Cybersecurity
Action Team

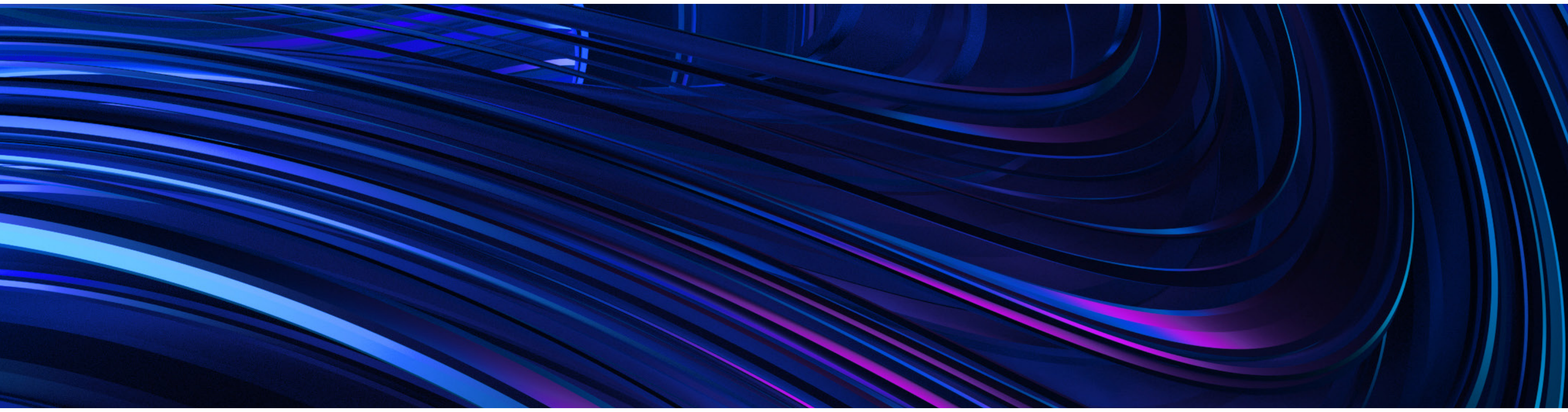
Perspectives on Security for the Board

July 2023 – Edition 2

Google Cloud

July 2023
For more information, visit gcat.google.com

Table of contents



Foreword

With the proposed SEC requirements putting increased emphasis on U.S. organizations to address their cybersecurity risks, the demand for cybersecurity experts in boardrooms is increasing in parallel. But who is the right person to assign for the job? You might think it's a technical expert with all the certifications in the world, but someone who fits that description is not necessarily the best choice.

In general, Boards will benefit most from having someone who has an overarching goal of raising the Board's security IQ. A Board security expert shouldn't be out to ask "stump the chump" questions to the CISO. Instead, they should be guiding a productive conversation and asking the right questions. Do we have the right protections in place? Can we defend against the threats that matter most to us? Are we meeting our compliance requirements? The list goes on, and it's more than what can be covered in a single meeting.

A cybersecurity expert's role may also extend beyond interacting with the Board. Karenann recently attended a cybersecurity subcommittee meeting chaired by the cybersecurity leader on the Board of an organization. The meeting, which took place ahead of the full Board meeting and involved external expertise, produced key security insights and led to greater discourse at the Board level. This is an idea that cybersecurity Board experts should be advocating for.

The idea of raising a Board's security IQ and asking the right questions informed the topics we chose to cover in this edition of our Board report. We (1) cover the Board's role and responsibilities in cloud adoption, with a focus on the security aspects; (2) provide an overview of Q2 2023 threat trends, explaining how businesses are being impacted and what you can do to be protected; (3) provide an update on artificial intelligence, and a look at how our Secure AI Framework (SAIF) is helping address security and risk concerns.

We hope you find this report informative, and we look forward to connecting with you more on these important topics.

Karenann Terrell (Technology Advisor & Google Cloud Advisory Board)
Phil Venables (CISO, Google Cloud)

The Board's Role in Cloud Adoption

We are often asked if the cloud is more secure than on-premise infrastructure. The short answer is that, in general, it can be. The complete answer is more nuanced and is grounded in a series of cloud security "megatrends" that drive technological innovation and improve the overall security posture of cloud providers and customers. An on-premises environment can have the same default level of security as a reputable cloud provider's infrastructure. Conversely, a weak cloud configuration can give rise to many security issues. But in general, the base security of the cloud coupled with a suitably protected customer configuration is stronger than most on-prem environments.

As we noted in the last issue, we encourage Boards to adopt the following three principles for effective oversight of cloud adoption: 1) **get educated**; 2) **be engaged**; and 3) **stay informed**.

Get Educated

Migrating to the cloud can be complex, but for many organizations, it's an organic step in their digital transformation journey. A prudent migration is based on strategic alignment and thoughtful planning. An organization's adoption of cloud is not simply a new series of risks to manage - rather, the adoption of cloud is, in many cases, an increasing imperative for organizations to remain competitive and to fully realize technology, data and overarching business strategies. Beyond that, the adoption of cloud is a significant opportunity for organizations to reimagine how whole classes of enterprise risk can be better managed, presenting opportunities to tackle risks that previously would have been commercially unrealistic to fully address.

Putting this in action

- Effective organizational transformation requires more than "lifting and shifting" existing applications to the cloud, but rather a senior-leadership supported holistic approach that positions the organization for scalable innovation, operational efficiencies, and data-driven insights to inform decision making.
- Adopt cloud technologies and adjust business practices, processes and operating models to fully realize the advantages of cloud, providing your organization with an opportunity to step change the management of operational risk.

Be Engaged

A key element to success is creating a collaborative, cross-functional culture. The Board plays a key role in overseeing and supporting the cloud journey, and should consider certain key questions regarding the overall governance, operating model, impact to the organization's risk profile and appetite, and regulatory compliance posture. It's also important to set a tone from the top that breaks down silos and encourages partnership amongst the business, technology, and control oversight and assurance functions – for instance, making clear the expectation that business product owners collaborate with cybersecurity, compliance and risk, and internal audit functions for a comprehensive view of applicable risks and mitigants.

(The Board's Role in Cloud Adoption, cont'd.)

The rapid technological change of pace and dynamic regulatory environment hinge commercial success on modernization through innovation. Consider how to cultivate such a culture through educational initiatives, as leveraging a secure and compliant cloud infrastructure is only part of the critical requirements for success - the other aspect is ensuring a secure implementation in the cloud. This aspect of security in the cloud includes managing identity and access rights, the configurations for each service, implementing data security controls, and securely deploying applications to the cloud, among other operational requirements.

A comprehensive and sustained learning plan to develop deeper expertise in cloud technologies, and specifically focused on security and other significant aspects of risk mitigation, may be particularly beneficial. For instance, level-setting / upskilling on cybersecurity through targeted persona-based training programs such as Google's Cybersecurity Certificate may form an integral part of your training curricula. Training provides learning opportunities and enables personnel from various groups to "speak the same language," encouraging cross-functional exchanges and enabling opportunities for continuous learning through sharing of best practices and opinionated recommendations and architectural frameworks to support secure cloud implementation.

Putting this in action

- Consider how technology is leveraged to achieve strategic outcomes, and can be used to modernize how software is designed, delivered, and managed across the organization to enable the desired outcomes.
- Refactor security, controls and risk governance processes to ensure that the organization stays within risk appetite and in compliance with regulations throughout your digital transformation.
- Implement new organizational and operating models, to enable a broad and deep skills and capabilities uplift, and foster the right culture for collaboration and success.

Stay Informed

Boards should stay informed of their organization's digital transformation and provide a robust feedback loop that encourages frank dialogue, informed decision making, and continuous risk management.

Putting this in action

- Consider posing the following questions to your management team:
  - » How is the use of cloud technology being governed within the organization? Is clear accountability assigned and is there clarity of responsibility in decision making structures?
  - » How well does the use of cloud technology align with and support the technology and data strategy for the organization, and the overarching business strategy, such that the cloud approach can be tailored to achieve the intended outcomes?
  - » How is the organization's structure and operating model evolving to both fully leverage cloud and increase the likelihood of a secure and compliant adoption?

Navigating the Global Threat Landscape — Zero(-day) to Sixty

It goes by many names. A breach. An attack. A compromise. Call it what you will, but when it happens to your organization, you need to be ready to respond. For Boards, part of being ready means having an understanding of the latest cybersecurity threats, and how your organization (and others) stand to be impacted.

In a crisis, time means everything, especially in those early moments. The less time spent catching up leaders on what exactly is happening, the more focus can be placed on the highest priority actions that Boards and other key teams need to be taking.

Board members and executives who do not understand the cyber threat landscape are not well-equipped to lead their organization to recovery from attacks that could result in significant financial, reputational, and other damages.

Zero-day abuse in Q2 2023

The second quarter of 2023 featured heavy use of high-impact zero-day vulnerabilities. We consider a zero-day to be a vulnerability that was exploited in the wild before a patch was made publicly available, and the attacks involving zero-days in Q2 2023 have resulted in data theft and myriad other problems for organizations worldwide.

Here's a rundown of some of the zero-day activity Mandiant researchers, analysts and consultants responded to, investigated, and reported on in recent months:

- **What happened?** A zero-day vulnerability in the Barracuda Email Security Gateway (ESG) had been exploited in-the-wild as early as October 2022. Mandiant identified a suspected China-nexus actor, UNC4841, targeting a subset of Barracuda ESG appliances for espionage purposes, impacting organizations across multiple regions and sectors.
  - **For your CISO**: The Barracuda guidance. Mandiant's Barracuda research. Mandiant's Barracuda hardening recommendations.
- **What happened?** A Chinese espionage group, UNC3886, was observed exploiting a zero-day vulnerability in VMware solutions. The group targets these technologies because they traditionally do not support endpoint, detection and response solutions, and therefore the attackers could better evade detection. UNC3886 targets include defense, technology, and telecommunication organizations located in the U.S. and JAPAC regions.
  - **For your CISO**: The VMware advisory. Mandiant's VMware research. Mandiant's VMware detection, containment, and hardening guidance.
- **What happened?** A zero-day vulnerability in the MOVEit Transfer secure managed file transfer software was widely exploited for data theft. Mandiant attributes the activity to cybercrime group FIN11, which later threatened to release the stolen data if victims did not pay an extortion demand.

(Navigating the Global Threat Landscape — Zero(-day) to Sixty, cont'd.)

The operation impacted organizations worldwide, including in Canada, U.S. and India, and in a wide range of industries.

» **For your CISO**: The official guidance from Progress. Mandiant's MOVEit research. Mandiant's MOVEit containment and hardening guide.

Putting this in action

Understanding threats and responding to them is an important component of security. While the guidance we provided can be shared with CISOs and security teams to ensure your organizations are protected against these specific zero-day threats, the role of the Board in security is not simply about doling out recommendations on specific issues and asking: "Is this addressed?"

Boards are in a prime position to help lead their organizations through a growing number of broader security challenges. Understanding the threat landscape not only helps Boards lead their organizations through breaches, it also helps inform other key security conversations and decision making. Ask your CISO and other security leaders:

- What are our vulnerability and exposure management strategies to reduce the risk posed by these types of threats?
- How are we tracking security issues with the technologies we use, and how quickly do we apply security updates, patches and guidance for known threats?
- Are we practicing sound security fundamentals such as least privilege and hardening to reduce attack surface, and thus, potential impact of zero-day attacks?
- Are we using threat intelligence to identify the threats that matter most to us, and have we taken measures to protect against, detect, and respond to those threats?
- Are we being proactive about security? Are we hunting for activity typically associated with vulnerability abuse?
- How is our defense in depth holding up, and are specific control layers in that defense in depth under more pressure than others? If so, why is that?
- Are our new technologies (such as artificial intelligence) or cloud architectures helping us be more inherently defended against zero-day and other similar threats?
- Are teams monitoring networks at the operating system layer, while also continuing to patch, maintain, and monitor the appliances that are running the underlying infrastructure?

Boards should be viewing security as a complex, integrated organizational function requiring a mix of personnel and technologies to be successful — not unlike traditional functions such as sales, engineering or marketing. These days, poor security practices can be the downfall of what could be an otherwise successful business, especially with the increasing amount of pressure on organizations to meet compliance and other requirements.

Cybersecurity is challenging for even the most security mature organizations, and sometimes it helps to have the right partner. Boards can work with their CISOs to bring external cybersecurity partners such as Google to the table to help reduce the threat posed by zero-day vulnerabilities, and translate frontline intelligence into actionable information.

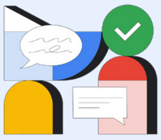
Taking the Next Step on Securing AI Systems with Google's Secure AI Framework

In the last report, we explored how Boards can support their organizations on their AI journey, including taking a bold and responsible approach to these technologies. To advance this effort, we recommended that Boards work with the CISO to take a three-pronged approach to secure, scale, and evolve.

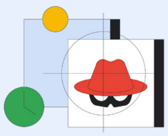
In this report, we're diving deeper into the first prong and introducing the Secure AI Framework (SAIF), a conceptual framework for secure AI systems that Boards can use to help ensure their organizations utilize AI in a responsible way. SAIF offers a practical approach to address top of mind concerns for every organization including security, AI/ML model risk management, and privacy and compliance. We recommend Boards work with the CISO to implement SAIF's six core elements in their organizations.

Google's Secure AI Framework

AI is advancing rapidly, and it's important that **effective risk management strategies** evolve along with it.



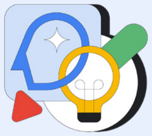
Expand strong security foundations to the AI ecosystem



Extend detection and response to bring AI into an organization's threat universe

Automate defenses to keep pace with existing and new threats

Harmonize platform level controls to ensure consistent security across the organization



Adapt controls to adjust mitigations and create faster feedback loops for AI deployment

Contextualize AI system risks in surrounding business processes

(Taking the Next Step on Securing AI Systems with Google's Secure AI Framework, cont'd.)

First, Boards should understand how their organization plans to **expand strong security foundations to the AI ecosystem**. This includes a basic familiarity with how the CISO intends to leverage secure-by-default infrastructure protections and expertise to protect AI systems, applications and users.

Putting this in action

- Partner with the CISO to conduct a review of existing security controls across your organization's security domains and whether they apply to AI systems, and determine whether additional investment is needed.

Second, Boards should work with the CISO to understand how best to **extend detection and response to bring AI into an organization's threat universe**. Timeliness is critical in detecting and responding to AI-related cyber incidents, and extending threat intelligence and other capabilities to an organization improves both.

Putting this in action

- Partner with the CISO to understand how your organization plans to monitor inputs and outputs of generative AI systems to detect anomalies and use threat intelligence to anticipate attacks.
- Request an annual briefing on the threats relevant to your organization's specific AI usage scenarios.

Third, Boards should understand how their organization plans to **automate defenses to keep pace with existing and new threats**. The latest AI innovations can improve the scale and speed of response efforts to security incidents. Adversaries will likely use AI to scale their impact, so it is important to use AI and its current and emerging capabilities to stay nimble and cost effective in protecting against them.

Putting this in action

- Partner with the CISO to identify your organization's priorities for automated AI security capabilities to help secure AI systems and training data pipelines, and determine whether additional investment is needed.
- Understand your organization's top security challenges and whether cybersecurity leaders have the right AI-powered tools to address threat overload, toilsome tools, and the talent gap.

Fourth, Boards should work with the CISO to **harmonize platform level controls to ensure consistent security across the organization**. Consistency across control frameworks can support AI risk mitigation and scale protections across different platforms and tools to ensure that the best protections are available to all AI applications in a scalable and cost efficient manner.

Putting this in action

- Request an annual briefing on how your organization plans to prevent fragmentation of controls and standardize tooling and frameworks to mitigate risk to AI systems.
- Partner with the CISO to implement a process for periodic review of AI usage to identify and mitigate security risks.

Fifth, Boards should understand how the CISO plans to adapt controls to adjust mitigations and create faster feedback loops for AI deployment. Constant testing of implementations through continuous learning can ensure detection and protection capabilities address the changing threat environment.

(Taking the Next Step on Securing AI Systems with Google's Secure AI Framework, cont'd.)

Putting this in action

- Request an annual briefing on your organization's efforts to conduct regular red team exercises to improve safety assurance for AI-powered products and capabilities.
- Partner with the CISO to create a feedback loop that ingests key learnings and quickly incorporates them into your system's protections.

Sixth, Boards should understand how their **organizations contextualize AI system risks in surrounding business processes**. This includes an assessment of the end-to-end business risk, such as data lineage, validation and operational behavior monitoring for certain types of applications.

Putting this in action

- Request an annual briefing on your organization's end-to-end risk assessment related to how your organization will deploy AI to help inform business decisions.
- Partner with the CISO to establish a model risk management framework and build a team that understands AI-related risks.
- Partner with the CISO to build an inventory of AI models and their risk profile based on the specific use cases and shared responsibility when leveraging third-party solutions and services.

Boards should consider SAIF as a useful tool for getting **educated**, being **engaged**, and **staying informed** on AI and cybersecurity issues. We'll continue to explore these topics in more detail in future reports. For more on SAIF implementation, see here and here.

Conclusion

There is no shortage of security considerations for Boards of Directors. Cloud adoption and new technologies offer many opportunities, but evolving threat trends show how attackers are flexible, so Boards need to understand the risks and be ready to respond. We hope this report helps Boards of Directors by providing them with information and insights they need to make informed decisions about cloud, artificial intelligence, and overall security posture. To help address this challenge, Boards should continue to leverage the three principles for effective 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.

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.

Google Cloud