



AI IN CYBERSECURITY

Special Supplement to the NACD-ISA
Director's Handbook on Cyber-Risk Oversight

Contributors

INTERNET SECURITY ALLIANCE

JR Williamson, Leidos

Tracie Grella, AIG

Jon Brickey, Mastercard

Deneen DeFiore, United Airlines

Dimitrios Stratakis, BNY Mellon

Kris Lovejoy, Kyndryl

Brad Maiorino, RTX

Tim Held, US Bank

Ted Webster, Centene

Patrick Hynes, Ernst and Young

Niall Brennan, SAP

Brigadier General Greg Touhill, US AIR FORCE
(RET.)

Franck Journoud, National Association of
Manufacturers

Richard Rocca, Bunge Limited

David Badanes, AES Corp

Patrick Reidy, GE Aerospace

Michael Higgins, L3 Harris

Tim McKnight, UnitedHealth Group

Nicola Sanna, Safe Security and The FAIR Institute

Mike Woods, GE Vernova

Mike Gordon, McDonalds

Larry Clinton, Internet Security Alliance

Omar Khawaja, Databricks

Robyn Bew, Ernst and Young

Murray Kenyon, US Bank

NATIONAL ASSOCIATION OF CORPORATE DIRECTORS

Dylan Sandlin

Program Manager, Digital and Cybersecurity Content

Lucy Nottingham

Senior Director, Content

Margaret Suslick

Manager, Copy Editing & Knowledge Management

Ellen Errico

Art Director

Jack Ung

Senior Marketing Communications Creative Associate

Table of Contents

1. Introduction: AI Friend and Foe	4
<i>Larry Clinton, Internet Security Alliance, and Murray Kenyon, US Bank</i>	
2. Defining AI and Its Impact on Cybersecurity	7
<i>Omar Khawaja, Databricks, and Murray Kenyon, US Bank</i>	
3. Implications for Corporate Oversight of Cybersecurity	11
3.1: AI as a Cybersecurity Risk and Force Multiplier	11
<i>Patrick Hynes and Robyn Bew, EY; JR Williamson, Leidos; and Murray Kenyon, US Bank</i>	
3.2: How AI Will Impact Cybersecurity Regulatory and Disclosure Matters	15
<i>David Badanes, AES; Niall Brennan, SAP; Larry Clinton, Internet Security Alliance; JR Williamson, Leidos; and Murray Kenyon, US Bank</i>	
3.3: How AI Impacts Board Readiness for Oversight of Cybersecurity and AI Risks	21
<i>Brigadier General Gregory Touhill, USAF (Ret.), CISSP, CISM, and NACD.DC™; Murray Kenyon, US Bank; and Nicola Sanna, Safe Security and The FAIR Institute</i>	
4. Boardroom Tool Questions for Directors to Ask About AI	23
<i>Larry Clinton, Internet Security Alliance, and Murray Kenyon, US Bank</i>	

© 2025 by the National Association of Corporate Directors and the Internet Security Alliance. All rights reserved.

Except as permitted under the US Copyright Act of 1976, no part of this publication may be reproduced, modified, or distributed in any form or by any means, including, but not limited to, scanning and digitization, without prior written permission from the National Association of Corporate Directors or the Internet Security Alliance.

This publication is designed to provide authoritative commentary in regard to the subject matter covered. It is provided with the understanding that neither the authors nor the publishers, the National Association of Corporate Directors and the Internet Security Alliance, is engaged in rendering legal, accounting, or other professional services through this publication. If legal advice or expert assistance is required, the services of a qualified and competent professional should be sought. This material is for authorized users only and is subject to NACD's Terms of Use (see <https://www.nacdonline.org/about/terms-of-use>).



1. Introduction: AI Friend and Foe

Larry Clinton, Internet Security Alliance, and Murray Kenyon, US Bank

Artificial intelligence (AI) has already significantly impacted business, with greater impacts for efficiency and productivity predicted as AI quickly becomes more widely integrated. In truth, with business adoption of AI reaching 72 percent in 2024, it already has.^{1,2} Overall, it's estimated that AI will contribute a 21 percent net increase to the United States GDP by 2030.³ As more companies and consumers adopt AI in their operations and daily lives, there will be an accompanying increase in the risks and benefits, both known and unknown, that this technology will bring to companies and their cybersecurity. Businesses' rapid adoption of AI introduces new risks alongside its benefits to innovation and productivity, suggesting that AI, like any other enterprise risk, needs to be overseen and governed at the board level.

When applied to a company's cybersecurity program, AI can enhance capabilities in areas like automatic cyber threat detection, alert generation, malware identification, and data protection.^{4,5} AI's enhanced data analysis capabilities can significantly reduce the signal-to-noise ratio among log data coming into the security operations center—reducing false positives and quickly directing the security team's attention toward the most important and critical threats. AI also has the potential to help predict weaknesses and assist security teams in making changes to prevent the breach in the first place. This capability allows companies to “get left of theft,” thereby making it much harder for the attackers to succeed. Overall, AI, when applied correctly, can be a force multiplier to corporate cybersecurity teams, strengthening a business's defense systems while increasing efficiency, productivity, and profit in business operations.

¹ Camilo Quiroz-Vázquez and Michael Goodwin, “What is artificial intelligence (AI) in business?” February 20, 2024. (<https://www.ibm.com/topics/artificial-intelligence-business>)

² Alex Singla, Alexander Sukharevsky, Lareina Yee, and Michael Chui, with Bryce Hall, “The state of AI in early 2024: Gen AI adoption spikes and starts to generate value,” posted on mckinsey.com on May 30, 2024. (<https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai/>)

³ Katherine Haan (Lauren Holznienkemper, reviewer), “22 Top AI Statistics And Trends In 2024,” Updated October 16, 2024. (<https://www.forbes.com/advisor/business/ai-statistics/>)

⁴ Camilo Quiroz-Vázquez and Michael Goodwin, “What is artificial intelligence (AI) in business?” February 20, 2024. (<https://www.ibm.com/topics/artificial-intelligence-business>)

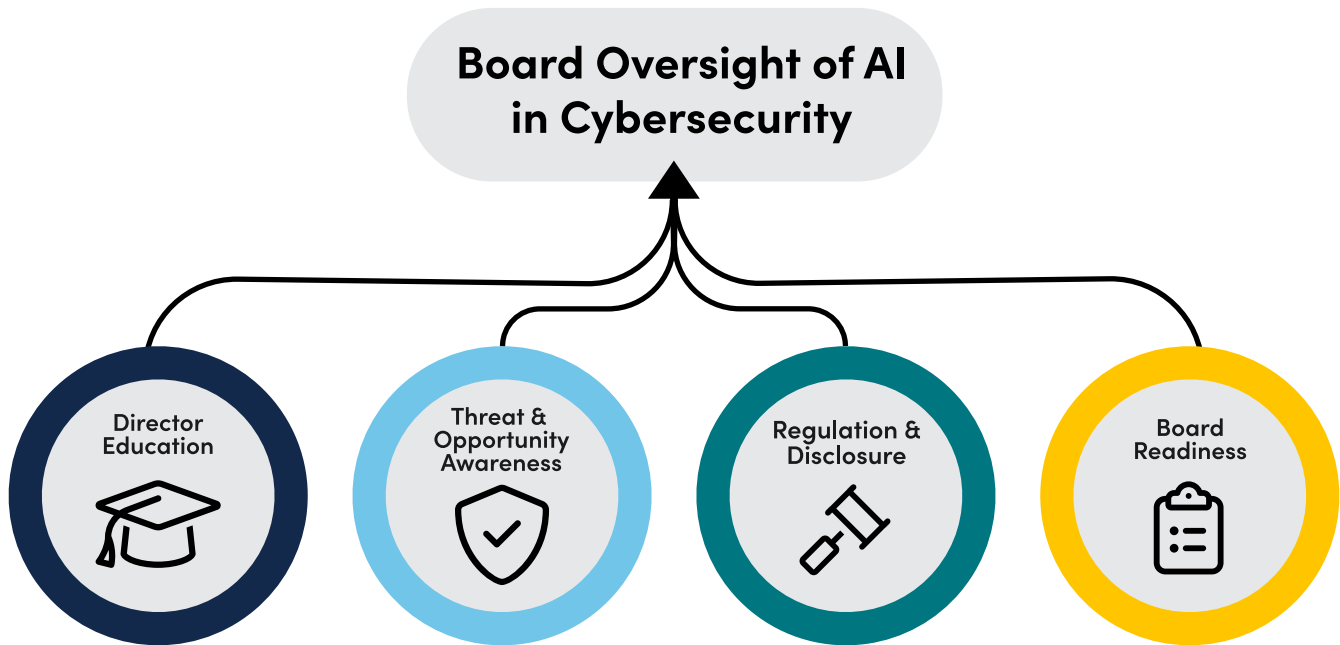
⁵ “Artificial Intelligence (AI) in Cybersecurity,” FORTINET, accessed July 25, 2024. (<https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity>)

However, despite its promise, as with all new technology, implementing AI brings new risks. A key risk is the lack of widespread awareness of AI's potential dangers, as only a few leaders possess the necessary experience and education to understand the societal, organizational, and individual risks.⁶ The entirety of AI risks and benefits has yet to be discovered, highlighting the imperative for continuous board education about the potential unknown,

future organizational and cybersecurity consequences this technology could bring.⁷

While AI can improve corporate cybersecurity performance, AI also provides new tools to threat actors. AI lowers the barrier to entry for cybercriminals by reducing the technical know-how required to launch cyberattacks and turbocharging the evolution of existing tactics, techniques, and procedures.⁸ Criminals and

AI in Cybersecurity Oversight Imperatives



Source: NACD

⁶ Benjamin Cheatham, Kia Javanmardian, and Hamid Samandari, "Confronting the risks of artificial intelligence," April 26, 2019. (<https://www.mckinsey.com/capabilities/quantumblack/our-insights/confronting-the-risks-of-artificial-intelligence>)

⁷ Douglas Broom, "AI: These are the biggest risks to businesses and how to manage them," July 27, 2023. (<https://www.weforum.org/agenda/2023/07/ai-biggest-risks-how-to-manage-them/>)

⁸ Giulia Moschetta and Joanna Bouckaert, "AI and cybersecurity: How to navigate the risks and opportunities," February 29, 2024 (<https://www.weforum.org/agenda/2024/02/ai-cybersecurity-how-to-navigate-the-risks-and-opportunities/>); "The near-term impact of AI on the cyber threat," National Cyber Security Centre, January 24, 2024 (https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat#-section_5); and Richard Watson, Richard Bergman, and contributors Jim Guinn II and Piotr Ciepiela, "How can cybersecurity transform to accelerate value from AI?" May 1, 2024 (https://www.ey.com/en_us/insights/consulting/transform-cybersecurity-to-accelerate-value-from-ai).

nation-state adversaries are already exploring the use of AI tools to enhance their tradecraft, improve the veracity and efficacy of their attack campaigns, and train less experienced workers to combat companies and governments using AI for defense.

Protecting the company's workforce from AI's harms and opportunities for misuse represents another risk area. Many companies' greatest asset and product is their people. But how are they to leverage AI in a responsible, ethical, and compliant manner that delivers strategic benefits but does not simultaneously expose the organization to risk levels above appropriate thresholds? Boards should ensure that their company's leadership understands how AI is in use in their companies; adopts a governance and security framework that accounts for AI's unique risks; develops use cases aligned with the company's purpose, values, and governance principles; and communicates the responsible use of AI within their products and services. This transparency is essential to establishing and maintaining stakeholder and shareholder trust.⁹

Imperative for Boards

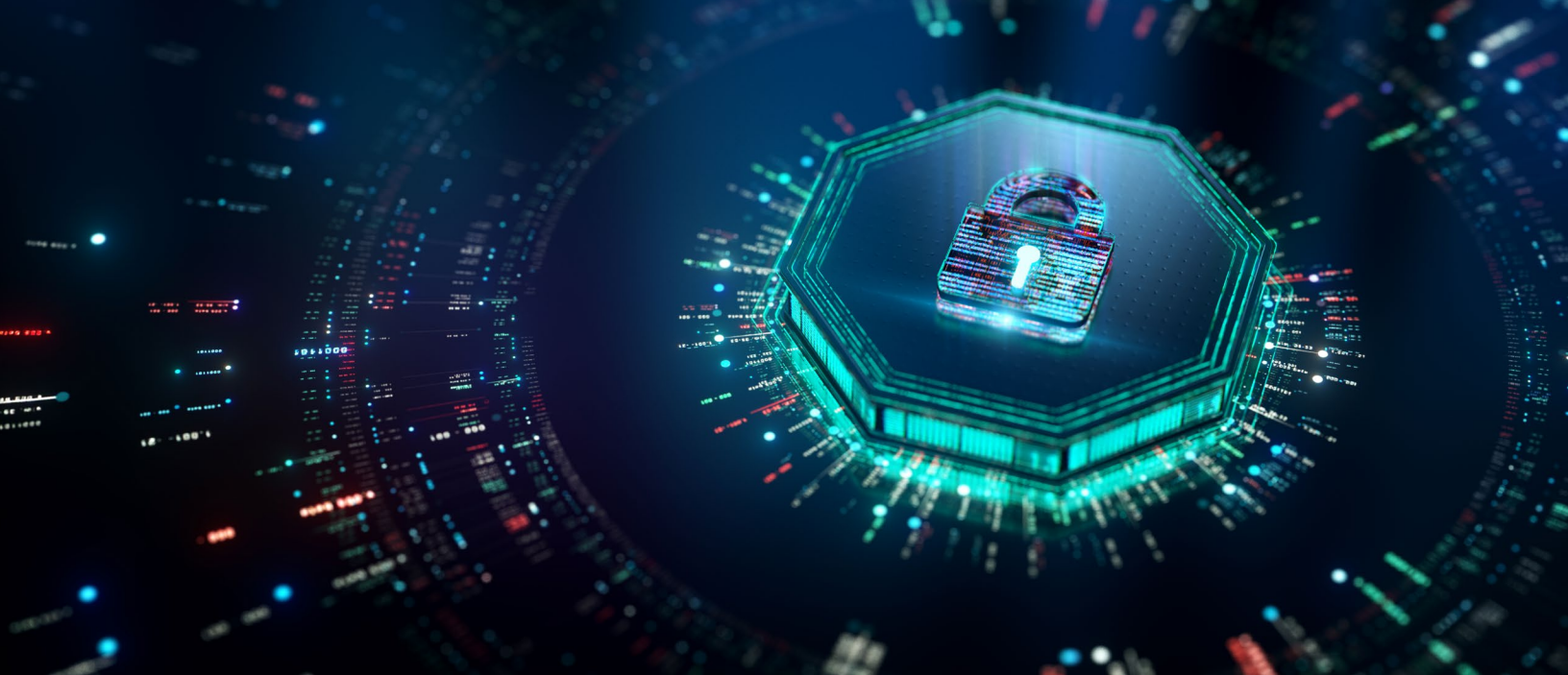
Boards must educate themselves about AI's implications within cybersecurity and operations. Understanding and awareness of AI's technical advancements, new risks, and regulatory implications will be necessary for effective risk oversight. Boards cannot allow management to fall into the trap of either overlooking potential perils or overestimating an organization's risk-mitigation capabilities.¹⁰ In order to fully realize the benefits of AI in their cybersecurity departments and their overall business, directors must be aware of what artificial intelligence is, its benefits, and the potential consequences or risks it can bring to their organizations.

Boards are uniquely positioned to play an important role in ensuring management provides a safe and responsible use of AI to manage cyber risk across the organization, as described in detail in Principles Four and Five of the NACD-ISA 2023 *Director's Handbook on Cyber-Risk Oversight*.¹¹ This report is a supplement to that handbook, designed to educate directors about this critically important topic. By educating themselves in the various types of AI, the current applications of AI in cybersecurity departments, and regulatory and disclosure implications, directors and boards will better understand the intersection of AI and cybersecurity and be better positioned to provide oversight of this strategically important technology.

⁹ NACD, *Technology Leadership in the Boardroom: Driving Trust and Value* (Arlington, VA: NACD, 2024), p. 17 and p. 20. (<https://www.nacdonline.org/all-governance/governance-resources/governance-research/blue-ribbon-commission-reports/BRC/2024/tech-leadership-in-the-boardroom/>)

¹⁰ Benjamin Cheatham, Kia Javanmardian, and Hamid Samandari, "Confronting the risks of artificial intelligence," April 26, 2019. (<https://www.mckinsey.com/capabilities/quantumblack/our-insights/confronting-the-risks-of-artificial-intelligence/>)

¹¹ NACD and ISA, *2023 Director's Handbook on Cyber-Risk Oversight* (Arlington, VA: NACD, 2023), pages 28 through 37. (<https://www.nacdonline.org/all-governance/governance-resources/governance-research/director-handbooks/nacd-directors-handbook-on-cyber-risk-oversight/>)



2. Defining AI and Its Impact on Cybersecurity

Omar Khawaja, Databricks, and Murray Kenyon, US Bank

Companies are adopting AI tools for a variety of applications, cybersecurity use cases included. As cybersecurity teams deploy AI, it is critical to understand the underlying AI models and techniques that power these cybersecurity capabilities.

Outside of data science, AI is new to most teams across organizations. Their understanding of the risks associated with AI and how to mitigate them is relatively new. While many of the risks associated with AI may, on the surface, seem unrelated to cybersecurity (e.g., fairness, explainability¹², regulatory, trustworthiness, etc.), many canonical controls that have been managed by cybersecurity teams (e.g., authentication, access control, logging, monitoring, etc.) for decades can be deployed to mitigate many non-cybersecurity risks of AI.

However, AI amplifies both positive and adverse outcomes. Unless adverse outcomes are effectively overseen and managed, the net benefit of AI will be negative.

¹² For a definition of “explainability” as used in AI, please see Palo Alto Networks’ Cyberpedia definition of the word. (<https://www.paloaltonetworks.com/cyberpedia/ai-explainability>)

DEFINING FORMS OF AI

Traditional AI

- ▶ Traditional AI, or classical AI, involves methods that humans explicitly program. These methods include rule-based systems, decision trees, and logical inference. Traditional AI systems are designed to solve specific problems—performing best where rules are well-defined and the problem space is not overly complex. Their behavior is also deterministic, meaning that the same input will always produce the same output.

Machine Learning

- ▶ Machine Learning (ML) is a subset of AI that involves creating models that can learn from data. ML models are trained on data which they use to make predictions or decisions, such as predicting customer churn or recognizing images, instead of solving explicit problems. ML involves a variety of training techniques, including supervised, unsupervised, and reinforcement learning.
- ▶ Generative AI (GenAI) is a subfield of AI that uses machine learning to generate original content and not to analyze data per se. Generative AI relies on the ability of computers/systems to use models to generate novel content like images, text, music, code, synthetic data, and much more.

Large Language Models (LLMs) and Their Applications

- ▶ Large language models, the most common example of generative AI, are systems trained on massive datasets and designed to process and analyze vast amounts of natural language data and then use that information to generate humanlike responses to user prompts. Using advanced machine learning algorithms, these systems learn the patterns and structures of human language and are capable of generating coherent and contextually relevant, natural-language responses to a wide range of written inputs.

Recent advancements have focused the spotlight on generative AI and large language models and made them a viable tool across a range of business functions. They include these:

- ▶ **Advancements in Training Techniques:** Over the past few years, significant advancements in the techniques used to train these models have resulted in big leaps in performance. Notably, one of the largest jumps in performance has come from integrating human feedback directly into the training process.
- ▶ **Increased Accessibility:** The release of ChatGPT opened the door for anyone with Internet access to interact with one of the most advanced LLMs through a simple web interface. This brought the impressive advancements of LLMs into the spotlight, since previously, these more powerful LLMs were only available to researchers with large amounts of resources and those with very deep technical knowledge.
- ▶ **Growing Computational Power:** The availability of more powerful computing resources, such as graphics processing units (GPUs) and better data processing techniques, allowed researchers to train much larger models, improving the performance of these language models.
- ▶ **Improved Training Data:** LLM performance has improved dramatically alongside improvements in collecting and analyzing large amounts of data.
- ▶ **Improving the Use of Prompts:** The models themselves can also help to teach humans how to optimize their use of the system. Just like those who understand the syntax of complex search engines can generally significantly improve their search results with mainstream tools like Google and Bing, humans can learn how to effectively interact with GenAI tools to increase their efficacy, reliability, and usefulness.

WHY LLMS ARE CREATING NEW RISKS AND OPPORTUNITIES FOR INFORMATION SECURITY

While AI offers the opportunity to enhance cybersecurity, it's critical to note that threat actors are also using AI and that use of AI in cybersecurity without proper oversight can increase risk to an organization. Security risks involved with the use of AI include these:

- ▶ **Lack of AI Proficiency:** The need for AI-proficient cybersecurity professionals will grow as AI technologies, like LLMs, become more prevalent. However, this current skills gap leaves many cybersecurity teams lacking the necessary expertise to effectively manage the risks associated with LLMs and fully harness the potential that AI can empower their teams to achieve.
- ▶ **Unmanaged Model Drift:** LLMs are trained on vast amounts of data, often from diverse and uncontrolled sources. The complexity of this training data makes it difficult to fully understand and control what the model has learned, which threatens the reliability of the model and, therefore, its usefulness to the cybersecurity team. Potential negative outcomes include data leakage or the generation of inappropriate content.
- ▶ **Lack of Transparency:** LLMs, like many AI models, are often seen as "black boxes" because their internal workings are not easily interpretable by humans. This lack of transparency can make it difficult to predict or explain the model's output, leading to potential risks in decision-making processes. Ultimately, these tools need to become more resilient through explainability, dependability, and tamper resistance, in order to become trusted resources supporting the cybersecurity mission.
- ▶ **Autonomous Content Generation:** LLMs have the ability to generate new content autonomously. While this can be useful and improve speed-to-decision processes, it also means that they can produce harmful or misleading information without human intervention and oversight.
- ▶ **Evolving Frameworks:** The rapid advancement of LLMs and other AI technologies has outpaced the development and adoption of regulatory and industry frameworks. This can lead to misuse of the technology and difficulties enforcing accountability.
- ▶ **Increased Risk Tolerance:** The potential benefits of AI technologies like LLMs are driving a strong appetite for their implementation among businesses. However, this eagerness can lead to an implicit increase in risk tolerance, as businesses may rush to adopt these technologies without fully understanding or mitigating the associated risks. This is particularly problematic when tech teams, due to various constraints, are unable to meet the pace expectations to deliver safe LLM solutions. As a result, businesses may end up deploying AI solutions that have not been adequately vetted for security or ethics, thereby increasing their vulnerability to data breaches, misuse, and other potential liability harms to the organization.
- ▶ **Data Use Implications:** As generative AI models become increasingly sophisticated, they rely on vast amounts of data for training. This raises concerns about the ethical implications of data usage and the potential for misuse. Additionally, traditional information release practices have not fully considered the implications of data being used to train AI models. This can create a disadvantage for more conservative companies, who may hesitate to release data, while less cautious organizations may inadvertently share sensitive information.



3. Implications for Corporate Oversight of Cybersecurity

3.1: AI AS A CYBERSECURITY RISK AND FORCE MULTIPLIER

Patrick Hynes and Robyn Bew, EY; JR Williamson, Leidos; and Murray Kenyon, US Bank

AI and New Risks

US Cybersecurity and Infrastructure Security Agency (CISA) Chief Jen Easterly likely voiced the concerns of many CEOs and board members in describing the impact on cybersecurity of generative AI (GenAI). Easterly said, “A powerful tool will create a powerful weapon. . . . It’ll exacerbate the threat of cyberattacks . . . [by making] people who are less sophisticated actually better at doing some of the things they want to do.”¹³

Commonly cited cyber-risk factors related to AI, and particularly GenAI, include the following:¹⁴

- ▶ More advanced and effective social engineering campaigns that leverage AI to create increasingly realistic imitations of documents, videos, images, and voices
- ▶ Faster identification of high-value targets and vulnerable systems by bad actors
- ▶ Reduced cost for cyberattack tools, lowering the barriers to entry for less-sophisticated cybercrime actors
- ▶ Developing novel attack techniques based on AI modeling and simulation that subvert a system’s inherent weaknesses rather than known vulnerabilities
- ▶ Data poisoning that corrupts underlying AI model data in order to manipulate outputs
- ▶ Prompt injection attacks, where specifically engineered prompts trick GenAI systems into allowing bad actors to bypass security, privacy, or other system guardrails

Even more sobering, as leading cyber experts have pointed out, is the fact that some unintended downstream consequences or second-order effects of artificial intelligence use-cases are as yet unknown.¹⁵

¹³ Ina Fried, “AI makes it easier for anyone to become a cybercriminal, top official says,” posted on [axios.com](https://www.axios.com/2024/05/10/ai-cybersecurity-artificial-intelligence-csa) on May 10, 2024. (<https://www.axios.com/2024/05/10/ai-cybersecurity-artificial-intelligence-csa>)

¹⁴ See “The near-term impact of AI on the cyber threat,” National Cyber Security Centre, January 24, 2024 (https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat#section_5); and Richard Watson, Richard Bergman, and contributors Jim Guinn II and Piotr Ciepiela, “How can cybersecurity transform to accelerate value from AI?”, May 1, 2024 (https://www.ey.com/en_gl/insights/consulting/transform-cybersecurity-to-accelerate-value-from-ai).

¹⁵ Phil Venables, “Where the Wild Things Are: Second Order Risks of AI,” May 4, 2024. (<https://www.philvenables.com/post/where-the-wild-things-are-second-order-risks-of-ai>)

Applying AI to Cybersecurity

However, advances in AI and GenAI also have the potential to improve companies' cybersecurity posture in several ways, and could potentially tip the scale in favor of cybersecurity teams against attackers. While AI is considered a cybersecurity risk multiplier, AI can also be considered a "force multiplier."¹⁶ AI can allow organizations to anticipate threats in advance and respond to cyberattacks faster than the attackers can move.¹⁷ As the threat landscape continues to grow and evolve, AI is poised to become a prominent tool used to address many cybersecurity risks, and boards must understand the benefits and risks it will bring to their organizations.

A promising area of opportunity is the ability to apply AI-driven network, asset mapping, and visualization platforms to "provide a real-time understanding of an expanding enterprise attack surface."¹⁸ Using AI, ML, and LLM tools to automate parts of key cybersecurity functions like threat detection and incident response can enable quicker and more efficient mitigation.¹⁹

LLMs provide the most value to organizations when used for threat detection and remediation.²⁰ These LLMs can be trained on data that is constantly being updated, such as continuously updated data from the Internet and data generated by internal security assessments.²¹ This data allows LLMs to understand and detect new cyberattacks before the human cybersecurity teams can.²² In addition to threat detection, LLMs are also valuable in threat and vulnerability remediation. These models can analyze alerts and system log data, evaluate cyberattack information, and produce the best steps for remediation.²³

AI's ability to learn from data and make predictions or decisions makes it a powerful tool in the field of cybersecurity. Generative AI can also improve the human-to-machine interface, demystifying complex cybersecurity terms and architectures and greatly reducing the friction that some may feel working with the cybersecurity team.

¹⁶ Ed Bowen, Wendy Frank, Deborah Golden, Michael Morris, and Kieran Norton, "Cyber AI: Real defense," December 7, 2021. (<https://www2.deloitte.com/us/en/insights/focus/tech-trends/2022/future-of-cybersecurity-and-ai.html>)

¹⁷ Ibid.

¹⁸ Ibid.

¹⁹ "AI in Cybersecurity: Enhancing Protection and Defence," Institute of Data, February 22, 2024. (<https://www.institutedata.com/us/blog/ai-in-cybersecurity/>)

²⁰ Joseph Harisson, "The Impact of Large Language Models (LLMs) on Cybersecurity," posted on IT Companies Network's IT Blog, updated on February 19, 2024. (<https://itcompanies.net/blog/llm-cybersecurity>)

²¹ Ibid.

²² Ibid.

²³ Ibid.

Cybersecurity use cases for AI include these:

- ▶ **Threat Detection and Response:** Cybersecurity teams can use AI security tools to analyze threat indicators from millions of endpoints in exponentially less time than without them. This rapid detection and response capability is crucial to minimizing the impact of a security breach.
- ▶ **Advanced Analytics:** AI enables advanced analytics that help close the gap between an attacker's speed and a defender's ability to detect malicious activity; for example, by being able to execute two to three times more threat hunts per analyst.
- ▶ **Incident Investigation and Response:** AI can help determine risk and impact and automate decisions during a cyber incident. This can significantly speed up the response time and minimize potential damage.
- ▶ **Enriching Threat Indicators:** AI can enrich threat indicators and metadata on terabytes of streaming data, improving the security posture with high-performance analytics. This helps to lower the signal-to-noise ratio to improve the efficacy of the alerts an analyst needs to investigate.
- ▶ **Cost Reduction:** Automation of cybersecurity processes with AI can help reduce costs. Although the tools themselves are not cheap, as the volume of security data rises at such large rates, we typically need more analysts to interpret and operate on that data. AI can help augment the capacity of existing analysts, so that they can address a greater volume of data with higher quality decision-making and speed, without the need to increase your staff in a commensurate manner. Since labor is frequently the largest single cost category of a cybersecurity program, AI can enable a cybersecurity program to expand its capacity and maturity without driving up labor costs.

In addition to these, AI can also be used for insider threat detection, identity and access management (IAM), account protection for Software as a Service accounts, and threat hunting.

The critical advantage AI offers, though, is its ability to benefit the currently strained cyber workforce by both enhancing their work and potentially leading to improved job satisfaction.²⁴ AI-powered security and compliance automation platforms are already delivering this as

these tools can “streamline workflows, enabling teams to respond to incidents faster and with greater precision.”²⁵ This, in turn, allows the cybersecurity professionals to focus on more valuable strategic initiatives and higher-level threat analysis.²⁶ With the potential for improved performance and value creation, boards should evaluate the organization's cybersecurity workforce and leadership to assess their readiness for AI and determine how AI may impact the company's current and future cybersecurity workforce needs.²⁷

²⁴ Ed Bowen, Wendy Frank, Deborah Golden, Michael Morris, and Kieran Norton, “Cyber AI: Real defense,” December 7, 2021. (<https://www2.deloitte.com/us/en/insights/focus/tech-trends/2022/future-of-cybersecurity-and-ai.html>)

²⁵ Emily Bonnie, “How Artificial Intelligence Will Affect Cybersecurity in 2024 & Beyond,” posted to the Secureframe blog on December 7, 2023. (<https://secureframe.com/blog/how-will-ai-affect-cybersecurity>)

²⁶ Ibid.

²⁷ NACD in partnership with Data & Trust Alliance, *Director Essentials: AI and Board Governance* (Arlington, VA: NACD, 2023), p. 12. (<https://www.nacdonline.org/all-governance/governance-resources/governance-research/director-faqs-and-essentials/ai-and-board-governance/>)

AI can improve cybersecurity effectiveness, but it is not a panacea, and it introduces new risks boards and management teams must monitor. Board members' first acknowledgment should be that cybercriminals also have access to AI tools.²⁸ AI can be helpful in detecting threats; however, "cyber criminals evolve their attack strategies to evade it."²⁹ ³⁰ Further, these tools are prone to high false positive rates, making it difficult to identify novel threats.³¹

Imperative for Boards

AI's ability to be both a force and risk multiplier—for companies' business models generally, and within the cybersecurity landscape specifically—amplifies the importance of the NACD-ISA 2023 *Director's Handbook on Cyber-Risk Oversight's* Principle One regarding the need for boards to consider cybersecurity as a matter of strategy and enterprise risk, rather than simply as a technology issue. In addition, AI's multiplier effect on cyber risks heightens the need for collective action to improve systemic resilience, as outlined in Principle Six of the Handbook.

²⁸ Nick Huber, "Why cyber risk managers need to fight AI with AI," posted to ft.com on May 2, 2024. (<https://www.ft.com/content/7cea944c-2863-43c7-ae9f-c28c76f2f7b7>)

²⁹ "What Is the Role of AI in Threat Detection," Cyberpedia, paloaltonetworks.com, accessed August 6, 2024. (<https://www.paloaltonetworks.com/cyberpedia/ai-in-threat-detection>)

³⁰ Nick Huber, "Why cyber risk managers need to fight AI with AI," posted to ft.com on May 2, 2024. (<https://www.ft.com/content/7cea944c-2863-43c7-ae9f-c28c76f2f7b7>)

³¹ Hannah Murphy, "Is artificial intelligence the solution to cyber security threats?" posted to ft.com on January 16, 2024. (<https://www.ft.com/content/35d65b91-5072-40dc-861c-565d602e740e>)

3.2: HOW AI WILL IMPACT CYBERSECURITY REGULATORY AND DISCLOSURE MATTERS

David Badanes, AES; Niall Brennan, SAP; Larry Clinton, Internet Security Alliance; JR Williamson, Leidos; and Murray Kenyon, US Bank

Human Impact & Corporate Alignment

Recognizing that AI is fundamentally a human endeavor is crucial and imperative to successful implementation of AI technology. AI models often lack transparency. Black-box algorithms make it challenging to understand decision-making processes. As AI can inherit biases from training data, governance models should be reviewed to ensure equitable treatment and frequent tuning of the models to ensure that they are operating within expected risk tolerances.

Approaching AI from the perspective of a company's mission and values aligns strategic decisions. Responsibility for AI oversight can reside with the full board, existing committees (e.g., audit or technology), or dedicated AI committees.

Regulatory Impact

Traditional regulatory models struggle to keep pace with rapidly evolving technology, and national legislation complicates this issue. The current state of AI regulation is a patchwork of mandatory and voluntary AI frameworks.

According to NACD's 2025 Trends and Priorities Survey data, almost one-third (30%) of corporate directors believe that artificial intelligence will be a top priority for their business in 2025, with another 41 percent of directors selecting cybersecurity threats as a top trend.³² There are many facets to this assessment, but inherent in this conclusion is the evaluation that AI raises the general risk posture of any entity employing these new technologies. As such, the management of that risk becomes an important factor of which boards need to be aware. In addition to the operational and security challenges incurred by an enterprise with the implementation of rapidly evolving AI systems, an essential factor to consider when evaluating the potential impact of AI is the increasingly complicated regulatory and compliance risk that accompanies such a transformation.

Regulatory and compliance risks are compounded by the fact that there is limited widespread AI expertise and the AI regulations that do exist are "nascent and highly fragmented."³³ A Swimlane and Sapio Research survey of 500 cybersecurity decision-makers at companies found that 44 percent of them said that it's a challenge to find and retain the personnel that have AI expertise.³⁴ Similarly, an NACD survey found that only 28 percent of board respondents have AI as a regular feature in board conversations.³⁵

³² NACD, *2025 Governance Outlook*, "Directors Should Prepare to Address Five Board Dilemmas in 2025" (Arlington, Virginia: NACD, 2024). (<https://www.nacdonline.org/all-governance/governance-resources/governance-research/outlook-and-challenges/2025-governance-outlook/preparing-for-five-crucial-board-balancing-acts-in-2025/>)

³³ NACD in partnership with Data & Trust Alliance, *Director Essentials: AI and Board Governance* (Arlington, VA: NACD, 2023), p. 12. (<https://www.nacdonline.org/all-governance/governance-resources/governance-research/director-faqs-and-essentials/ai-and-board-governance/>)

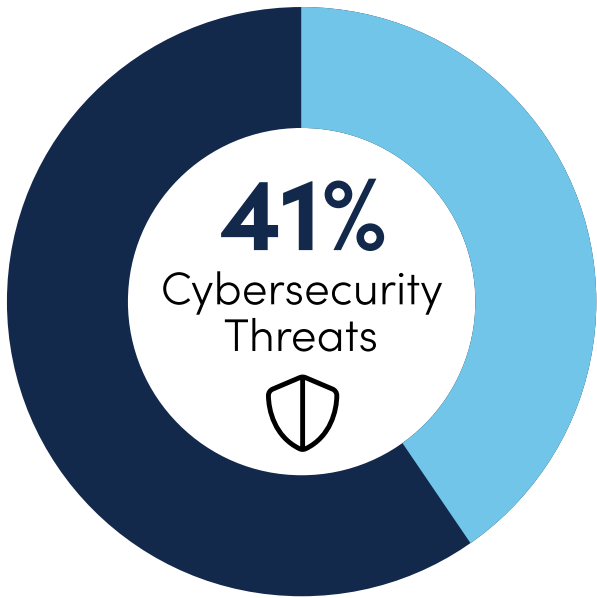
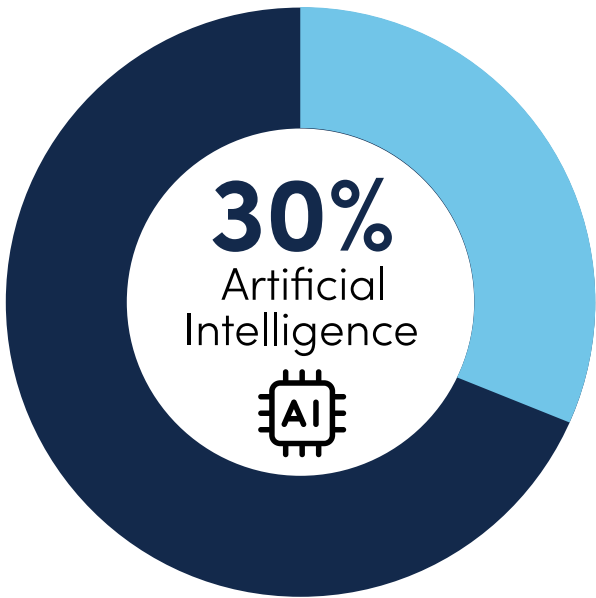
³⁴ Katie Bykowski, "AI, Cybersecurity and Compliance," posted to swimlane.com on May 30, 2024. (<https://swimlane.com/blog/ai-cybersecurity-compliance/>)

³⁵ NACD, *2023 NACD Public Company Board Practices and Oversight Survey* (Arlington, VA: NACD, 2023), p. 3. (<https://www.nacdonline.org/all-governance/governance-resources/governance-surveys/surveys-benchmarking/2023-nacd-public-company-board-practices-and-oversight-survey/>)

Cybersecurity regulation is still a challenge for companies of all shapes and sizes, with only 40 percent of cybersecurity decision-makers believing that their organizations “have made the necessary investments to fully comply with relevant cybersecurity regulations, while 19% admit to having done very little.”³⁶ The addition of artificial intelligence adds a new, more intricate layer of regulatory/compliance risks that boards will have to consider.

A recent case study from EY found that “regulators often take a wait-and-see approach to nascent technology, with guidance trailing innovation by three to five years.”³⁷ In regard to compliance, “historically, compliance professionals have treated technological innovation with skepticism.”³⁸ Nonetheless, as with the rapid growth of cybersecurity regulation globally over the last few years, when the regulation does come, it comes fast and furiously. We are beginning to see signs that the new

Cybersecurity & AI as Top Trends for Directors in 2025



Source: 2025 NACD Trends and Priorities Survey, n=251

³⁶ Katie Bykowski, “AI, Cybersecurity and Compliance,” posted to swimlane.com on May 30, 2024. (<https://swimlane.com/blog/ai-cybersecurity-compliance/>)

³⁷ Don Johnson and Alex Treuber, authors, and Adam Meshell, contributor: “How AI will affect compliance organizations,” posted on ey.com on July 18, 2023. (https://www.ey.com/en_us/insights/financial-services/how-ai-will-affect-compliance-organizations)

³⁸ Ibid.

paradigm is shortening the three-to-five-year window referenced above. At their peril, many companies adopting a similar “wait and see” approach regarding AI regulation will find themselves overwhelmed as they struggle to effect compliance with limited resources and short timelines. Boards need to anticipate and understand that as AI advances occur at an increasingly rapid rate, the difficulty that companies will experience in keeping pace with emerging regulation and understanding its effect on business will be compounded.³⁹ This will inadvertently bring about additional regulatory and compliance risks around AI deployment.

As such, “new AI technologies will force compliance professionals to rethink existing operational models and

approaches to risk management.”⁴⁰ A more proactive approach, on the part of both government and deployers of AI technologies, in crafting sensible regulation may act as a positive force in the smooth incorporation of AI into business functions. As noted by NACD, fulfilling the compliance responsibility “for AI regulation will be challenging, but regulations may become a lever to ensure that companies are engaging with AI systems safely and responsibly.”⁴¹

The vast majority of pending legislation, both domestically and internationally, call for a ranking of risk typically organized by prohibited risk, high risk, minimal risk, and low risk.

³⁹ NACD in partnership with Data & Trust Alliance, *Director Essentials: AI and Board Governance* (Arlington, VA: NACD, 2023), p. 12. (<https://www.nacdonline.org/all-governance/governance-resources/governance-research/director-faqs-and-essentials/ai-and-board-governance/>)

⁴⁰ Don Johnson and Alex Treuber, authors, and Adam Meshell, contributor: “How AI will affect compliance organizations,” posted on ey.com on July 18, 2023. (https://www.ey.com/en_us/insights/financial-services/how-ai-will-affect-compliance-organizations)

⁴¹ NACD in partnership with Data & Trust Alliance, *Director Essentials: AI and Board Governance* (Arlington, VA: NACD, 2023), p. 13. (<https://www.nacdonline.org/all-governance/governance-resources/governance-research/director-faqs-and-essentials/ai-and-board-governance/>)

AI Seven-Step Governance Program



Currently, virtually all the evolving regulatory structures are tending to suggest that high-risk AI use cases should follow a seven-step governance program embodied in current EU regulatory structures:⁴²

1. **Confirm High Quality Data Use:** “High-quality data” as a term generally means data being used for high-risk AI is material and relevant to the exercise.
2. **Continuous Monitoring:** Ensure there is continuous monitoring, testing, and auditing pre- and post-deployment of the high-risk use of AI.
3. **Risk Assessment:** Perform risk assessments based on the pre-deployment testing, auditing, and monitoring of the AI. This will require close communications with the enterprise AI management team to ensure that the required processes are in place.
4. **Technical Documentation:** Ensure that all required technical documentation and risk mitigation have been implemented based on the continuous monitoring process—all users, licensees, and deployers of AI must do their own testing.
5. **Transparency:** Licensors and licensees of AI will be expected to be fully transparent with end users as to the capabilities and limitations of the AI.
6. **Human Oversight:** Trusted AI legal frameworks intend for there to be a degree of human oversight to correct deviations from expected uses in real time. This may require a human research scientist within the company who would have the ability to adjust the AI model to bring it back into safety parameters.
7. **Fail-Safe:** In the event that AI cannot be restored to approved parameters, there would need to be a fail-safe “kill switch” if remedial mitigation steps cannot be effectuated.

⁴² Dominique Shelton Leipzig, *Trust: Responsible AI, Innovation, Privacy and Data Leadership* (South Carolina: Forbes Books, 2023), pages 147–153.

As is the case with the model for cybersecurity advocated in the NACD-ISA 2023 *Director's Handbook on Cyber-Risk Oversight*, AI security should not be “bolted-on” at the end of the process.⁴³ Rather, AI systems, like cybersecurity, are best integrated through the full life cycle of development. Most of these steps listed above are relatively low-cost at the outset, and boards should assure they are in place early in the process, as it is better to build the company's AI in accordance of regulator expectations from the outset rather than investing in AI use cases that may eventually be deemed noncompliant.

Ultimately, the internal use of AI in the conduct of the company's business or embedding AI into the company's products and services needs to be meticulously governed. Customers and shareholders will want to have confidence and trust that the company's use of AI is being done in a manner that will accelerate growth in shareholder equity without the deep risks of regulatory or quality harms that may come from a company that is not using AI responsibly.

A governance and engineering framework is desired to ensure that all components of AI use occur through a human-centered AI approach. The AI Act is the approach for trustworthy AI use in Europe as described above.⁴⁴ There are also a variety of voluntary frameworks to help guide responsible and trustworthy development and use of AI, including the National Institutes of Standards and Technology's (NIST) AI Risk Management Framework, the Government Accountability Office's (GAO) AI Accountability Framework, and the OECD's Principles on Artificial Intelligence. There are also private-sector AI frameworks that address specific industries, cybersecurity concerns, system safety, tool acquisition, and frameworks for rapidly-accelerating agentic systems.

Boards should stay informed about emerging legislation and regulation and adapt quickly should regulatory frameworks evolve. Although some aspects of AI remain unregulated, organizations must create their own guidelines and safeguards to maintain trust with their customers, shareholders, and partners.

⁴³ NACD and ISA, 2023 *Director's Handbook on Cyber-Risk Oversight* (Arlington, VA: NACD, 2023), p. 11. (<https://www.nacdonline.org/all-governance/governance-resources/governance-research/director-handbooks/nacd-directors-handbook-on-cyber-risk-oversight/>)

⁴⁴ Please see The Act Texts at <https://artificialintelligenceact.eu/the-act/>.

Disclosure Imperatives

Adoption of and compliance with the above mentioned, and emerging, laws and frameworks brings various implications for corporate disclosures. The following categories provide a reference for boards and directors of companies deploying, developing, selling, or using AI tools to consider how their company's use of AI may impact their disclosure obligations.

Transparency and Accountability

Organizations deploying AI in cybersecurity can leverage the following best practices to disclose their use of AI-driven tools. This transparency ensures that stakeholders, including customers and investors, understand the technology's role in security operations. Regulators should also play a crucial role by mandating transparency regarding AI models, training data, and decision-making processes. By doing so, organizations can build trust and demonstrate their commitment to ethical practices.

Risk Assessment and Mitigation

When adopting AI, organizations must conduct thorough risk assessments. These assessments should consider both the benefits and limitations of AI in enhancing security. A detailed model for modern cyber-risk assessment is provided under Principles 4 and 5 in the NACD-ISA 2023 *Director's Handbook on Cyber-Risk Oversight*.⁴⁵ Grafting in AI-specific use cases and requirements, as noted above, in the EU Framework and others will help ensure that AI-specific risks are identified and addressed early on in the acquisition life cycle. By disclosing these assessments, organizations can inform stakeholders about potential risks and how they plan to mitigate them. Effective communication around risk management ensures that AI adoption aligns with overall security objectives.

Incident Reporting and AI Failures

Prompt incident reporting is essential when AI-related incidents occur. Organizations should disclose any failures or security breaches promptly. Regulators need mechanisms to track these incidents and assess their impact on overall security. Transparency in reporting ensures that corrective actions can be taken promptly, minimizing harm and maintaining trust. Having human-centered AI principles built into your AI strategy and operations helps to ensure that harms from potential unreliable AI results are quickly addressable.

Imperative for Boards

Corporate oversight of AI in cybersecurity requires a holistic approach that balances strategic opportunities, risk management, and ethical considerations. By recognizing the human dimension of AI and staying informed about regulation, boards can effectively navigate this transformative landscape.

⁴⁵ NACD and ISA, *2023 Director's Handbook on Cyber-Risk Oversight* (Arlington, VA: NACD, 2023), pages 28 through 37. (<https://www.nacdonline.org/all-governance/governance-resources/governance-research/director-handbooks/nacd-directors-handbook-on-cyber-risk-oversight/>)

3.3: HOW AI IMPACTS BOARD READINESS FOR OVERSIGHT OF CYBERSECURITY AND AI RISKS

*Brigadier General Gregory Touhill, USAF (Ret.), CISSP, CISM, and NACD.DC™;
Murray Kenyon, US Bank; and Nicola Sanna, Safe Security and The FAIR Institute*

Ensuring the board of directors is ready and able to effectively provide the strategic direction necessary to successfully integrate AI capabilities into their organization is a significant contemporary challenge. Artificial intelligence systems are transformative technologies that are disrupting entire industries and reshaping societal interactions. Their capabilities offer tremendous opportunities to organizations, yet, like other automated systems, they also present noteworthy new risks, as they are susceptible to significant cyber vulnerabilities.

Boards must ensure they have access to the right knowledge, data, and talent to understand and carefully weigh the balance between opportunities and risk to make timely and well-informed decisions regarding how to best incorporate AI capabilities (e.g., those used for analysis, assistance, augmentation, or autonomy) into their organization. Companies can and should leverage existing risk assessment frameworks to evaluate AI risk in economic terms and evaluate the most effective risk-mitigation controls.

Boards need to pay close attention to the cyber risks associated with AI systems. Nation-state and cyber-criminal groups have AI systems in their sights and are actively using and targeting them. The volume and severity of these threats continues to grow, targeting vulnerabilities that include those emerging from poor software coding and security practices used by well-intentioned AI system developers eager to rush their products to market. Acquiring and using an AI system that is poorly designed and includes material defects will likely expose your organization to unacceptable risks. Before acquiring AI systems and capabilities, boards should ensure their organization exercises due care and diligence in verifying their suppliers are indeed following best practices in AI engineering, including incorporating

DevSecOps software engineering principles into the development of the software-intensive systems. For example, the Software Engineering Institute at Carnegie Mellon continues to highlight best practices in AI engineering, software engineering and cybersecurity to guide developers to make AI systems the best they can be.⁴⁶ Further, risk quantification can help boards distinguish true risk signals from noise. Organizations should consider using available comprehensive models to quantify AI risks to account for potential severity and secondary losses.

In addition to cyber threats directed against vulnerabilities in AI systems, there are also risks emerging regarding the data used to train, maintain, and enrich AI systems. Data poisoning attacks, where a malicious actor deliberately tampers with data sources used by AI systems to negatively influence the efficacy of and trust in the system, are a legitimate threat to the integrity of AI systems. So is the consumption of data used to train the models that is not “ethically sourced” (e.g., data that contains personally identifiable information, intellectual property, or government classified information without the data owner’s permission or curation). Using AI systems whose data provenance and security protections are suspect may expose an organization to significant liabilities. Boards should ensure their organizations verify that their suppliers have appropriate rights to the data used by their systems and implement best practices in data security. Those suppliers should also be disclosing what AI models they subscribe to and use to augment or enhance their product offerings to your company. Additionally, boards should consult with their general counsel to identify any liabilities emerging from third-party failures to maintain proper data security and provenance controls.

⁴⁶ The CERT Division of Carnegie Mellon University’s Software Engineering Institute (SEI) created the Artificial Intelligence Security and Incident Response Team (AISIRT) in mid-2023 to confront the rising tide of AI-related cybersecurity threats to software algorithms, models, data sets, hardware, and supply chains. (<https://www.sei.cmu.edu/about/divisions/cert/>)

Boards are advised to secure an experienced and trusted independent third-party AI technical advisor. They also should invest in AI-related training opportunities from trusted sources such as NACD and Carnegie Mellon.⁴⁷

A purpose-built technology or product committee for companies that develop AI products can help focus the company on overseeing the necessary details of AI governance; however, boards should consider making AI

an agenda item for the entire board to consider as part of their overall strategic process as well.

Imperative for Boards

With AI disrupting so many business and societal models, boards need to act now with velocity and precision to ensure their organization remains competitive and secure.

⁴⁷ For more information, please see the web pages about the CERT Certificate in Cyber-Risk Oversight available on the NACD website (<https://www.nacdonline.org/education-and-events/elearning-courses-on-demand-courses/CERT-cyber-risk-oversight/>) and on the website of the CERT Division of the Software Engineering Institute (<https://insights.sei.cmu.edu/credentials/national-association-of-corporate-directors-nacd-cyber-risk-oversight-program/>) at Carnegie Mellon University.



4. Boardroom Tool Questions for Directors to Ask About AI

Larry Clinton, Internet Security Alliance, and Murray Kenyon, US Bank

High-performing boards comprise a diverse set of directors who ask direct and insightful questions as they seek knowledge to make informed decisions. Here are sample questions boards ought to ask about AI and cybersecurity:

GENERAL QUESTIONS

- ▶ How are our competitors using AI?
- ▶ How are we using AI?
- ▶ Do we feel obligated to do this?
- ▶ When we do “this” what is happening to our risk?
- ▶ How fast should we be, and/or do we need to be going?
- ▶ How can we use AI to disrupt our business and our industry?
- ▶ What are the risks of investing in AI versus maintaining the status quo?
- ▶ What’s our plan to acquire AI capabilities?
- ▶ Who can help us?
- ▶ How much will AI cost, and what is the expected return on investment?
- ▶ Who will lead our AI effort, and what makes them qualified to do so?
- ▶ How do we measure success?
- ▶ Do we need a Chief AI Officer?
- ▶ What is our risk exposure if malicious cyber actors use AI-enabled technology to attack our infrastructure? How do we know?
- ▶ How can we use AI capabilities to reduce our cyber-risk exposure?
- ▶ Is the use of AI representing the shareholders’ interests?
- ▶ Does the board have a clear understanding of what our organization considers ethical use of AI to be?
- ▶ Has the organization clearly defined and communicated what ethical AI use means for us?
- ▶ Do we have internal processes in place to adequately communicate the ethical use of our AI systems?
- ▶ Do we have channels in place with entities outside our organization to adequately and appropriately communicate about the ethical use of our AI use cases?

QUESTIONS REGARDING AI RISKS

- ▶ What are the risks for our expected uses of AI? Can they be quantified?
- ▶ How will the use of AI disrupt the company's business and industry?
- ▶ What are the governance implications of the use of AI and related policies and controls?
- ▶ Have we segregated training data, so we know the provenance of the data used to train our models?
- ▶ Have we established an AI governance board or committee?
- ▶ How can we review and approve governance policies for AI that include human review by management?
- ▶ What is our CDO's (Chief Data Officer) or Data Governance leader's strategy for handling data sharing requests at the scale the business is implementing AI?
- ▶ What is our third-party risk associated with AI?
- ▶ Who are our riskiest vendors, and how is our organization managing that risk? (Most vendors are basically writing off as much AI risk as possible on the licensee, especially because this market is largely unregulated at this point.)

QUESTIONS REGARDING REGULATION OF AI

- ▶ Have we explored the operational and regulatory challenges related to the proposed use of AI?
- ▶ Where does the proposed AI use case rank on the EU Artificial Intelligence Act scale of risk (unacceptable risk, high risk, limited risk, or minimal risk) for both the provider and user?⁴⁸
- ▶ Are we developing AI in accordance with putative legislative and regulatory expectations?
- ▶ Have we assigned responsibility for tracking AI regulatory matters to a chief legal officer or general counsel as regulations develop?
- ▶ Are our policies, processes, procedures, and practices related to the mapping, measuring, and managing of AI risk in place, transparent, and implemented effectively? How do we know?
- ▶ Do our accountability structures ensure appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks?
- ▶ Are policies and procedures in place to address AI risks from third-party software and other supply-chain issues?
- ▶ Are we using protected data to train the model that can be subject to opt-out or removal requests?
- ▶ Have we reviewed our insurance policies for AI-related risks and use cases?

⁴⁸ Please see The Act Texts at <https://artificialintelligenceact.eu/the-act/>.

QUESTIONS REGARDING THE BOARD'S ABILITY TO OVERSEE AI

- ▶ Does the current board possess adequate expertise to properly and effectively perform oversight of our use of AI?
- ▶ Does the board need to institute its own AI board education program to enable it to properly carry out its fiduciary responsibility?
- ▶ Should the board hold periodic virtual sessions to consider/educate board members about AI as it pertains specifically to our business?
- ▶ Do we need to restructure the board to effectively manage our extended cyber risk due to our current and anticipated use of AI?
- ▶ Do we need a new committee to focus on AI?
- ▶ Should all the board committees be discussing AI?
- ▶ Should our AI/cyber risk be considered as a separate matter for board discussion and action, or should it be integrated as a part of our overall operations? Or both?

QUESTIONS REGARDING OVERSIGHT AND MANAGEMENT OF AI

- ▶ Does our corporate structure ensure management is balancing the potential benefits of AI with potential risk?
- ▶ Is the board considering AI risks simultaneously with economic benefits from AI use cases?
- ▶ Does our budgeting process ensure adequate funding for continuous monitoring, testing, and auditing of AI risk?
- ▶ Is there appropriate and sufficient employee training, including budget, to assure that relevant portions of the organization's workforce are able to implement the AI-based use case?
- ▶ Have we engaged "red teams"⁴⁹ to assess generative AI use cases, thus assuring that all necessary aspects of the organization have had proper input into the development and deployment of safe and resilient AI solutions?
- ▶ Have we considered the company's outsourcing plan with respect to AI and the risks outsourcing may entail?
- ▶ How do we know that our AI supplier is using best practices?
- ▶ Has the management team conducted adequate due diligence to determine the degree of risk associated with a specific AI use case based on the pre-deployment testing process?
- ▶ Are our testing, monitoring, auditing, and mitigation efforts reflected in our logging and metadata emanating from the AI itself, or is a human in the loop?
- ▶ Has the management team adequately and empirically determined that the proposed AI use case risk can be mitigated or transferred in line with the organization's risk appetite?
- ▶ Are processes in place to maintain an acceptable risk profile over time and accounting for the potential for the AI to "drift"?⁵⁰

⁴⁹ See NIST's Computer Security Resource Center's Glossary entry for "Red Team." (https://csrc.nist.gov/glossary/term/red_team#:~:text=Definitions,Sources)

⁵⁰ NIST provides a definition of "drift" in the *AI RMF Playbook*, under the "MEASURE 2.4" section. NIST defines "drift" this way: "This effect, often referred to as 'drift,' means AI systems no longer meet the assumptions and limitations of the original design." (https://airc.nist.gov/AI_RMF_Knowledge_Base/Playbook/Measure)

About the Internet Security Alliance

The mission of the Internet Security Alliance (ISA) 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. For more than 20 years, ISA has created a comprehensive theory and practice for cybersecurity covering 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. The ISA board has created a companion book, *Cybersecurity for Business* (with a foreword from NACD president and CEO Peter Gleason), that translates the board-level principles into roles and practices for a corporation's management team.

ISA has also defined a new approach to public policy on cybersecurity in its new book, *Fixing American Cybersecurity: Creating a Strategic Public Private Partnership*. Many of the proposals ISA makes in *Fixing American Cybersecurity* are integrated into the new National Cybersecurity Strategy recently released in 2023.

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



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 more than 47 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 nacdonline.org.





1100 Wilson Blvd.
Suite 2500
Arlington VA 22209
▶ nacdonline.org