Office of the CISO

Perspectives on Security for the Board

March 2024 – Edition 4

Google Cloud

March 2024

For more information, visit our Board of Directors Insights Hub

Table of contents

Foreword

One year ago, Google Cloud embarked on a mission to empower boards of directors to take a more active role in overseeing their organization's cyber risk. Since then, the threat landscape has only grown more complex and unpredictable. Artificial intelligence (AI), while a powerful tool, is now being used by adversaries, amplifying the dangers of disinformation and advanced malware. That said, AI also represents an inflection point for digital security, one where we can tilt the cybersecurity balance from attackers to defenders.

Effective risk governance requires identification and mitigation of cyber risk, and while cyber insurance does not eliminate the need for proactive and resilient cyber controls, it offers a safety net for potential financial loss. The financial and legal ramifications of cyber attacks demand meticulous insurance strategies, yet crafting them requires a deep understanding of the evolving risks. While boards typically have defined processes to oversee an organization's general insurance strategy, many questions are emerging specific to cyber risk, forcing boards to reevaluate their governance approaches due to the unique complexities and rapidly evolving nature of cyber threats.

Over the last year, we also had interactive discussions with CISOs around the relentless pressure on them to deliver, revealing a landscape where expectations are sky-high, resources are limited, and the threat of cyber attacks looms large. Leadership's vision and mission can only be realized when employees are empowered with the necessary resources to do their jobs effectively. In this edition, we share actionable advice on how boards can support and strengthen the psychological well-being of their CISO team.

Psychological resilience is a rarely discussed yet critical component of effective cybersecurity leadership. An individual CISO feeling like it is all on them to manage, lead, and protect the safety of an organization's most valuable assets is taking on a burden that is not wholly theirs to carry (even if their personality and psychological make-up mean they welcome carrying it). Supporting the physical, emotional and psychological well-being of the CISO team needs to be a joined-up whole system approach, similar to other significant executive roles.

This report brings these interconnected themes into sharp focus and builds upon the foundation of our previous editions, offering actionable insights into:

- Understanding how AI is transforming approaches to cybersecurity;
- Recognizing sound governance and risk management practices, including the nuances of cyber insurance; and
- Supporting and strengthening the psychological well-being of cybersecurity teams.

By proactively addressing these challenges, organizations can not only survive, but also gain a competitive edge by creating a culture where the people supporting their mission thrive in this digital age.

Phil Venables, CISO, Google Cloud

Tameron Chappell, Chartered Occupational Psychologist, aThinka Limited, Contributor to Google Cloud's CISO Community

Attackers Are Interested in AI, and So Are Defenders

Since 2019 attackers have been using AI to conduct phishing and social engineering, and in disinformation campaigns. Recently released powerful generative AI tools—applications that generate fabricated text, images, videos, and other content—are likely to amplify these threat actor trends, enabling actors with limited resources to increase the scale and efficiency of their operations significantly, while also crafting even more convincing content. Additionally, these tools will help skilled malware authors, and empower less technical malware developers.

For business leaders, the bottom line is that these threats can potentially result in brand reputation damages, data compromise, and financial losses.

How disinformation actors will leverage gen AI

- Images and videos: The most immediate threat for the spread of disinformation due to the availability of sophisticated and accessible image/video generation tools.
- Text: Using powerful language models to generate articles, narratives, and social media posts to mislead target audiences.
- Audio: Fake recordings, impersonations, and potentially inflammatory public service announcements could be very effective.

Areas where gen AI improves social engineering

- Scaling operations: Gen AI helps actors produce larger amounts of high-quality disinformation content far beyond their normal capacity.
- Fabricating realistic content: These tools create very convincing fakes—articles, political images, audio recordings of public figures—heightening the persuasive power of an operation.
- Removing language barriers: Chatbots built using large language models could help threat actors more easily tailor disinformation in multiple languages.

Using LLMs to develop malware

- Writing code: Large language models (LLMs)—powerful applications that can create and understand text—will help with both creating new malware code and improving existing malware.
- Barrier to entry: LLMs will assist skilled malware developers significantly, and empower attackers who aren't as technically proficient.

Despite growing threat actor interest in gen AI, current adoption is limited. The most immediate threat is distinguishing real content from AI-generated fakes, which can be used in both social engineering and information operations.

(Attackers Are Interested in AI, and So Are Defenders, cont'd.)

Reversing the Defender's Dilemma With AI

A common saying in the security world is that attackers only have to be right once, while defenders have to be right every time. This is the Defender's Dilemma; a struggle that the security industry hasn't been able to properly address—until now. We are currently in a period of great technological innovation, and fully believe recent AI advancements will help tilt the scale into the defender's favor.

How exactly? Today, cyber defenders are learning new ways to use gen AI and related technologies to strengthen detection, response, and attribution of adversaries at scale, and to speed up analysis and other time-consuming tasks such as reverse engineering.

On the technology front, security solutions supercharged with AI will help organizations more quickly identify the threats that matter most, reduce toil and manual work, and simplify security for experts and non-experts alike. Where people are required, AI will also play a big role. Because time is of the essence when responding to attacks, Mandiant consultants have found innovative ways to use AI in their incident response engagements, including to write rules used for hunting threats, and to help analyze malware.

We've covered the crossroads of security and AI in previous Perspectives on Security for the Board reports, including AI and red teaming, and securing AI systems through Secure AI Framework (SAIF).

Putting this in action

Discuss the following with your CIO/CTO and CISO

- **Threat intelligence and risk assessment**: Understand potential threats to your organization to proactively identify and mitigate risks. This includes having a comprehensive vulnerability management strategy.
- **Proactive security measures**: Implement security solutions that prevent security incidents, and strengthen security posture. Employ a multi-layered approach that includes endpoint protection and network security; requires regular security training for all employees, including social engineering awareness; and follows best practices for access control and privilege management.
- **Testing and simulation**: Evaluate the effectiveness of security controls, processes, and personnel through controlled simulations and exercises. This includes conducting regular red team exercises to test security operations.
- **Incident response and recovery**: Predefine steps and procedures to quickly respond to security incidents and recover from them, ultimately helping to minimize damage. Develop and test incident response and disaster recovery plans. your organization stay ahead of and respond to them. Boards can help ensure their organizations are prepared for and protected against attacks that begin with phishing, smishing, infected USB drives, and zero-day vulnerabilities by sharing the research and guidance we provided with their CISOs and security teams. Boards can — and should — also participate in broader security conversations on these topics.

We're Insured, Right? Optimizing Your Protection Through Collaboration

Boards play a crucial role in overseeing their company's insurance strategy. Through effectively collaborating with management (often via the CFO), the business and relevant risk professionals, the board defines an organization's overall risk tolerance. While boards typically have a defined process to oversee an organization's general insurance strategy, many questions are emerging specific to cyber risk. For comprehensive cyber risk management, the board should facilitate cooperation between the CISO (focused on technical aspects) and Finance (focused on financial impacts).

Take action by asking the right questions:

Have we defined our risk appetite?

Cyber risk cannot be solely managed with technology. Boards of directors play a crucial role in defining their company's risk appetite—the level of risk they're willing to accept to achieve strategic goals. This decision must consider the current macro environment, the company's growth stage, resources, skills, and available technologies. Risk appetite should be deeply woven into the overall risk management strategy.

To effectively define risk appetite, leadership must thoroughly understand the risks they face. This includes reviewing past incidents, potential threats, and relevant industry trends. Risk quantification, which models potential losses, can be a valuable tool in this process.

Do we have the right checks and balances?

For effective cybersecurity, boards should foster checks and balances within the organization. The CISO's technical expertise is invaluable, but true power comes from translating risks into their potential financial impact on the business. By collaborating with Finance, and utilizing public breach data alongside the company's own incident history, companies can develop a robust cyber risk model.

This alignment between the CISO, finance team, and the broader business creates a holistic overview for the board. A structured cyber risk model leads to better insights and preparedness for potential cyber attacks. While insurance strategies often drive the initial push to model cyber risk in financial terms, a well-aligned model has far wider applications. It can guide a whole range of cyber risk decisions, extending its impact well beyond insurance alone.

Are we optimizing our insurance program?

Armed with an improved understanding of cyber risk, boards can employ a systematic approach to compare the risk transferred through insurance versus the risk the company retains. Tracking the retained risk against consistent company metrics such as revenue, operating income or market cap—over time—ensures a methodical and optimized insurance strategy that scales alongside the business's growth.

(We're Insured, Right? Optimizing Your Protection Through Collaboration, cont'd.)

Have we clarified exclusions and coverage?

Boards must thoroughly understand their cyber insurance policy to avoid surprises during a cyber event. They should pay close attention to exclusions that limit coverage for widespread events such as cyber war or concentration risk caused by third parties. Coverage for emerging risks, such as AI, is also changing rapidly as information on the technology emerges and case law matures. Although AI isn't typically excluded from cyber policies, generative AI exclusions are starting to pop up. While you might not be able to alter these, stay vigilant in reviewing changes to your policy each year and ensure you're aware of specific exclusions, coverage limits, and all reporting requirements. Proactively inquire about coverage for scenarios such as ransomware, data breaches, business interruption and war.

Are we considering secondary considerations beyond cyber risk?

Cyber insurance isn't the only coverage facing significant changes. The risk of securities claims following a cyber attack is increasing, with claims alleging that directors and officers were negligent in their decision-making. This trend, stemming from high-profile cases targeting CISOs, adds pressure to the role. Boards must carefully review their Directors and Officers (D&O) coverage, strategically deciding which security leaders to explicitly name on the policy. assessments. The team should also implement a governance and management model, with specific working groups aligned to functional responsibilities.

Putting this in action

- **Ask the right questions:** The cyber insurance landscape is complex and constantly evolving, and boards need to ask the right questions. Fine print, exclusions, and coverage limits can significantly impact how a policy responds during a crisis. Leverage the questions from this section when discussing cyber insurance with your CISO, CFO, and the business.
- **Incorporate cyber insurance into cyber risk management:** Much of the analysis and approach required to develop a robust cyber insurance strategy overlaps with the broader approach to managing cyber risk. To effectively put this into action, the first step organizations should take is to ensure that the two processes are integrated, rather than operating in parallel.

Lifting the Invisible Weight: Psychological Resilience in Cybersecurity Leadership

CISOs are facing increasing levels of legal accountability for their organization's cybersecurity posture. This stems from a growing number of high-profile data breaches, stricter regulatory requirements, and a greater public awareness of the consequences of cyber attacks. As a result, CISOs can be held personally liable for negligence or failure to implement adequate security measures. This includes potential fines, civil lawsuits, and even criminal charges in cases of severe breaches or misconduct.

The cybersecurity landscape is constantly changing. New threats emerge regularly, requiring that CISOs remain in a state of constant vigilance if they want to stay ahead of attackers. The fear of failure, knowing that even the strongest defenses can be breached, adds immense psychological pressure. Budgetary and talent challenges add to the pressure, and may impact a CISO's ability to implement effective security protocols. CISOs must also navigate the complexities of communicating vital security risks to business focused senior executives. **The job truly never feels "off-duty."**

This combination of factors puts CISOs in a demanding position that takes a psychological toll. Constant pressure can manifest in chronic stress and anxiety, which can result in physical health symptoms like headaches, insomnia, and more. Overwork and an inability to find work-life balance lead to burnout. The burden of carrying the ultimate responsibility for cybersecurity can make CISOs feel isolated and unsupported. However, individuals do not exist in a vacuum—they are part of a team, part of a department, part of an organization, part of a society; and all of these systems interact to create healthy or unhealthy patterns.

Boards should prioritize the psychological resiliency of the CISO and security team as a core component of their overall business strategy. To prevent and combat the psychological strain, Boards need to have realistic expectations aligned with risk tolerance and open communication with their CISO to understand what resources are needed to deliver on those expectations. Investing in building skilled security teams and promoting healthy work-life balance are crucial, as a rested CISO is more likely to make clear-headed decisions. Emphasizing self-care and building peer support networks for CISOs further reduces isolation, and encourages vital sharing of challenges and

(Lifting the Invisible Weight: Psychological Resilience in Cybersecurity Leadership, cont'd.)

expertise.

Putting this in action

- **Reframe the question**: Rather than reviewing reports on metrics or compliance, Boards asking open-ended questions of security teams fosters meaningful dialogue and deeper insights. Instead of asking a question like "Do you have the right security budget?", reframe the question in an open-ended way like, "How can we ensure our security budget aligns with our current risk assessment and business priorities?" This can provide additional points of view, highlight potential areas for improvement, and demonstrate the board's commitment to proactive risk management.
- **Prioritize cybersecurity investment**: Treat cybersecurity as a core business risk rather than an IT cost center. Ensure the CISO has an adequate budget and resources to implement and maintain a robust security program. Invest in every level of leadership (not just the most senior) so that the required behaviors permeate the whole function.
- **Cultivate interpersonal skills, resiliency of people, and team effectiveness**: Ensure the Board supports a company culture that fosters diverse personalities. Different personality types bring unique problem-solving skills. Some might be highly analytical, others more intuitive, and some more naturally risk-averse. This mix fosters out-of-the-box thinking and innovative solutions to security challenges. Intentional management of team dynamics and inclusive leadership practices are key to preventing natural differences from hindering overall effectiveness. 24/7 on-call services are physically and psychologically taxing. Support management in finding the right work-life balance for employees.
- **Collaborative risk management**: Cybersecurity is everyone's responsibility, but our personalities heavily influence our decision-making and risk tolerance. Culture shapes how these behaviors manifest daily. In cybersecurity, setbacks are inevitable; there's no perfect system. Instead of striving for the impossible, focus on raising risk awareness throughout the organization. This fosters a security mindset, not fear. Boards should challenge management to design processes and training that acknowledge human tendencies. Use behavioral design nudges to make secure choices simpler. Approach mistakes with a focus on learning and root-cause analysis, not blame, to improve safety for everyone.
- **Words are powerful**: Think carefully about the words you use when discussing security. Overuse of alarmist terms like "war" and "battlefield" create unnecessary anxiety, and invite reliance on "heroes." This can be counterproductive if the actual threats stem from internal oversights or misunderstandings.

For more reports like this please visit: cloud.google.com/solutions/security/board-of-directors

Google Cloud