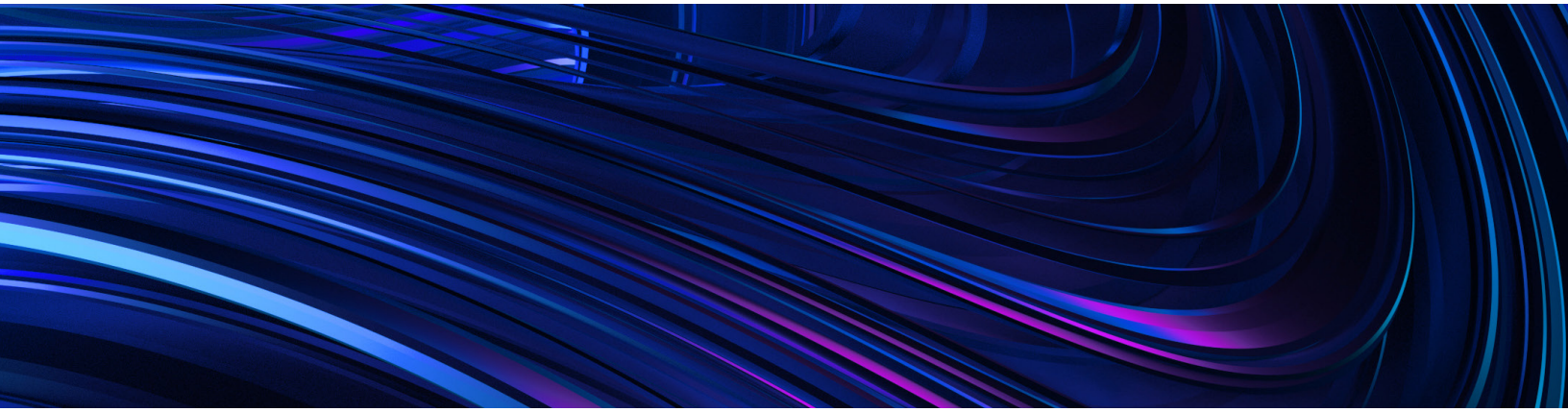
Perspectives on Security for the Board

April 2023 – Edition 1

Office of the CISO

April 2023

Table of contents



Foreword

As a Board Member and a CISO, we frequently engage with company leadership across sectors on cybersecurity and technology risk. In these engagements, it is clear that cyber is top of mind for every organization.

As such, we thought it would be timely to share our perspective on how the Board can best address cybersecurity and risk along with ways to take a more proactive role in these areas - now and in the future. One lesson we've learned is that **Board awareness and subsequent guidance in this area is absolutely critical** to every organization's long term success.

When we engage on these issues, Board members often ask: what types of conversations should we be having about cybersecurity and what types of questions do we need to be asking our C-Suite? The answer is that Boards should work to ensure that security management teams inventory critical assets and business processes, convey top risks and mitigations (and measure their success), and communicate accepted residual risk. Above all, Boards, CEOs and other executives should ask probing questions about technology and digital capability, not just review what are often lagging indicators of cyber performance.

Office of the CISO's Perspectives on Security for the Board report. This report series is intended to help Board members sharpen their cybersecurity knowledge – including how to address cyberattacks and understand how likely they are to impact their organization – and prepare them for potential regulatory obligations.

In this inaugural report, we (1) cover the Board's roles and responsibilities in cyber risk oversight; (2) provide guidance on how Boards should navigate the cyber threat landscape; and (3) explain how Boards should engage on emerging issues surrounding artificial intelligence (AI) and cybersecurity. We hope you find it informative and look forward to connecting with you more on these important topics.

Betsy Atkins (Chairman, Google Cloud Advisory Board)
Phil Venables (CISO, Google Cloud)

The Board's Role in Cyber Risk Oversight

Cyber-related risk remains one of the top concerns facing organizations today. Addressing cyber risk is a challenge for nearly any company and its Board, so it is increasingly important for Board members to conduct relevant oversight and help guide risk management priorities. Governments globally are increasingly implementing regulatory measures to raise compulsory cybersecurity baseline standards, including requirements to report cyber incidents to the relevant government authorities. In recent weeks, we've seen two such initiatives from the U.S. Securities and Exchange Commission, which contain hundreds of pages of proposed rules on cybersecurity, incident reporting, and systems integrity.

To be effective, Boards should view cyber risk through the lens of overall business risk. This requires that Boards integrate cybersecurity and resiliency into their business strategy, risk management practices, budgeting, and resource allocation to underpin that cyber risk is everyone's responsibility.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) (CSF) can be a useful tool for Boards when thinking about cybersecurity. The NIST CSF is designed for use across multiple industries of different sizes, and provides a structured way and a common taxonomy for Boards to have more impactful discussions with their CISO and cybersecurity teams. What the NIST CSF and other frameworks can do is enable us through their structures to achieve better cybersecurity outcomes. The Framework is made up of five functions - Identify, Protect, Detect, Respond, and Recover.

- **Identify**: Assists in understanding what matters most to the organization, including critical business services, systems, people, assets, data, and capabilities.
- **Protect**: Outlines appropriate safeguards to ensure delivery of critical services and supports the ability to contain the impact of a potential cybersecurity incident.
- **Detect:** Helps in defining the appropriate activities to identify a cybersecurity event in a timely manner.
- **Respond**: Focuses on appropriate activities to take in the event of a cybersecurity incident while supporting the ability to contain the impact of a potential cybersecurity incident.
- **Recover**: Defines activities to maintain resiliency plans and to restore services that were impacted due to a cybersecurity incident.

As regulatory risk increases at federal and state levels, Boards' understanding of cybersecurity is more critical than ever. We expect these trends will continue and blur across borders, geographies, and sectors over time. Boards will play an important role in how organizations respond to these trends and should prepare now for this future state. We encourage Boards to adopt the following three principles for

(The Board's Role in Cyber Risk Oversight, cont'd.)

effective cyber risk oversight: 1) **get educated**; 2) **be engaged**; and 3) **stay informed**.

First, Boards should **get educated** about key topics to ensure that cyber and broader technology risk is embedded in operational risk and strategic discussions and organizational decisions. This includes understanding the impact cyber has on risk management and resiliency frameworks. It also includes the Board of directors playing an integral role in overseeing any organization's cloud-enabled digital transformation.

Putting this in action

- Assess Board structure and expertise; consider your committees and see which one is most appropriate to oversee this risk.
- Organize briefings and in-depth discussions with internal and external experts (e.g., Google Cloud, law enforcement).

Second, Boards should **be engaged** with the CISO, other C-Suite leaders and key business stakeholders to build better relationships, and understand critical gaps and resource needs while ensuring this risk is treated as a priority for all executives – not just the cybersecurity team.

Boards must work with the CISO, along with technology, business, and compliance stakeholders to identify top risks and quantify them, and assess how they align with overall risk appetite.

Putting this in action

- Make cyber a key business priority by having line of business leaders present on this risk as part of their strategic business risks supported by the CISO.
- Invite the CISO to strategy discussions on broader business and technology decisions.
- Schedule regular deep dives with the CISO, CIO, CTO on risk priorities, budgets, and long-term planning.

Third, Boards should **stay informed** about ongoing reporting activities, ask questions, and work with the CISO and other leaders to understand cyber risk metrics. Boards should strive to create a robust feedback loop that encourages frank dialogue, informed decision making, and continuous risk management, in line with good practices for operational risk management. Boards should also stay engaged with relevant external organizations (like Google) to stay informed of the latest cybersecurity trends and practices. .

Putting this in action

- Understand the top risks to your organization and how the business in partnership with the CISO plans to address them.
- Require a periodic report on the CISO's efforts to evaluate risk, and track and measure progress.
- Stay engaged with peers and Google through our Cybersecurity Board Campaign.

Boards can use these three principles to conduct better oversight and help build a better relationship with the CISO and company leadership. As the threat landscape continues to evolve, however, Boards will need to further adapt their approach. We explore some of these trends in the next section.

Helping Boards Navigate the Global Threat Landscape

In 2022, Mandiant, now part of Google Cloud, helped over 1,800 customers prepare for or recover from the most critical cybersecurity incidents. Through this ongoing, frontline engagement, our experts saw **more of everything**: more zero-day vulnerabilities, more threat actor groups, more supply chain compromises, and more extortion tactics designed to hurt company reputations. We also observed unprecedented developments like the first time cyber operations played a prominent role in war. The threat landscape remains dynamic and complex, and we expect these trends to continue in 2023 and beyond.

At the same time, we've seen several positive cybersecurity trends emerge. First, cybersecurity leaders believe that cloud modernization presents better security improvement opportunities than with on-prem, including a step change in detection and response capabilities. Second, frontline defenders are getting better at shortening the cybersecurity gap (i.e. the time it takes to discover a compromise and push out protections to organizations). When we shorten that timeframe as a community, we raise the cybersecurity bar for everyone.

As Boards consider these trends, they must understand the connection between threat intelligence and risk mitigation. In most cases, cybersecurity leaders understand the need for better intelligence on threat actors, but many of them make decisions without fully understanding who is attacking their organization and why. In a recent survey of business and IT leaders, more than three-quarters of respondents said that they make decisions without insights on who could be targeting their organization and only about one-third had a comprehensive understanding of different threat groups and their tactics, techniques, and procedures. These visibility gaps mean defenses may not meet their intended goals.

Boards can work to bridge these intelligence gaps and ensure this information is playing a leading role in risk management decisions. To help encourage this connection and consistent with the three principles for effective oversight described above, Boards should **ask the CISO three key questions on a quarterly basis**:

- **How good are we at cybersecurity?** Boards should learn more about the people and expertise on the cybersecurity team, and their experiences. This is important because Boards can't rely solely on compliance dashboards and cybersecurity controls to answer this question. Almost every victim we respond to appears to have various dashboards and controls–but Boards need to work to understand more about their team's practical capacity to respond to events. One way to test your cybersecurity team's capabilities is to ask the CISO to conduct Red Team exercises and request a copy of the report.

(Helping Boards Navigate the Global Threat Landscape, cont'd.)

- **How resilient are we?** Boards should ask the CISO about how prepared your organization is to keep the business running through an event like a ransomware attack. This is similar to planning for an earthquake or other disaster, and can involve scenarios like operating off the Internet, restoring data back ups, etc. One way to assess resilience preparedness is to ask the CISO to conduct periodic cyber resilience exercises like a ransomware attack to test organizational response.
- **What is our risk?** At a minimum, Boards should ensure that the CISO's risk management framework addresses five key areas: 1) an assessment of current threats to your organization; 2) an explanation of what the cybersecurity leadership is doing to mitigate against those threats; 3) examples of how the CISO is testing whether mitigations are working; 4) an assessment of the consequences if those threats actually happen; and 5) an assessment of risks that you aren't going to mitigate, but will otherwise accept. One way to get to the bottom of this is to ask the CISO to present on this topic to the full Board roughly twice a year.

In today's threat environment, cybersecurity teams are under tremendous pressure to protect their organizations from a variety of threats. For Boards, this means asking the right questions to ensure that relevant intelligence gets to the right stakeholders to drive optimal cybersecurity and business decisions. Boards can also work with the CISO to bring external cybersecurity partners like Google to the table to help translate frontline intelligence into actionable information.

Board Engagement on Artificial Intelligence and Cybersecurity

Organizations everywhere are seeking to leverage the power of AI – and rightly so. The smart applications of AI enable organizations to improve, scale, and accelerate the decision-making process across most business functions. We're committed to helping developers and organizations stay on top of these developments – that's why we recently announced new generative AI capabilities for our Google Cloud AI portfolio and committed to launching a range of products that responsibly infuse generative AI into our offerings.

As Boards consider how to best support their organizations on this journey, we encourage them to take a bold and responsible approach to these technologies. We were one of the first to introduce and advance responsible AI practices, and these principles serve as an ongoing commitment to our customers worldwide who rely on our products to build and grow their businesses safely. To maximize the benefits of AI technologies and minimize risks, we recommend that Boards work with the CISO to take a three-pronged approach to **secure, scale, and evolve**.

First, Boards should understand how their organization plans to **deploy secure AI systems**. This includes a basic familiarity with how the CISO intends to protect data and control access to machine learning models and AI applications.

Putting this in action

- Partner with the CISO to schedule a full Board review of the CISO's plans to securely deploy AI systems, and determine whether additional investment is needed.
- Understand your organization's data responsibilities and whether cybersecurity leaders have the right tools to protect machine learning data.

Second, Boards should work with the CISO to understand how best to **leverage the power of AI to achieve better cybersecurity outcomes at scale**. While AI technologies don't offer a one-stop solution for all cybersecurity problems, we've seen a few early use cases emerge for how AI is helping to level the cybersecurity playing field, including detecting anomalous and malicious behavior, automating cybersecurity recommendations, and scaling the productivity of cybersecurity specialists.

Putting this in action

- Request an annual briefing on your organization's top cybersecurity pain points and how AI technologies can solve them, which will help the Board weigh potential investments.
- Understand your organization's long term cybersecurity investment plan in AI technologies and how it intersects with business priorities and strategic decisions.

(Board Engagement on Artificial Intelligence and Cybersecurity, cont'd.)

Third, the Board should work with the CISO to **stay informed on developments in this space to anticipate threats.** We operate from the basic assumption that attackers will seek out these technologies and attempt to use them to circumvent defenses, and we're building towards that future state.

Putting this in action

- Organize regular briefings from internal and external experts to spot emerging AI trends and novel security risks.
- Assess the CISO's plans to partner with others to develop best practices, tools, and threat models that address typical AI interactions and risks.

Together, our approach reinforces a **continuous cycle where frontline intelligence meets AI-powered cloud innovation**. We'll continue to explore these topics in future Board Horizons reports.

Conclusion

Cybersecurity can be a challenging topic for Boards to oversee. To help address this challenge, Boards should adopt three principles for effective cyber risk oversight: 1) get educated; 2) be engaged; and 3) stay informed. This approach–coupled with a strong relationship with the CISO and technology, business, and compliance stakeholders–will help foster greater transparency and collaboration between Boards and company leaders. Moving forward, it is clear that Board awareness and subsequent guidance in this area is critical to every organization's long term success. At Google Cloud, we look forward to working with you towards that goal. Please click here for more information.

Check out our Board of Directors Insights Hub for more actionable cybersecurity resources.

Looking Back

Threats to Organizations in January 2023

- Suspected Chinese and Russian espionage
- Data theft, and gaining access to organizations
- Distribution of malware via infected USB devices
- Reconnaissance, and attempted compromises of major cloud service providers

Threats to Organizations in December 2022

- Chinese, Iranian, North Korean and Russian espionage
- Data theft, extortion, and gaining access to organizations
- Exploiting recently disclosed vulnerabilities

Threats to Organizations in February 2023

- Suspected Russian and North Korean espionage
- Ransomware and data theft extortion, phishing and spear phishing
- Government, research and education, operational technology targeting

Looking Forward

Prioritize efforts to understand AI opportunities and risks. We see organizations are exploring how to leverage it to achieve better cybersecurity outcomes at scale.

Ask your CISO:

- What is our AI investment plan, and what are our plans to deploy AI securely?
- How are we preparing to manage data responsibilities with AI systems and what steps do we need to take to address them?
- What role will AI play in enhancing our cybersecurity capabilities?

Work with the CISO to better understand attackers and what they are after. Ransomware is a financially motivated extortion attack we don't see slowing down anytime soon. All organizations are at risk and need to be ready.

Ask your CISO:

- What data and assets are most important to our organization, and are they secure?
- Do we have a backup strategy if an attacker were to steal and prevent access to our data?
- Have we performed ransomware defense assessments to test our ability to detect and respond to financial threats?

Learn from the past to prepare for the future. We see continued interest in targeting organizations across sectors worldwide. Boards must ensure their organization is prepared.

Ask your CISO:

- What assurance do we have that our organization is prioritizing the right security capabilities against the most relevant threats?
- How are we using current threat intelligence to inform decisions?
- How are we testing our defenses? Do we conduct red team and tabletop exercises?

Ensure you have a plan to protect users from common attacks. Phishing is one of the most common ways that attackers breach organizations. They will also use techniques to bypass multi-factor authentication and abuse identity systems.

Ask your CISO:

- What can our security, IT and business teams be doing to protect all employees?
- How are we minimizing the risk of social engineering threats from reaching our employees?
- How do we make our employees aware of phishing and other social engineering?
- What is our strategy around adoption of phishing resistant hardware/tokens?

Google Cloud