NACD | INTERNET SECURITY ALLIANCE

Director's Handbook on Cyber-Risk Oversight

FIFTH EDITION

(COVER 2)

ABOUT NACD

The National Association of Corporate Directors® (NACD®) is the leading member organization for corporate directors who want to expand their knowledge, grow their network, and maximize their potential. For almost 50 years, NACD has helped boards and the business community elevate their performance and create long-term value. Our leadership continues to raise standards of excellence and advance board effectiveness at thousands of member companies. NACD's value insights, professional development events, and resources, such as the NACD Directors Summit™ and the NACD Directorship Certification® program, support boards in navigating complex challenges. With a growing network of more than 24,000 members across more than 20 Chapters, boards are better equipped to make well-informed decisions on the critical, strategic issues facing their businesses today.

Learn more at www.nacdonline.org.

Join NACD: www.nacdonline.org/membership

ABOUT THE INTERNET SECURITY ALLIANCE (ISA)

ISA's Mission is to integrate advanced technology with economics and public policy to promote a sustainably secure cyber system. The ISA board consists of cyber leaders (typically chief information security officers) from virtually every critical industry sector. Over the last 25 years, ISA has created a comprehensive theory and practice for cybersecurity for both enterprise risk management and government policy. ISA's consensus principles and practices, developed in collaboration with NACD and the World Economic Forum, are the foundation of this program and are contained in ISA's numerous *Cyber-Risk Handbooks* now available on four continents and in five languages. The Journal of Cybersecurity has labeled this work as the "de facto international standard for cyber-risk oversight." ISA's companion book *Cybersecurity for Business* translates the board-level principles into roles and practices for the management team.

ISA has also called for a broad re-thinking of cybersecurity public policy in response to the elevated cyber risk coming from sophisticated actors using AI and other advanced technologies. This alternative approach—articulated in ISA's new book, *Fixing American Cybersecurity: Creating a Strategic Public Private Partnership*—would reform the unsuccessful cybersecurity regulatory paradigm in favor of a market-oriented approach, addressing the economics and well as the technology of cybersecurity. Many of ISA's proposals are being reflected in updated National Cybersecurity Strategies.

More information regarding ISA can be found at isalliance.org.

ABOUT THE DIRECTOR'S HANDBOOK FOR CYBER-RISK OVERSIGHT

The Director's Handbook on Cyber-Risk Oversight, now in its fifth edition, continues a decade-long legacy as the definitive guide and standard for corporate boards engaged in cyber-risk oversight. This Handbook presents six independently validated cyber-risk oversight principles that have previously been shown to improve security budgeting and security outcomes for organizations.

The current edition includes a specialized toolkit to help directors respond to incidents, oversee third-party risks, and work with law enforcement like the FBI to elevate cybersecurity across the ecosystem. While adaptable to an organization's specific size and industry, these principles are applicable to boards of public, private, and nonprofit organizations alike, as no entity is immune to modern cyber threats and all can benefit from effective cyber-risk oversight.

Director's Handbook on Cyber-Risk Oversight

FIFTH EDITION

PREPARED BY LARRY CLINTON
President and CEO
Internet Security Alliance

WITH SUPPORT FROM

SEAMUS CREIGHTON-KIRK
Internet Security Alliance

DAVID BADANES
Internet Security Alliance

DYLAN SANDLIN
NACD

Contents

Acknowledgments

NACD recognizes the contributions of the following staff members in the creation of this handbook:

DYLAN SANDLIN
Program Manager, Digital and Cybersecurity Content

ELLEN ERRICO
Art Director, Marketing and Communications

LUCY NOTTINGHAM
Senior Director, Governance Content

MARGARET BROWN
Program Manager, Content Editing

KYLEY WEIGL
Analyst, Content Development

NACD also thanks the following staff members who supported this handbook's development:
Jo Spiker, Chase Jordan, Shannon, Bernauer, Blair Petring, and Jack Ung.

NACD would also like to recognize and thank the following directors for the insights and expertise shared in the development of this handbook *(in alphabetical order)*:
Christine Larsen, Joanna Burkey, Kim Box, Paul Connelly, and Tom Petro.

Larry Clinton acted as chief author of this handbook and is President and CEO of ISA. He would like to thank the following authors for contributing to the Principles in this handbook: *(NOTE: Authors of tools are credited on the first page of each tool.)*

INTERNET SECURITY ALLIANCE

JR WILLIAMSON,
Senior Vice President & Chief Information Security Officer
Leidos

TRACIE GRELLA,
Global Head of Cyber Insurance
AIG

JON BRICKEY,
Senior Vice President, Cybersecurity Evangelist, SHIELD Program Owner
Mastercard

TED WEBSTER,
Chief Security & Privacy Officer, Enterprise Privacy & Security Risk Management
CENTENE

LARRY CLINTON,
President and CEO
Internet Security Alliance

PATRICK HYNES,
Principal, Technology Consulting — Cybersecurity
Ernst & Young

NIALL BRENNAN,
VP, Strategic Security Engagement
SAP Global Security

GREGORY TOUHILL,
CISSP, CISM, NACD.DC, Brigadier General, USAF (ret), Director, CERT Division Software Engineering Institute
Carnegie Mellon University

PATRICK REIDY,
Senior Executive, Chief Information Security Officer
GE Aerospace

MICHAEL HIGGINS,
Vice President and Chief Information Security Officer
L3Harris

TIM MCKNIGHT,
Chief Security Officer (CSO)
UnitedHealth Group

NICOLA SANNA,
President, *SAFE Security;*
Founder, *FAIR Institute*

MIKE WOODS,
Vice President, Cyber Security
GE Vernova

MIKE GORDON,
Senior Vice President, Chief Information Security Officer
McDonald's Corporation

KRIS LOVEJOY,
Global Security & Resiliency Practice Leader
Kyndryl

BRAD MAIORINO,
Corporate Vice President and Chief Information Security Officer
RTX

MURRAY W. KENYON,
Cybersecurity Partnership Executive, Information Security Services
U.S. Bank

ROBYN BEW,
Director, Americas Center for Board Matters
Ernst & Young

JOHN HAUSER,
Cyber Due Diligence Leader, Parthenon Americas Transaction Support
Ernst & Young

SEAMUS CREIGHTON-KIRK,
Director of Policy and Government Affairs
Internet Security Alliance

CONTRIBUTORS

Star Bottomley, Office Manager,
Internet Security Alliance

Kat Caleca, Research Assistant,
Internet Security Alliance

Trish Nguyen, Research Assistant,
Internet Security Alliance

Markina Parker, Research Assistant,
Internet Security Alliance

Mikael Zurnachian, Research Assistant,
Internet Security Alliance

Foreword

Nick Andersen, Acting Director and Deputy Director,
Cybersecurity and Infrastructure Security Agency (CISA)

Managing cyber risk is no longer just an information technology concern, it is an enterprise-wide and boardroom issue. Delaying or ignoring your organization's cybersecurity posture can lead to major financial exposure.

Since the last version of this handbook in 2023, global losses from cyberattacks have continued to rise as attackers remain relentless and artificial intelligence broadens the surface of exposed vulnerabilities. Across the United States and the world, small and medium-sized businesses are broadly exposed, and large enterprises continue to face targeted, persistent attacks. These risks can impact stakeholder confidence, market stability, continuity of service, and long-term viability.

Chief among cyber risks, technical debt has become a serious national liability. Legacy systems are ticking time bombs: easy targets for attackers and the biggest challenge for defenders. Time after time, organizations postpone modernization efforts and, as a result, the inherent risk from outdated systems grows into a matter of national security as the potential impact of a cyber-attack extends beyond an individual company into their supply chains, partners, and even end consumers. **The time to modernize is now.** Not next year, or deep in your long-term plan, but right away. Every moment of delay opens the risk window just a bit wider for a bad actor to gain access to your legacy systems.

Board members and senior executives must set the tone. Decisions to invest in secure technologies and modernized IT infrastructure not only reduce an organization's risk but can also positively impact thousands of people in ways that may not be immediately apparent.

Boards determine priorities, boards decide investments, and boards signal what matters. When cybersecurity is prioritized at the highest level, organizations behave differently. They patch faster, implement security-forward policies, and modernize quicker. Cybersecurity must be a standing item on the agenda every quarter and across every sector.

Board members don't have to be technologists to have an immense impact on their organization's cyber risk posture, but they drive the expectation that cybersecurity is integrated into every decision at every level.

The good news is that boards, CEOs, CISOs, technology leaders, and investors have become frontline defenders in ways that were unimaginable a decade ago. We have seen leaders begin to shift the entire ecosystem by demanding accountability and visibility. When boards make cybersecurity a standing agenda item, executives prioritize it.

The threats we face are real and daunting, but manageable through proactive leadership. Our national cyber defense posture depends on your judgement, your investment, your coordinated priorities, and the tone that you set from the top.

While the risks certainly keep us busy protecting networks and systems, they have also opened new doors and created opportunities to work together and strengthen our collective defenses.

America's cybersecurity depends on you. Technical or not, if you're reading this, you're one of our nation's cyber leaders and it is up to you to lead. Lead by example. Lead non-technical executives toward understanding cyber risk as critical infrastructure risk. Lead your organizations into partnerships that raise the collective cyber defense of our nation and global allies.

You don't have to do it alone. **CISA is here to help.**

CISA remains dedicated to working hand-in-hand with organizations of all sizes across industry, government, and critical infrastructure, recognizing that no single entity, not even the Federal Government, can address these risks alone.

For example, in September of 2025, CISA, in collaboration with the National Security Agency and 19 international partners, launched a ""A Shared Vision of Software Bill of Materials (SBOM) for Cybersecurity" enabling organizations to identify components, assess risks, and take informed action to protect critical systems. As modern software increasingly relies on third-party and open-source components, a software bill of materials is essential for managing vulnerabilities. This guide not only strengthened relationships, but it also further secured the IT and software systems being deployed across our critical infrastructure.

CISA also continues a proactive approach to strengthening our collective cybersecurity defenses and working with our industry and government partners to safeguard the systems we rely on every day. Together, we've exposed nation-state intrusions, AI-enabled ransomware operations, and ever-evolving threats targeting critical infrastructure. We have delivered actionable insights and technical guidance to help partners navigate an increasingly complex threat landscape, protect critical systems, and ensure operational continuity.

That is the power of partnership.

The importance of partnerships cannot be overstated, because we can all agree that we are operating in an environment where the threat landscape is more dynamic, more complex, and more unforgiving than ever before.

I ask that you, as leaders of your respective organizations, reach out and invite us to your investment summits, governance forums, technical conferences, and other cybersecurity-related events. We can provide the latest briefings on emerging threats, systemic risks, trends intelligence, and known vulnerabilities across the cyber community, and provide guidance to inform your cybersecurity and modernization efforts.

Our collective cybersecurity is not just about protecting networks, devices, and accounts, it is about protecting the stability and resilience of the critical systems every American relies on. CISA stands ready to support you every step of the way.

Find out more at CISA.gov.

INTRODUCTION

The New Mandate for Cyber Oversight

Kris Lovejoy, Global Security & Resiliency Practice Leader, Kyndryl and
Larry Clinton, President & CEO, Internet Security Alliance

A convergence of escalating threats, growing business opportunities enabled by new technologies, and a transformed regulatory landscape has created a new reality: cyber risk *is* a business risk and business opportunity.

The emphasis though is not singularly on bigger walls and faster detection. The importance of technology to most companies' success, and the economy more broadly, means cybersecurity must be a core pillar of an organization's strategy development, financial planning, and operational execution. As a result, cybersecurity oversight is a core component of a board's fiduciary oversight duties.

Globally, according to Microsoft's Digital Defense Report, over 600 million cyberattacks are tracked per day.[1] Other sources estimate that the economic losses from cyberattacks will soon approach $20 trillion a year – up from $8 trillion in 2022. For example, one major international retail company reported that a single 2025 ransomware attack originating from its supply chain is expected to erase one-third of its annual profits by disrupting core business operations. Similarly, an international luxury automobile company had to halt production in multiple locations due to a ransomware attack, affecting thousands of suppliers and demonstrating cascading effects across its supply chain.

More broadly, US critical infrastructure, including our energy, water, and telecommunications networks, has been compromised by nation-state related actors who have been able to remain undetected in these systems for over two years, "living off the land", giving them the ability to launch attacks that create unforeseen impacts and losses.

The expanding threat environment demands renewed vigilance from boards. The era of passive oversight is over. Cybersecurity has evolved from a peripheral technology issue into a central pillar of corporate governance and a core element of fulfilling the board's fiduciary duties.

A convergence of escalating threats, new technologies, and a transformed regulatory landscape has created a new reality: cyber risk *is* business risk, and its effective governance is now a major, and direct, responsibility of the board.

This new environment is defined by four interconnected forces:

1. **Centrality of Technology to Strategic Success:** Emerging technologies like generative AI are creating a triple challenge for companies and boards. These technologies offer the potential for immense value creation and productivity gains, but they are being weaponized to create more effective attacks while also serving as an attack vector and introducing novel risks to the enterprise. Attacks have already moved from AI-assisted to AI-generated and managed cyberattacks and 380 of the Fortune 500 companies, 76 percent, included an AI risk factor in their disclosures.[2] AI is now a routine agenda item for 62 percent of public company boards — more than double the number from 2023.[3] Yet few boards have taken steps to assess AI risks, integrate AI oversight into board committee responsibilities, or evaluated the AI impacts on corporate strategy.[4]

2. **Increased Sophistication of Attackers and Adversaries:** Ransomware syndicates to state-sponsored groups like China's "Volt Typhoon" are operating with unprecedented sophistication. They are no longer just breaching networks; they are infiltrating critical infrastructure and exploiting the entire digital supply chain, as evidenced by a **431% surge** in such attacks in recent years.[5]
3. **The Transformation of Legal and Regulatory Liability:** Regulators are now formally codifying the board's role in cyber oversight. The SEC's 2023 disclosure rules, which mandate board-level reporting on cyber governance, and the EU's NIS2 Directive, which can impose direct liability on management bodies, have made effective oversight a matter of legal compliance, not just best practice.
4. **Expanded Board Responsibilities and Expectations:** Board oversight of cybersecurity has evolved from a technical IT concern to a fundamental governance responsibility. Directors are now expected to understand how cyber risks impact enterprise value, strategic objectives, and stakeholder trust.

The confluence of these forces means that a reactive, technically focused approach to cybersecurity is no longer defensible. Boards must now lead from the front, ensuring that a robust, proactive, and resilient governance model is in place. This new approach includes:

- Positioning cybersecurity as a strategic business issue aligned to business objectives
- Maturing organizational cybersecurity strengths and allocating appropriate resources to manage technology risk

- Bolstering resilience for effective recovery from incidents and disruptions
- Elevating security across the ecosystem and industry to promote collective cybersecurity

Ultimately, the shifting environment demands rigorous board-level engagement that moves beyond a reactive, compliance focused, "check-the-box" mentality towards a proactive, risk and data informed, strategic governance approach. Boards that fail to improve their cyber-risk oversight in this new environment risk more than just operational disruption; they risk poor strategy development and execution, erosion of shareholder value, and a loss of shareholder and stakeholder trust. Directors can leverage the principled guidance in this handbook to proactively integrate cyber-resilience into the corporate strategy, ensuring that the organization is not merely defending its walls, but is strategically positioned to navigate and respond to the inevitable volatility of the digitally-enabled economy. The mandate is clear: govern with foresight or remain vulnerable to the consequences of inaction.

ENDNOTES

1. Microsoft, "Microsoft Digital Defense Report: 600 million cyberattacks per day around the globe," CEE Multi-Country News Center, November 29, 2024, https://news.microsoft.com/en-cee/2024/11/29/microsoft-digital-defense-report-600-million-cyberattacks-per-day-around-the-globe-2/.
2. Sean Greaves, "Their capital at risk: The rise of AI as a threat to the S&P 500," Autonomy Institute, 2025, https://autonomy.work/wp-content/uploads/2025/07/Sp-500-capital-at-risk_-3.pdf.
3. NACD, "Data Pack: Artificial Intelligence," NACD 2025 Public Company Board Practices and Oversight Survey, nacdonline.org, July 28, 2025, https://www.nacdonline.org/all-governance/governance-resources/governance-surveys/surveys-benchmarking/bpo-tables/ai-oversight-activities-conducted-by-the-board.
4. Ibid.
5. Samuel Goldstick, Lauren Hudon, "Combatting Supply Chain Cyber Threats: Safeguarding Data and Protecting Digital Supply Chains in a Rapidly Evolving Cyber Landscape," Foley & Lardner, October 30, 2025, https://www.jdsupra.com/legalnews/combatting-supply-chain-cyber-threats-6876192/.

PRINCIPLE ONE

Treat Cybersecurity as a Strategic Risk

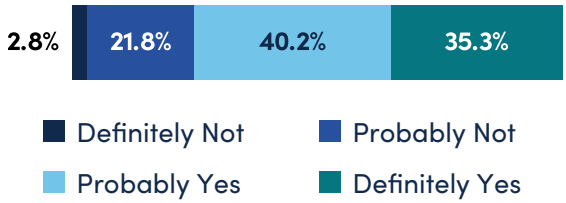
Case for Action

Cybersecurity is an enterprise-wide risk that can profoundly impact an organization's strategic success, financial health, reputation, and operational continuity. Beyond direct costs, cyber-incidents and data breaches can erode customer trust, disrupt supply chains, and invite regulatory scrutiny leading to material impacts that can threaten core assumptions of the company's strategy, its competitive position, and its legal and social license to operate.

Technology is a fundamental driver of business model success and value creation. NACD survey data reveals that 72 percent of directors state they are likely to pursue technology investments as a growth initiative in 2026, ahead of other organic and inorganic forms of growth like introducing new products, M&A opportunities, and workforce realignment.[1] AI provides another example, with survey data revealing that 76 percent of directors "probably" or "definitely expect" AI investments to factor into their organization's growth strategy.[2] While directors correctly identify technology as a means to strategic success, failing to properly protect and secure these systems can quickly erode any expected growth based on these tools and investments.

Leading boards understand the risks and opportunities inherent in digital technologies, and approach cyber-risk oversight with the same rigor as any other top-tier strategic threat, ensuring oversight and response reside at the highest level of the organization. A well-governed and managed cybersecurity program helps an organization achieve business objectives through successful identification, management, and mitigation of cyber-risks. This approach helps maintain cyber-risk

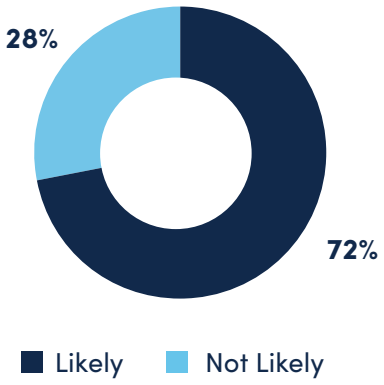
Expectations on How AI Investments Factor into 2026 Growth Strategies



Source: NACD 2026 Governance Outlook Survey, n=363

Q: Do investments into artificial intelligence factor into your organization's growth strategy in 2026

Directors Expect to Pursue Growth Through Technology Investments in 2026



Source: NACD 2026 Governance Outlook Survey, n=362

Q: What growth initiatives are your board and management team likely pursue in 2026?

within tolerable levels so that the organization is better able to execute its strategy, allocate resources efficiently, and seize emerging technology opportunities faster and more confidently than less-prepared peers.

To do this, boards must understand how cyber-risk impacts the company's strategy and core value drivers. In instances where cyber-risks present a material business impact or threaten the viability of the company's strategy, the board must engage with management to understand the risk and either adjust the strategy or allocate additional resources to manage the risk within accepted levels.

Treating cyber-risk as a strategic imperative ensures that the organization's pursuit of its strategic objectives and innovation does not outpace its ability to protect the value it creates.

BOARD ACTIVITIES

To effectively govern cybersecurity as a strategic imperative, the board can actively drive impact through the following core activities:

- **Incorporate Cybersecurity in Strategy Development and Decision Making:** Much like financial and legal issues, the board should ensure that cyber risk is deeply embedded into strategy development and execution. When strategy discussions are on the agenda, cybersecurity should be a component, including:
  - Rigorously reviewing the company's cybersecurity priorities.
  - Ensuring cybersecurity priorities are linked to business objectives and organizational sustainability.
  - Challenging management to detail the processes for identifying, measuring, and mitigating cyber risks across every business vertical.
  - Assessing whether all departments and management are aligned to enable the organization's cybersecurity priorities.
  - Evaluating each major technology and digital transformation project through the lens of cyber risk from its inception.
- **Drive Strategic Value Through Security:** Ensure the cybersecurity strategy supports business goals, such as digital transformation or customer data protection. Review budgets to confirm adequate resources for cyber defenses, balancing prevention, and response capabilities. Boards can challenge executives to find opportunities where robust cybersecurity, responsible AI stewardship, and secure ecosystem management can be leveraged as a market differentiator and a business driver to enhance trust and customer confidence.
- **Integrate Cyber Risk into Enterprise Risk Management (ERM):** Boards should ensure cybersecurity is a core component of the organization's ERM framework, not siloed in IT. This involves aligning cyber-risk assessments with business objectives, such as protecting intellectual property or ensuring operational uptime.
- **Perform Data-Driven Cyber-Risk Decision Making Based on Quantified Financial Impact:** Boards can request management to model the financial implications of potential cyber incidents, including direct costs (e.g., ransom, legal fees) and indirect costs (e.g., lost revenue, reputational damage). This helps boards evaluate strategic trade-offs, scrutinize budgets, and prioritize investments in cybersecurity.
- **Modernize Data and AI Security and Governance:** Data has emerged as a critical value driver and strategic differentiator, and boards should review how management is modernizing the organization's data security and governance frameworks to address AI-driven complexities as well as other new technology risks. Key board activities include inquiring about data access controls and the processes used to map how data is transformed by AI models, championing a shift to dynamic data classification and post-quantum encryption, and ensuring the ethical and privacy concerns arising from AI-derived insights are proactively addressed.

SUCCESS INDICATORS

Progress in governing cybersecurity as a strategic imperative can be measured by observing the following activities, behaviors, and information flows:

- **Cybersecurity is a Recurring, Substantive Item in Board Strategy Discussions**: Board conversations evolve from focusing solely on prevention and technical updates to in-depth discussions on resilience, recovery capabilities, and the impact of cyber risk on business strategy. These discussions should include the CEO and other C-suite members engaged in strategy setting with the expectation that management and the board understand strategically significant cyber-risks and their potential impacts.
- **Clear Cyber Reporting and Risk Metrics Detailing Impacts Aligned with Business Objectives:** The board receives regular, digestible reports that show how cyber risk impacts business strategy and trends over time across critical business and performance metrics (e.g., dashboards that show key performance indicators (KPIs).
- **Data Driven Strategic Decision-Making:** Major digital transformation initiatives, especially those involving AI or significant third-party dependencies, are not approved without a thorough cyber-risk assessment from their inception. Budget allocations reflect prioritized investment in cyber resiliency capabilities, not just preventative controls.
- **Stakeholder Confidence:** Positive feedback from investors, customers, or auditors on the organization's cyber posture reflects board effectiveness.
- **Security Culture Drive Greater Collaboration:** Management actively fosters a culture where security is embedded by design into new strategic initiatives, products, and services. The "assumed breach" mentality is understood across the enterprise, leading to stronger collaboration between IT, security, and business units.
- **External Communications and Market Position:** The company can credibly and responsibly leverage its strong cybersecurity posture and responsible data stewardship practices as a competitive advantage and a reason for customers to place their trust in the brand.

QUESTIONS FOR THE BOARD TO CONSIDER

- Are we regularly reviewing our cyber strategy to ensure that management is identifying, measuring, and mitigating our cyber risk in every business vertical?
- Does management model the direct and indirect costs of cyber incidents in empirical and economic terms?
- Does cybersecurity feature in all of the board's strategic discussions? Are the right management team members participating in these discussions and are they properly informed and aware about the impacts of the organization's strategic cyber-risks?
- Do we have mechanisms to balance the organization's use of modern and emerging technology (including AI) with corporate risk?
- Have we updated our processes to account for risks arising from legacy infrastructure, the cloud, third-party risks, operational technology as well as transformative technologies such as AI and Quantum?
- Have we updated our data security and governance process to account for AI and Quantum technologies?
- How is management performing adequate due diligence, including contractual agreement and continuous monitoring of our third-party partners to ensure they meet our security standards?
- Do we have the right people in place on our executive team to effectively manage cyber risk? Are our CEO and CISO capable of executing the organization's cyber-risk management strategy?
- Is management identifying how our cyber strategy can be leveraged for market differentiation and business growth?

ENDNOTES

1. Friso van der Oord, Ted Sikora, "Boards Shift Their Focus to Execution," NACD 2026 Governance Outlook Report, www.nacdonline.org, December 10, 2025, https://www.nacdonline.org/all-governance/governance-resources/governance-research/outlook-and-challenges/2026-governance-outlook/boards-shift-their-focus-to-execution/.
2. Ibid.

PRINCIPLE TWO

Monitor Legal and Disclosure Implications

Case for Action

Directors are expected to be active, informed participants in overseeing their organization's cyber-risks as cyber governance is a matter of public record and regulatory scrutiny. SEC Item 106 mandates board-level cyber oversight disclosure and public companies must describe in their Form 10-K annual reports how their board supervises cybersecurity risk and how management assesses and manages material cyber threats.

The U.S. Securities and Exchange Commission's (SEC) 2023 cybersecurity disclosure rules further outlined US board obligations. The rules require public companies to report material cyber incidents within four business days and disclose annually how the board oversees cybersecurity strategy and risk management.[1] This framework assumes directors have already approved, tested, and reviewed internal processes for incident escalation, materiality determination, and public disclosure—well before any crisis occurs. These rules apply to public companies, but they are raising the cyber-risk oversight expectations of private company boards. As such, the new mandate focuses on preparedness and oversight rather than solely on reactive responses.

This shift is global and accelerating. The EU's Network and Information System Directive (NIS2) imposes direct board-level obligations, with penalties reaching €10 million or 2 percent of global turnover.[2] In the U.S., state attorneys general are increasingly coordinating enforcement actions, such as the $49.5 million Blackbaud settlement, which mandated enhanced board reporting procedures.[3] Delaware courts are also expanding Caremark liability, signaling that cybersecurity failures may now constitute a "mission-critical" risk requiring heightened board attention.[4]

Finally, the data compliance environment has become increasingly fragmented and demanding, with overlapping federal mandates (e.g., SEC, CIRCIA), evolving state-level privacy laws across 19 jurisdictions, and international frameworks such as the NIS2, the Digital Operational Resilience Act (DORA), and the General Data Protection Regulation (GDPR).[5] Each regime introduces unique definitions, thresholds, and timelines, creating complex legal and operational challenges for companies and boards.

BOARD ACTIVITIES

These trends converge to create six key factors increasing both organizational and personal board exposure. To fulfill their fiduciary and legal obligations, the following board activities are recommended:

Prepare for Rapid Reporting Under Compressed Disclosure Timelines

- Review the company's cyber incident response playbook, ensuring it clearly defines escalation protocols, materiality determination procedures, and outlines roles and responsibilities between the board and management.
- Consider receiving simulation reports and updates at board meetings and review simulations that test the company's readiness to meet deadlines such as the SEC four-day rule.

- Confirm that cross-functional coordination—legal, technical, communications—is seamless and documented.

Mitigate Personal Liability for Directors

- Institutionalize standing legal oversight by assigning responsibility to a designated board committee (e.g., Technology, Cyber, Risk, or Audit).
- Ensure board minutes reflect deliberation and direction, not just briefings.
- Receive regular legal briefings on emerging case law and regulatory changes affecting directors' personal liability.
- Maintain documentation showing active, informed engagement to create a defensible record.

Navigate Fragmented Regulatory Obligations and Enforcement Risks

- Request management maintain a current registry of cybersecurity compliance obligations across federal, state, and international jurisdictions, including reporting timelines and regulatory chains.
- Monitor both regulatory evolution and enforcement trends through regular briefings from counsel on new legal requirements, pending investigations, and industry enforcement actions.
- Ensure corporate policies—including breach notification protocols and third-party governance—are regularly updated to reflect evolving legal requirements and benchmark against recent enforcement actions to identify vulnerabilities.

Elevate Oversight of Mission-Critical Cyber Risks

- Confirm that the board receives direct, unfiltered reporting from the CISO and general counsel on top cyber risks.
- Regularly evaluate whether cyber-risk oversight is integrated into strategic discussions alongside financial and operational risks.
- Ensure management has conducted risk assessments that identify potential cascading failures or systemic vulnerabilities.

Assess Insurance Coverage and Alignment with Actual Exposure

- Oversee a coordinated review of all cyber-relevant policies, including Director and Officers (D&O) and standalone cyber insurance to ensure coverage aligns with the organization's risk exposure. This can include examining exclusions, sub-limits, and real-world claim scenarios.
- Perform an annual validation of coverage against current risk conditions.

SUCCESS INDICATORS

Boards can gauge progress through these observable outcomes:

- **Disclosure Preparedness:** Simulations confirm readiness to meet regulatory timelines; results are reported to the board.
- **Personal Liability Mitigation:** Board minutes reflect deliberation and informed decision-making on cyber-legal issues.
- **Regulatory Mapping:** The company can produce a current registry of all cyber compliance obligations.
- **Mission-Critical Integration:** Cyber risks are explicitly discussed as part of core enterprise risk management.
- **Insurance Adequacy:** Coverage is validated annually and aligned to evolving risk profiles.
- **Legal Awareness Embedded:** Directors receive ongoing legal education and briefings on enforcement trends with the literacy and expertise to understand their implications for the organization.

QUESTIONS FOR THE BOARD TO CONSIDER

- Do we have adequate rapid internal coordination and escalation processes in place, enabling us to meet the SEC's four-day rule and similar mandates?
- How are we keeping abreast of expanding regulatory regimes and case law that impose direct responsibility on directors?
- How are we navigating the growing patchwork of federal, state, and international laws? And how are we performing against regulatory expectations, both current and anticipated?
- Are there gaps in our insurance coverage, leaving our organization and the directors exposed, and what is the potential scale/cost of that exposure?

ENDNOTES

1. U.S. Securities and Exchange Commission, "SEC Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," Release Nos. 33-11216; 34-97989, (September 5, 2023), https://www.govinfo.gov/content/pkg/CHRG-111hhrg50208/html/CHRG-111hhrg50208.htm.
2. European Parliament, Council of the European Union, "Directive (EU) 2022/2555 (NIS2 Directive)," Art. 20 (Dec. 14, 2022).
3. New York State Attorney General, "Attorney General James and Multistate Coalition Secure $49.5 Million from Cloud Company for Data Breach," press release, October 5, 2023, https://ag.ny.gov/press-release/2023/attorney-general-james-and-multistate-coalition-secure-495-million-cloud-company.
4. Construction Industry Laborers Pension Fund v. Bingle (SolarWinds), C.A. No. 2021-0940-SG (Del. Ch. Sept. 6, 2022), aff'd (Del. May 17, 2023).
5. National Conference of State Legislatures, "Cybersecurity 2024 Legislation," www.ncsl.org, effective May 7, 2025, https://www.ncsl.org/technology-and-communication/cybersecurity-2024-legislation.

PRINCIPLE THREE

Establish Board Oversight Structures and Access to Expertise

Case For Action

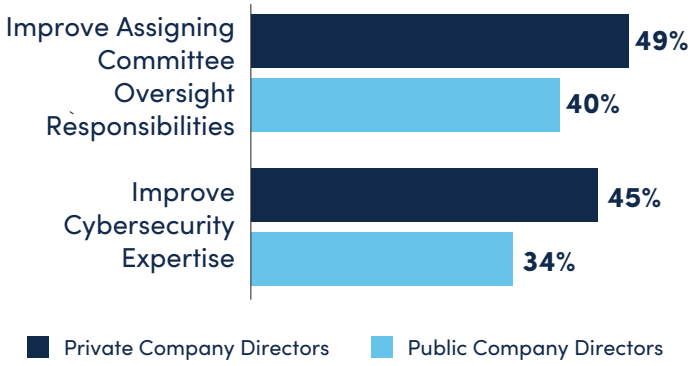
Cyber-risk oversight requires the presence and integration of effective governance structures and cybersecurity expertise. In combination, these elements position the board to provide substantive cyber-risk oversight while fulfilling its fiduciary responsibilities. Well-crafted governance structures and practices provide the necessary scaffolding for proper oversight, but they remain hollow without the substantive board cybersecurity fluency and expertise required to challenge management's technical assumptions. Conversely, isolated expertise lacks utility if it is not integrated into a practice of regular, structured boardroom deliberation.

Regulators, investors, and customers expect boards to demonstrate competence in cyber governance, and many boards, both public and private, are focused on improving cyber governance. For example, survey research shows roughly one third, 34 percent, of public company directors believe it is either "very" or "extremely important" to improve their cybersecurity expertise, while 40 percent say the same for improvements in assigning committee oversight responsibilities for cyber-risk.[1]

Private company directors express a greater need for improvement, with 45 percent stating it is very or extremely important to improve board-level cybersecurity expertise while 49 percent state improvements in committee oversight responsibilities for cyber-risk.

Without a structured approach to incorporate cyber knowledge and expertise—whether through directors, committees, or advisors—boards will lack the necessary understanding and processes to address the cyber-risks facing the organization and align cyber strategy with broader organizational goals.

Directors See Room to Improve Board Cyber-Risk Expertise and Oversight Structures



Source: 2025 NACD Public Company Board Practices and Oversight Survey, n=156; 2025 NACD Private Company Board Practices and Oversight Survey, n=86

Q: How important is it that your board improves in the following areas related to cyber-risk oversight?

BOARD ACTIVITIES

- **Define Necessary Cyber Expertise and Address Gaps:** Boards should define the level of cybersecurity expertise and competence necessary for their specific situation informed by the organization's strategy and level of risk. To help in this effort, boards can leverage a skills matrix to map directors' cybersecurity knowledge and identify knowledge gaps for key areas such as cloud security, incident response, or regulatory requirements (e.g., GDPR,

CCPA). If gaps are identified, the board should agree on methods to address these gaps, such as increasing overall board cybersecurity competency, recruiting directors with qualified or demonstrated cybersecurity expertise, or securing additional access to independent, third-party expertise.

- **Formalize Oversight Responsibilities Across Committees:** The nominating and governance committee should define and document in committee charters the cyber-risk oversight responsibilities across relevant committees (audit, risk, technology, strategy, etc.), to ensure clarity and prevent overlap. The responsible committee should maintain an adequate level of cybersecurity expertise with cybersecurity as a consistent agenda item with a formalized cadence across these committees and at the full board-level, with regular updates from the CISO and risk management team.
- **Establish Access to Independent Expertise:** Even with qualified in-house staff, cyber risk evolves faster than many organizations can track internally. Boards can consider retaining access to independent experts or third-party assessors who can provide technical and strategic evaluations of the company's posture. This includes regular validation of the company's cybersecurity programs, threat modeling, and risk assessments. Boards can also engage third-party experts to provide briefings on emerging risks and threats.
- **Enable Director Education and Maintain Board Cyber Literacy:** All directors must build and maintain a foundational understanding of cyber risk. This process can include onboarding sessions with security leaders, regular management and third-party briefings, access to vetted resources, and opportunities to attend conferences or tabletop exercises. Directors should also regularly engage in cybersecurity education. Education can include sessions on emerging risks and regulatory and geopolitical developments in cybersecurity. Further, boards can consider recruiting directors with cyber expertise to ensure that the board's level of cyber-expertise is aligned to both the strategy and the level of risk facing the organization. As many directors lack a background in cyber-risk assessment, annual or biannual training sessions may be an effective process to maintain the necessary board cyber competence.
- **Establish and Strengthen Communication and Verification Protocols:** A "trust but verify" approach demands that directors validate information presented by management using objective benchmarks, performance dashboards, and third-party intelligence. Regular one-on-one briefings with CISOs and cross-functional leaders (legal, compliance, operations) enable directors to deepen their understanding of the organization's cyber security.

THE QUESTION OF ADDING A CYBER EXPERT TO THE BOARD

Cybersecurity continues to be an in-demand area of expertise among the boards of many companies. For example, 86 percent of Fortune 100 companies disclose cybersecurity as an area of expertise sought on the board or cited in at least one director biography.[2] However, the question of whether to add a "cyber expert" director is an open one for many boards and the right approach will look different for each board.

Ultimately, the board should evaluate its needs against its alignment to the organization's strategy and the criticality of the risk. Board-level-expertise also helps maintain the board's independence, so they are not reliant entirely on management's assessment and can practice healthy skepticism.

When evaluating whether to recruit a director with cybersecurity expertise boards should consider the following questions:

- Based on our strategy and risk profile, is our current board composition and expertise appropriate?
- What candidate profile do we need and how are we defining a "cyber expert"? For example, is the board looking to add a cyber expert only, or is broader technology expertise needed?
- What company factors are important? For example
  - The organization's industry or sector
  - Where the company is in its lifecycle
  - Maturity of the company's cybersecurity program and CISO
- Is this strategy really deferring to one individual a responsibility that the full board should undertake? The board should not view the addition of a cyber expert director as a reason to not maintain a foundational level of cyber-risk understanding and competence among all board members.
- Does placing a cyber expert on the board set a precedent for assigning seats to other specialized oversight areas?

SUCCESS INDICATORS

- **Defined Oversight Structure:** Clear committee charters or board policy outlining cyber risk responsibilities, with regular updates to the full board.
- **Cyber Security Board Dashboard Review as a Standing Agenda Item:** Including regular operational and business impact metrics-based reporting on attempted breaches, vulnerability status, third-party risk, and incident response readiness presented at least quarterly.
- **Standard, Prioritized Agenda Item:** Cybersecurity from a strategic and business perspective becomes a substantive agenda item at full board and committee meetings.
- **Effective Questions:** Board discussions include informed, specific questions to management reflecting competence.
- **Timely Risk Identification:** The board flags and discusses emerging risks before incidents occur, based on advisor or management input.
- **High Director Engagement and Preparedness:** Directors build a strong relationship with their CISOs, security team, and independent experts and can regularly articulate key risks.
- **Ongoing Education:** As cyber risk evolves quickly, cybersecurity education is built into the board's calendar and is monitored and evaluated. Directors attend internal and external webinars, briefings, and conferences to maintain their knowledge.

- **Formalized Management Reporting:** A reporting line between the board and CISO or CISO equivalent is established and maintained.
- **Director Onboarding Procedures:** Cybersecurity is incorporated into the new director onboarding process including meeting with the CISO or CISO equivalent, reviewing the organization's cybersecurity strategy, attending committee meetings where cybersecurity is discussed, and reviewing the major cyber-risks facing the organization.

QUESTIONS FOR THE BOARD TO CONSIDER

- What level of cyber expertise is necessary to meet our cyber-risk oversight needs? Who on our board has the qualified expertise to address cyber risk, and does it meet our expertise needs?
- Do we need to add someone with deeper expertise on this topic to our board, or augment our knowledge with outside consultants, education, or training?
- How does our board skills matrix assess board cyber expertise, and how frequently is it updated to reflect emerging technologies such as AI, cloud, and quantum as well as geopolitical, regulatory, and AI-driven cyber risks?
- How do our committee charters specify cyber oversight responsibilities, and are there gaps or overlaps that might create blind spots? Do we need to create a dedicated committee or subcommittee to provide a deliberate focus on cybersecurity risks? If so, do we have the right talent composition to be successful?
- Is there an established management reporting structure and process that delivers cybersecurity information to the board in a timely, accurate, and effective manner?
- How are we validating that management's cyber posture reporting is accurate, independently verified, and aligned with recognized frameworks?
- How is cyber-risk accountability distributed across executive leadership, and does the board understand where responsibilities begin and end?
- How do we benchmark our cyber oversight maturity against peer boards, sector standards, and NACD best practices?
- Do we have the right board composition and organization to provide timely and effective governance and oversight regarding the identification, technical appraisal, business impact, and risk assessment of emerging technologies?
- Does the board have the right talent and experience to effectively govern the introduction of new technologies into our business in a manner that does not compromise our cybersecurity requirements? What are our gaps?

ENDNOTES

1. NACD, "Survey Analysis: Cybersecurity Oversight," NACD 2025 Public Company Board Practices and Oversight Survey, www.nacdonline.org, July 28, 2025, https://www.nacdonline.org/all-governance/governance-resources/governance-surveys/surveys-benchmarking/2025-public-company-board-practices--oversight-survey/2025-board-practices-oversight-cybersecurity/.
2. Pat Niemann, Barton Edgerton, Alison Nashed, "Cyber and AI oversight disclosures: what companies shared in 2025," www.ey.com, October 14, 2025, https://www.ey.com/en_us/board-matters/cyber-disclosure-trends.

PRINCIPLE FOUR

Adopt an Enterprise Framework for Managing Cyber Risk

Case for Action

The evolving threat and regulatory landscape demands an enterprise framework that helps organizations identify, manage, and reduce cybersecurity risks and aligns strategy, execution, and accountability from the boardroom to the front line.

At the core of effective governance lies a clear division of responsibility: the board provides strategic oversight and works with management to define the organization's risk appetite; management executes those directives through a risk-based program, continuous assessment, and transparent reporting. This dual structure—oversight and execution—ensures accountability, fosters agility, and embeds cyber resilience within enterprise decision-making. Boards leveraging this framework gain not only compliance confidence but also strategic advantage: a trusted, adaptable, and well-governed enterprise capable of pursuing digital innovation without unacceptable risk.

BOARD ACTIVITIES

- **Set the Tone at the Top:** The board establishes cyber risk management as a strategic priority equal to other major risk categories, such as credit, legal, market, and operational risk. Directors must make clear that cybersecurity is integral to business strategy, M&A decisions, and third-party relationships. The risk or audit committee, or other delegated committee should maintain cybersecurity as a standing agenda item, and the board chair reinforces the expectations that cyber resilience is a shared enterprise objective.
- **Approve and Review the Cyber Risk Appetite:** The board works with management to define the organization's cyber risk appetite—the amount and types of risk it is willing to accept in pursuit of its objectives. This appetite should be explicit, quantitative where possible, and expressed in business or financial terms. Directors assess that the appetite statement aligns with strategic priorities, regulatory obligations, and stakeholder expectations. The board periodically reviews the risk appetite in light of emerging threats and business changes.
- **Oversee Resilience and Preparedness:** Directors have a responsibility to assess how management regularly tests and updates incident response, crisis management, and business continuity plans. Leading boards also participate in scenario exercises and tabletop simulations that test decision-making under stress, ensuring lessons learned are implemented. Oversight extends to monitoring key resilience metrics that include time to detect, contain, and recover; percentage of critical vendors assessed; and performance against risk thresholds. The board can also review budgets for redundancy (e.g., backup systems, multi-cloud strategies) and resilience drills, such as tabletop exercises.

- **Clarify the Role of Management in Operational Execution:** While the board governs, management executes. Key management responsibilities include:
  - **Developing and executing strategy:** Led by the CEO, management assesses the strategy and how cyber-risks may impact the success of accomplishing business objectives. This includes translating the board-approved risk appetite into specific controls[1], investments, and operating procedures aligned with business objectives.
  - **Continuous risk assessment:** Maintaining real-time visibility of the cyber threat landscape and assessing internal and third-party exposures using quantitative and scenario-based approaches.
  - **Risk Communication:** Reporting exposures and mitigation progress in business and financial terms to enable board understanding of potential impact.
  - **Cross-Functional Governance:** Integrating cybersecurity into finance, legal, compliance, HR, and business operations so that risk ownership extends beyond IT.
  - **Incident Response and Recovery:** Establishing and testing response protocols; conducting post-incident reviews; and applying lessons learned to strengthen defenses. The board can review management's performance against these responsibilities through dashboards, program reviews, and independent assurance activities. Where gaps are found, directors can probe processes for corrective actions, adequate resourcing, and accountability mechanisms.
  - **Promote Cross-Functional and Continuous Governance:** Cyber risk spans organizational boundaries. The board can support a cross-functional cyber-risk approach that brings together business, risk, compliance, and technology leaders that could include the establishment of a cyber risk committee. This approach can drive enterprise alignment, prioritize investments based on quantified risk, and report routinely to the board committee responsible for cyber oversight.
  - **Evaluate and Refine the Organization's Cyber-Risk Management Framework:** At least annually, the board can commission an evaluation of the cyber governance structure—committee charters, reporting cadence, escalation protocols, and independence of assurance functions—to ensure continued relevance and maturity. External benchmarking or audits can provide an objective view of effectiveness.

SUCCESS INDICATORS

- **Documented Governance Charter:** A formal policy delineates the respective roles of the board, management, and the CISO, supported by committee charters and reporting lines.
- **Quantified Risk Appetite:** A board-approved risk appetite statement defines acceptable cyber risk in measurable, financial terms, integrated into the broader enterprise risk management (ERM) framework.
- **Active Resilience Testing:** Tabletop and crisis simulations are conducted and can involve directors along with senior management, with results tracked to closure.
- **Cross-Functional Engagement:** A cross-functional cyber-risk team or forum meets regularly, and business leaders share accountability for mitigation actions.

- **Evidence of Continuous Cybersecurity Program Improvement:** Metrics such as reduced incident frequency, improved mean time to recovery, and increased control coverage demonstrate program maturity and effectiveness.

Boards that embed an enterprise framework elevate cybersecurity from a reactive technical discipline to a proactive business function. By defining clear governance boundaries, empowering management, and fostering informed oversight, directors ensure that the organization can innovate, compete, and grow with confidence in the face of evolving digital risks. The outcome is an enterprise that not only withstands disruption but also strengthens its market credibility through demonstrable governance maturity and digital trust.

QUESTIONS FOR THE BOARD TO CONSIDER

- What are the top cyber threats facing our industry, and how do our cybersecurity capabilities and maturity compare to peers and established frameworks?
- What validated models and governance processes are in place to quantify, accept, remediate, or transfer cyber risks?
- How does our cybersecurity spending align with our financial risk appetite and the risks we face?
- Is cybersecurity addressed in a cross-functional manner, and how are we assessing this?
- How are leaders across the organization held accountable for their role in the cyber-strategy?

ENDNOTES

1. Leading frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), Center for Internet Security (CIS) Critical Security Controls, the FAIR Standard, ISO/IEC 27000 family of standards, or the PCI Security Standards

PRINCIPLE FIVE

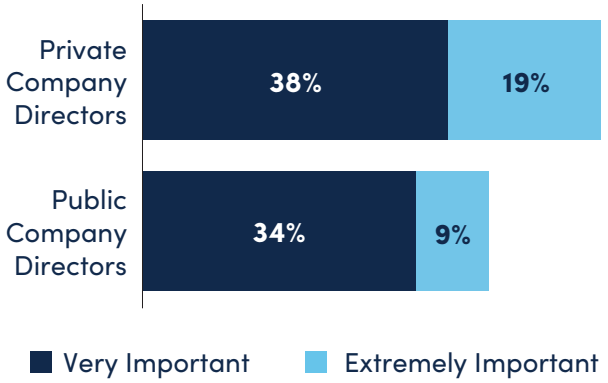
Guide Cybersecurity Risk Measurement and Reporting

Case for Action

Effective board oversight of cyber risk depends on the quality of the information it receives. Directors recognize the impact management's reporting has on their ability to oversee cyber-risk, nearly half (43 percent) of public company directors and 56 percent of private company directors, state improvements in the quality of management's cyber-risk reporting were "very" or "extremely important" in the coming year.

Without clear, consistent, and business-aligned reporting, boards cannot assess whether the organization's cybersecurity posture is adequate, whether resources are appropriately allocated, or whether management's actions align with the enterprise's defined risk appetite.

Directors Focus on Management Cyber-Risk Reporting



Source: 2025 NACD Public Company Board Practices and Oversight Survey, n=158; 2025 NACD Private Company Board Practices and Oversight Survey, n=85

Q: How important is it that your board improves in the following areas related to cyber-risk oversight?

Many boards still receive cybersecurity updates that are overly technical, inconsistent across business units, or disconnected from business objectives. In such cases, directors are left with little ability to gauge risk exposure in financial or operational terms or to fulfill regulatory expectations for disclosure and accountability.

Done effectively, sound cyber risk reporting goes beyond compliance and creates strategic advantage. When boards receive concise, quantitative, and forward-looking reports, they can connect cybersecurity performance to business outcomes, assess trade-offs, and prioritize investments that reduce the most material risks. Over time, such reporting strengthens trust among regulators, shareholders, and customers, reinforcing the organization's reputation for resilience and governance maturity.

BOARD ACTIVITIES

Establish a Standardized Cyber Risk Reporting Structure

The board should direct management to design and maintain structured reporting that ensures consistent, business-relevant communication of cyber risk. Reports should align with the broader enterprise risk management (ERM) process, using the same language, cadence, and metrics used for other forms of material risk.

To enable objective decision-making, the board can encourage the use of standard risk quantification models that translate technical metrics into probable financial loss and likelihood distributions.

A structure for the required content for board and committee reports typically includes:

- Executive summary of current cyber posture and trends
- Top risk scenarios and quantified potential financial impacts
- Risk exposure across common areas such as third-party, supply chain, data, legacy infrastructure and operational technology risks
- Incident response and resilience metrics
- Regulatory compliance status
- Key investment and staffing indicators

Define Reporting Frequency and Escalation Protocols

Cyber risk reporting should occur at least quarterly and immediately following any material incident or significant change in risk exposure. Management and the board can clarify clear formalized escalation criteria—such as thresholds for financial impact, customer exposure, or operational disruption—that trigger special board updates. This enables timely awareness and swift alignment between management and directors when high-impact events occur.

Review Enterprise Cyber Risk Posture

The board's periodic review can begin with an executive-level dashboard summarizing:

- Top risk scenarios with estimated likelihood and impact
- Key threat trends and emerging vulnerabilities
- Current exposure against the board-approved risk appetite
- Progress on major remediation initiatives and strategic milestones
- Year-over-year trends demonstrating improvement or deterioration.

Dashboards should be visual, concise, and comparable across reporting periods and business units. The objective is not to drown the board in data, but to elevate insights for strategic oversight.

Evaluate High-Impact Risk Scenarios

Directors can devote time to analyzing a few critical scenarios that could significantly affect enterprise value—such as ransomware on core systems, compromise of customer data, or failure of a critical vendor. For each, the board may request:

- Quantified exposure in financial terms
- Current control maturity and coverage
- Identified gaps and remediation timelines
- Dependencies across internal systems or external partners

This scenario-based approach allows the board to focus attention on the risks that truly matter while confirming that management's mitigation efforts are prioritized accordingly.

Oversee Incident Reporting and Response Readiness

Boards must receive timely, complete briefings on material cyber incidents. Boards and management teams should align on the escalation protocols, reporting framework, and information that works best for their situation. Common incident reporting practices include:

- Description of the incident and affected systems
- Immediate response actions and containment measures
- Communication strategy and regulatory notifications
- Recovery timelines and business impact
- Lessons learned and actions taken to prevent recurrence.

Boards can also participate in tabletop exercises involving both executives and directors to test response coordination and crisis communication under simulated conditions.

Monitor Regulatory and Compliance Status

Directors should be provided with clear reporting on compliance with applicable regulations, including SEC, NIS-2, DORA, HIPAA, and sector-specific standards. Reports should outline:

- Current compliance status
- Outstanding audit findings or deficiencies
- Plans, budgets, and timelines for remediation

This enables directors to confirm that management is proactively managing regulatory risk rather than reacting to external pressure.

Track Cyber Risk Metrics and KPIs

While directors need not engage with deep technical indicators, they can monitor concise Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs) that demonstrate program maturity and trend direction. Key board focus areas should include whether metrics show improvement, stability, or deterioration over time, and whether the pace of change aligns with strategic risk appetite.

Common Key Risk Indicators can include:

- Quantified risk exposure by business unit
- Number and severity of incidents over time
- Mean time to detect and contain incidents
- Patch cycle compliance rate for critical systems
- Third-party risk concentration and exposure levels
- Percentage of employees completing security training

Assess Investment Adequacy and ROI

The board's fiduciary duty includes ensuring that cybersecurity resources are commensurate with risk. Periodic reviews should compare the cybersecurity budget and staffing to benchmarks, risk reduction results, and business growth. Boards can ask management to demonstrate that investments—especially in automation and AI—yield measurable efficiency gains and exposure reduction.

Foster Transparent and Continuous Dialogue

Cyber risk reporting should be an ongoing conversation, not a one-way presentation. In providing oversight, directors may challenge assumptions, request alternative scenarios, and ask for comparisons across time or industry peers. Open dialogue between the board and management strengthens mutual understanding, reinforces accountability, and fosters a culture of transparency.

SUCCESS INDICATORS

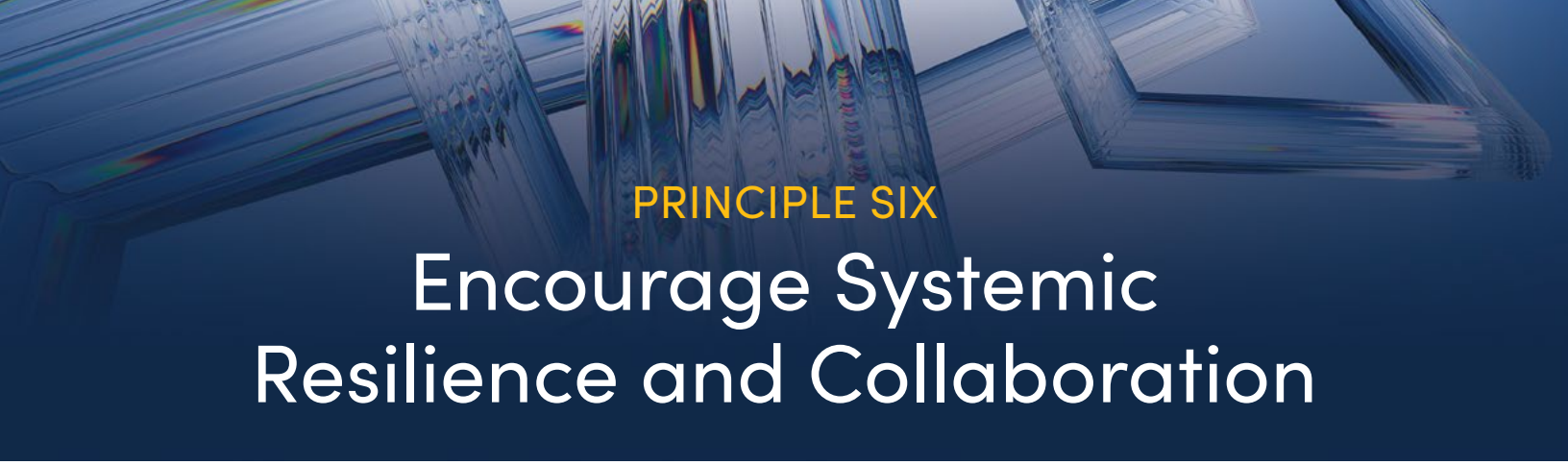
- **Consistent Reporting Cadence:** The board receives structured, standardized cyber risk reports at least quarterly, plus ad-hoc updates anticipating and/or following material incidents.
- **Business-Aligned Dashboards:** Reports present cyber risk in financial and operational terms, not purely technical metrics, with visual summaries aligned to the risk appetite.
- **Scenario-Driven Oversight:** Directors routinely review a defined set of high-impact scenarios with a documented understanding of likelihood, impact, and mitigation progress.
- **Incident Transparency:** All material incidents are reported to the board within defined timeframes, with post-incident reviews tracked to completion.
- **Quantified Exposure Trends:** Risk metrics demonstrate measurable changes—such as reduced expected loss, shorter containment time, or improved control coverage.
- **Regulatory Readiness and Compliance:** Compliance audits confirm readiness for SEC, NIS-2, and DORA reporting, with no major unresolved findings.

- **Investment Effectiveness:** Budget reviews link spending to measurable reductions in risk and improvements in efficiency or resilience.
- **Integrated ERM Alignment:** Cyber metrics and dashboards align seamlessly with the broader enterprise risk reports reviewed by the board.
- **Informed Board Dialogue:** Meeting minutes reflect active questioning/challenging, data-driven debate, and clear direction to management.

Boards that achieve this standard of cybersecurity reporting transform oversight from reactive compliance to strategic leadership. They gain a dynamic view of exposure, enabling them to steer the enterprise toward resilience, competitiveness, and trust. Management, in turn, benefits from informed direction, clearer priorities, and stronger support for investment in controls and innovation. Ultimately, effective cyber risk reporting ensures that directors can fulfill their fiduciary duty with confidence—protecting enterprise value while enabling the pursuit of opportunity in a digital world.

QUESTIONS FOR THE BOARD TO CONSIDER

- What are our most critical assets and business initiatives, what is their estimated financial risk exposure, and what types of financial losses are we measuring (e.g., productivity loss, incident response costs, fines, reputational damage)?
- Do reports include backward-looking results and forward-looking projections that estimate exposure under different threat scenarios?
- Are our cyber dashboards tied directly to the board-approved risk appetite and prioritized by business impact?
- Does management provide a clear, consistent narrative on cyber trends, emerging threat vectors, and how these impact enterprise value? Does our reporting include trendlines across quarters and years to identify emerging patterns, not just point-in-time snapshots?
- Are we receiving reporting that translates technical risks into potential financial exposure, including plausible loss ranges and likelihood?
- How frequently does management test and update its reporting framework for accuracy, completeness, and relevance?
- What are the top systemic risks we track—such as critical vendor failures or cloud dependencies—and how are these reported?
- How does management validate the completeness of incident reporting, including near-misses and unreported low-level events?



PRINCIPLE SIX

Encourage Systemic Resilience and Collaboration

Case for Action

In the current hyper-connected digital economy, cyber risk is not confined within a single organization or threat vector. The architecture of the internet and business ecosystems enables vulnerabilities in one enterprise to cascade into large-scale, systemic failures in a similar way to how systemic risks can impact financial systems and markets. Organizations must appreciate systemic resilience as a core component of organizational security that depends on fostering public-private cooperation, dismantling silos, and promoting active participation in industry-wide and government-inclusive threat intelligence sharing.

Cybersecurity should be governed with an understanding that it is a shared responsibility that extends beyond corporate boundaries. A resilient enterprise requires resilient partners, sectors, and systems. Emerging technologies such as AI and quantum computing further amplify systemic vulnerabilities. These technologies increase the attack surface while tightening interconnectivity, creating new points of failure and escalation.

Collaboration also aligns with growing regulatory expectations and stakeholder demands for responsible governance. Proactively building resilience through partnerships enhances trust, reduces risk exposure, and positions the organization as a leader in cyber maturity. Cybersecurity cannot evolve in isolation; but develops with shared information, collaborative defense, and a commitment to protecting the broader digital environment.

BOARD ACTIVITIES

To fulfill their fiduciary and strategic obligations under this principle, boards can pursue the following core activities — many of which are already in place or emerging in leading organizations — to promote systemic resilience and collaboration:

- **Champion Ecosystem-Wide Risk Awareness:** Boards can request risk assessments that go beyond enterprise boundaries and account for interdependencies with critical third parties, shared infrastructure providers, and industry-specific cyber threats. Some companies are beginning to map their digital supply chain exposures, which boards can leverage as a foundation for broader ecosystem oversight.
- **Engage Ecosystem Partners:** Ensure management is participating in industry forums or ISACs (Information Sharing and Analysis Centers) to share threat intelligence and learn of sector specific threats and risks. Directors can validate management's engagement effectiveness by requesting updates on actionable intelligence gained, information contributed, and how collaboration is enhancing resilience. In less-regulated industries, boards may need to initiate management's participation.
- **Oversee Systemic Resilience Planning:** Boards can expand oversight to include how resilience planning extends to shared

services, upstream and downstream vendors, and systemic weak points (e.g., reliance on a single software supplier) and ensure management is aware of and addressing these risks. Some leading organizations are incorporating systemic risk simulations into board-level tabletop exercises.

- **Foster Peer Governance Networks:** Directors can leverage cross-board peer networks such as NACD chapter roundtables and industry governance groups, sharing insights from these forums among board members and with management and using them to benchmark their organization's cyber governance maturity. Peer exchanges can also drive alignment on sector-wide standards and response expectations.
- **Promote Cyber Defense from an Ecosystem Perspective:** Directors can assess if management has successfully integrated cyber stewardship into their organization's culture. Boards should seek metrics and narratives on how the company is supporting the cyber resilience of customers, suppliers, and the broader digital ecosystem.

SUCCESS INDICATORS

Boards can evaluate their organization's progress in promoting systemic resilience and collaboration by observing the following behaviors, structures, and results:

- **Endorsing Shared Responsibility:** The organization embraces the view that cyber resilience is a shared responsibility. Language in board materials and management reports reflects systemic thinking rather than an inward-only focus.
- **Active Industry Participation:** The company is recognized as a leader or active participant in sector-specific ISACs, cross-sector partnerships, or cyber defense alliances. Management regularly shares intelligence and participates in multi-entity simulations.
- **Collaborative Incident Response Readiness:** Resilience and crisis response planning explicitly incorporate cross-organizational communication and interdependent response protocols. Contracts with third parties include clauses that support joint incident notification and mitigation. Vendor contracts include clear cyber requirements, with audits showing 90 percent and greater compliance.
- **Expanded Risk Visibility:** Board dashboards include metrics on systemic risk exposure, such as concentration of digital dependencies, critical software reliance, and shared vendor relationships, alongside enterprise-specific risks.
- **Regulatory and Governmental Engagement:** The board encourages constructive engagement with public sector agencies, including voluntary information sharing with law enforcement and regulatory bodies. These relationships are maintained such that they can be contacted in the event of an incident. The company participates in national or regional critical infrastructure resilience programs. The company receives positive feedback from regulators or no findings in compliance audits (e.g., CISA, SEC).
- **Enhanced Market Trust and Stakeholder Recognition:** The organization is viewed by customers, partners, and regulators as a responsible ecosystem steward — valued for transparency, proactive cooperation, and its role in elevating collective cybersecurity outcomes.
- **Resilience Metrics:** Tabletop exercises or simulations show improved response times (e.g., < 24 hours to isolate a breach) and recovery capabilities.

QUESTIONS FOR THE BOARD TO CONSIDER

- Do we actively participate in cross-sector cybersecurity organizations? Do we have relationships established with federal and law enforcement agencies?
- Do we actively share cyber risk information with trusted outsiders?
- Do we conduct regular tabletop exercises to test our incident response plan? Do these tabletop exercises include our critical suppliers and partners?
- How effective are our business continuity and disaster recovery plans?
- How resilient are we to third-party cyber incidents, and what mitigation actions are in place to effectively manage this risk?

Cyber-Risk Oversight Principle and Tool Alignment Table

The following table maps the cyber-risk oversight tools to the principles. By aligning these practical resources with the Handbook principles, the toolkit enables boards to implement each principle through actionable and measurable governance practices.

Tool Alignment with Principles	
PRINCIPLE ONE: **Treat Cybersecurity as a Strategic Risk**	▶ **Tool C:** Board Discussion Guide on Adapting to Emerging Technologies ▶ **Tool D:** Board Discussion Guide on Quantum Computing ▶ **Tool E:** Discussion Guide for Board Decisions on AI ▶ **Tool I:** Cybersecurity Considerations During M&A Phases
PRINCIPLE TWO: **Monitor Legal and Disclosure Implications**	▶ **Tool A:** The Board's Role in Ransomware Preparedness and Response ▶ **Tool B:** The Board's Role in Cyber Incident Response ▶ **Tool M:** Cybersecurity Oversight Disclosures – 10 Questions for Boards ▶ **Tool O:** Incident Response and Reporting to the FBI
PRINCIPLE THREE: **Establish Board Oversight Structures and Access to Expertise**	▶ **Tool J:** Building a Relationship with the Chief Information Security Officer (CISO) ▶ **Tool K:** Board-Level Cybersecurity Metrics
PRINCIPLE FOUR: **Oversee an Enterprise Framework for Managing Cyber Risk**	▶ **Tool C:** Board Discussion Guide on Adapting to Emerging Technologies ▶ **Tool D:** Board Discussion Guide on Quantum Computing ▶ **Tool E:** Discussion Guide for Board Decisions on AI ▶ **Tool F:** Overseeing Cloud Services Security ▶ **Tool G:** Overseeing Insider Threats and Human Risk Management ▶ **Tool H:** Board Oversight of Third-Party & Supply Chain Cyber Risk
PRINCIPLE FIVE: **Direct/Guide Cybersecurity Risk Measurement & Reporting**	▶ **Tool K:** Board-Level Cybersecurity Metrics ▶ **Tool L:** Example Cybersecurity Board Reporting ▶ **Tool J:** Building a Relationship Between the Board and Chief Information Security Officer (CISO)
PRINCIPLE SIX: **Encourage Systemic Resilience & Collaboration**	▶ **Tool B:** The Board's Role in Cyber Incident Response ▶ **Tool H:** Board Oversight of Third-Party & Supply Chain Cyber Risk ▶ **Tool M:** Cybersecurity Oversight Disclosures – 10 Questions for Boards ▶ **Tool O:** Incident Response and Reporting to the FBI


TOOLKIT

TOOL A:

The Board's Role in Ransomware Preparedness and Response

Mike Woods, Vice President, Cyber Security, GE Vernova

This tool outlines how directors can structure oversight of ransomware preparedness and response, focusing on risk governance, scenario planning, and decision-making under pressure.

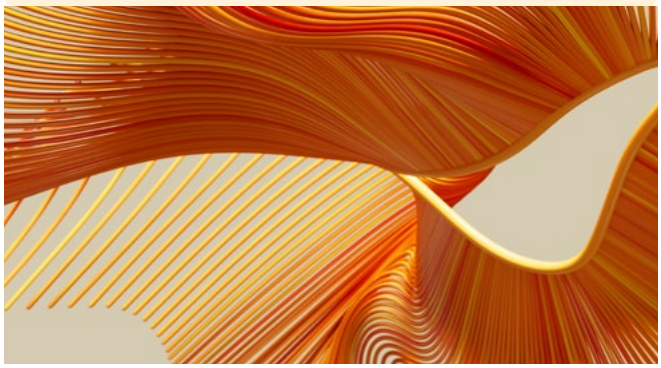
INTRODUCTION

Ransomware has become one of the most disruptive and persistent threats facing businesses. For boards, ransomware is a strategic business risk that can compromise operations, reputation, and financial stability.

Effective oversight of ransomware preparedness and response goes beyond high-level updates, incorporating quantified impact analyses, scenario-tested response plans, and clear decision-making authorities.

Ransomware now threatens life-critical infrastructure

In February 2024, the ALPHV/BlackCat ransomware attack on Change Healthcare disrupted the claims and payment processing systems for 1 in 3 U.S. patients, impacting every hospital nationwide.[1] 74 percent of hospitals reported direct patient care disruption, and many experienced months-long recovery delays and halting essential services.



KEY FOCUS AREAS FOR BOARDS

- Ensure management develops and tests a comprehensive ransomware incident response plan.
- Review risk transfer strategies (e.g., cyber insurance) and how they align with the company's risk appetite and business model.
- Confirm cross-functional involvement in ransomware response, including legal, compliance, communications, and operations.
- Evaluate whether ransomware risks are being quantified using economic and empirical data.
- Establish clear escalation protocols for reporting ransomware incidents to the board.
- Establish relationships with external parties and stakeholders that may be required such as law enforcement, regulators, and customers.

1. Strategic Risk Framing

Request that management present ransomware scenarios as part of the organization's broader enterprise risk management (ERM) framework. This includes stress-testing assumptions about recovery times, operational continuity, and financial losses.

Viewing ransomware through the lens of strategic risk allows the board to evaluate trade-offs between investments in resilience, cyber insurance, and potential downtime costs.

2. Empirical and Economics-Based Assessment
Request quantitative risk models that measure ransomware impacts in dollars and probabilities. This enables informed decisions about whether to invest in preventive technologies, purchase additional insurance coverage, or accept certain residual risks. Questions should focus on whether management uses frameworks for cyber risk quantification (e.g., FAIR model) and whether the data is benchmarked against industry peers.

3. Board Oversight of Incident Response
Ransomware attacks unfold rapidly, leaving little time for ad hoc decision-making. Confirm that a pre-approved ransomware incident response plan is in place and is cross-functional—legal, finance, communications, IT, and operations all play critical roles. The plan should also include pre-negotiated retainers for response services such as digital forensics and incident response (DFIR) services, breach counsel, dark web intelligence services, and ransom negotiators that can enable quick activation in the event of an incident. Consider participating in or observing tabletop exercises that simulate a ransomware event.

4. Decision-Making and Escalation
A central governance question is: Who decides whether to pay a ransom? Confirm that clear escalation thresholds exist, and that they specify whether management or the board is responsible for those decisions. Directors may not make the final call, but they must be briefed on the rationale, legal implications (e.g., OFAC restrictions on payments to sanctioned entities), and alternatives, such as restoring from backups.

5. Resilience and Business Continuity
Probe whether the organization can withstand an extended outage. This involves understanding recovery point objectives (RPOs) and recovery time objectives (RTOs) for critical systems, as well as reliance on cloud providers for rapid restoration. Investments in offline, immutable backups are now considered table stakes.

6. Legal and Disclosure Obligations
Ransomware often triggers regulatory disclosure requirements (e.g., SEC cyber disclosure rules, GDPR breach notification in Europe). Boards must know whether management has a framework for timely reporting and how decisions are documented to demonstrate due diligence.

7. External Relationships and Systemic Risk
Ransomware resilience is not solely internal; supply chains and cloud vendors are frequent attack vectors. Boards should expect reporting on vendor risk assessments, contractual obligations for incident reporting, and participation in industry collaboration bodies (e.g., ISACs, CISA JCDC).

Questions Boards Can Ask Management About Ransomware With Sample Responses

- **Preparedness:** Does management have a tested incident response plan for ransomware, and how often is it updated and exercised? Is there dedicated response, legal, and communications support "on call" via retainers?
  - *Sample Response: Our Incident Response plan has specific scenarios on ransomware and is updated and exercised annually.*
- **Economic Impact:** How do we quantify the financial exposure from ransomware attacks, and how does it affect our enterprise risk appetite?
  - *Sample Response: We employ quantified risk assessments aligned with enterprise risk appetite.*
- **Decision Rights:** Who has the authority to decide whether to pay a ransom, and under what circumstances would that decision be elevated to the board?
  - *Sample Response: Our policy strongly discourages paying ransomware demands, in alignment with US law enforcement guidance and ethical risk practices. However, in a scenario where human safety or existential business survival is at risk, we reserve the right to escalate and consult*

law enforcement and legal counsel before deciding. All payments, if ever considered, require board notification and compliance checks.

- **Resilience:** What redundancies (backups, cloud failover, business continuity plans) are in place to sustain critical operations if systems are locked, and have they been tested?
  - *Sample Response: Our redundancies include regular backups, failover solutions, and comprehensive business continuity plans.*
- **Legal and Disclosure:** What are our regulatory obligations for disclosure of ransomware events, and is the board informed of them in real time?
  - *Sample Response: Internal policies and processes drive how we commit to our disclosure obligations.*
- **Third-Party Risks:** How are we evaluating ransomware vulnerabilities in our supply chain and cloud service providers?
  - *Sample Response: Our contracts contain supplier risk assessments and audit rights that are reviewed by the security team to ensure they remain aligned with the organization's risk appetite.*

FURTHER READING

- CISA Ransomware Guidance and Resources
  https://www.cisa.gov/stopransomware/ransomware-guide
- NIST
  - Cybersecurity Framework
    https://www.nist.gov/cyberframework
  - Incident Response Playbooks
    https://csrc.nist.gov/projects/incident-response
- Treasury Department/OFAC Guidance on Ransomware Payments
  https://ofac.treasury.gov/recent-actions/20210921

ENDNOTES

1. Zack Whittaker, "How the ransomware attack at Change Healthcare went down: A timeline," Tech Crunch, January 27, 2025, https://techcrunch.com/2025/01/27/how-the-ransomware-attack-at-change-healthcare-went-down-a-timeline/.

TOOL B:

The Board's Role in Cyber Incident Response

Mike Woods, Vice President, Cyber Security, GE Vernova

This tool provides a strategic path for boards in overseeing and strengthening an organization's incident response (IR) capabilities over four core pillars.

WHY CYBER INCIDENT RESPONSE MATTERS

In an ever-expanding and hyper-connected digital landscape, cybersecurity incidents are not only likely—they are inevitable. For publicly traded companies and critical infrastructure operators, the impacts of ransomware, data theft, insider threats, cloud service failures, or artificial intelligence (AI) driven cyberattacks extend beyond IT—they touch revenue, brand, compliance, and trust from investors and consumers.

Effective cyber-IR is the cornerstone of organizational resiliency and is based on four core pillars: **governance, preparedness, response, and recovery.**

GOVERNANCE AND OVERSIGHT: THE ROLE OF THE BOARD

Governance begins with clearly assigned ownership of the IR program, typically under a senior executive (e.g., CISO or chief information officer) with cross-functional authority.

The board should

- Review IR plans annually or when they change materially.
- Receive briefings on regulatory obligations, reporting requirements, and potential liabilities from legal counsel.
- Validate that third-party risks are being effectively managed.
- Be informed of emerging threats, including generative AI misuse and autonomous malware.

PREPAREDNESS: BUILDING THE FOUNDATION BEFORE THE CRISIS

Preparedness is the most controllable phase of IR. It includes

- **Clear IR Playbooks:** Scenario-based guides for ransomware, cloud compromise, insider misuse, AI manipulation, and third-party breaches.
- **Asset and Data Inventory:** Knowing where sensitive data resides (e.g., multi-cloud, on-premises, and operational technology environments) as well as any third-party dependencies is critical to containment.
- **Communications Protocols:** Pre-drafted internal/external holding statements, social media monitoring, and spokesperson readiness
- **Tabletop Exercises and Simulations:** Tabletop exercises that occur regularly with realistic risks and threats, such as state-sponsored threat actors, cloud security, third-party and supply chains, as well as emergent AI-generated attacks.
  - Ideally, tabletop exercise scenarios should be relevant to the organization's risk profile and aligned to the types of incidents the organization may face.
  - These scenarios help uncover operational and communication gaps, especially in federated IT and hybrid cloud environments.

- **IR Service Readiness:** An IR plan will also include pre-negotiated retainers for response services such as DFIR services, breach counsel, dark web intelligence services, and ransom negotiators that can enable quick activation in the event of an incident.

RESPONSE AND CONTAINMENT: ACTING UNDER PRESSURE

When a cyber incident strikes, time is the most precious resource. Boards should understand the maturity and agility of their organization's IR program:

- **Rapid Triage:** understanding scope, affected assets, and potential data exposure
- **IR Service Activation:** leveraging and coordinating with response services on retainer
- **Containment and Eradication:** segmenting affected systems, disabling compromised accounts, and isolating infected workloads
- **Legal Coordination:** securing attorney-client privilege, notifying regulators, and engaging with law enforcement
- **Insurance Coordination:** understanding impact of cyber threats and options available with current cyber insurance representatives
- **Business and IT Alignment:** prioritizing systems that support revenue, customers, and operations
- **Third-Party Notification:** coordinated response and disclosure involving cloud providers, vendors, or integrators

Contact and Communication Obligations

In the wake of a significant incident, multiple stakeholders must be contacted promptly, often within legally mandated timeframes:

- **Regulators:** Depending on the scope and jurisdiction, state, federal, and other national entities must be notified.
- **Law Enforcement:** FBI Cyber Division, Cybersecurity, and the Infrastructure Security Agency, local authorities, and if applicable, Interpol or Europol
- **Cyber Insurance Carriers:** Immediate notice is usually required to ensure coverage
- **Cloud and Technology Providers:** Providers such as Amazon Web Services, Microsoft, Google Cloud, and key software service vendors must be engaged to identify shared responsibility actions.
- **Customers and Clients:** Depending on the data affected, organizations may need to notify individuals, businesses, or partners—often within 72 hours.
- **Investors and Analysts:** In the US, public companies must assess materiality and make appropriate 8-K or equivalent disclosures within four days of a determination of materiality.
- **Media and the Public:** A designated spokesperson should manage communications to preserve trust and reduce misinformation.
- **Banks, Credit Bureaus, and Financial Services Partners:** Boards should ensure proactive engagement and relationship building with these stakeholders.
    - Pre-built templates, holding statements, legal review, and designated contacts for each stakeholder group should be part of the IR plan.
    - It is important to remember that information that is known frequently changes during an incident. Boards should ensure they are properly informed and communicate the necessary information as it becomes available.

RECOVERY AND LEARNING: EMERGING STRONGER

Cyber resilience is not just about bouncing back—it is about bouncing forward. Post-incident recovery should go beyond technical restoration. Boards can assess that the outcomes include

- restoration of critical functions (e.g., finance, operations, customer access) before full infrastructure rebuild
- transparent and timely stakeholder communications
- root cause analysis and process review
- updates to playbooks, policies, and employee training based on findings
- changes in architecture or tooling, particularly with AI detection and cloud posture management, if needed

Questions Boards Can Ask About IR and Sample Responses

- Who owns our cyber-IR program?
  - *Sample Response: The program is led by the CISO with joint oversight from legal and risk. A formal IR steering committee meets quarterly.*
- Have we conducted realistic tabletop exercises in the last 12 months?
  - *Sample Response: Yes, our most recent tabletop simulation involved a ransomware attack that impacted cloud infrastructure and required multi-party coordination. A separate scenario focused on the misuse of generative AI to craft convincing spear-phishing emails.*
- How mature are our detection and response capabilities, and does this maturity minimize business impacts of an incident within agreed-upon thresholds?
  - *Sample Response: Our average detection time is under two hours, and containment playbooks target a 24-hour resolution window for our most critical assets.*
- Do we have a board-level escalation process?
  - *Sample Response: Yes, the IR plan includes clear thresholds for when and how to brief the board depending on financial, legal, or reputational impact.*
- What are our disclosure obligations and procedures for regulators, customers, and suppliers?
  - *Sample Response: We track global obligations via legal counsel, including the US Securities and Exchange Commission (SEC) rules on material cyber incidents, state breach notification laws, and GDPR obligations.*
- Are we aligned with our cyber-insurance policy coverage?
  - *Sample Response: Our IR plan aligns with our cyber-insurance policy, including the use of approved vendors and timely notification requirements.*
- Are our backups protected and tested?
  - *Sample Response: Backups are encrypted and stored in isolated cloud environments with quarterly restoration testing. We also conduct readiness testing of backup integrity and immutability.*
- Can we quantify the business impact of cyber scenarios?
  - *Sample Response: Yes, we model potential losses for scenarios such as disruption of cloud services, ransomware, domain takeover, and AI data poisoning using impact matrices and dollar estimates.*

- What lessons have we learned from recent incidents? What lessons were learned from other incidents involving companies of similar size or within our industry?
  - *Sample Response: After a 2024 phishing incident in human resources, we added conditional access and changed onboarding procedures for all cloud software services (SaaS). We also expanded email security filters to detect AI-generated content.*
- How are we preparing our IR plans for emerging threats like AI-driven cyberattacks? How are these scenarios different? Do they create additional exposure and do they require new tools?
  - *Sample Response: We have incorporated AI-related threats into our tabletop exercises, including scenarios involving deepfake phishing and malicious AI-generated code. Our detection tools are being updated to monitor for generative AI misuse, and we are assessing AI-related third-party risks. Governance includes internal guidelines for responsible AI use to limit exposures.*

TOOL C:

Board Discussion Guide on Adapting to Emerging Technologies

JR Williamson, Senior Vice President & Chief Information Security Officer, Leidos
Patrick Haynes, Principal, Technology Consulting—Cybersecurity, Ernst & Young
Robyn Bew, Director, Americas Center for Board Matters, Ernst & Young

The tool presents cybersecurity-related questions the director should consider in discussions within the board, with management, and with other interlocutors regarding emerging technologies and their impact on the organization's strategy.

STRATEGIC IMPACT

High-performing boards address emerging technologies as part of their board agenda, with many often actively seeking technologies with the potential to be disruptive or transformational in their market. They deliberately align the introduction of new technologies with the organization's purpose and values. Strategic decisions for the board include whether to posture the company as an early adopter, to move with the market, or stand fast.

As technology providers race to deliver capabilities to the market, cybersecurity protections in their products and services often fall subordinate to other requirements, exposing their customers and users to unexpected risks. Accordingly, boards should clearly recognize cyber-security requirements of emerging technologies as a core element of the organization's long-term strategy, define the board's role in technology and data oversight, and ensure the board is postured to provide effective technology governance.

Questions Boards Can Consider About Emerging Technologies

- What role does the board have in evaluating the strategic landscape for emerging technologies that can impact our business?
- Do we have the right board composition and organization to provide timely and effective governance and oversight regarding the identification, technical appraisal, business impact, and risk assessment of emerging technologies?
- Does the board have the right talent and experience to effectively govern the introduction of new technologies into our business in a manner that does not compromise our cybersecurity requirements? What are the gaps?
- Do we have sufficient access to information from a variety of independent sources to make informed decisions regarding the cybersecurity impacts/risks of the proposed new technology?
- Are our existing cyber-risk management processes sufficient as disruptive new technologies are introduced into the marketplace? If not, what needs to change?
- What is our cyber-risk appetite toward the adoption of emerging technologies into our business? Is the method of determining our risk appetite adequate in this environment? Does this align with our enterprise risk appetite, threshold, and tolerance?

- Do we need to create a dedicated committee or subcommittee to provide deliberate focus on cybersecurity risks? If so, do we have the right talent composition to be successful?
- Do we have the right people in place on our executive team to effectively and efficiently introduce emerging technology with the right cybersecurity capabilities to support our strategy? Are our CEO, chief information officer, and CISO, capable of successfully overseeing such a project and integrating it with our strategy?
- Is our executive team properly organized to introduce new and emerging technologies with sufficient cybersecurity capabilities to support our business strategy? What are the gaps?
- Does our executive team conduct sufficient competitor analysis and market research to identify the cybersecurity risks and opportunities of emerging technology? Do they deliberately share that information with the board?
- Is our executive team challenging itself by constantly evaluating our strategy against market forces? Does our competitive analysis program include cybersecurity assessments?
- Does the executive team actively maintain relationships with trusted and recognized technical experts and organizations to gather independent assessments of emerging technologies?
- Is the executive team an eager and competent participant in modeling and testing cybersecurity and other risk assessment planning assumptions before introducing emerging technology into the business?
- Are we bold enough to test something that may fail, learn from it, and keep trying?
- Do we understand the risks and opportunities to our business and how quantum technology impacts our business strategy and ultimately its long-term growth and viability?
- Are we able to effectively interpret and assess management and third-party presentations on quantum technologies, as well as their answers to our questions?

Questions Boards Can Ask Management About Emerging Technologies

- How are you surveying the strategic landscape to identify and assess emerging technologies that could potentially disrupt our industry?
- What are the emerging technologies you have identified as most critical to our business and why?
- What are our competitors doing with these new technologies, and how is it impacting them?
- How does the introduction of this technology affect our business strategy and position in the market? Our supporting cybersecurity strategy? Do we need to rethink our strategy?
- Have we broadened our aperture to evaluate various competing technologies to identify the best contenders and minimize our risk exposure?
- How are our investments in new emerging technologies aligned with our strategy and business forecasts? What are the trade-offs? What changes will we make to fund the new emerging technology initiative?
- What are the cybersecurity and other risks to our organization if we adopt this technology? What is the risk if we do not? How do you know? What data do you have to measure the risk?

- How capable are the cybersecurity protections of this new product or service in today's contentious cyber environment? How do you know?
- What are our cybersecurity requirements when contemplating the acquisition of emerging technologies?
- What third-party cybersecurity risks are associated with this new technology?
- Has the emergent technology been subject to an independent third-party penetration and red teaming test protocol? What were the results?
- How can we effectively and efficiently mitigate cybersecurity risks associated with emergent technologies?
- Do you have a future-proof technology road map that incorporates this emerging technology and includes cybersecurity capabilities? Is the roadmap congruent with our investment strategy?
- Does this emerging technology enable us to reduce costs by retiring legacy systems and processes? If so, which ones, and what are the savings?
- What effect will the introduction of practical quantum technologies into the marketplace have on our business? What is the impact on our business if a quantum computer can decrypt all our data?
- What means of modeling and simulation are there to assess our current strategy's effectiveness in a post-quantum world?
- How prepared are we to thrive in a quantum-enabled marketplace?
- What is our risk exposure if all our data can be decrypted by quantum computers? How much will it cost in time and resources to implement post-quantum cryptography?
- What decisions do we need to make to remain competitive in a quantum-enabled marketplace?

TOOL D:

Board Discussion Guide on Quantum Computing

Gregory Touhill, Director, CERT Division, Software Engineering Institute, Carnegie Mellon University
Larry Clinton, President and CEO, Internet Security Alliance

This tool presents an overview of anticipated impacts and applications of quantum technologies, and provides suggested cybersecurity-related questions for board members to discuss with management as the technology matures and transitions into the marketplace.

INTRODUCTION

Quantum computing presents both opportunity and existential risk. While its commercial applications remain nascent, its potential to break widely used cryptographic systems—including RSA and Elliptic-Curve Cryptography (ECC)—makes it one of the most significant emerging risks in cybersecurity governance. Quantum threats are not hypothetical; adversaries may already be "harvesting now, decrypting later," collecting encrypted data with the expectation of unlocking it once quantum capability matures.

Quantum computing research is advancing quickly; with many experts forecasting "Q-Day," that will likely arrive before the end of this decade. Q-Day refers to the day when quantum computers will be able to use multistate quantum bits or "qubits" to break the encryption algorithms at the heart of digital security technologies currently used to secure the internet and digital devices.

KEY TERMS

Post-Quantum Cryptography (PQC) and Post-Quantum Encryption (PQE) are closely related, often overlapping terms in the context of securing data against future quantum computer attacks. PQC refers to the creation of the mathematical algorithms, methods, and cryptographic techniques themselves (e.g. lattice-based or code-based algorithmic structures). PQE is a broader term that specifically emphasizes the application of these new quantum-resistant algorithms to encrypt data (i.e. the post-quantum resistant solution or technology.)

The National Institute for Standards and Technology (NIST) has published approved PQC standards and selected algorithms.[1] Boards should be aware that these select algorithms have been "proofed" to be post-quantum resilient, eliminating the need for most organizations to launch their own PQC creation programs. Organizations should move quickly to update the encryption of their data using PQE.

PREPARING FOR Q-DAY

The pertinent question for board members is not when will quantum computing arrive; it is rather will your organization be ready?

When Q-Day arrives, critical data—including intellectual property, banking information, personally identifiable information, personal health information, and other "secrets"—will be susceptible to decryption by quantum computers, making all current information vulnerable to exposure. The degree of quantum readiness will also likely become an audit/compliance issue.

Many experts are advising that boards should be planning for the coming quantum transition now. However, current research suggests that is not generally the case. A 2026 Bain & Company analysis found that 90 percent of companies are unprepared for quantum security threats, even though many executives expect such threats to materialize within the next five years.[2]

A 2025 Information Systems Audit and Control Association (ISACA) study found that only 4 percent of organizations have a defined quantum strategy despite growing concern about the durability of existing encryption.[3] Similarly, a survey conducted by the Trusted Computing Group found that 91 percent of businesses lack a roadmap to protect against quantum threats.[4]

Boards cannot afford to ignore quantum risk until the technology is fully realized. Transitioning a reasonably sophisticated IT system to accommodate quantum impacts could take years and substantial expense. It may cost several million dollars just to do the review and discovery of needed alterations and twice that much for planning and testing. Doing this transition retrospectively may cost many times these amounts.

Delayed preparation for Q-Day substantially increase costs, but could also make adequate and timely transition impractical due to the lack of qualified technical staff. Multiple studies indicate that quantum risk is widely recognized, yet workforce planning for post-quantum transition has barely begun.[5,6] In practice, post-quantum cryptography has moved beyond a research challenge to an execution challenge—and execution depends on people.[7]

Should a cryptographically relevant quantum computer arrive within the next few years, most organizations (including critical infrastructure providers), would be unable to transition in time—not for lack of awareness, but because the workforce needed to do so does not yet exist at scale.

THE QUANTUM OPPORTUNITY

There are several major points of consensus regarding the advent of quantum computing:

- Q-Day will occur in the foreseeable future, likely by or in the 2030s.[8]
- Q-Day will compromise almost all the current encryption/security systems. Implementing plans for quantum transition may require substantial time and expense—delayed planning and implementation will substantially increase these costs.
- There is an extreme shortage of qualified and trained people to properly implement quantum translon. Once Q-Day comes, these shortages will be magnified—there will likely not be enough for everyone who needs to do the transition.
- Organizations that have adequately prepared for the quantum transition prior to Q-Day will likely have a substantial—possibly unassailable—market advantage over competitors.

High-performing boards will prioritize preparing their organization to migrate to post-quantum cryptography at the top of their agendas to ensure their organizations will be ready to thrive in a post-quantum marketplace.

The following provides practical guidance for directors to operationalize the handbook principles in addressing quantum risk.

Principle 1: Treat Cybersecurity as a Strategic Risk

- Integrate quantum risk into the enterprise risk register and strategic technology roadmap.
- Ensure the board understands the potential disruption to customer trust, intellectual property, and national security obligations.

Principle 2: Monitor Legal and Disclosure Implications

- Oversee alignment with regulatory requirements such as NIST's post-quantum cryptography (PQC) standards and anticipated disclosure expectations.
- Ensure the organization discloses material risks related to quantum vulnerabilities in financial filings if applicable.

Principle 3: Establish Board Oversight Structures and Access to Expertise

- Confirm that at least one director or advisor has expertise in emerging technologies, including quantum.
- Assign oversight of quantum risk to an innovation, risk, or technology committee.

Principle 4: Adopt an Enterprise Framework for Managing Cyber-Risk

- Require quantification of the potential impact of quantum-enabled decryption on sensitive data.
- Assess the cost-benefit trade-offs of early adoption of PQC versus delayed transition.

Principle 5: Guide Cybersecurity Risk Measurement and Reporting

- Ensure management has assessed risk exposure to the organization arising from quantum computing technologies.
- Assess and receive updates on management's progress in migrating to PQC.

Principle 6: Encourage Systemic Resilience and Collaboration

- Encourage management to participate in cross-industry collaboration on PQC adoption.
- Require evidence of alignment with government and industry standards bodies (e.g., National Institute of Standards and Technology [NIST] and ETSI).

Questions the Board Can Ask to Assess Their Quantum Understanding

- Do we thoroughly understand the implications of this potentially market disrupting technology and its impacts on our business and its strategy?
- Does our board have the right literacy to address quantum technology issues? What is this quantum literacy, and is it sufficient to meet our needs?
- Do we need to add a board member with deeper expertise on this topic to our board or bring in outside consultants?
- Do we have adequate and diverse sources of technical expertise to present the board with sufficient knowledge to make informed decisions on this topic?
- Do we have the right people in place on our executive team to lead the incorporation of quantum technology to support our strategy? Is our CEO capable of successfully overseeing such a project and integrating it with our strategy?
- Do we understand the risks and opportunities to our business and how quantum technology impacts our business strategy and ultimately its long-term growth and viability?
- Are we able to effectively interpret and assess management and third-party presentations on quantum technologies, as well as their answers to our questions?

Questions the Board Can Ask Management to Assess Quantum Readiness

- How prepared are we to thrive in a quantum-enabled marketplace?
- What is our risk exposure if all our data can be decrypted by quantum computers? How much will it cost in time and resources to implement PQC?
- What decisions do we need to make to remain competitive in a quantum-enabled marketplace?
- How will the introduction of quantum technologies support our existing strategy or force a change in strategy? How can we use quantum technology to improve our business?
- How will our risk posture be affected by the introduction of quantum technologies?
- What are our competitors doing in the quantum technology space?

- Who are the leaders in quantum technology? Who is delivering the best results? How do you know?
- Who has the best quantum technology adoption roadmap?
- Do we have the right talent to be successful?
- What effect will the introduction of practical quantum technologies into the marketplace have on our business? What is the impact on our business if a quantum computer can decrypt all our data?
- What means of modeling and simulation are there to assess our current strategy's effectiveness in a post-quantum world?

FURTHER READING

- National Security Agency (NSA) Post-Quantum Cybersecurity Resources
  https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/

ENDNOTES

1. National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography," Computer Security Resource Center, www.nist.gov, effective December 15, 2025, https://csrc.nist.gov/projects/post-quantum-cryptography.
2. Nicole Kobie, "90% of Companies Are Woefully Unprepared for Quantum Security Threats—Analysts Say They Need to Get a Move On," ITPro, January 22, 2026. https://www.itpro.com/security/90-percent-of-companies-are-woefully-unprepared-for-quantum-security-threats-analysts-say-they-need-to-get-a-move-on.
3. ISACA, "Quantum Computing's Rapid Rise Is a Risk to Cybersecurity and Business Stability," Press release, April 28, 2025. https://www.isaca.org/about-us/newsroom/press-releases/2025/quantum-computings-rapid-rise-is-a-risk-to-cybersecurity-and-business-stability.
4. Trusted Computing Group, "91% of Businesses Do Not Have a Roadmap in Place to Protect Against Quantum Threats, Finds New Industry Survey," December 2, 2025. https://trustedcomputinggroup.org/91-of-businesses-do-not-have-a-roadmap-in-place-to-protect-against-quantum-threats-finds-new-industry-survey/
5. Kobie, 2026.
6. ISACA, 2025.
7. ISC2, "2025 ISC2 Cybersecurity Workforce Study," Cybersecurity Certifications and Continuing Education, December 4, 2025. https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study
8. Tran Duc Le and Phuc Hao Do and Truong Duy Dinh and Van Dai Pham, "Are Enterprises Ready for Quantum-Safe Cybersecurity," arXiv, (2025): https://doi.org/10.48550/arXiv.2509.01731

TOOL E:

Discussion Guide for Board Decisions on AI

Gregory Touhill, Director, CERT Division, Software Engineering Institute, Carnegie Mellon University

This tool provides information to help directors successfully understand rapidly evolving AI capabilities, the risks and opportunities of AI investments, and provide the leadership, governance, and oversight that will enable the business to thrive in the age of AI.

INTRODUCTION

Artificial intelligence (AI) capabilities are rapidly transforming the business landscape and our societal institutions. Because there are many types of AI capabilities and various use cases for the incorporation of AI across business units, many organizations may invest in multiple AI capabilities tuned for specific business functions and outcomes.

KEY TERMS

- **Agentic AI:** An autonomous AI system of algorithms that can independently observe the environment and proactively act with minimal human interaction (e.g., a system that sees that your connecting flight is canceled, automatically rebooks you to another flight, and notifies you and others, such as your car rental or hotel, of the change).
- **Machine Learning (ML):** Algorithms that learn from data to find patterns (e.g., your streaming TV service, favorite streaming music platform, or online retail sales platform use ML to predict what you would next like to see, hear, or buy and make tailored recommendations for you).
- **Deep Learning:** A subset of ML, deep learning uses a layered structure of algorithms called a neural network to intake raw data, identify patterns, and develop an output (e.g., your virtual assistant, your phone's facial recognition unlock feature, self-driving cars, and other various products use deep learning to translate vast troves of data into meaningful outputs).
- **Natural Language Processing (NLP):** Algorithms that enable computers to understand human language.
- **Computer Vision:** Algorithms that allow AI to interpret and understand visual information (e.g., facial recognition).
- **Generative AI:** Systems that create new content, including images, video, conversations, stories, music, data synthesis, and more (e.g., ChatGPT, Gemini, etc.).
- **Expert systems:** Algorithms that mimic human decision-making for specific functions (e.g., decision trees).
- **Shadow AI:** Unauthorized use of AI tools, applications, or features by employees without the knowledge, approval, and oversight of the company, creating significant risks like data leakage, compliance failures, and security vulnerabilities.

Questions Boards Can Ask About AI

General

- How can AI transform our business and how do we measure success?
- How are our market competitors using AI and what risks are presented by their efforts?
- What are the risks of incorporating AI into our business model? What are the risks if we don't?
- Does the board have the right expertise to make informed decisions regarding incorporating AI capabilities into the organization?

The Board's Ability to Oversee AI

- Do we need to restructure the board to effectively manage our extended cyber risk due to our current and anticipated use of AI?
- Should our AI/cyber-risk be considered as a separate matter for board discussion and action, or should it be integrated as part of our overall operations? Or both?
- What are the governance implications of the use of AI and related policies and controls?

Oversight and Management of AI

- Does our corporate structure ensure management is balancing the potential benefits of AI with potential risks?
- Is the board considering AI risks simultaneously with economic benefits from AI use cases?
- Who are our riskiest vendors, and how is our organization managing that risk?

Regulation of AI

- Have we explored the operational and regulatory challenges related to the proposed use of AI?
- Are policies and procedures in place to address AI risks from third-party software and other supply-chain issues?
- Have we reviewed our insurance policies for AI-related risks and use cases? Are we covered if our AI system fails or acts in a manner that results in an adverse effect external to our organization?

AI Risks and Cybersecurity

- Have we identified AI-related risks across all business functions (e.g., customer experience, user experience, intellectual property, operations, support functions, brand & reputation, etc.)?
- What is the state of our data governance program? Who is responsible for data governance? Do we have a complete inventory of our data, where it resides, appropriate security and access controls?
- What are the governance implications of the use of AI and related policies and controls?
- What is our third-party risk associated with AI?
- Who are our riskiest vendors, and how is our organization managing that risk?
- What actions are we taking to prevent Shadow IT and unauthorized AI use? How are we measuring success?
- What measures are we employing to protect our organizations and its employees from AI-enabled advanced social engineering attacks such as realistic deepfakes (e.g., audio, video, and text) and sophisticated, personalized targeting campaigns? How are we testing the efficacy of these measures?
- Are our cyber defenses capable of detecting and appropriately acting in response to an AI-enabled cyber attack? How do we know? How do we test their effectiveness?

- Are our AI systems hardened against cyber attacks, such as prompt injections, data poisoning, and "jailbreaking" (i.e., manipulating the AI system to bypass its security controls and guardrails to generate content it was designed to withhold)? How is the system tested, certified, and continuously monitored?
- How are we managing AI "identity" (i.e., ensuring AI agents are only granted protected access to authorized data sources, and nothing else)? How is this tested for performance and security effectiveness?
- What is our plan if our AI system fails or is unavailable? What is the impact on business? What is our plan B? How do we test our plan for effectiveness?
- What does the current AI-related threat environment look like, and where are we vulnerable? How are we addressing the risk?

TOOL F:

Overseeing Cloud Services Security

Mike Woods, Vice President, Cyber Security, GE Vernova

This tool provides boards with a structured approach to governance of cloud use, focusing on oversight of vendor selection, shared responsibility, and measurable risk management.

INTRODUCTION

As organizations migrate operations and data to the cloud and leverage cloud infrastructure as a critical component of companies' AI strategies, directors must ensure that cloud service management is subject to rigorous oversight. Cloud services reduce costs and increase scalability, but also introduce new dependencies, regulatory exposure, and systemic vulnerabilities. Cloud adoption is now mainstream, but with it comes concentrated risk.

Large enterprises are getting serious about adopting the cloud. They aspire to have roughly 60 percent of their environment in the cloud by 2025, but *The 2024 Cost of a Data Breach Report* discovered that 40 percent of all data breaches involved data distributed across multiple environments, meaning that these best-laid plans often fail in the cloud environment.[1] A small number of large providers (Amazon Web Services, Microsoft Azure, Google Cloud) host critical services for thousands of companies, raising systemic questions that boards must address. Boards that fail to scrutinize provider dependencies may face hidden vulnerabilities in resilience, compliance, and cost predictability. By reviewing empirical risk assessments, establishing a clear division of responsibilities, and maintaining strong internal expertise, directors can turn cloud adoption from a source of exposure into a strategic advantage.

KEY FOCUS AREAS FOR BOARDS

1. **Ensure that cloud migration decisions align with the overall business strategy.** Questions directors can ask to ensure strategic alignment include: Does cloud adoption create new competitive advantages? Does it expose us to the risk of dependence on vendors that could alter their terms unilaterally?
2. **Review economic analysis of cloud risks (e.g., downtime costs, contract lock-in, overrun pricing).** Boards can request empirical assessments of cloud reliance evaluated against the organization's risk appetite and business objectives.
   - What is the potential financial impact, including direct losses and indirect costs, of cloud downtime on our organization?
   - How do cloud pricing models affect long-term cost predictability?
   - What is the probability and financial impact of a provider data breach?

   Quantifying these factors ensures directors can evaluate whether investments in redundancy, hybrid architectures, or insurance are justified.
3. **Confirm that roles and responsibilities between the provider and the customer are clearly defined.** Many cloud incidents stem from misunderstandings of who is

responsible for security controls. Boards should insist that management documents and communicates this division of responsibility, especially in multi-cloud or hybrid environments. Contracts should explicitly outline liability, indemnification, and notification requirements.

4. **Conduct rigorous due diligence before providers are selected.** This includes audits, compliance certifications (ISO 27001, SOC 2), and continuous monitoring. Boards must ask how management tracks vendor compliance over time and how third-party risks flow into the organization's enterprise risk reporting.
5. **Probe the organization's exit strategy and contingency plans.** Questions directors can ask to ensure strategic alignment include:
   - Do we have a plan if the provider suffers a breach or prolonged outage?
   - Are backups stored in an alternative environment, and have they been tested?
   - Has management tested its ability to shift workloads to another provider in a crisis?
6. **Establish processes for monitoring compliance with legal, contractual, and data protection obligations.** Cloud arrangements may cross jurisdictions with different disclosure or privacy requirements. Boards should be briefed on how the company maintains compliance with regulations such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), or the new Securities and Exchange Commission cyber disclosure rules.
7. **Ensure management adopts a formal cloud governance framework aligned with ERM.** Adopting a formal framework integrates cloud security risks within ERM, ensuring they are visible, governed, and strictly aligned with the organization's established risk appetite.
8. **Oversee whether sufficient in-house cyber expertise exists to evaluate cloud risk and contracts.** Boards should evaluate whether the organization possesses the internal expertise to evaluate cloud risks, vet third-party cloud risks, and negotiate contracts that protect the company. The board should also maintain literacy about cloud risks and technologies aligned to their strategic and operational importance.

Questions the Board Can Ask Management About Cloud Security with Sample Responses

- **Shared Responsibility:** How does management ensure we fully understand our responsibilities versus those of the cloud provider for security and compliance?
  - *Sample Response: Roles are clarified through contracts or documented agreements across providers.*
- **Vendor Oversight:** What due diligence is performed before selecting or renewing contracts with cloud providers, and how do we monitor their performance?
  - *Sample Response: Our due diligence includes security assessments, compliance checks, and performance benchmarks; ongoing monitoring via service-level agreements (SLAs) and regular audits.*
- **Economic Risk:** How is the financial impact of cloud downtime, service disruption, or data breaches quantified for the board?
  - *Sample Response: Financial impact is quantified through risk assessments, incident response (IR) cost analyses, and insurance coverage reviews.*
- **Expertise:** Do we have adequate internal expertise at the board and management levels to interpret cloud contracts and evaluate technical risks?

- *Sample Response: Our expertise is ensured through dedicated roles, training programs, and consultations with external experts.*

- **Resilience:** What are our contingency plans if a cloud provider experiences a prolonged outage or cyber incident?
  - *Sample Response: Contingency plans include multi-cloud strategies, disaster recovery plans, and readiness drills.*
- **Compliance:** How does management ensure cloud services meet our regulatory, disclosure, and data protection obligations across jurisdictions?
  - *Sample Response: We ensure compliance through audits, legal reviews, and alignment of cloud services with the global regulatory landscape.*
- **Exit Strategy:** What provisions are in place to avoid vendor lock-in and ensure data portability in the event we change providers? Have we tested this plan?
  - *Sample Response: Provisions include data portability clauses in our vendor contracts and standardized data formats and testing required.*

FURTHER READING

- Cloud Security Alliance Guidelines
  https://cloudsecurityalliance.org/research/guidance#

ENDNOTES

1. IBM Corporation, Cost of a Data Breach Report 2024 (Armonk, NY: IBM Corporation, 2024), 29, https://wp.table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf.

TOOL G:

Overseeing Insider Threats and Human Risk Management

Niall Brennan, VP, Strategic Security Engagement, SAP Global Security

This tool defines insider threat, outlines categories of insider incidents, and types of insider threat actors. Further, it outlines the board's responsibilities with specific actions they can perform to ensure executive management is adequately addressing insider threats.

INTRODUCTION

Human risks and insider threats represent a significant yet often underestimated cyber-risk to organizations. As more work has shifted to remote locations following the COVID-19 pandemic, the prospect of insider compromise has increased.[1] While external cyber-attacks often dominate headlines and governance discussions, insider cyber threats can be equally, if not more, damaging because insiders have access to and knowledge of internal systems and processes. Insider threat incidents are also not always malicious but can arise from negligence or intentional bypassing security policies where, for example, they cause too much friction in employees' workflows.

Precisely because the delivery system for this threat involves leveraging the legitimate access of "trusted insiders" (employees, contractors, vendors, and others) to an organization's network, systems, and data, it can be harder to detect than other threats in which the forensic indicators of compromise are more immediate and obvious. Further, as agentic AI systems are introduced into corporate workflows and systems, management and oversight of this risk area must evolve.

WHAT IS AN INSIDER THREAT?

CISA defines an insider threat as the potential for an individual or individuals with authorized access, or understanding of an organization to harm that organization.[2] This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities.

As with other forms of unauthorized breaches, insider threat incidents involve unauthorized access to an organization's assets or causing harm to an organization for the following purposes:

- sabotage
- fraud
- intellectual property theft
- espionage
- loss of share value
- loss of consumer confidence

Types of Insider Threat Actors

Insider attacks are generally carried out through the following types of actors:

- careless or negligent employees
- disgruntled or departing employees
- criminally "planted" insiders
- third-party partners (e.g., contractors with privileged access)

Common Indicators of Insider Threats

There are certain warning signs companies can watch for to identify an insider threat, including:

- Poor performance appraisals
- Voicing disagreement with policies
- Disagreements with coworkers
- Financial distress
- Unexplained financial gain
- Odd working hours and behaviors
- Unusual overseas travel
- Leaving the company

THE ROLE OF THE BOARD IN INSIDER RISK MITIGATION

The board plays a crucial role in the organization's management of insider risk, ensuring that oversight policies and procedures are in place to protect organizational assets against potential threats. These include understanding the risks, implementing robust controls, fostering a culture of cybersecurity awareness, continuous improvement of the program, and establishing reporting and communication protocols.

1. **Understanding and Oversight**
    - The board should have a clear understanding of the organization's human risks and insider threat landscape, including the types of risks, vulnerabilities, and potential impacts.
        - Include briefings at regular intervals from both internal and external subject matter experts on the evolving dynamics of the insider threat. These briefings can include tailored reports on insider risk-management activities, including annual assessments, specific security incidents, and control effectiveness based on metrics and evaluations.
        - Review annual assessments prepared by operational security management, which address, among other items identified below, the organization's specific risk and vulnerability profile vis-à-vis the insider threat. If necessary, these assessments should be supplemented with advisories at designated intervals, subject to shifting dynamics.
        - Review that management has the necessary resources and expertise to effectively manage insider risks.
2. **Implementing Controls**
    - The committee responsible for cyber-risk oversight should ensure management addresses insider risks, such as ensuring the implementation of access controls, data protection measures, and other security controls to prevent and detect insider threats.
        - The annual assessment should detail the full range of security controls and data protection measures focused on preventing insider breaches, complete with metrics regarding relevant detections, events, incidents, and interventions.
    - Ensure strong policies and procedures are in place to guide and incentivize employee behavior to prevent insider threats.
        - These policies should require employees to follow specific procedures with regard to handling sensitive data and assets.
        - Policies should mandate reporting certain defined infractions of security policies.
3. **Fostering a Security Culture**
    - The board should promote a culture of cybersecurity vigilance and awareness and ensure management embodies and communicates this throughout the organization.
        - The board should ensure that cybersecurity awareness training, such as online and in-person training, education, and communication programs, that help employees recognize and report suspicious activity is being performed while reviewing whether the training is effective in reducing poor security behaviors by employees.

- The board should evaluate whether there is sufficient collaboration and coordination between the CISO and chief human resources officer (CHRO) and other C-suite executives in conducting training and promoting cybersecurity awareness across the organization.
- All board members should practice strong personal security to further promote a strong security culture, reduce their own risk profile, and set the proper "tone at the top."

4. **Continuous Improvement**
   - The board should review and oversee whether the organization's human and insider risk-management program keeps pace with evolving threats and vulnerabilities.
     - Boards should monitor whether management is effectively applying lessons learned from past insider threat incidents, and the program demonstrates improvement over time.

Questions Boards Can Ask about Insider Threats and Human Risk

- What is our probable loss exposure related to the insider threat scenarios?
- What are the most effective controls, and which ones should be prioritized?
- Boards can follow up with more detailed questions regarding the organization's practices to defend against insider threats:
  - Does the organization have a documented insider threat mitigation plan with clearly designated oversight, management, and reporting responsibilities?
  - Who are the appropriate stakeholders to involve in the insider threat mitigation plan within the organization—information security, physical security, general counsel, human resources, corporate investigations, privacy, etc.?
- How does the organization measure the effectiveness of its insider threat mitigation plan? Does it periodically test the plan with internal assets and external parties to validate its effectiveness?
  - Does its insider threat mitigation plan maintain procedures to properly document incidents or insider threat activity?
  - Does it maintain metrics to identify and analyze patterns of insider threat activity to assist with reducing vulnerability?
- Does the organization have adequate programs in place to sensitize employees to insider risks and train them to detect, report, and mitigate potential incidents?
  - Do we have a security awareness program in place? Are we tracking metrics of this program to identify progress or problem areas?
  - Is there a disciplinary or continuing education framework for employees failing tests? Does it show improvement in employee behavior?

ENDNOTES

1. C. David Hylender, Philippe Langlois, Alex Pinto, Suzanne Widup, "Verizon 2024 Data Breach Investigations Report," (Verizon Business, 2024), www.verizon.com/dbir
2. IBM Corporation, Cost of a Data Breach Report 2024 (Armonk, NY: IBM Corporation, 2024), 29, https://wp.table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf.

TOOL H:

Board Oversight of Third-Party and Supply Chain Cyber Risk

Kris Lovejoy, Global Security & Resiliency Practice Leader, Kyndryl

This tool provides questions directors can ask to ensure that key components of third-party and supply chain risk management are being managed effectively.

INTRODUCTION

While third-party technology and services are essential for business, they introduce significant and escalating risks that can impact profitability and reputation.

This threat is accelerating and expanding. According to Verizon's 2025 Data Breach Investigations Report, compared to 2024 data "the percentage of breaches where a third party was involved doubled, going from 15% to 30%."[1] Adversaries are increasingly targeting everything from major software vendors to foundational open-source tools, as seen in the 2024 XZ-utils backdoor incident.[2]

A board's oversight must now extend beyond the company's walls to its third- and fourth-party dependencies. This expanded responsibility is underscored by new SEC disclosure rules requiring boards to report on their governance of third-party cyber risk.

Questions Boards Can Ask Management About Third-Party and Supply Chain Cyber-Risks

Governance and Strategy — Who Owns This?

- **Objective:** Third-party risk is treated as a core enterprise risk, not a siloed issue, with clear accountability.
  - Is there a centralized function or a designated executive who owns this risk across the enterprise, and how does the board receive clear assurance of their effectiveness?
  - How is management assessing the impact of new technologies like AI in this risk area?
  - How well is our third-party risk management program integrated into our overall enterprise risk management program?
  - Do we need to make additional investments into third-party risk management, and are these investments aligned to our business objectives?

Risk Management and Due Diligence — Do We Know Our Exposure?

- **Objective:** A structured process is in place to identify, prioritize, and mitigate risks based on business impact.
  - How do we classify vendors based on the criticality of their service and their data access, rather than just on contract size?
  - Can management confidently identify our most critical dependencies, including key fourth parties, which could put us at risk?
  - What is our strategy for managing risks from new and emerging supply chain dependencies, such as open-source software and the use of AI components?

Resilience and Response — Are We Prepared to Fail?

- **Objective:** The organization can withstand and recover from a related incident.
  - Are clear cybersecurity standards and responsibilities defined in our contracts, and more importantly, are they enforceable?
  - What are the limits of our liability and insurance coverage for a third-party incident, and are they adequate?
  - Have we conducted realistic simulations that specifically model a failure or disruption from one of our most critical third parties?

Real-World Examples of Third-Party and Supply Chain Security Failures

SNOWFLAKE

Timeline: 2024

Description: A cybercrime campaign where attackers used stolen credentials to breach hundreds of company accounts hosted on the Snowflake cloud data platform. The attackers specifically targeted accounts that were not protected with multi-factor authentication (MFA).

Lesson: This incident highlights a failure in managing a third-party relationship under the cloud's shared responsibility model. While the vendor platform was not breached, the customer's failure to implement basic controls on that platform led to a catastrophic breach. Ensure management is accountable not just for vetting vendors, but for securing the company's own configurations within those third-party services.

MOVEIT

Timeline: 2023-Ongoing

Description: A single vulnerability in a popular secure file transfer software product was exploited by a ransomware group, leading to a cascading data breach affecting thousands of organizations globally.

Lesson: This is a textbook example of systemic software supply chain risk. A flaw in one widely used tool can create a catastrophic, industry-spanning event, underscoring the need for a robust inventory of sensitive data handled by third-party applications.

KASEYA

Timeline: 2021

Description: A ransomware attack on a major IT management firm's software product had a cascading impact, disrupting nearly 1,500 downstream businesses.

Lesson: This demonstrates immense "concentration risk" in the software supply chain. Question management on dependencies related to widely used software to understand the potential for systemic disruption.

FURTHER READING

- **National Institute of Standards and Technology (NIST) Special Publication 800-161: Cybersecurity Supply Chain Risk Management Practices**
  https://csrc.nist.gov/pubs/sp/800/161/r1/final
  - This is the foundational U.S. government framework for C-SCRM. It provides comprehensive guidance to organizations on identifying, assessing, and mitigating supply chain risks. It is considered the gold standard for building a formal program.
- **European Union Agency for Cybersecurity (ENISA) Threat Landscape for Supply Chain Attacks**
  https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
  - This report provides a crucial European perspective on the threat landscape. It maps and studies supply chain attacks, analyzes attacker techniques, and offers mitigation recommendations tailored to the EU's regulatory environment.

ENDNOTES

1. C. David Hylender, Philippe Langlois, Alex Pinto, Suzanne Widup, "Verizon 2025 Data Breach Investigations Report," (Verizon Business, 2025), 11, verizon.com/dbir.
2. Jai Vijayan, "Attacker Social-Engineered Backdoor Code Into XZ Utils," Dark Reading, April 24, 2024, https://www.darkreading.com/application-security/attacker-social-engineered-backdoor-code-into-xz-utils.

TOOL I:

Cybersecurity Considerations During M&A Phases

John Hauser, Cyber Due Diligence Leader, Parthenon Americas Transaction Support, Ernst & Young

This tool reviews cybersecurity risks at key stages of a merger or acquisition transaction and provides suggested questions for board members to discuss with management at each stage.

INTRODUCTION

Cybersecurity remains a core business challenge for most corporate entities. Mergers and acquisitions (M&A) only increase that risk. An intentional process for understanding and mitigating cyber risk throughout the transaction lifecycle will significantly reduce that risk and enable a successful inorganic growth strategy.

THE MULTI-FACETED AND STRATEGIC NATURE OF M&A RISK

Cyber risk is pronounced during M&A because of several factors:

1. **Increased Leverage for Cyber Threat Actors:** Entities that study cyber threat actor behavior know that M&A transactions are favorite targets for hackers. M&A draw attention to companies from investors, regulators, and the public, making them vulnerable to publicly disclosed cyber-attacks, which create negative publicity. An FBI advisory warned that "The FBI assesses that ransomware actors are very likely using significant financial events, such as mergers and acquisitions, to target and leverage victim companies for ransomware infections." The FBI found that ransomware actors would threaten to release nonpublic information to negatively affect the stock valuation.[1]
2. **Increased Opportunity for Hackers:** Hackers will often infiltrate the acquired company's network first, using the transition to expand their attack to the acquiring company to exploit and damage both. This occurred as early as 2013, when an attack on a major retailer captured millions of customers' credit cards. In a hotel chain breach, the personal information of hundreds of millions of customers was stolen. Both of those incidents resulted in multi-year class action litigation and settlements of hundreds of millions of dollars.
3. **Increased Attack Surface and Unexpected Security Issues That Require Additional Investment:** The acquirer takes ownership of the acquired entity's environment (and all cybersecurity weaknesses and vulnerabilities) at a time when there is business pressure to quickly connect and integrate systems.
4. **Regulatory and Compliance Risk:** Every developed nation now has regulatory standards for protecting personal information, with some regimes like the General Data Protection Regulation in Europe carrying potential monetary penalties of four percent of global annual revenue. In addition, security regulations are becoming increasingly common worldwide,

especially in critical infrastructure sectors. Acquiring companies assume an increased compliance risk for companies that process personal information, are critical nodes in systems like payment processing, or provide services essential to the economy.

SUCCESSFUL RISK MITIGATION THROUGHOUT THE TRANSACTION LIFECYCLE

Best practices in each phase of the transaction lifecycle can significantly mitigate all the risks described above.

1. **Due Diligence Phase**
    - **Considerations:** Proper due diligence by an experienced team can uncover significant security and compliance gaps, provide a high-level estimate of investment required for compliance and security, provide insights into the sufficiency of cyber insurance coverage, and reduce the likelihood of major surprises in later stages. To accomplish this, the diligence team should have a deep understanding of cybersecurity best practices, regulatory requirements, and the nature of corporate transactions, and be able to respond to assistance requests on very short notice.
    - **Leading Practices:** A robust methodology will include both traditional due diligence practices, such as documents and interview requests, and technical testing to obtain irrefutable data. This technical component is important because even the most forthcoming security teams of acquired companies may miss hidden or undiscovered risks across the enterprise. Another practice is to incorporate remediation costs into the overall transaction cost to avoid additional funding requests by IT and security teams after the transaction when these funds are more difficult to obtain.
2. **Integration Phase**
    - **Considerations**: Integration is a period when both business-related synergies can be realized. Cybersecurity risks increase during integration due to increased access among the two companies, and the reality that any incidents will be managed by two teams that have never worked together.
    - **Leading Practices:** Strong governance of integration-related activities (such as granting access to IT systems) needs to be in place, and the cybersecurity team needs a seat at the table throughout the process. Network connectivity should be carefully designed and monitored, and responses to incidents should be rehearsed, enhancing cooperation and reducing reaction and decision time. Acquiring companies need to have a clear vision for what a combined entity looks like, including necessary human resources, technology, policies, and budget. This will both reduce security risk and optimize costs. The combined security organization should be able to manage any new security and compliance risks created by the acquisition.
3. **Divestitures**
    - **Considerations:** Divestitures create their own set of cybersecurity risks. Critical information like intellectual property needs to be protected. The cybersecurity team must create two new teams and manage the disruption that naturally follows. The "Remainco" team will likely need to provide cybersecurity services to "Spinco," which will need to be defined contractually in a transition services agreement (TSA) and successfully managed. "Remainco" will need to stand up a security team for a new organization and plan to exit TSA services as soon as practical.

- **Leading Practices:** Managing all the aspects of a divestiture is a significant burden, and the security team will need to staff the effort appropriately. The security team needs to be tightly integrated with the other divestiture workstreams to inform team leaders about security requirements and keep up with significant transaction milestones. Creating a high-level but clear vision of the Remainco and Spinco security teams will help minimize rework during the transaction and set both new organizations up for success.

4. **Sell-Side Readiness**

   - **Considerations:** Managing cybersecurity properly during the sell-side process is a way to prevent unexpected value erosion. Acquiring companies will naturally want to understand what risks and costs they are assuming, so preparation of an honest but persuasive narrative will reassure acquiring companies that cybersecurity is not a factor in the decision to move forward.

   - **Leading Practices:** Cybersecurity teams can make inexpensive investments in their program to increase security and address buyer concerns. Examples include remediating vulnerabilities in software, updating insurance coverage, and rehearsing to respond to a cyber incident. Teams can also prepare a thoughtful narrative on their program's strengths and weaknesses. Most acquiring companies expect some incidents will have occurred but will expect to see lessons learned and what action was taken to strengthen the cybersecurity program. Acquiring companies more easily accept gaps in security best practices if the seller is aware of them and develops a realistic plan to address them.

Questions Boards Can Ask Management About M&A Cybersecurity Considerations

- How will this transaction change our overall cyber and privacy risk, and what is our plan to mitigate that risk?
- How are we preparing to protect ourselves against the increased risk of threat actor interest if we move forward with this transaction?
- What is our approach to understanding cyber risk and protecting ourselves before we sign?
- Have we incorporated the costs of additional cybersecurity controls or remediation into the transaction cost structure?
- How are we planning to monitor the cybersecurity programs of our acquisitions to ensure they are mitigating cyber risk?
- How are we planning to effectively respond to intrusion incidents in our acquisitions?
- (For integrations) How will we capture synergies as we build a combined cybersecurity team?
- (For divestitures) How will we mitigate dyssynergies as we split our cybersecurity team?

ENDNOTES

1. Federal Bureau of Investigation, "Ransomware Actors Use Significant Financial Events and Stock Valuation to Facilitate Targeting and Extortion of Victims," *FBI Private Industry Notification*, PIN Number 20211101-001, (November 1, 2021), https://www.cisa.gov/sites/default/files/publications/PIN_202111101.pdf.

TOOL J:

Building a Relationship Between the Board and Chief Information Security Officer (CISO)

JR Williamson, Senior Vice President & Chief Information Security Officer, Leidos

This tool outlines how boards can strengthen relationships with cyber-risk leaders to promote strategic integration, resiliency, transparency, accountability, and trust.

INTRODUCTION

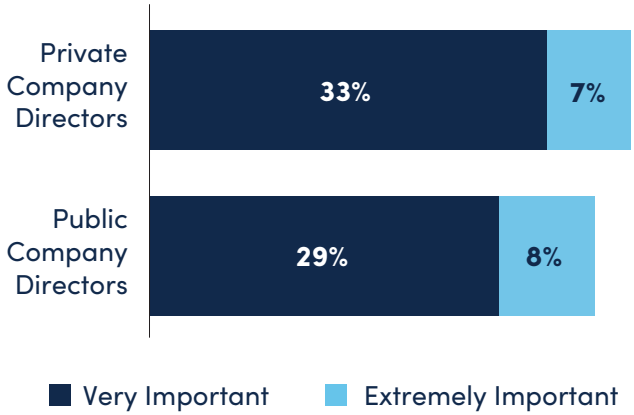
Boards cannot oversee cyber risk effectively if they only interact with the CISO during annual presentations or after a crisis has occurred. Sustained, structured engagement with the CISO (or the equivalent person who is accountable for cybersecurity for the corporation) helps directors view cybersecurity as an enterprise-wide strategic concern rather than a technical sidebar.

The CISO's rise to the C-suite comes with more engagement with the boardroom, an audience with the CEO, and the power to make strategic decisions for the business. The CISO is a critical executive role that should receive board-level coaching and development to signal that cybersecurity is a strategic business priority and not just an operational cost.

While many directors acknowledge a positive relationship with their CISO, there remains room for improvement. The NACD 2025 Board Practices and Oversight Survey reveals that 37 percent of public company directors and 40 percent of private company directors say it is "very" or "extremely important" to improve the board – CISO relationship. Maintaining a healthy relationship is an important aspect of improving cyber-risk reporting, aligning cybersecurity to strategic business objectives, fostering transparent communication, and promoting a strong cyber-risk aware culture.

Strong board–management relationships in cybersecurity are not about frequency of meetings alone; they are about trust, shared language, and consistent integration of cyber issues into strategic discussions.

Directors are Focused on the Board-CISO Relationship



Source: 2025 NACD Public Company Board Practices and Oversight Survey, n=154; 2025 NACD Private Company Board Practices and Oversight Survey, n=84

Q: How important is it that your board improves in the following areas related to cyber-risk oversight?

1. Cybersecurity as Strategic Risk

Boards should push for reporting from the CISO that uses **business metrics** (e.g., potential revenue loss, downtime costs, regulatory penalties) rather than purely technical jargon. Directors should approach cyber risk conversations as they would financial or operational reviews: what are the strategic exposures, what is the economic impact, and how does this risk align with business objectives?

2. Board Operations

Boards should ensure their governance practices and structures for engaging the CISO and receiving cyber-risk reporting are fit for purpose.

- Establish regular, non-crisis communication channels between the board and CISO.
- Review how the board agenda and committee structures support ongoing cyber engagement.
- Support a culture of open dialogue so that issues are escalated early rather than hidden.
- Monitor CISO engagement in the broader industry as both a contributor and a learner.

3. Systemic Resilience and Collaboration

Cyber resilience depends on coordination across the enterprise and with external partners. Encourage management to include the cyber-risk team in enterprise-wide resilience exercises (e.g., supply chain disruptions, operational continuity planning). They should also ask how the organization collaborates with industry and cross-sector peers, ISACs, and regulators to address systemic cyber threats.

4. Board–CISO Relationship

Boards should cultivate direct, recurring interactions with the CISO or equivalent executive. Best practices include:

- Scheduling cyber as a standing agenda item for relevant committees.
- Holding periodic deep-dive sessions focused on specific risks such as ransomware, AI, or cloud security.
- Encouraging informal dialogue outside of scheduled meetings to build trust.
- Encouraging development of new skills for the CISO beyond cybersecurity and risk management.

5. Transparency and Culture

If the cyber risk team feels pressure to deliver only good news, boards will be blind to systemic weaknesses. Reinforce that the board values transparency, and that escalation of problems will not be punished, but used constructively. Questions should focus on what is not being reported and how near-misses are used to improve processes.

6. Integration into Enterprise Risk Management

Cyber reports should not be isolated from other risk areas. Boards should require that cyber risk metrics be presented alongside financial, operational, and strategic risk dashboards. This integration enables directors to see how cyber exposures affect overall business objectives.

7. Building Expertise at the Board Level

Even with strong reporting, boards must have sufficient baseline literacy to interpret what they hear. Boards can develop this expertise and competence through training, appointing cyber-experienced members, or retaining independent advisors. Without it, relationships risk becoming performative and circular rather than substantive.

8. Collaboration Across Business Units

The board should ask how the cyber risk team works with legal (regulatory compliance), operations (business continuity), finance (quantifying losses), and HR (training employees) and whether the CISO participates in strategic discussions and decision making with other senior leadership. Further, boards should also review whether the current positioning of the cybersecurity team within the organization and the CISO's reporting line remain fit for purpose.

Questions Boards Can Ask to Strengthen Relationships With Cyber-Risk Leaders

- **Engagement:** How frequently does the CISO (or equivalent) brief the board, and is this engagement focused on strategic risk, not just technical details?
- **Integration:** How is cyber-risk reporting aligned with financial, operational, and strategic risk reporting?
- **Resource Adequacy:** Does the CISO have the necessary resources?
- **Transparency:** Does management encourage an environment where cyber incidents, near-misses, and vulnerabilities are reported promptly without fear of blame so that residual risk can be appropriately addressed? Does the CISO have a direct reporting line to the board or is cyber-risk reporting filtered through a CIO or other senior leader?
- **Evaluation:** How do we assess the capability of our CISO/equivalent? What is the succession planning for CISO skills?
- **Collaboration:** How does the cyber-risk team interact with other functions (e.g., finance, contracts, legal, compliance, technology, supply chain, and operations), and how are those interactions reported to the board? How well is the CISO and their team integrated with industry and customer/partner/supplier/government organizations to help inform their cyber-risk understanding? What is the relationship between the CISO/equivalent and the CIO/CTO/Chief Data/AI officers?
- **Escalation:** What thresholds trigger direct communication between the CISO and the board?
- **Board Expertise:** Does the board have enough cyber knowledge to interpret reporting and ask the right questions, or should it supplement with external advisors, a director with expertise, and/or supplemental training?
- **Resilience:** How is the organization using insights from the CISO to inform broader resilience strategies across supply chains, partners, and industry? How are emerging cyber threats factored into strategic planning across the corporation?

FURTHER READING

- CISA Cybersecurity Performance Goals
  https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
- NIST Cybersecurity Framework (governance and communications guidance)
  https://www.nist.gov/cyberframework
- World Economic Forum, Principles for Board Governance of Cyber Risk
  https://www.weforum.org/publications/principles-for-board-governance-of-cyber-risk/

ENDNOTES

1. NACD, "Survey Analysis: Cybersecurity Oversight," 2025 NACD Public Company Board Practices and Oversight Survey, July 28, 2025, https://www.nacdonline.org/all-governance/governance-resources/governance-surveys/surveys-benchmarking/2025-public-company-board-practices--oversight-survey/2025-board-practices-oversight-cybersecurity/.

TOOL K:

Board-Level Cybersecurity Metrics

JR Williamson, Senior Vice President & Chief Information Security Officer
Michael Higgins, Vice President & Chief Information Security Officer, L3Harris
Nick Sanna, President, SAFE Security

This tool outlines how directors can leverage key cybersecurity metrics to evaluate organizational performance, benchmark against industry practices, and fulfill their fiduciary duties.

INTRODUCTION

Boards rely on metrics to guide their strategic and oversight responsibilities across all forms of enterprise risk—including cybersecurity, market, credit, and operational risk. Cyber-risk metrics, when framed appropriately by management, allow directors to assess the effectiveness of cybersecurity programs and ensure alignment with broader business objectives.

While operational metrics may offer valuable insights, the board's focus should remain on strategic indicators that reflect the company's overall approach to cyber risk.

It is management's responsibility to translate technical cybersecurity data into business-relevant terms that enable informed board-level discussions. The following metrics and questions—organized into five key categories—provide a framework for ensuring that meaningful, actionable cyber-risk metrics are presented to the board. The level of depth should be tailored to the organization's size, maturity, and risk profile.

Questions the Board Can Ask Management About Cybersecurity Metrics

1. What is the Threat Environment We Face?

Boards should expect management to regularly brief them on the evolving threat landscape and how it impacts the organization and its peers. Insightful questions include

- What are the top cyber threats currently facing our industry?
- How many cyber incidents have we experienced in the last reporting period?
- How significant have these threats been to peer organizations?
- To what extent are any emerging threats—such as ransomware trends, zero-day attacks, or AI-driven exploits—impacting our business performance?
- Can we measure how mature and effective our threat intelligence capabilities are, and how they compare to peers?

2. What is Our Cyber Loss Exposure in Economic Terms?

Cyber-risk oversight increasingly demands a clear understanding of potential financial losses. Boards and regulators expect management to quantify cyber risk

in economic terms, using credible models. Questions to consider include

- What are our most critical assets ("crown jewels"), and can we measure the level of cyber risk they carry?
- What are the top cyber risks we face, expressed in terms of probable frequency and financial impact?
- What cyber risk quantification model are we using? Has it been independently validated?
- What types of loss are we measuring and reporting on (e.g., productivity loss, incident response costs, fines, reputational damage)?
- What is our cyber risk appetite for key risk scenarios, expressed in financial terms? How are we tracking against this target?
- How are we determining if our current cybersecurity spending is properly aligned with the threats we face and our defined risk appetite?

3. What is Our Cyber Risk Profile?

Boards should be briefed on the maturity and effectiveness of the cybersecurity program through validated assessments and benchmarking. Directors might ask

- How mature is our cyber risk management program, as assessed by an independent third party?
- How do we perform against established frameworks such as NIST CSF, CMMC, or CIS Controls? Are we comfortable with the rate that we are improving?
- What are our key control effectiveness metrics, and how do they compare to industry standards?
- How are we tracking control improvements to remain within our risk appetite?
- What is our external vulnerability rating, and how do we compare to industry benchmarks?
- What were the key findings from recent penetration testing conducted by external providers?

4. What is Our Supply Chain Exposure?

As organizations increase reliance on third-party vendors—especially in the context of digital transformation and AI adoption—the board must assess risks across the supply chain. Relevant questions include

- Which third-party vendors present the greatest cyber risk to our organization?
- What is the estimated likelihood and potential impact of a breach involving these vendors?
- Do we have a measure of how resilient we are to third-party cyber incidents?
- What mitigation actions can we take internally, and what should we require from vendors to reduce this risk? How do we measure their effectiveness?
- Should we consider alternative vendors that better align with our cyber risk tolerance?
- Are there systemic risk scenarios in which a single vendor dominates the industry and creates a potential concentration risk—and where we should consider introducing a redundant or alternative provider?

5. Are We Making the Right Business and Operational Decisions?

Directors must ensure that cyber risk is a core consideration in strategic initiatives, including digital transformation, product innovation, AI adoption, and M&A. Key questions include

- What is our estimated cyber loss exposure associated with major business initiatives?
- What governance processes should we use to measure if our cyber risk acceptance, remediation, and transfer are consistent with our risk appetite?
- How are we measuring which cyber risks should be addressed through internal controls? How does our cyber insurance

protect the organization from residual risk beyond the internal controls?

- How much cyber insurance do we carry? Does it adequately cover our current risk landscape?
- What is the return on investment of our cybersecurity initiatives and overall program?
- Which controls are delivering the greatest risk reduction per dollar invested? Which are underperforming or redundant?

By asking these targeted questions and insisting on clear, business-aligned metrics, boards can elevate their oversight of cyber risk to the same level as other forms of enterprise risk. The board's partnership with management on these issues is essential to building organizational resilience and maintaining stakeholder trust.

TOOL L:

Example Cybersecurity Board Reporting

Gregory Touhill, Director, CERT Division, Software Engineering Institute, Carnegie Mellon University

This tool provides examples of foundational practices and metrics boards may leverage to determine the soundness of cyber-risk oversight during regularly scheduled cybersecurity briefings. It provides suggested cyber risk-related questions for board members to discuss with senior management.

INTRODUCTION

Cyber-risk oversight is a set of activities designed to ensure that realized risks are kept within tolerable levels and do not endanger the operational resilience of the corporation. The board's role is to challenge management to identify the right balance between effort/expense and outcomes with the understanding that it is constantly moving and changing.

It's important to remember that cyber risk cannot be managed to zero risk. High-performing boards understand this fact and strive to reduce the likelihood and severity of disruptive cyber events, rather than eliminate them entirely. Focusing on the "critical few" issues aligned with strategic business objectives improves clarity of analysis and aids decision-making.

CYBER-RISK OVERSIGHT AREAS

1. Purpose and Cadence of Cyber-Risk Reports

Boards want a clear view of **risk**, **readiness**, and **response**. Report types can include:

REPORT TYPE	TRIGGER	FORMAT	OBJECTIVE
Cyber-Risk Brief (standing agenda item)	Every board meeting	Two-page executive memo + dashboard	Trend analysis, resource needs
Material-Incident Update	Within 24 hours of the determination of materiality (aligns with SEC Item 106)	One-page incident sheet + follow-up call	Facts, impact, containment, disclosure steps
Deep-Dive Session	Quarterly	Thirty-minute workshop	Strategy, emerging threats, and budget alignment

2. Key Focus Areas for Boards

- **Cyber Risk Posture at a Glance**
  Heat-map of top five enterprise risks (likelihood vs. Impact) mapped to business objectives. If possible, quantify their business impact on these objectives and include scenarios.

- **Key Metrics (Quarter-on-Quarter Trend)**
  Industry standard metrics used to assess due care and due diligence in the effectiveness and management of cyber risk controls. Boards should track these metrics and their trends over time to assess performance.

CATEGORY	EXAMPLE METRICS (TARGET)	WHY IT MATTERS
Exposure	Percent critical assets with Multi-Factor Authentication (MFA)(> 98%)	Attack-surface reduction
Resilience	Mean time-to-detect (MTTD) and mean time-to-recover (MTTR)	Operational continuity
Hygiene	Critical vulnerabilities > 30 days old (< 5%)	Patch discipline
Third Party	Vendors with cybersecurity SLAs (> 90%) Vendors with current SOC 2 Type2 (> 90%)	Supply-chain assurance
Culture	Phish click rate (< 2%)	Human firewall strength
Data Security	Percent of sensitive data (PII/PHI/financial) classified and inventoried (> 95%) Percent of third-party data processors with current security assessments (> 90%)	Visibility drives down risk Third-party data-flow risk management

- **Significant Events Since Last Report**
  For each incident ≥ "Medium" severity or above a defined expected impact threshold:
  - what happened (attack vector, timeline, affected systems)
  - business impact (financial, operational, reputational, legal)
  - containment and recovery status (completed/in progress)
  - root cause and lessons learned (process or control gaps)
  - regulatory filings (e.g., SEC 8-K, CIRCIA 72-hour, state breach laws)

- **Compliance and Assurance Snapshot**
  - status vs. compliance obligations (NIST CSF 2.0, ISO 27001, CMMC, HIPAA/PCI/etc.)
  - audit findings, penetration test results, cyber insurance posture

- **Forward-Looking Plan and Investment Needs**
  - roadmap of priority initiatives for next two quarters (and associated metrics)
  - budget requests are tied to quantified risk reduction

- **Industry Best Practices**
  - comparison of corporate cyber-risk controls to industry peers
  - industry trends in cyber-risk management (e.g., introduction of new technical or procedural controls)
- **Emerging Threats**
  - introduction of emerging threats to the business, potential impact and risks, and proposed actions to address anticipated risks (with timelines and associated metrics)

Questions Boards Can Ask to Assess Their Cyber-Risk Board Reports

- Do the risk reports allow the board to comprehensively understand the sources (both internal and external) of cyber risk?
- Do the risk reports show if cyber risks are within established limits of organizational risk appetite and risk tolerance?
- Have the full implications (e.g., life safety, revenue, and reputation) of realized cyber risks been analyzed and quantified?
- Is the board being presented with timely, accurate, and relevant metrics and appraisals of cyber risk?
- Are we able to effectively interpret and assess management and third-party presentations on cyber risk, as well as their answers to our questions?
- Do we have adequate and diverse sources of technical expertise to present the board with sufficient knowledge to make informed decisions on this topic?

Questions Boards Can Ask Management About the Cybersecurity Program

- Are corporate strategy and cyber-risk management practices aligned? How are areas of potential misalignment identified and analyzed?
- Do you have access to the quantity and quality of resources necessary to manage cyber risk effectively?
- Are we keeping pace with the threat environment? How does this compare with our competitors?
- Do we have a program of independent third-party testing and evaluations of cyber control activities and functions?
- Which models/frameworks/standards of practices are informing our cyber-risk management practices? How were these selected?
- Have the potential sources and consequences of cyber incidents been examined, and specific business impacts determined?
- Are we striking an appropriate balance in our cyber practices to manage both conditions (e.g., defend) and consequences (e.g., recover)?
- Do we have justifiable and quantifiable confidence in the efficiency of cyber-risk management practices? If so, how was this determined?
- Do we have adequate visibility and authority to measure conformance with requirements in third-party relationships (e.g., public cloud service providers)?
- How are critical cybersecurity/cyber-risk management skills cultivated and kept contemporary?
- How does the introduction of emerging sophisticated technologies (e.g., agentic AI and quantum computing) alter our cyber risk roadmap and strategy?

TOOL M:

Cybersecurity Oversight Disclosures – 10 Questions for Boards

Robyn Bew, Director, Americas Center for Board Matters, Ernst & Young
Patrick Hynes, Principal, Technology Consulting – Cybersecurity, Ernst & Young

This tool provides questions for directors to consider in preparing a proxy statement or other disclosures related to the board's oversight of cybersecurity.

INTRODUCTION

Cybersecurity remains front and center on corporate agendas, as risks and regulatory requirements both continue to proliferate, and AI introduces new dimensions to the threat landscape. Business leaders recognize that a strong cybersecurity posture can help build customer and stakeholder trust and strengthen competitive positioning: in a 2025 survey, no less than 85 percent of CEOs said they view cybersecurity as a critical component to achieving business growth.[1]

Investors and other stakeholders are paying attention and seeking more information on how boards and company leaders oversee and manage cyber-risks.[2] BlackRock, the world's largest asset manager, stated, "[We believe] that data security is a material issue for more and more companies and regularly [engage] boards and management teams regarding the oversight and management of data privacy and security, crisis preparedness and response as well as related company disclosures."[3]

The SEC's rules on cybersecurity disclosures, which became effective in 2023, include several components related to board oversight, such as where oversight responsibilities are allocated and the process by which the board is informed about cyber risks.[4] EY's Center for Board Matters has tracked large-cap companies' proxy statement disclosures related to cybersecurity oversight for several years. Beyond the now-required disclosures, we continue to see companies and boards disclosing additional information about their cybersecurity oversight activities on a voluntary basis. A few themes stand out:

- **Audit committees are still the main focus for cybersecurity oversight**, with 78 percent of large-cap companies disclosing that cybersecurity oversight is housed there.
- **Cyber expertise is a sought-after boardroom skill.** While the exact definition of "expertise" differs, 74 percent of companies included cybersecurity skills in at least one board member's biography, up from 46 percent who disclosed this information in 2019.
- **A majority of companies are engaging in cyber-preparedness exercises**, with 58 percent reporting the use of simulations, tabletop exercises, or other tests, as compared to just 3 percent of companies that shared this in their proxies in 2019.

Increases in voluntary disclosures indicate companies are responding to demand for cybersecurity oversight information from investors and stakeholders, who see it as a vital area to the firm's business strategy and risk profile. Figure 1 contains more detailed findings from our large-cap company analysis.

Questions Boards Can Ask About Cybersecurity Disclosures

Use these ten questions to inform boardroom discussions about enhancing cybersecurity communications to investors and other stakeholders:

1. Do we understand the priorities of our company's major investors and other key stakeholders (suppliers, customers, employees, regulators, etc.) related to cybersecurity, data privacy, the impact of AI on cybersecurity, and other key technology risk and strategy issues?
2. How is the company using disclosures to effectively communicate the rigor of our cybersecurity risk management program, and related board oversight activities, to investors and other stakeholders?
3. How do we describe which board committee (or committees) have responsibility for oversight of cybersecurity matters? How do we describe how the full board is involved in cybersecurity oversight, in addition to the activities of key committees?
4. Is cybersecurity included in our board skills matrix, or other description of skills resident on the board? Do we identify one or more directors as having cybersecurity expertise, and what is the criteria by which the board defines such expertise? How do professional cybersecurity experience, credentials, or other knowledge appear in directors' biographies?
5. Do we disclose any education board members are receiving on cybersecurity topics, including certifications, briefings from our external advisors, law enforcement, or other third-party experts?
6. How do we describe how the board and/or key committees receive information from management about cybersecurity matters? How do we describe how the board and/or key committees consider cybersecurity matters as part of their deliberations on strategy, financial oversight, and enterprise risk management?
7. How does the prominence and/or specificity of cybersecurity risk factors compare between our current enterprise risk assessments and our quarterly and annual reports?
8. How do we describe cybersecurity risk management activities, including
    a. Policies and procedures
    b. Response planning, disaster recovery, or business continuity
    c. Simulations and tabletop exercises related to cyberattacks or breaches
    d. Education and training efforts
    e. Information sharing with industry peers, law enforcement, etc.
    f. Use of an external independent advisor to support management and/or attest to cybersecurity assessment findings
9. How do our disclosures on board cybersecurity oversight compare to those of our competitors and industry peers?
10. How effective are our cybersecurity-oversight disclosures in balancing the need for confidentiality against the need and opportunity to demonstrate rigorous, structured oversight to stakeholders?

Figure 1. Selected Fortune 100 company cybersecurity oversight disclosures, 2019–2025

The following data is excerpted from EY's analysis of the 80 companies on the 2025 Fortune 100 list that filed Form 10-Ks and proxy statements for 2019 through July 31, 2025.[2] The data shows the shift in voluntary disclosures related to boards' cyber-risk oversight practices from 2019 to 2025. Please refer to the article for the full data set.

TOPIC	DISCLOSURE	2025	2019
Board-level committee oversight	Disclosed that at least one board-level committee was charged with oversight of cybersecurity matters*	96%	81%
	Disclosed that the audit committee oversees cybersecurity matters	78%	62%
Director's skills and expertise	Cybersecurity is disclosed as an area of expertise sought on the board or cited in at least one director biography	86%	53%
Management reporting to the board	Provided insights into management reporting to the board and/or committee(s) overseeing cybersecurity matters	100%	57%
	Identified at least one management role providing cybersecurity insights to the board (e.g., the CISO or CIO)	89%	27%
	Included language about the frequency of management reporting to the board or committee	99%	44%
Response preparation	Disclosed alignment with external framework or standard**	73%	4%
	Referenced response readiness, such as planning, disaster recovery, or business continuity considerations	99%	59%
Education and training	Disclosed use of education and training efforts to mitigate cybersecurity risk	86%	25%
Use of an external advisor	Disclosed use of an external independent advisor	99%	14%

* Percentages are based on total disclosures for companies. Some companies designate cybersecurity oversight to more than one board-level committee.

** Some companies disclose that they seek to align with more than one external framework or standard. Such frameworks or standards cover different scopes and may not cover all aspects of the enterprise; some include external certification or attestation. Other frameworks or standards include Payment Card Industry Data Security Standards, Health Information Trust Alliance, System and Organization Controls 1 and 2, and more.

ENDNOTES

1. Gartner, "Gartner Survey Finds 85% of CEOs Say Cybersecurity is Critical for Business Growth," press release, April 22, 2025, https://www.gartner.com/en/newsroom/press-releases/2025-04-22-gartner-survey-finds-85-percent-of-ceos-say-cybersecurity-is-critical-for-business-growth.
2. Pat Niemann, Barton Edgerton, Alison Nashed, "Cyber and AI oversight disclosures: what companies shared in 2025," www.ey.com, October 14, 2025, https://www.ey.com/en_us/board-matters/cyber-disclosure-trends.
3. John McKinley, Gaia Mazzucchelli, Eddy Gan, Tanya Levy-Odom, Giovanni Barbi "Our approach to data privacy and security," BlackRock Inc., July 2022, https://www.blackrock.com/corporate/literature/publication/blk-commentary-our-approach-to-data-privacy-and-security.pdf.
4. U.S. Securities and Exchange Commission, "SEC Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," Release Nos. 33-11216; 34-97989, https://www.govinfo.gov/content/pkg/CHRG-111hhrg50208/html/CHRG-111hhrg50208.htm.

TOOL N:

Personal Cybersecurity Protection Guide for Corporate Directors

United States Secret Service

This boardroom tool provides practical, actionable steps to minimize directors' personal risk exposure, reduce corporate risk exposure, and strengthen resilience against sophisticated cyber threats.

COMMON ATTACKS TARGETING BOARD MEMBERS

- **Spear Phishing and Whaling Attacks:** These malicious cyber activities employ highly personalized, deceptive communications specifically crafted using publicly available information to target high-value, executive-level individuals and trick them into revealing credentials or installing malware. This publicly available information can be pulled from social media, public appearances, or speaking engagements.
- **Executive Impersonation and Deepfakes:** Threat actors creating false personas mimicking company executives' or fellow board members' identities can trick directors, executives, or employees into authorizing financial transactions, granting access to sensitive information and accounts, or taking other actions on behalf of the threat actor. New AI technologies are improving the effectiveness of such techniques, driving the need for additional awareness and training.
- **Mobile Device Targeting:** This malicious activity leverages specialized malware or device exploits to target smartphones and tablets, which can contain both corporate and personal sensitive data.
- **Home Network Infiltration:** Gaining unauthorized access to vulnerable residential networks and connected devices can provide backdoor access to personal or corporate systems.

PERSONAL CYBERSECURITY PROTECTIONS

Passwords and Accounts

- Use a password manager.
- Use strong passwords unique to each site/account.
- Minimize or prevent password reuse.
- Use phishing-resistant authentication when possible. Wherever possible, disable SMS, email, or phone one-time passwords (and similar authentication or account recovery options) to ensure effective protection using multifactor authentication.
- Ensure remote wipe capability (iOS/Android "find My Device") or corporate Mobile Device Management (MDM) solution capability.

Operational Security

- Assess your personal risk profile and be aware of your social media presence.
  - Understand and inventory the information you are sharing or providing a potential adversary. Be mindful of what you share online personally or professionally; it could be used against you.
- Backup critical personal information using the "3-2-1" rule: 3 copies, 2 different media types, and 1 offsite/alternate storage location.
- Separate personal and business communications/accounts where possible.
- Elevate your phishing awareness and responsiveness. Be hyper-aware of phishing/vishing and smishing scams designed to steal confidential information.
- Establish secondary/backup communications processes to defend against deepfake voice impersonation.
- Use reputable and secure sites for financial, email, and board portal services with end-to-end encrypted communications where appropriate and permissible.

Antivirus and Path Management

- Use reputable software and hardware sources/vendors.
- Enable active monitoring/alerting to allow for more rapid response to potential compromises, limiting the dwell time of malicious actors, and reducing potential damage.
- Enable automatic updates on personal computer, mobile, home office, and internet of things (IoT) devices when available.

Mobile Security

- Use an alphanumeric-based password containing numbers, letters, and special characters.
- Enable biometrics when possible.
- Consider enabling iOS lockdown mode or Google's Advanced Protection option.
- Enable "Stolen Device Protection" and "Find My iPhone".
- Ensure remote wipe capability is available and active.
- Only install applications from reputable sources.

FURTHER READING

- United States Secret Service
  https://www.secretservice.gov
- Cybersecurity and Infrastructure Security Agency
  https://www.cisa.gov
- Federal Trade Commission/Identity Theft
  https://www.identitytheft.gov
- Internet Crime Complaint Center (IC3)
  https://www.IC3.gov

TOOL O:

Incident Response and Reporting to the FBI

FBI Cyber Division

This tool covers actions the Federal Bureau of Investigation (FBI) and US Department of Justice (DOJ) can take against cyber actors, and when and how to report a cyber incident.

INTRODUCTION

The benefits of reporting a cyber incident to the FBI are more evident today than ever before. The FBI can assist your organization with a cyber incident **within one hour within the continental United States and within one day in more than 70 countries**. With that speed, we bring unique investigative and intelligence-derived insights to mitigate the threat your organization is facing.

HOW CAN THE FBI ASSIST AFTER A CYBER INCIDENT?

When you report a cyber incident, the FBI may be able to take the following actions:

Identifying and stopping the activity

- **Information Sharing:** FBI agents who are familiar with patterns of malicious cyber activity can work with your security and technical teams to help you quickly identify threats and understand the context of the incident.
- **International Partnerships:** The FBI has Cyber Assistant Legal Attachés around the world and can leverage the assistance of international law enforcement partners to locate stolen data and identify perpetrators.
- **Recovery Asset Team (RAT):** The FBI's RAT was established in February 2018 by the FBI's Internet Crime Complaint Center (IC3) to streamline communication with financial institutions and assist with the recovery of funds for victim companies that made transfers to domestic accounts under fraudulent pretenses. The FBI's RAT had a 66 percent success rate in 2024, freezing over $469 million of fraudulent domestic transfers and $92 million of international transfers.
- **Apprehend or Impose Costs on Cyber Actors:** The DOJ and FBI can bring forth indictments and other deterring actions to degrade cyber actors' capabilities.

Seizing or disrupting the actor's technical infrastructure

- DOJ and FBI have a mounting record of successful court-authorized operations to disrupt cyberattacks, counter ransomware, or neutralize botnets that have hijacked millions of innocent computers worldwide. The DOJ and FBI's unique authorities allow actions to be taken against cyber actors' technical infrastructure **that private companies cannot legally take on their own.**

Sharing valuable insights from other investigations that may help mitigate damage and prevent future incidents

- Disclosing information about an incident to the FBI enables investigators to make connections among related incidents.
- This enhances the FBI's abilities to share valuable insights and information regarding the perpetrator's tactics, tools, and techniques. Such information may allow you to better protect your company's network and assist the FBI in identifying and warning you (and others) of future malicious activity.

Supporting your organization's data breach response

- Under many state laws, law enforcement may be able to temporarily delay otherwise mandatory state data breach reporting when law enforcement determines doing so is appropriate for investigative reasons.
- Proactive reporting to law enforcement may help your organization deal with government regulators such as the Federal Trade Commission, which has declared that it will look more favorably on a company that has reported a cyber incident to law enforcement and cooperated with the investigation than companies that have not.
- If an incident becomes public, cooperation may strengthen your organization's position with shareholders, insurers, lawmakers, and the media.

WHEN SHOULD YOU REPORT A CYBER INCIDENT?

Organizations should report a cyber incident as soon as the incident is verified. This should be done as timely as possible to best enable attribution of an attack—since speed is often the critical element of a credible attribution. Additionally, reporting to the FBI avails the organization of protections provided to victims and witnesses. The FBI's cyber mission puts victims first, and the FBI will continue to treat victim information as sensitive and safeguard it from unwarranted or unnecessary disclosure.

Organizations that experience a cybersecurity incident are encouraged to preserve original evidence relevant to the incident. Generally, the most important pieces of evidence are log files (from critical servers, network appliance, security information and event management (SIEM) solutions, etc.), malware samples, and pre-remediated access to disk drives and memory of compromised computers. Such information is generally not privileged information (attorney-client, work product, etc.), and the voluntary and proper sharing of cyber threat information by a company/company's counsel for cybersecurity purposes generally does not expose companies to additional liability. Furthermore, any report should be done in coordination with the organization's legal team to comply with statutory and regulatory requirements, as applicable.

Electronic evidence dissipates over time, so speed is essential in a cyber-intrusion investigation. Enlisting the FBI's help during an incident enables quick investigative action and allows the preservation of evidence, which increases the odds of a successful prosecution or other action to disrupt the perpetrators.

Proactively building relationships with key government agencies, especially your local FBI field office, and with your sector risk management agencies, facilitates a successful response to a cyber incident. The FBI provide companies with a dedicated point-of-contact if an incident should occur and provides access to FBI cyber mitigation resources.

WHAT SHOULD BE REPORTED?

An array of technical data and incident information can prove helpful for investigators, including

- indicators of compromise (IOCs), i.e., threat actor IP addresses
- threat actor tactics, techniques and procedures (TTPs)
- threat actor communications, e.g., ransom notes, TOR addresses
- event timeline
- nature of the incident
- point of contact for regular communication with investigators
- logs from the affected machines
- images of the affected machines
- actions that have been taken
- forensic reports

HOW WILL THE FBI PROTECT MY ORGANIZATION'S INTERESTS AND INFORMATION?

Federal law enforcement agencies investigating cyber incidents seek first and foremost to assist victim entities as well as identify and apprehend those responsible for a cyber incident. The FBI is not a regulatory agency, and efforts are directed toward investigating the intrusion, not judging the adequacy of defenses in place.

The FBI needs technical details about an intrusion (e.g., malware samples) to advance its investigation, not privileged communications or other documents or communications unrelated to the incident. The FBI will work closely with a victim company's counsel to address concerns about access to information.

The FBI is mindful of the reputational harm that a cyber incident can cause a company or organization. As such, the FBI does not publicly confirm or deny the existence of an investigation and will ensure that information that may harm a company is not needlessly disclosed.

The FBI prioritizes causing as little disruption as possible to normal business operations. On-site investigations are carefully coordinated with your company to minimize the impact, including, for example, by working around your organization's schedule and minimizing system downtime.

HOW DO I CONTACT THE FBI TO REPORT A CYBER INCIDENT?

- Local FBI Field Office: https://www.fbi.gov/contact-us/field-offices
- The FBI's Internet Crime Complaint Center (IC3): https://www.ic3.gov/
- Online Tips and Public Leads Form: https://tips.fbi.gov/
- FBI Tip Line: 1-800-CALL-FBI (1-800-225-5324)
- International FBI offices: https://www.fbi.gov/contact-us/legal-attache-offices
- National Cyber Investigative Joint Task Force (https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force)

FURTHER READING

- **InfraGard:** https://www.infragard.org/
  - InfraGard is an association of people and organizations who represent businesses, academic institutions, state and local law enforcement agencies, and others, dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard has more than 80 chapters across the United States.
- **Domestic Security Alliance Council (DSAC):**
  - DSAC is a partnership between the US government and US private industry that enhances communication and the timely and effective exchange of security and intelligence information between the federal government and the private sector.
- **The Department of Justice:**
  - The Computer Crime and Intellectual Property Section (CCIPS) and Computer Hacking and Intellectual Property (CHIP) Program provide a network of federal prosecutors trained to pursue computer crime and IP offenses in each of the 94 United States Attorneys' Offices. CCIPS produced the Best Practices for Victim Response and Reporting of Cyber Incidents as a resource: (https://www.justice.gov/criminal-ccips/file/1096971/download). The National Security Cyber Specialist (NSCS) is a nationwide network of DOJ headquarters and field personnel trained and equipped to handle national security-related cyber issues. It includes specially trained prosecutors from every US Attorney's Office, along with experts from the National Security Division and the Criminal Division. To contact a NSCS representative, email DOJ.Cyber.Outreach@usdoj.gov or NSCS_Watch@usdoj.gov.

GOVERNANCE DOESN'T STOP HERE.

This handbook is part of NACD's ongoing commitment to advancing board leadership through insights created **by directors, for directors**.

As a member, you gain access to exclusive research, practical boardroom tools, and a powerful network of peers committed to stronger oversight and long-term value creation.

Join NACD and continue strengthening board leadership and governance excellence.

Visit www.nacdonline.org/membership.

The Internet Security Alliance convenes senior leaders from across industry to advance cybersecurity governance, policy, and best practices. Organizations interested in joining ISA's leadership network are encouraged to learn more at **www.isalliance.org**.

(COVER 3)

FSCFPO

NACD®

1100 Wilson Blvd., Suite 2500
Arlington, VA 22209
Phone 571–367–3700
nacdonline.org

INTERNET SECURITY ALLIANCE

2500 Wilson Blvd., Suite 245
Arlington, VA 22201
isalliance.org