Google Cloud
Security

Perspectives on Security for the Board

March 2026 - Edition 10

Office of the CISO

For more information, visit our Board of Directors Insights Hub

Contents

Foreword

The way that the enterprise uses data has undergone a fundamental state change over the past few years. Information is no longer treated as a static, passive asset to be locked away for safekeeping. Future-forward businesses now use data as the lifeblood of their organizations — a revving engine that drives everything from automated decision-making to customer experience.

Effective governance that ensures data integrity and operational resilience is fundamental to the board's oversight mandate.

Boards can meet this new standard of oversight through targeted, high-quality inquiry of management. This scrutiny requires board members to actively navigate pressures that blur traditional boundaries:

- **Integrity gaps:** AI models lose reliability when the underlying data used for training no longer accurately reflects current realities. This degradation increases the risk of making high-stakes decisions on weakened foundations.
- **Side-door entry:** Modern Software-as-a-Service (SaaS) ecosystems have evolved into unintended repositories for critical infrastructure secrets. By housing administrative credentials, API keys, and long-lived access tokens used to manage cloud environments, these third-party platforms have become one of the enterprise's most vulnerable—and direct—entry points for attackers.
- **Personal exposure:** A shift where the digital breadcrumbs of an executive's life can create a path for corporate sabotage, rendering physical barriers insufficient.

This transition is underscored by a 2026 regulatory calendar that shifts the enterprise from a period of voluntary guidance to one of accountability. These future global milestones are examples of a clear move toward holding boards directly responsible:

- **June 3, 2026 (U.S. Securities and Exchange Commission Regulation S-P[1]):** The final compliance window for small entities to implement robust incident response and prove active oversight of third-party service providers.
- **August 2, 2026 (European Union Artificial Intelligence Act):** The full application of transparency and governance rules; Boards are expected to verify the provenance and integrity of high-risk AI models.
- **December 10, 2026 (Australian Privacy Act Reforms):** Updated requirements mandating disclosure of how personal information is used in automated decision-making.

This report serves as a strategic map for navigating new boundaries, and to help board members and management prepare to answer the critical questions necessary to maintain effective oversight in a high-paced environment.

– Nick Godfrey, Senior Director, Office of the CISO, Google Cloud

[1] Large Entity Window: 18 months after publication (December 3, 2025)

From AI theater to Total Information Mastery: A new fiduciary frontier

The corporate landscape is undergoing what physicists call a state change, shifting from an old model of static data storage toward a new era of "kinetic data," where information is an animating force powering the business. In this environment, cybersecurity is more than a defense — it is a guardian of this energy, allowing the business to accelerate without sacrificing integrity and resilience. As AI becomes the primary driver of this momentum, board oversight is expanding, too.

This environment is a departure from AI theater—differentiated from authentic AI experimentation by cycles of small, unscalable AI pilots that prioritize the appearance of innovation over operational impact. Instead, organizations can pursue Total Information Mastery, a new strategic mandate that fundamentally redesigns the organization around harnessing data as a differentiated, value-creating asset.

The board's oversight role should evolve accordingly, said Ryan McManus, founder, techtonic.io, and president, National Association of Corporate Directors New York, on a recent episode of The Cyber Savvy Boardroom podcast.

He said that "the idea of total information mastery really breaks down the road map of artificial intelligence largely in a business transformation sense," and emphasized that this "gets very much into the fiduciary responsibilities that we have as directors."

McManus further observed that while many companies focus on asking how to do things "better, faster, and cheaper," the real fiduciary challenge is asking how to bring entirely new value to markets.

"That's where all of the disruption and the surprise comes from," he said, suggesting that the board's role is to ensure the organization focuses on more than incremental gains.

A strategic imperative: Navigating synthetic data and model collapse

Fiduciary oversight of this engine is tested by the reality that the data used to train models and drive decisions is beginning to erode.

For an enterprise, building a strategy on this data is like building a foundation on digital sand. This instability requires more rigor in verifying data integrity to ensure that unverified information doesn't lead to flawed executive decisions.

This threat is both external and internal. When an AI system begins to learn from its own outputs instead of validated information, it triggers a loop known as model collapse where the model loses its utility over time.

Without validation of the accuracy and consistency of the model's outputs, the organization risks eroding its competitive edge and decision-making precision. Mastering this feedback loop is a critical component of ensuring that the kinetic energy of the enterprise remains a force for growth rather than a source of hidden risk.

Strategic oversight: Metrics for mastery and security

To move past the surface level of AI theater, boards can look for specific indicators that signal whether these investments are translating into a true structural advantage. The following examples illustrate the types of signals that define a move toward mastery:

Metric	Target	Strategic and security significance
ROI per dollar	2x to 10x value creation	Measures if AI is driving financial impact.
Workflow redesign %	Core processes rebuilt for AI	Measures if we have baked in security controls to the new AI workflows.
Resilience signaling	Manual override rates	High override rates signal that the AI's logic is diverging from human expert reality.

Putting this into action

To facilitate a move to strategic mastery, the following questions are proposed for discussion with the CEO, business executives, CISO, and CHRO:

- **Optimized business models:** How are we using AI to do what we already do better, faster, and cheaper, and how are we using it to bring entirely new value to our markets?
- **Data integrity:** What is our strategy for securing our data sets to ensure our AI remains a reliable strategic asset?
- **Model oversight:** How do we ensure our AI systems do not degrade over time? How can we evolve our current data governance framework to ensure the high-quality grounding required to minimize model hallucinations?
- **Cognitive gap:** As we automate junior security and analyst roles, how are we ensuring that future cyber-savvy leaders are gaining the foundational expertise needed to oversee automated systems?

The side door entry: SaaS integration attacks

Digitalization, while enhancing our operational capabilities, has also created complex new risk surfaces that require strategic oversight from boards. High-profile ransomware incidents in 2025 demonstrated that cybercriminals are increasingly comfortable targeting the fabric of modern infrastructure, from cloud instances to outsourced business functions (a trend discussed in previous Board Perspective reports).

One area of aggressive focus for threat actors is the modern Software-as-a-Service (SaaS) ecosystem. These are platforms where critical business applications and data are hosted and managed by third-party providers in the cloud. SaaS platforms are uniquely attractive targets because they serve as centralized repositories for high-value data and, critically, often act as unintended repositories for infrastructure secrets. By housing administrative credentials, API keys, and long-lived access tokens used to manage cloud environments, these platforms have become one of the enterprise's most vulnerable—and direct—entry points for attackers.

Cybercriminals often target single sign-on (SSO) solutions to gain access. They've recently increased the scope and intensity of their attacks against SSO systems in part because it's a centralized authentication system that allows an employee to log in once and gain access to all authorized applications. Since employees don't need separate passwords for each application, threat actors can use compromised accounts to gain widespread access to SaaS providers and significantly expand intrusions beyond traditional infrastructure.

This sharp increase in identity-based attacks should force organizations to mature their defenses. Robust multi-factor authentication and heightened help desk vigilance can make this entry vector significantly harder to breach.

Consequently, threat actors have pivoted to a weaker underbelly: SaaS integrations.

SaaS integration attacks explained

SaaS integration attacks target vulnerable third-party add-ons, much like picking a side door lock to sneak into a house.

These attacks are an enormous risk for organizations. The potential for widespread disruption was starkly illustrated during the campaign targeting the Salesloft Drift platform in August 2025, a popular AI-driven customer engagement tool used by Salesforce customers. The threat actors compromised Drift integration to steal digital keys that granted them authorized access to over 700 corporate environments. Masquerading as the trusted application, the attackers used the Salesforce Bulk API to quietly steal massive volumes of customer data.

SaaS integration attacks are automated and opportunistic. They can easily impact hundreds of organizations across many sectors, as the August 2025 campaign involving Drift did.

It's crucial for boards to understand that a SaaS integration attack is often a means to an end. Attackers will search the stolen data for plaintext secrets, including cloud access keys and sensitive login credentials, to pivot from the SaaS platform into a victim's cloud infrastructure and internal network.

Putting this into action

By recognizing the significance of secure SaaS integrations, boards can provide essential leadership in developing proactive security measures that strengthens an organization's entire cybersecurity posture. The following recommendations provide a roadmap for enhancing resilience against SaaS-focused risks.

- **Re-evaluate platform versus ecosystem risk:** Most organizations' third-party management prioritize their primary vendors, such as cloud, SaaS, and infrastructure providers. Boards have an opportunity to drive a wider and more cohesive approach that includes oversight of the connected ecosystem we plug into these platforms.
- **Demand visibility on mass exfiltration:** Attackers increasingly hide in plain sight by exploiting legitimate access tokens to gain entry before hijacking authorized processes to steal data. Robust identity-based security controls should therefore be complemented by monitoring for anomalous data movement, regardless of whether the protocol or process used is authorized.
- **Acknowledge the "stepping stone" risk:** If a SaaS integration is compromised, incident response plans should trigger a broader reset of credentials and access permissions across interconnected infrastructure to prevent lateral movement. Boards can ensure this protocol is formalized in their response and risk identification policies.

Unified protection: Securing the executive digital footprint

Ten years ago, executive protection was a fortress built of armored cars, private jets, and bodyguards. As business grew online, so did threats against business leaders, and Google Threat Intelligence Group began observing a notable surge of digital targeting against company executives starting in 2024.

Executives are gateways to critical assets, sensitive information, and the extended supply chain. To better combat attempted exploits of the executive's placement and high-level access, we believe that executive protection professionals need to prioritize mitigating online vulnerabilities along with physical security measures. Investing heavily in physical protection, meticulously assessed travel plans, and secure transport is simply not enough anymore.

Effectively minimizing modern risks to executives requires the convergence of cyber and physical intelligence. Rather than managing these risks in silos, organizations should deploy a unified strategy where digital signals directly inform physical security strategies.

Organizations should extend this same level of rigorous defense to the executive's digital footprint, and not leave their personal data and online activities vulnerable to adversaries.

Threat actors seek a wide range of personal information to target executives, including:

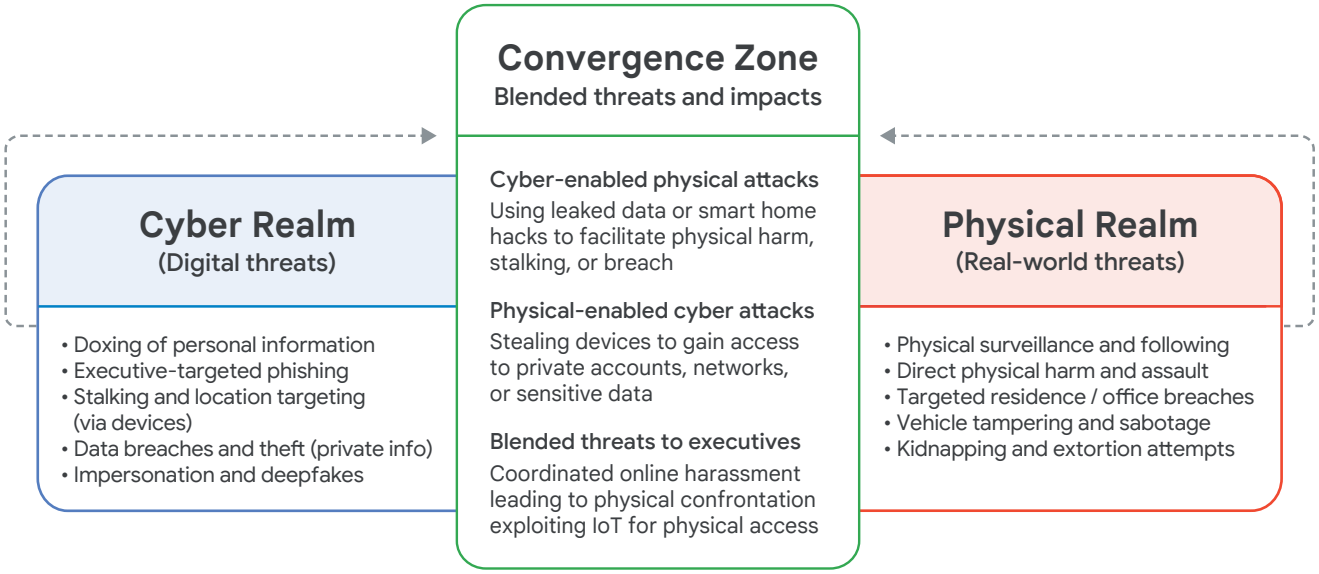
- Personal life, including contact information, hobbies, health status, political interests, family dynamics, and academic and professional backgrounds.
- Financial and corporate assets, including real estate portfolios, vehicle details, and business connections.
- Patterns and habits, including real-time or predictive movements, routines, and travel schedules, which can all be used to support harassment, kidnapping, extortion, and physical surveillance.

Attackers then use this data to craft highly-tailored cyber and physical campaigns against their targets. They also conduct broader reconnaissance by exploiting the online activity of entire executive networks, including family members, close friends, and professional associates, to establish a soft-entry point.

We have observed attackers generating highly-deceptive social engineering attacks that used family members' names and pictures, compromised accounts of relatives and close associates, and created spoofed accounts. These attacks exploit personal trust and relationships to harvest sensitive information and steal privileged credentials.

By analyzing key patterns and critical risk vectors within an executive's digital ecosystem, security teams can preempt threats before their personal data is weaponized into a physical or cyber assault. Ultimately, the goal is to transform the executive from a high-value target into a hardened asset, where digital invisibility becomes the most effective form of physical armor.

The convergence of cyber and physical threats



Putting this into action

Beyond standard security protocols, supporting executives through education and proactive risk mitigation remains a key priority. Clear insight into the evolving threat landscape empowers executives to secure their personal and professional lives.

- **Data broker exposure:** What is our current process for auditing the presence of executive PII on data broker or open source sites, and what is the risk of internal data being exposed?
- **Social media hygiene:** How are we supporting executives and their families in implementing social media settings to ensure their private lives are not being used as reconnaissance for a corporate breach?
- **Location privacy:** How are we protecting the travel routes of executives to highly-visible events? Do we have a formalized policy regarding real-time geo-tagging and check-ins for executives and their families to prevent the broadcast of their precise physical locations?
- **Venue oversight:** For high-profile public engagements, what is the protocol for auditing physical exit routes and digital security at third-party venues?
- **Network segmentation:** How can we confirm whether executive home networks are physically segmented so that third-party service providers and IoT devices cannot access corporate workstations or devices?
- **Executive spoofing:** What tools are we using to monitor for deepfakes and spoofed social media profiles that could impact our brand or stock price?
- **MFA ubiquity:** Are all personal and professional platforms for our leadership team enrolled in multi-factor authentication (MFA) to mitigate identity theft?

How boards can learn more

To delve deeper into these critical discussions and explore all of our Perspectives on Security for the Board reports, including AI and cybersecurity, cyber risk oversight, cloud adoption risk mitigation, supply chain security, and insider risk, please visit our dedicated Board of Directors Insights Hub.

Google contributors

Alicja Cade, Senior Director, Financial Services & Advocacy, Office of the CISO

Jamie Collier, Lead Threat Intelligence Advisor (Europe), Google Threat Intelligence Group

Nick Godfrey, Senior Director and Head of Office of the CISO

Kerry Helby, Executive Audience Lead, Security Solutions

David Homovich, Board Security Advisor and Advocacy Lead, Office of the CISO

Samantha Lewis, Manager, Google Threat Intelligence Group

Taylor Long, Senior Analyst, Google Threat Intelligence Group

Seth Rosenblatt, Cybersecurity Editor, Google Cloud Blog

Lia Wertheimer, Program Manager, Office of the CISO

Google Cloud