CROWDSTRIKE

WHITE PAPER

Cybersecurity Risk Oversight:

A Governance Guide for Board Directors

In This Guide

Cyber risk has evolved from a technical concern to a central business risk facing modern enterprises. For boards of directors, this shift transforms cybersecurity from a compliance exercise into a core governance mandate. Boards are facing increased scrutiny while threats are accelerating, and AI disrupts how both attackers and defenders operate.

This white paper provides pragmatic guidance to help boards strengthen cyber-risk oversight and helps define what "good" looks like. In short, effective cyber oversight means establishing clear accountability, agreed risk appetite, measurable resilience outcomes, and regular board-management operating cadence — supported by independent validation. The paper distills key cyber risk principles — how threats have evolved, how to assess impact, and how to ensure resilience — and translates them into actionable expectations for management and directors alike.

KEY TAKEAWAYS:

1. **Cyber risk oversight is part of a board's duty of care** and requires a baseline understanding and access to expertise.

2. **AI is shifting the cybersecurity landscape.** Attackers and defenders are in an arms race to harness AI to make themselves faster and more effective. Meanwhile, rapid adoption of AI tools in the corporate space introduces new dimensions of security risk.

3. **Understanding attackers makes for stronger defense.** Boards should ensure their companies maintain a functional understanding of attacker motives, tactics, and trends.

4. **Embed resilience into strategy.** Security and resiliency are more closely linked than ever. Resiliency planning doesn't stop at your network perimeter but extends to critical partners and service providers.

Strong cyber oversight is not about technical mastery — it's about governance maturity. Directors who engage proactively in this domain strengthen stakeholder trust, protect shareholder value, and ensure their organizations are equipped to navigate disruption with confidence.

Table of Contents

Cyber risk has been a boardroom topic for years, but its status has fundamentally changed. What was once treated as an operational or IT issue is now a **top-tier enterprise risk** with direct implications for financial performance, operability, reputation, and regulatory compliance.

The 2023 U.S. Securities and Exchange Commission (SEC) rule on cybersecurity disclosures cemented this reality. By requiring transparent governance and timely reporting of material cyber incidents, the SEC elevated expectations for board fluency. Just as Sarbanes-Oxley transformed financial oversight two decades ago, the new rule has introduced a similar demand for cybersecurity expertise at the board level. And the trend is global — regulations like the EU NIS2 directive, recent enforcement of Australia's Corporations Act, and other regulatory measures create similar impetus for increased board oversight worldwide.

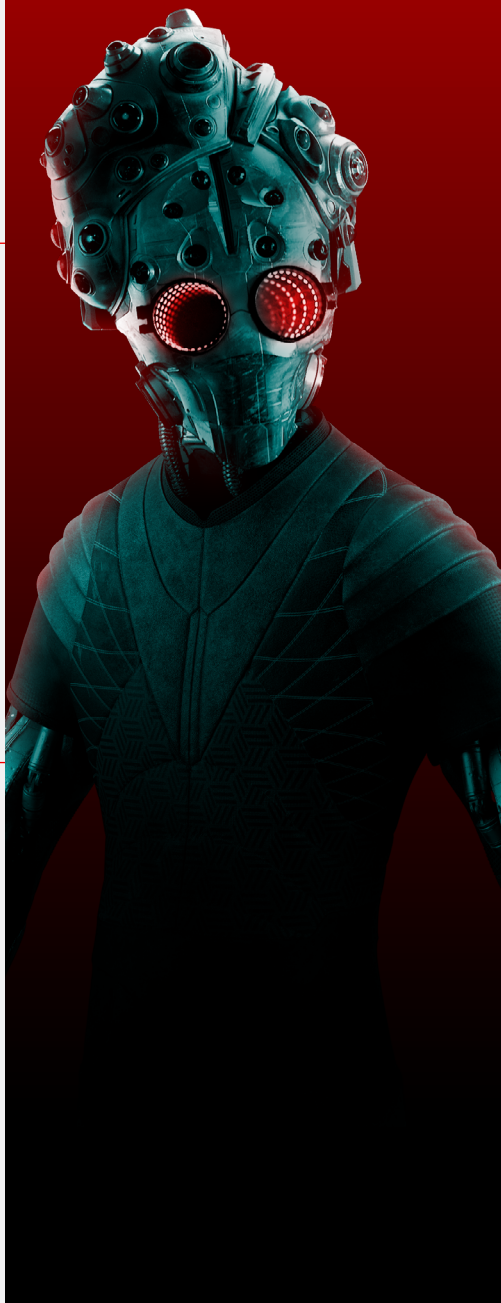
This white paper is designed to help board members strengthen their understanding of cyber risk and oversight responsibilities. It is not a technical manual but a practical guide to bridge the language of security and business.

Cyber Risk Fundamentals

At its core, cybersecurity is an exercise in managing risk. **The basic risk formula of "risk = likelihood x impact" still applies.** But the drivers of those variables are different. Likelihood is a function of who the threat actors are, their motives, how they operate, and the efficacy of an organization's defenses in stopping their attacks. Impact is a function of which assets are affected by a successful attack, in what manner, and for how long.

The following sections delve into each of these variables and outline what boards should expect management to demonstrate, including how cyber risk is assessed, prioritized, and governed in line with the organization's risk appetite.

» **RISK = LIKELIHOOD X IMPACT**



Understanding Likelihood

Cyber Threats

Cybersecurity is not merely a technology problem — it is a **human and strategic problem**. Every cyberattack begins with a motivated threat actor pursuing specific objectives. Understanding the threat actor's identity, incentives, and methods is essential to effective oversight.

The board should expect the organization it oversees to have access to this threat intelligence and be able to answer the following questions:

Who is targeting us?

CrowdStrike monitors over 280 different adversaries and categorizes them as follows:

- **Nation-state actors** seek competitive advantage, geopolitical leverage, or access to intellectual property. They tend to be the most advanced and capable threat actors.
- **Cybercriminal groups** pursue financial gain through ransomware, extortion, or fraud. They tend to be less advanced than nation-state groups but are sophisticated, aggressive, and highly dangerous.
- **Hacktivists and insiders** act on ideology, grievance, or opportunity. Hacktivists and insiders tend to be the least sophisticated, but in the case of insiders, their existing access enables them to have considerable impact.

How are they likely to target us?

Each threat actor group uses different tactics, techniques, and procedures to pursue their targets. Some utilize stolen credentials or hijack vendor access, while others seek to exploit software vulnerabilities.

Knowing who is likely to target the organization, what they want, and how they are likely to operate allows security teams to focus on the **areas of greatest risk**. The board should expect management to factor this information into the organization's risk management program. Management should be able to demonstrate how they prioritize based on these factors and report major changes in the threat landscape to the board.

ANATOMY OF AN ATTACK

01 An attacker identifies a trusted insider to impersonate.

02 The help desk is manipulated into resetting access.

03 The attacker logs in as a legitimate employee.

04 Critical systems and administrators are identified and compromised.

05 Ransomware is deployed. Operations halt.

Consider this scenario. A threat actor uses LinkedIn to identify IT workers at a company they want to target and begins gathering information about specific individuals from public sources and personal information stolen in prior data breaches. The threat actor then calls the company's help desk number, pretending to be one of these IT workers. They explain that they have a new phone and are locked out of their account and need their access restored. They are clever, persistent, and able to provide basic information like a date of birth or Social Security number. The help desk resets their password and enrolls the new phone in the company's multifactor authentication system.

With a username, a new password, and a second factor of authentication, the threat actor is able to log into company systems. Because they are impersonating an IT worker, they have access to many parts of the network. They begin looking around for targets of value within the network. Perhaps they consult internal wikis to understand the architecture of critical systems, or they ask the company's new AI-powered digital assistant to help identify critical business platforms and who the administrators are for those applications.

The threat actor then targets the administrators, stealing their access keys to critical systems. They copy sensitive data from those systems into non-corporate-controlled cloud systems. They disable or delete the system that creates backups of the data. Then they deploy ransomware software — which they licensed through a criminal marketplace — to shut down critical systems and extort the victim company.

Aligning Defenses to Threats

Some version of the scenario above has played out hundreds of times in recent years. Depending on what systems were affected and how badly, victims have suffered operational disruptions that lasted weeks or months and cost hundreds of millions of dollars.

While there are many other types of scenarios, most attacks and most attackers follow some kind of pattern of activity. They share common steps, like reconnaissance, capturing credentials, and escalating levels of privilege. Different threat actors follow different patterns, so if an organization knows who is likely to target it, it can begin to anticipate how it will be targeted and orient its defenses accordingly.

Most mature security teams leverage industry frameworks to formalize tracking of specific tactics, techniques, and common knowledge. For example, CrowdStrike maps its threat intelligence to the **MITRE ATT&CK® Framework**. (ATT&CK stands for adversarial tactics, techniques, and common knowledge.)

Mapping defensive capabilities to ATT&CK or a similar industry-standard framework allows security teams to evaluate where their defenses are more and less robust and identify priorities based on what attacker behaviors they want to counteract.

As a board member, you may not need to know the specifics, but you should understand if your organization is using a standard framework to evaluate coverage and maturity of different elements of its security program. It may also be helpful to understand major trends in how threat actor tactics evolve over time and what the business is doing to respond to those trends.

Here are three current trends most boards should understand:

1. Identity is the new perimeter.

Malicious files and code were once the hallmarks of nearly every cyberattack. But increasingly sophisticated security tools have made bad files easier to detect and stop — so much so that fewer than 1 in 5 interactive intrusions involve malware.[1] Instead, attackers focus on compromising identities — legitimate user accounts and the credentials to access them. And they rely on legitimate software, such as remote management tools used by IT help desks, to carry out their attacks. Identities are also the keys to the vast cloud infrastructure and software-as-a-service applications that so many enterprises rely upon. In fact, modern attacks may not ever traverse the workstations or servers that comprise a traditional computer network. These shifts mean a greater emphasis on securing, managing, and monitoring user accounts and having tighter controls over what types of business software and cloud resources are permitted.

2. Speed defines modern intrusions.

CrowdStrike has for years tracked a metric called "breakout time." It is the time between when an attacker first gains access to a system on a network and when they begin accessing additional systems elsewhere in the environment. In 2025, the average breakout time dropped to less than 30 minutes, and the fastest time CrowdStrike observed was a mere 27 seconds as the adoption of AI tools allows attackers to streamline their operations and move faster than ever.[2] For defenders, automation and AI-powered defensive capabilities can help counteract increasingly sophisticated attack tactics, as can a unified security platform. Legacy best-of-breed security tools are often siloed, creating complexities that slow defenders down and create gaps attackers can slip through. A single integrated platform simplifies security processes, giving defenders a chance to keep pace. Even so, modern security tools require continuous improvement and innovation in the face of an adversary that is doing the same.

3. Attack surfaces are expanding.

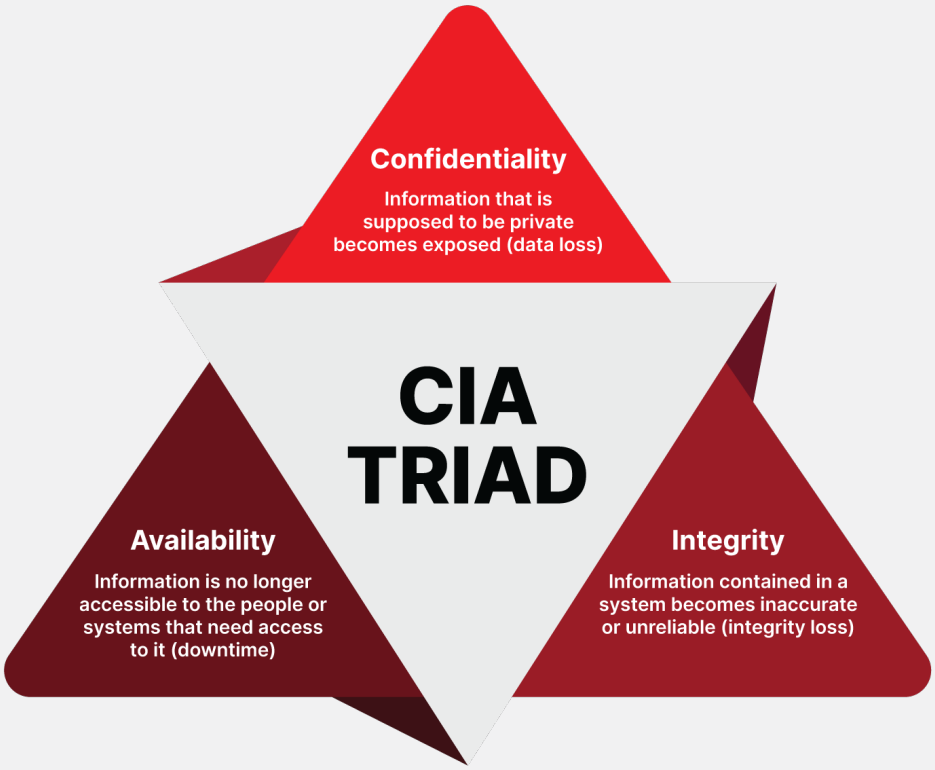
Cloud adoption, remote work, and interconnected third parties have upended the traditional concept of a perimeter in modern networks. They have also made networks far more complex. Victims often remark that the attackers have better knowledge of their own networks. To counteract this, security teams need visibility into all of the different planes of the network (e.g., cloud, endpoint, network, identity, browser). But they also need help — now more than ever, cybersecurity is a team sport. Security teams need internal partners that are willing to explore the security ramifications of adopting new technologies and external partners that can provide perspective and advice as modern networks continue to evolve.

[1] CrowdStrike 2025 Threat Hunting Report
[2] CrowdStrike 2026 Global Threat Report

Understanding Potential Impact

Prioritizing Defenses

It is not practical to defend everything equally. Cyber defenders must understand what is important to their business and provide a strong baseline level of defense with more comprehensive defenses around the critical areas of their business. Many companies maintain a list of "crown jewels" — critical assets that are essential to the business. When considering the impact of a cyber incident on any of those systems, the CIA triad — confidentiality, integrity, and availability — is a useful lens. This is a foundational principle in cybersecurity that is easily applied to business impact:



The board should ensure that the chief information security officer (CISO) — or whichever executive is responsible for cyber risk management — is engaged with the business at the right level to understand what is critical. This executive should have a comprehensive program for providing a baseline level of security across the whole organization and additional controls for securing the most critical areas.

How data or systems are affected has vastly different impacts on the business. As an example, consider the network supporting the shop floor of a manufacturing facility and how each type of effect has broadly different ramifications. A **confidentiality** attack may result in the theft of proprietary designs or manufacturing processes. An **availability** attack may result in an operational disruption, bringing production to a halt. An **integrity** attack could result in products being manufactured to the wrong specs, or in the worst cases, machinery operating in an unsafe state, causing physical damage.

Resiliency and Security

As cyberattacks have become more destructive and disruptive, security and resiliency have become increasingly intertwined. The ability to limit impact and recover quickly contributes to a more holistic security posture and lower overall risk. This has become increasingly important given the growing dependencies between modern enterprises and their vendors and the potential for a disruption in one company to cause cascading effects in others.

This convergence of security and resiliency is reflected in revisions to industry standards, such as those maintained by ISO and NIST, and in MITRE's updates to its cyber resiliency framework. CrowdStrike's own approach goes beyond these standards to emphasize a "resilient by design" approach. Overseen by a Chief Resilience Officer, this approach makes resilience a foundational principle for operations, emphasizes adaptability based on changes in the company's operating environment and customer needs, and incorporates resiliency planning into continuous improvement efforts.

Regardless of which approach the organization takes, the board should ensure that the organization it oversees has basic processes in place to bolster cyber resilience.

Organizations Should:

Identify critical business processes and the technologies, infrastructure, and dependencies that they rely upon. This knowledge fuels both security strategy and business continuity planning.

Identify critical business partners, and evaluate their security and resiliency posture. These dependencies should also be baked into continuity plans.

Maintain a "software bill of materials" for any technologies operating in the environment in order to better understand the full extent of how those technologies operate and the potential risks they may pose.

Perform regular exercises that test response and recovery capabilities against plausible scenarios. These exercises should include strategic (tabletop) and technical (red teaming and recovery) components, should be planned and facilitated by experts, and should occur at least annually. Lessons learned from exercises should be actioned by management to feed continuous improvement.

Boards should expect these resilience efforts to translate into measurable outcomes, such as the organization's ability to contain incidents quickly, recover critical systems within defined timeframes, and demonstrate improvement through lessons learned from exercises and real-world events.

The Security Implications of Artificial Intelligence

The broad adoption of AI tools accelerates many of the aforementioned trends. It enables less sophisticated threat actors to operate at a higher level and more sophisticated threat actors to operate with greater efficiency. It similarly allows security teams to be faster and more efficient. But these security gains are tempered by AI's further expansion of the surface area that defenders must protect. AI introduces a new attack surface of its own: the prompt and agent interaction layer, where models, tools, and non-human identities make decisions and take actions that can be manipulated.

This is not to suggest that companies eschew AI tools. Their promise and potential to power innovation is something most companies should champion. But they need to do so in a secure manner in order to maximize the benefits while minimizing the risk.

The board should expect management to understand how these dynamics are playing out in the organization and be able to address the following questions:

How are the threat actors targeting us using AI?

It is a quite common trend for AI to support social engineering attempts. At the simplest level, attackers use AI to make more compelling phishing emails. At more complex levels, they use video and voice filters to impersonate employees. Adversaries are also using AI to more rapidly identify and exploit flaws in enterprise software before IT teams can patch them. And once adversaries gain access, they're using AI to more quickly evaluate the network and identify the resources they're after.

How is our organization securing the AI tools we've adopted?

In the rush to capitalize on the promise of AI productivity tools, many employees are adopting AI without organizational oversight, creating a significant shadow AI challenge. Security teams need visibility into which AI tools are in the environment, what data and systems they have access to, and their runtime behavior. Organizations need security solutions and strategies that can seamlessly and securely enable AI workforce adoption, while preventing risks like generative AI data leaks that could cause data breaches and compliance violations.

How is our security team using AI?

Machine learning and behavioral analytics have been baked into advanced security tools — like the CrowdStrike Falcon® platform — for years and are a critical tool for detecting and stopping modern threats. But advanced security teams are transforming how they operate so that AI sits at the heart of much of the security team's operations. AI digital assistants streamline detection and response operations and put more information at analysts' fingertips.

How is our organization securing the AI tools we're developing?

Secure design principles take on outsized importance when including AI components in software (like AI chatbots) and infrastructure (like AI factories). Most strategies include a combination of architecting systems to place guardrails around AI components and validating and safeguarding the models being used, particularly when incorporating a third-party model. Some companies also perform penetration tests on large language models (LLMs) to identify whether they can be manipulated to behave erratically or maliciously.

The Board's Role in Incident Response

Every board has an obligation to oversee its organization's response capabilities. At a high level, the incident lifecycle includes three phases:

1. PREPARATION
2. ACTIVE RESPONSE
3. POST-INCIDENT ACTIVITIES

While boards have a role in each phase — and those roles may differ from company to company — many of the board's obligations are best fulfilled before or after an incident, rather than in the midst of the crisis. Most adversaries move in minutes, and countering them requires near-immediate response — an operational tempo that boards are not designed to maintain. But including discussions about response capabilities as part of the regular operating cadence between the board and management increases the ability of management — particularly the CISO or similar leader in charge of the response — to act quickly and with confidence.

Preparation Phase

The most important work of the board in incident response comes before an incident occurs. The officers of the company are responsible for maintaining a security program that is commensurate with the risks the business faces, and for developing plans and processes for handling any incidents that arise. The board is responsible for overseeing those efforts and ensuring they align with the board's expectations and risk appetite. As part of that responsibility, effective oversight requires clear accountability. Directors should understand which executives own cyber risk and incident response, how responsibilities are delegated, and how performance against those responsibilities is evaluated.

The preparation phase is also the time to establish clear expectations around when the board should be notified of different types of incidents. If there are specific decisions or processes that the board expects to be involved in, those should be documented in response plans as well.

The board should also expect the company to conduct incident response exercises at different levels of the organization at least annually. Some of these should include external partners that would support the response (e.g., legal counsel, forensics, and crisis communications). Having board members receive briefings on these exercises — in addition to reviewing the plans and playbooks that inform management responses — is a good way to both fulfill oversight obligations and explore company-specific questions around risk tolerance, notification thresholds, and other expectations.

Active Response Phase

Business leaders responding to cybersecurity incidents must make decisions with incomplete or uncertain information. This is the defining characteristic of cyber incident response. It is often difficult to ascertain when an event actually started or how far it has spread. It can be equally difficult to gain assurance that you've successfully eradicated the adversary, remediated the network, and are able to return to business as usual.

Most companies entrust their officers with the critical operational decisions during this phase of an incident — ideally with a kind of unified incident command structure with the CISO leading the response. Boards need to remain informed of major incidents and their impact, but they can also serve as resources to the CISO in these moments by providing experience and perspective. Oversight in these cases often consists of not only ensuring the officers are following existing plans, but also verifying they are getting the support they require.

Depending on the company, certain decisions may lie with the board or a subset of the board — for example, SEC-focused materiality decisions or the decision to pay a ransom demand.

Post-Incident Phase

The operational response to a cyber incident typically ends when the environment has been secured and normal operations have resumed. But for the business, these incidents often have a long tail that can include customer and public relations challenges, legal and regulatory suits, and issues with investors. Boards should ensure management is prepared to handle these ongoing issues and have access to the support and expertise they need to navigate them.

While those processes play out, operational responders should conduct a post-incident review to identify lessons learned and opportunities for improvement. Reviewing these action items — and holding officers accountable for following through on them — is a fundamental oversight responsibility for most boards.

In rare instances, an incident can be so severe, or the response so fraught, that it requires greater scrutiny. In these cases, boards may request an independent review of their company's security program and its response activities. When CrowdStrike's Professional Services team supports these types of inquiries, the focus often includes identifying areas where security controls could have prevented the incident, where response activities could have lessened the impact, and what types of improvements can best reduce the likelihood of similar failures in the future.

Board Incident Response Roles and Responsibilities

Groups	Preparation Phase	Active Response Phase	Post-Incident Phase
Officers	Response Planning Risk Management Security Program Management	Technical Response Crisis Response and Notifications Third-Party Support	After-Action Reviews Repairing Harm to Business
Shared	Delegation of Authorities Board Notification Thresholds	Ransom or Materiality Decisions	Applying Lessons Learned
Board	Risk Management Oversight Response Readiness Oversight	Response Oversight	Due Diligence

In Summary

Cybersecurity oversight is now inseparable from governance. It is a defining measure of board stewardship that links directly to resilience, regulatory compliance, and stakeholder trust.

Boards that treat cybersecurity as a strategic enterprise risk, rather than a technical domain, empower their organizations to act faster and recover stronger. They foster cultures where preparedness is continuous, accountability is clear, and resilience is built in by design.

CrowdStrike works with boards and executives worldwide to strengthen governance, readiness, and resilience, ensuring that when the next crisis arrives, leadership decisions are informed, measured, and decisive.

CrowdStrike can help your organization strengthen its readiness for all three phases. See all of the services that can help you prepare, respond to, and recover from an incident.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/

Follow us: Blog | X | LinkedIn | Facebook | Instagram

Start a free trial today: https://www.crowdstrike.com/free-trial-guide/