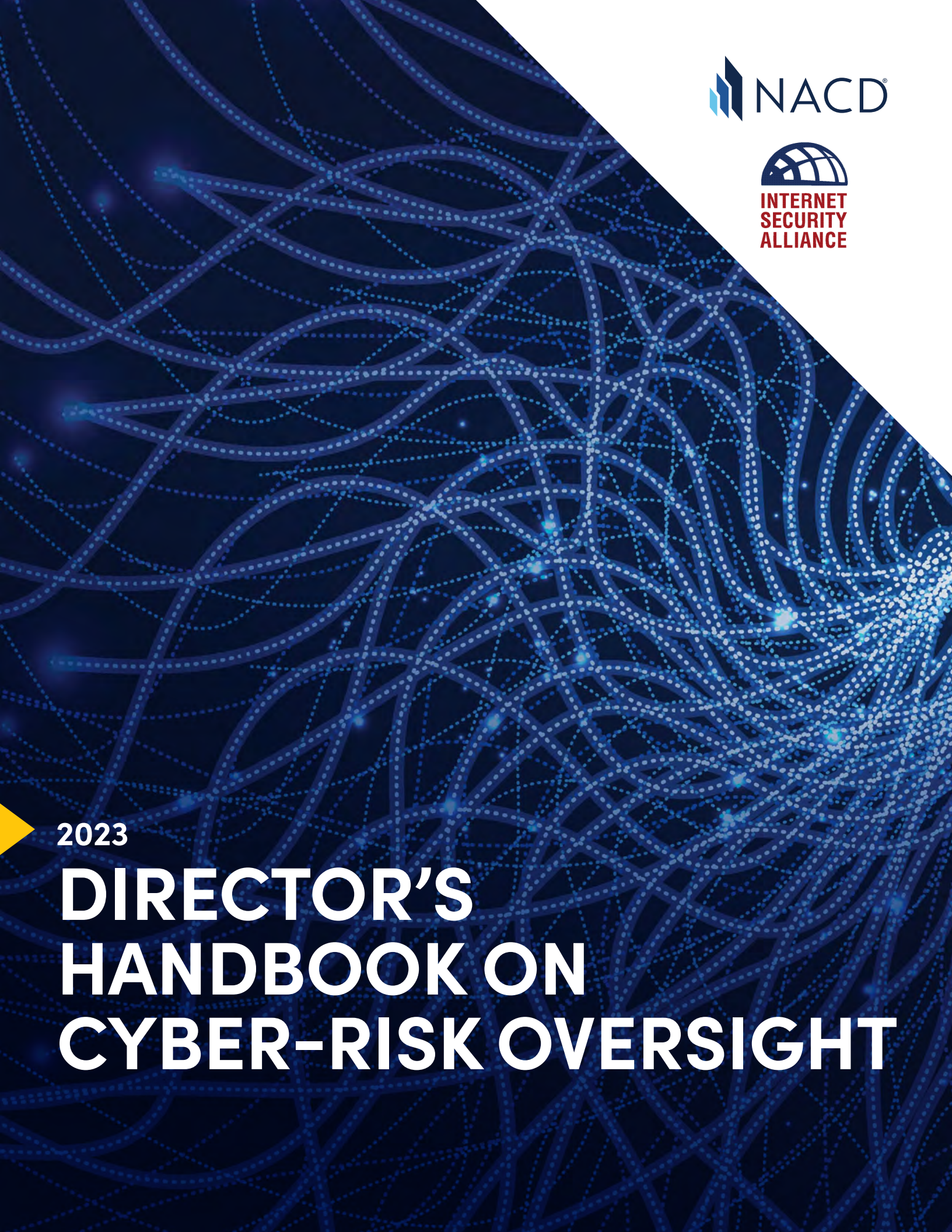

NACD

INTERNET SECURITY ALLIANCE

2023

DIRECTOR'S HANDBOOK ON CYBER-RISK OVERSIGHT

TOOL M

Board Decisions on the General Use of AI[1]

By Simon Sun and Larry Clinton, ISA

Much like the Internet itself artificial intelligence (AI) and machine learning (ML) are already becoming ubiquitous tools in many organizations. In 2021, private investment in AI totaled around $93.5 billion—nearly double the investment in 2020.[2] Also, as with the Internet, the use of AI and ML tools can provide dramatically enhanced business opportunities in terms of efficiency, innovation, and customer service. At the same time, the use of AI and ML can create vast new risks in terms of cybersecurity. The National Security Commission on Artificial Intelligence found that "AI applications are transforming existing threats, creating new classes of threats, and further emboldening state and non-state actors to exploit vulnerabilities in the US open society."[3]

Just as with the flip side of many other risks, certain applications of AI and ML tools can be used to enhance an organization's cybersecurity and lessen its risks. It is critical that the board work with management to understand the risk-reward balance of the specific uses of AI/ML their organization should embrace. This toolkit consists of two lists of questions to help guide the board's oversight of these advanced digital techniques. The first list is for the board's overall consideration of using various AI/ML techniques. The second list focuses on the specific issues in the use of AI for cybersecurity

DEFINING ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

"Artificial Intelligence (AI), a term coined by emeritus Stanford Professor John McCarthy in 1955, was defined by him as 'the science and engineering of making intelligent machines'. Much research has humans program machines to behave in a clever way, like playing chess, but, today, we emphasize machines that can learn, at least somewhat like human beings do."

"Machine Learning (ML) is the part of AI studying how computer agents can improve their perception, knowledge, thinking, or actions based on experience or data. For this, ML draws from computer science, statistics, psychology, neuroscience, economics and control theory."

Source: Professor Christopher Manning, Stanford University, 2020.[4]

GENERAL QUESTIONS FOR THE BOARD TO CONSIDER IN OVERALL USE OF AI/ML

1. **What is the goal for the company or organization to employ this system?**
2. **What is the plan to build or deploy this AI or ML application responsibly?**
3. **What type of system is the company using: process automation, cognitive insight, cognitive engagement, or some other type? Do our board and management understand how this system works?**
4. **What are the economic benefits of the chosen system?**
5. **What are the estimated costs of not implementing such a system?**
6. **Are there any potential alternatives to the AI or ML systems in question?**

7. How easy will it be for an adversary to execute an attack on the system based on the technical characteristics?
8. What is the organization's strategy to validate data set collection practices?
9. How will the company prevent inaccuracies that may exist in the data set?
10. What will be the damage incurred from an attack on the system in terms of the likelihood and the ramifications of the attack?
11. How frequently will the company review and update its data policies?
12. What is the organization's response plan for cyberattacks involving these systems?
13. What is the company's plan to audit the AI system?
14. Should the company create a new team to audit the AI or ML system?
15. Should the company build an educational program for its staff to learn about the use and risks of AI and ML in general?

QUESTIONS FOR THE BOARD OF DIRECTORS TO ASK WHEN DECIDING WHETHER TO USE AI FOR CYBERSECURITY PURPOSES[5]

1. What is the company's overall road map to implementing AI and/or ML in cybersecurity?
2. What are the cybersecurity goals that the organization is trying to achieve by implementing this AI or ML solution?
3. How will the system toughen the companies' security stance? How will success be measured?
4. What is the estimated harm that the company will face without the system?
5. What are the new cybersecurity vulnerabilities that the company will face in employing the system?
6. What type of cyberattack is the system designed to detect, predict, and respond to?
7. Is the system prepared to detect and weather a ransomware attack?
8. How would implementing such a system affect the organization's cybersecurity team? What are the benefits and risks associated with the tool's use by the team?
9. Should the company expand or update the current cybersecurity team?
10. How much would it cost for the company to create a new cybersecurity team?
11. Are there any positions that the company doesn't need any more due to employing the AI or ML cybersecurity system?
12. Should the company create a sub-team to monitor the outcomes and findings of the new system?
13. Will implementing such a system affect the company's cyber insurance enrollment?
14. Are there any potential legal consequences of not implementing AI/ML in a cybersecurity system?

ENDNOTES

[1] The following questions are designed primarily based on "A.I. and Risk Management: Innovating with confidence report" by Deloitte (https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/deloitte-gx-ai-and-risk-management.pdf) and "Attacking Artificial Intelligence: A.I.'s Security Vulnerability and What Policymakers Can Do About It" by Harvard Kennedy School Belfer Center for Science and International Affairs. (https://www.belfercenter.org/publication/AttackingAI).

[2] Daniel Zhang, Nestor Maslej, Erik Brynjolfsson, John Etchemendy, Terah Lyons, James Manyika, Helen Ngo, Juan Carlos Niebles, Michael Sellitto, Ellie Sakhaee, Yoav Shoham, Jack Clark, and Raymond Perrault, *The AI Index 2022 Annual Report* (AI Index Steering Committee, Stanford Institute for Human-Centered AI, Stanford University, March 2022), p. 3. (https://aiindex.stanford.edu/wp-content/uploads/2022/03/2022-AI-Index-Report_Master.pdf)

[3] June 10, 2022, tweet of the DAIMLAS Artificial Intelligence Ecosystem Builders, "AI applications are transforming existing threats, creating new classes of threats, and further emboldening state and non-state adversaries to exploit vulnerabilities in the US open society," Twitter. (https://twitter.com/daimlas/status/1535389680195207168)

[4] Christopher Manning, Stanford University Human-Centered Artificial Intelligence, *Artificial Intelligence Definitions* (September 2020). (https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf)

[5] The previous tool questions should apply in this section as both are referring to the use of AI systems.