Office of the CISO

Perspectives on Security for the Board

August 2024 – Edition 5

Google Cloud

August 2024

For more information, visit our Board of Directors Insights Hub

Table of contents

Foreword 03

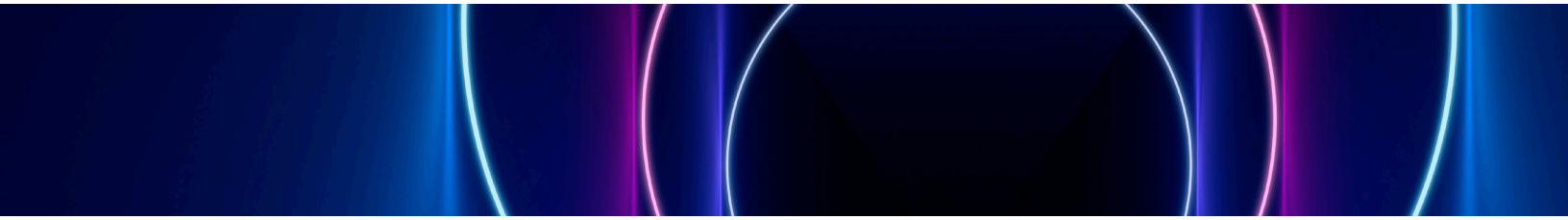
In Defense of Credentials 04

Navigating the Quantum Leap 06

Defining Borders in the Digital Age 09

Conclusion 12

Contributors 13



Foreword

As board members, we have a unique and critical opportunity to help shape our organization's cybersecurity strategy. We can help foster a culture of security and enablement, and we can play a vital role in preserving security and resiliency of our most valuable assets.

As cyber threat actors continue to pose substantial risk for all organizations, board and leadership teams are under unprecedented scrutiny. As board members, we should use this moment to ensure that our organizations are responding appropriately to today's rapidly-evolving digital landscape.

In this edition, we will tackle the pressing issues of credential theft, the looming risks posed by quantum computing, and the ongoing challenges in supporting digital sovereignty. We encourage you, as a board member, to collaborate closely with your CISO, CIO, CTO, and other relevant business stakeholders to address these complex topics. It's vital that we ensure robust, resilient strategies are in place and adequately resourced. Below are quick practical recommendations for each topic that we hope you find useful:

Prioritize Cybersecurity

Develop and implement a robust, well-funded cybersecurity strategy that mitigates top risks, including credential theft. If you are accessing sensitive board materials via email, talk to your team about implementing controls such as multi-factor authentication.

Prepare for Quantum Computing

Proactively develop a Post-Quantum Cryptography (PQC) strategy to safeguard against future quantum threats. Ensure your team is staying informed of advancements in both quantum computing and cryptography.

Assess and Adapt your Digital Sovereignty Strategy

Continuously evaluate your organization's digital sovereignty strategy, ensuring it remains relevant, effective, and aligned with evolving organizational goals. Collaborate with leaders across the organization to address shifting needs and maintain a proactive approach.

By actively engaging in these efforts, you can significantly reduce the risk of costly breaches that could severely impact your organization's reputation, your customers, your financial stability, and even improve the overall security of the general public.

Phil Venables, CISO, Google Cloud

In Defense of Credentials

Complicated, "fancy" cyberattacks might be technically fascinating, but they are the exception. Many of the big security breaches occur when someone steals a username and password, which you'll often hear referred to as credentials.

Credential theft is a global problem. The average cost of a breach is $4.88 million, according to a report published in July by IBM. However, security incidents can have more than just a financial impact. Reputation harm and psychological toll are all potential outcomes when an attacker targets your organization or even just your customers and partners.

Here are a couple of examples of recent threat activity involving credential theft:

- **Targeting Snowflake:** Google Cloud's Mandiant identified in April that attackers were compromising Snowflake customer instances using stolen credentials. They were attempting to extort victims and sell the data in cybercrime forums. The Mandiant investigation revealed that the stolen credentials were not protected with the appropriate controls. Read more about the Snowflake incident, and share our threat hunting guide with your security teams.
- **Targeting Brazil:** Credential phishing is a common threat affecting users and organizations in Brazil. Google has disrupted phishing activity hosted on Google Cloud that is targeting the region. We've seen North Korean actors use fake PDFs to try to steal usernames and passwords, and advertisements for stolen credentials on Brazilian Portuguese-language underground marketplaces. Read more about cyber threats targeting Brazil.

Deploy multifactor authentication (MFA). MFA means that you need more than a password to access your account. When you go to the ATM and use your bank card and a PIN, that's MFA. To access IT resources, you should use multiple factors for authentication, such as an authenticator app on your phone or a hardware key that you plug into your device. This means that access is dependent on something you know (a PIN or password), something you have (the phone or the hardware key), and perhaps even something you are (your biometric face scan on the phone). So, an attacker stealing a password no longer is a single point of compromise.

Many organizations, including Google, have already deployed MFA—or they are in the process of doing so. The Department of Homeland Security (DHS) recommends it, as do other agencies. It's become the de facto way to defend yourself. In fact, dare we say, you might look pretty negligent if in a few years you aren't enforcing MFA policies.

To dramatically reduce the risk of credential theft and account takeover boards need to ask the CISO, CIO and CTO how quickly your organization will deploy MFA. A good starting point is to require MFA for users who have privileges that would be beneficial for an attacker, including access to sensitive data.

Putting MFA into action

These investigations underscore the urgent need for credential monitoring, universal enforcement of MFA and secure authentication, alerting on unusual attempts to access accounts, and limiting access to sensitive data and especially your data crown jewels. Additional best practices for defending user accounts include using strong and unique passwords that are difficult for machines to guess and periodically reviewing who has privileges and whether or not that access is still required.

Discuss the following with your CISO, CIO and CTO:	
Partnership to combat credential theft	Boards should collaborate with their CISO, CIO, CTO, and business leadership to develop and implement a comprehensive strategy, equipped with adequate resources and security controls, to effectively mitigate the risks of credential theft.
Take a leading position	If you are accessing your sensitive board materials from an email account protected only by a password, we advise requesting board content to be protected by MFA. Ask your team what they need from the board to support implementing this practice.
Educate users	Require training of employees on cybersecurity best practices, including password hygiene, phishing awareness, and safe browsing habits.
Escalation to management	Establish well-documented processes for employees to report suspicious activity, and encourage employees to use said processes if they see something potentially problematic, such as suspected phishing emails.

Navigating the Quantum Leap

Quantum computers are a hot topic in the tech world. They're a new type of machine that uses quantum mechanics to solve complex mathematical problems that can stump traditional computers—and they could pose a risk to existing cybersecurity technology and practices.

If powerful enough, quantum computers could potentially crack the codes, or encryption, that protect our online communications and sensitive data. This could have serious consequences, jeopardizing online privacy and the security of our digital world.

Fortunately, there are alternative cryptographic systems known collectively as post-quantum cryptography (PQC) that offer a secure way forward. Standards to guide the development of "quantum-safe" cryptographic systems have just been finalized by National Institute of Standards and Technology (NIST)—and they run on today's conventional computers.

At Google, we take these risks seriously, and we're taking steps on multiple fronts to address quantum computing risks. We began testing PQC in Chrome in 2016, we've been using PQC to protect internal communications since 2022, and we've taken additional quantum computing protective measures in Google Chrome, Google servers, and in experiments for connections between Chrome Desktop and Google products (such as Gmail and Cloud Console.)

Additionally, Google engineers have contributed to official, formal quantum computing standards released by NIST, ISO, and other standards organizations, and are working with partners to produce formally-verified PQC implementations that can be used at Google and beyond.

Board members must understand this risk, expect and enable their CISOs to develop mitigation plans, and stay alert and prepared despite the unpredictable timeline for quantum breakthroughs.

Why act now?

- **Business impact of cryptography failing.** Cryptography uses mathematical techniques to transform data and prevent it from being read or tampered with by unauthorized parties. Quantum attacks could be able to break the cryptography deployed across environments and systems, used to protect the data that is critical to delivery of your most important business services, in unexpected ways.
- **Migrating cryptography takes a long time.** Upgrading cryptographic systems is a complex, resource-intensive process that can take years to complete. Although quantum-safe cryptographic algorithms are available and can be implemented on existing hardware, the transition to new cryptographic algorithms and protocols requires significant time and effort.

- **Harvest now, decrypt later.** Malicious actors are currently stockpiling vast amounts of encrypted data, biding their time until a powerful quantum computer emerges. This future technology could unlock the secrets hidden in that data—secrets that could be the very lifeblood of your organization, such as intellectual property, trade secrets, and sensitive communication records.
- **Standardization and upcoming regulations**. Well-recognized standards bodies, including NIST, have just released post-quantum cryptography standards. Even the White House is developing directives urging federal agencies to prepare for quantum computing advancements. We anticipate new regulations across various industries, and Google is actively participating in working groups such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the PQC Alliance to address these developments.

Putting PQC prep into action

Preparing for PQC doesn't need to be managed as a "big bang". As board members, you should speak with your CISO, CIO, and CTO about developing a post-quantum cryptography strategy. This should include preparing for integration of new, quantum-resistant algorithms into existing systems, while ensuring efficiency and scalability and weighing cost, risk, and usability.

Discuss the following with your CISO, CIO and CTO:	
Implement a PQC strategy	Develop and implement a PQC strategy to prepare for the quantum risk. Stay informed on both the latest developments in quantum computing and engineering, as well as in advances in cryptography. Acquire expertise to distinguish between hyped up announcements of small improvements, marketing, and actual advancement in quantum engineering. Follow up with both industry best practices including our post-quantum cryptography blogs and academic and industry research including Google's Quantum Research.
Assess the business risk	Conduct a risk assessment to identify critical data that is most vulnerable to quantum attacks. Identify where cryptography is utilized—it is likely pervasive throughout your systems. Create an inventory of all systems employing cryptography to safeguard data at rest, in transit, and in use. Classify the data and perform a threat analysis. Google's quantum threat analysis can serve as an example of how to determine which changes should be addressed first.
Analyze the broader risk	Assess the wider impact to other systems that might need to change. This could be like a Y2K problem where the format of data (for example, larger digital signatures) in databases and applications might need significant software changes beyond the cryptography.
Learn from the past	Reflect on how your organization successfully dealt with major cryptography-related issues in the past. This will help identify strategies that worked well and areas for improvement. Organize a tabletop exercise — a workshop for the organization's leadership (and board members) — to raise awareness of the complexities associated with migrating cryptographic systems, and to identify the necessary steps moving forward. Google's adoption of PQC, encompassing technological and procedural changes, can serve as an example for other organizations.

While we can debate how soon we'll see a quantum computer powerful enough to break today's current security, the task of adopting post-quantum cryptography is substantial. Additionally, with NIST's new PQC standards, regulators, governments, customers, and auditors are likely to question your organization about its PQC plans. Therefore, it's crucial for organizations to initiate the transition immediately.

Defining Borders in the Digital Age

For many organizations operating in multiple jurisdictions, especially those in the public sector and regulated industries, cultural and political concerns about data privacy and unauthorized third-party data access have triggered a swell of new regulations. Boards should be aware that these changes may impact the cost of and access to cloud services.

In recent years, governments around the world have taken steps to exercise tighter local control of data and digital infrastructure—a trend colloquially known as **digital sovereignty**. By 2025, 10% of global businesses will operate more than one discrete business unit bound to and by a specific sovereign data strategy.

Boards should be aware of new regulations that, in some cases, require technology providers to localize data storage and processing within their territorial boundaries. In others, regulations can restrict foreign technology providers from serving customers in critical sectors.

These measures have pushed technology companies, including cloud service providers, to make significant investment in new controls and partnerships with trusted local providers to better meet customers where they are. Increased geopolitical instability highlights the risk of service disruptions due to foreign interference or industrial accidents, driving demand for solutions that offer survivability and continuity of operations in crisis scenarios.

For example, a decade ago, the French National Cybersecurity Agency (ANSSI) introduced a trusted cloud certification known as SecNumCloud. It mandates European data residency and local operations, while limiting French critical infrastructure operators from using cloud services from foreign providers. For organizations operating in France, regulations like SecNumCloud may pose questions about cost and access to certain cloud products and features.

Google Cloud has responded to SecNumCloud and other global requirements by rolling out new sovereign controls. These controls include data residency in some jurisdictions, staffing by approved personnel, customer-managed encryption, and transparent audit logging. Further, we've partnered with Thales to launch the joint venture S3NS, which can provide independent oversight, operate the platform, and offer sovereign controls.

Google Cloud's approach reflects three distinct pillars of sovereignty in the cloud:

- **Data sovereignty**: We give organizations strong controls to govern where their data is stored and processed, and who has access to their data. Tools like customer-managed encryption keys help customers prevent unauthorized access to their data, whether by external actors or even the cloud provider itself, and approve administrative access only for specific provider behaviors they deem necessary.

- **Operational sovereignty**: We give organizations increased control over the personnel and entities operating and overseeing their cloud environment. This includes the ability to restrict access to Google Cloud staff within a given region or only to those with relevant security clearances. For customers requiring additional separation, we offer supervised cloud services in which we partner with trusted local IT providers, such as Thales, to operate customer controls.
- **Software sovereignty**: We provide organizations with tools built on open standards and APIs to enhance data and application portability. The ability to run the same application in our cloud, in our competitors' cloud, or on-premises—or even to run disconnected from the Internet—frees organizations from being locked in to a single provider, which enhances survivability resilience.

Putting digital sovereignty into action

The specific aspects of digital sovereignty that matter to an organization can vary, and these needs can shift rapidly over time. This makes it crucial for board members to regularly assess their current strategies and collaborate with leaders across the organization. This ensures that their digital sovereignty strategies remain relevant, effective, and aligned with the organization's evolving goals.

Discuss the following with your CISO, CIO, CTO, legal and regulatory affairs teams, and the business:	
First, ground the strategy by clarifying why digital sovereignty matters to your organization. Consider such factors as:	
Legal and regulatory compliance	Avoiding fines, sanctions, or legal challenges.
Data protection and privacy	Safeguarding sensitive company and customer data.
Business continuity	Minimizing disruptions due to changes in international regulations.
Reputation management	Demonstrating commitment to ethical data practices.
Competitive advantage	Positioning your company as a trustworthy data steward.
Next, consider the operational impacts of implementing a digital sovereignty strategy based on the most important factors. These may include:	
Data storage	Assessing where your data resides and if it complies with applicable laws.
Cloud service providers	Evaluating their compliance with sovereignty regulations and offerings to help operationalize sovereignty strategies.
Data transfers	Ensuring secure and compliant cross-border data flows.
Contractual agreements	Incorporating clauses into contracts with partners and vendors outlining how access to data is controlled.
Finally, consider how implementing your organization's digital sovereignty strategies will impact the board's strategic activities:	
Risk assessment	Identifying and quantifying sovereignty risks.
Compliance strategy	Developing a roadmap for compliance with relevant regulations with sovereignty requirements
Technology investments	Evaluating solutions that support data sovereignty (such as local data centers and encryption).
Partnerships and alliances	Collaborating with experts to navigate complex regulatory environments with sovereign requirements.
Communication	Keeping stakeholders informed about your company's data sovereignty efforts.

Conclusion

As board members, we have a unique responsibility to influence our organizations' cybersecurity strategy, and foster a culture of security and enablement. We should partner with CIOs, CTOs, and CISOs to drive enforcement of cybersecurity best practices, which can significantly reduce the risk of organizations being impacted by costly breaches.

These efforts can help teams prepare for future threats by resourcing mitigation plans in preparation for new innovations, such as quantum breakthroughs and investing in sovereignty efforts to protect against risk and ensuring compliance.

To combat today's cybersecurity challenges, organizations should think and act big, and need support to do so. Our Perspectives on Security for the Board series aims to bridge the gap by clarifying cybersecurity concepts and equipping board members with the insights needed to drive effective security strategies.

Google Cloud is committed to advancing security, consistently delivering cutting-edge solutions. As technology evolves, so does our understanding of threats and opportunities. We recognize the unique challenges leaders face and are committed to being your trusted partner in securing your organization. Explore the latest resources on our Board of Directors Insights Hub: http://g.co/cloud/Board

Contributors

Our Perspectives on Security for the Board: Edition 5 report features insights from:

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

Adam Greenberg, Sr. Content Manager

David Homovich, Solutions Consultant, Office of the CISO

Christiane Peters, Security Architect, Office of the CISO

Seth Rosenblatt, Content Marketing Manager

Robert Sadowski, Director, Product Marketing, Trust & Security

Phil Venables, CISO, Google Cloud

Google Cloud