Office of the CISO

Perspectives on Security for the Board

November 2024 – Edition 6

Google Cloud

November 2024

For more information, visit our Board of Directors Insights Hub

Table of contents

Foreword

This final 2024 edition of Perspectives on Security for the Board reflects on our recent conversations with board members, highlighting the critical intersection of cybersecurity and business value. Particularly in light of the far-reaching consequences of supply chain disruptions, these discussions underscore that cybersecurity is no longer solely an IT concern. It's a strategic imperative that demands unwavering attention to safeguard our organizations' future.

We'll explore three critical concepts essential for success in the current threat environment:

Strengthening resilience against supply chain attacks

We examine the evolving nature of supply chain risks and emphasize the importance of building resilience to withstand these attacks. This includes proactive measures such as vendor vetting processes, integrating threat intelligence, and making sure business leaders consider cyber risk in their supply chain analysis.

The power of information sharing

We explore how sharing threat intelligence and best practices create a digital immune system that empowers organizations to bolster their collective defenses and improve operational resilience. This collaborative approach recognizes that cybersecurity is no longer just a technical issue, but fundamental to safeguarding an organization's future.

Understanding "value at risk" from a cybersecurity perspective

We consider how cyberattacks, particularly those targeting our supply chain, can significantly impact our bottom line. This includes quantifying potential financial losses, reputational damage, and operational disruptions, and underscoring the need for effective operational resilience.

As board members, we have a responsibility to champion action on making sure cybersecurity is a first class business risk alongside other risks and that our "tone at the top" is joined with "resources in the ranks" to get the job done. This report is a call to action. It's a reminder that our commitment to cybersecurity is essential for navigating the complexities of today's business environment.

Perspectives on Security for the Board will return in 2025 with more insights and guidance to help you navigate the evolving cybersecurity landscape.

Phil Venables, CISO, Google Cloud

Getting Ahead of Supply Chain Threats

Organizations are increasingly embracing diverse digital supply chains. Working with different service providers across your organization can help to reduce costs and improve efficiency. However, expanding supply chains also introduce new and unforeseen risks that demand board-level attention.

Supply chains are a prime target for attackers aiming to compromise your organization, often by inserting malware into trusted software and code during the development process. When an organization then updates their product or inadvertently uses malicious code, they install malware on their systems. This tactic enables adversaries to target multiple victims with a single compromise, as well as gain access to targets that would be difficult to infect directly.

Few supply chain attacks have gained the notoriety of the 2020 SolarWinds incident, attributed to Russia-based espionage group APT29. Since then, the supply chain threat landscape has developed significantly. The growing number of supply chain attacks makes it vital for boards to stay abreast of the emerging supply chain risks to their organization.

Some of the top supply chain threats to consider:

- **North Korea tops the charts:** North Korean actors are one of the most prolific state perpetrators of supply chain compromises globally. North Korea's pursuit of technological advancement and financial stability fuels the volume and sophistication of these attacks. This was showcased by the first-observed double supply chain compromise in 2023.
- **Cybercrime on the rise:** Financially-motivated supply chain compromise almost tripled in 2023. These attacks facilitate a variety of goals, although there has been a particular focus on cryptocurrency platforms and wallets. Cybercriminals also frequently use supply chain attacks to steal sensitive information including credentials and credit card data.
- **Developers are a primary target:** Threat actors are increasingly exploiting developer tools and open-source public repositories like libraries, rather than final software products. This is because open-source software and code packages are widely used, and developers often have privileged access to sensitive systems.
- **File transfer software represents an information treasure trove:** The tools used to send and receive files are an enticing target for bad actors as they typically handle sensitive and confidential information. The MOVEit file transfer software had a hidden flaw. A group of cybercriminals (called FIN11) discovered this flaw and used it to steal sensitive customer data. The incident was the fourth time FIN11 has exploited a file transfer software vulnerability.

In addition to the surge of supply chain compromises last year, we saw widespread technology disruptions that underscore the need for boards and leaders to discuss how they can modernize their technology infrastructure. As part of their enterprise risk management strategy, organizations must use architectures where security is built in, not bolted on, to drive better security, agility, and efficiency.

Board members play a critical role in guiding organizations through this complex risk landscape. This involves fostering a culture of security awareness, ensuring robust resilience strategies are in place, and actively engaging with management to address evolving threats.

Putting this into action

Discuss the following with your CIO/CTO and CISO, as well as the business:

1. **Vet the security of your supply chain:** A comprehensive vendor and supply chain evaluation process should include assessing security practices, in addition to traditional factors such as cost, efficiency gains, and legal reviews. Understanding vendor security policies, verifying compliance attestations from third-party auditors, and examining their privacy program is key to understanding your organization's risk exposure.
2. **Operationalize threat intelligence:** Organizations should develop a more proactive response to threat intelligence briefings and updates. Identifying emerging supply chain threats can help organizations prioritize vulnerabilities and allocate resources effectively.

   For example, given the risks of open source tools, organizations should consider using a software bill of materials. Likewise, reviewing supply chain compromise incidents at other organizations can help executives understand their own risk exposure to supply chain compromise.
3. **Assume compromise:** Supply chain compromise is inherently difficult to detect as it abuses the trust we place in reputable vendors and code repositories. To mitigate potential risks, the board should direct security teams to incorporate redundancy measures in their cybersecurity strategy.

   These measures can help organizations analyze their third-party and supply-chain partners for high-risk impact if compromised. Boards should also ask their CIO and CISO about segmentation strategies for high-risk areas, such as developer environments. Implementing a Zero Trust model, such as Google's BeyondCorp, can also limit the blast radius of supply chain threats.

Don't Let Resilience Get Lost in Translation: The Importance of Cybersecurity Information Sharing

In today's data-driven world, reliable information sharing is crucial not only for technical defenses but also for achieving operational resilience. Board members and business leaders now understand that cybersecurity is no longer simply a technical concern; it's fundamental to an organization's ability to withstand and recover from attacks, safeguarding its operations, reputation, and ultimately, its future.

In the face of increasingly sophisticated and coordinated cyberattacks, including those targeting the software supply chain, we must recognize that security is a collective responsibility. No single organization can stand alone, so open communication channels are essential for sharing threat intelligence, vulnerability alerts, and industry best practices across the entire cybersecurity ecosystem.

This collaborative approach empowers us to proactively address risks, strengthen our collective defenses, and respond rapidly to attacks that can disrupt critical infrastructure, compromise sensitive data, and severely damage brand reputation.

Trusted partnerships

To be truly effective, information sharing must be built on a foundation of trust, requiring collaboration with reliable and vetted partners. Several organizations and initiatives play a crucial role in facilitating information sharing and reliably enhancing cybersecurity.

Information Sharing and Analysis Centers, more commonly known as ISACs, provide a trusted platform for organizations in specific sectors and industries to receive timely threat intelligence, share information confidentially, benefit from collective expertise, and participate in joint exercises and training. While ISACs are member-driven organizations with a focus on private sector collaboration, government agencies play a significant role in the ISACs acting as both a catalyst and a collaborator for information sharing.

Government departments and agencies, such as the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency's Cyber Collaboration Center, and the U.K. National Cyber Security Centre (NCSC) provide valuable resources, guidance, and support for managing cyber risks. Additionally, the FBI and other law enforcement agencies play a vital role in cybersecurity information sharing, acting as both a conduit and a shield in the fight against cybercrime.

It's crucial for boards to actively ensure their CISO and CIO participate in organizations such as the Coalition for Secure AI (CoSAI), the Post-Quantum Cryptography Alliance, and the Open Source Security Foundation, to address specific and evolving technological risks.

The power of information

Information sharing is a vital tool in our collective defense against cyber threats. By sharing threat intelligence (in real-time when possible), best practices, and lessons learned, critical infrastructure owners and operators can create a stronger, more resilient ecosystem.

This collaboration enables security teams, and ultimately the business, to:

- **Stay ahead of the curve:** Gain insights into emerging threats and vulnerabilities, allowing them to proactively strengthen your defenses and mitigate potential risks.
- **Understand attacker tactics:** Get a deeper understanding of attacker tactics, techniques, and procedures, enabling them to better anticipate and respond to potential attacks.
- **Improve incident response:** Learn from the experiences of others and improve their incident response capabilities, minimizing downtime and accelerating recovery in the event of a cyberattack.
- **Strengthen collective defenses:** Contribute to a collective defense against cyber threats, making it more difficult for attackers to succeed and enhancing the resilience of the entire ecosystem.

Putting this into action

While effective communication is crucial for fostering a security-conscious culture, it's equally important for board members to take direct action. By taking concrete steps, boards can ensure that cybersecurity operations are adequately understood, properly funded, and continually optimized, ultimately bolstering the organization's resilience through robust cyber information sharing.

Four ways to take direct action are to:

- **Champion active engagement:** Ask your CISO to prioritize active participation in relevant ISACs and other initiatives (industry consortia, open-source groups, government programs). Emphasize the importance of contributing threat data, using shared resources, and engaging in collaborative defense activities to bolster collective resilience.
- **Follow up on the engagement effort:** Have your CISO report back valuable insights. Ensure these collaborations translate into concrete actions for the business that strengthen the organization's security posture and resilience.
- **Oversee resource allocation:** Work with the CISO to dedicate appropriate budget for threat intelligence platforms, tools, and feeds that align with the organization's specific risks and industry. This investment should enable proactive identification of vulnerabilities and threats to resilience.
- **Foster a culture of shared fate:** Cultivate a culture where employees understand their role in protecting company and customer data. Promote awareness of best practices, encourage reporting of potential incidents, and recognize employees who contribute to a stronger security posture.

Cybersecurity: A Strategic Imperative for Protecting Value and Driving Business Resilience

Cyberattacks and data breaches can lead to significant financial losses. To better understand these risks, we use Value at Risk (VaR) — a concept from the financial industry that helps quantify potential losses and the likelihood of them occurring.

Cyberattacks, whether targeting an organization directly or disrupting our supply chain, can significantly impact an organization's VaR. From ransomware attacks and data breaches to sophisticated supply chain compromises, any successful intrusion can trigger a cascade of negative consequences, including:

- **Financial losses:** Imagine the costs associated with potentially recalling products, replacing compromised components, and compensating affected customers. We're potentially looking at millions of dollars in losses.
- **Reputational damage:** News of a breach can erode customer trust and loyalty, leading to a decline in sales and long-term damage to our brand image.
- **Legal and regulatory fallout:** We could face lawsuits from customers or even regulatory penalties for failing to adequately secure our supply chain.
- **Operational disruption:** Responding to a breach will inevitably divert resources and disrupt our operations, potentially straining relationships with partners and delaying production.

Understanding cyber risk in business terms

Cyberattacks can directly disrupt critical services, compromise sensitive data, damage brand reputation, and erode customer trust, ultimately impacting revenue streams and shareholder value. To effectively manage cybersecurity risk and embed it into our culture, companies must:

- **Quantify cyber risk:** Develop clear methods to assess the financial impact of potential cyber threats, translating technical jargon into business consequences to help decision makers understand the overall cyber risk exposure in financial terms.
- **Frame cybersecurity in business terms:** Communicate cybersecurity risks clearly, focusing on their potential impact on an organization's strategic objectives and priorities. Instead of technical metrics, use narratives that highlight how these threats could affect revenue and operations.

- **Prioritize investments with Return on Security Investment (ROSI):** Focus on security investments with measurable returns, including conducting risk modeling, cost-benefit analyses, and tracking performance metrics aligned with business goals. Demonstrate how these investments protect revenue, minimize downtime, and preserve reputation.

Putting this into action:

Discuss the following with your CIO/CTO and CISO, as well as the business:

- **Clearly define critical-business services:** Identify and prioritize these services, documenting their dependencies, including third party providers, and potential vulnerabilities.
- **Prioritize resilience:** Ensure cybersecurity measures protect against threats and enhance the resilience of critical services. Advocate for investments in redundancy, disaster recovery planning, and incident response capabilities.
- **Integrate security into all business processes:** Encourage active participation from all departments, ensuring security becomes an integral part of the organization's DNA — not just an afterthought.
- **Build a resilient workforce:** Attract, develop, and retain skilled cybersecurity professionals by offering competitive compensation and benefits, providing professional development opportunities, and fostering a positive work environment. Invest in comprehensive training and mentorship programs to cultivate cybersecurity and risk management skills throughout the organization.

A collaborative approach, with a focus on aligning cybersecurity with critical business services, strengthens the organization's security posture, protects its critical assets, and enhances its resilience against the ever-evolving cyber threat landscape.

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.

Contributors

Google Contributors:

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

Jamie Collier, Lead Threat Intelligence Advisor (Europe)

David Homovich, Solutions Consultant, Office of the CISO

Seth Rosenblatt, Content Marketing Manager

Phil Venables, CISO, Google Cloud

Guest Contributor:

Christian Karam, Co-Founder & CEO of ActionQuotient

Google Cloud