Cybersecurity

Empowering AI Leadership

Contents

3 **Introduction**

4 **Responsibilities**

5 **Oversight**

8 **Discussion Guide**

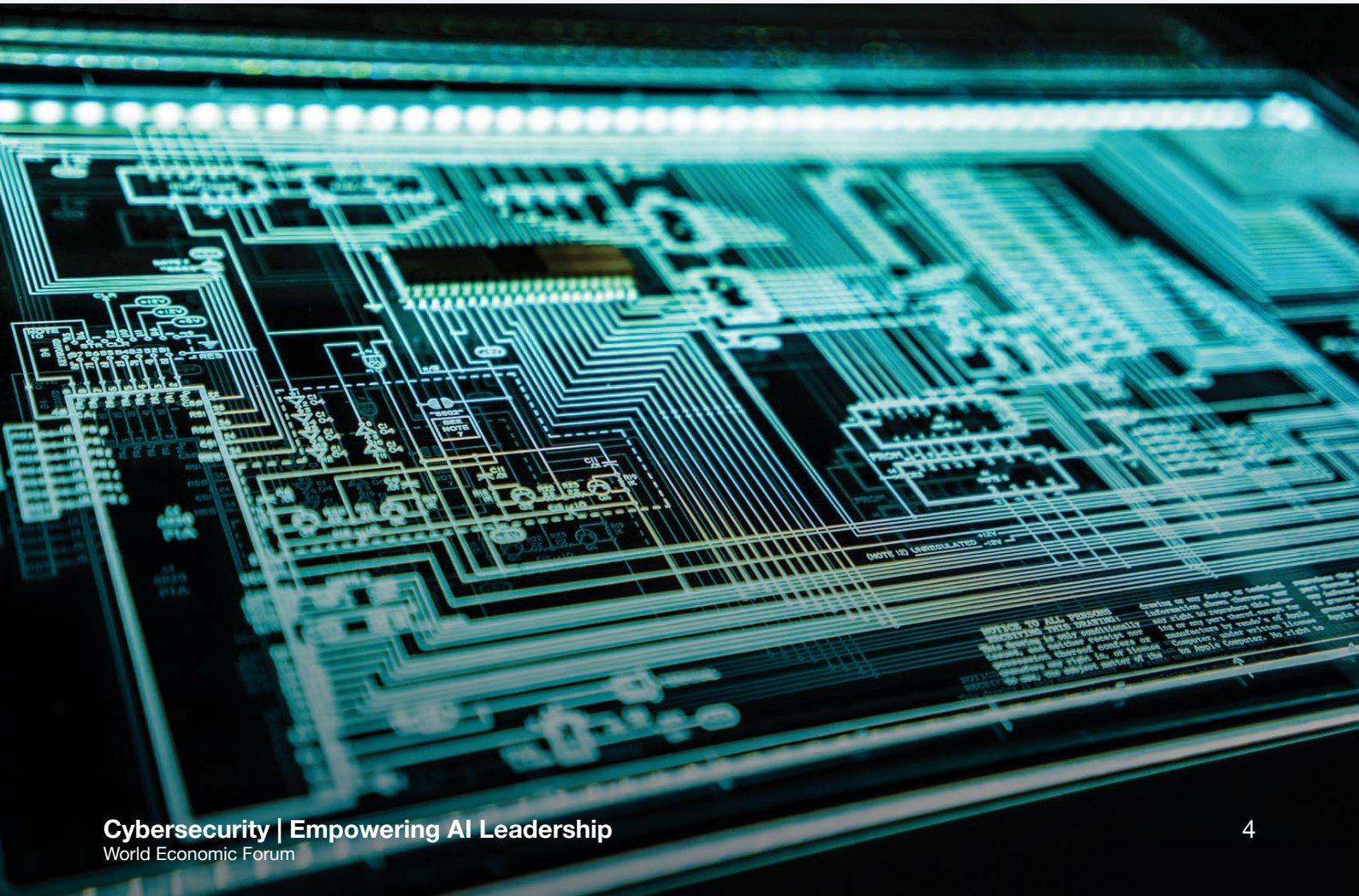
11 **Endnotes**

Introduction

Artificial intelligence (AI) capabilities present both exciting opportunities as well as complex risks related to an organization's cybersecurity and cyber-resilience capabilities. For example, AI can be used to support asset inventory, network monitoring and anomaly detection, improving critical elements of an organization's cyber-resilience programme. But the use of AI can also present new cyber-risks, stemming from technological vulnerabilities or issues related to the confidentiality, integrity and availability of data used for AI decision-making. Given the broad scope and potential impact of these opportunities and risks, the board should ensure it is prepared to assess and manage the cyber-risk and resilience implications of AI, integrated with the organization's overall enterprise risk-management framework.

Responsibilities

While AI may present unique use cases and concerns, its cyber-risk and resilience implications arise in the context of complex and highly interconnected ecosystems. The AI Oversight Toolkit provides guidance based on a general set of standards, including the G20/OECD Principles of Corporate Governance, 2015. With regard to the necessity for board governance of cybersecurity risks and resilience, the World Economic Forum and its partners have developed a comprehensive framework of ten core principles intended to enable boards to fulfil their responsibilities within that context. In order to ensure responsible oversight of cyber-risk and resilience related to AI, boards can draw upon this same framework to incorporate the cybersecurity implications of AI into their overall approach to cyber-risk and resilience.



Oversight

Principle 1:

Responsibility for cyber-resilience
The board as a whole takes ultimate responsibility for the oversight of cyber-risk and resilience, and it may delegate primary oversight activity to an existing committee or new committee.

Cyber-risk and resilience concerns arise whenever new technologies such as AI are introduced and used in different capacities within an organization (see Technology Module). Given the broad and diverse use cases for AI, the board should discuss whether and how the structure and process for reviewing cyber-risk and resilience associated with AI can be integrated into existing structures for oversight of cyber and new technology.

Principle 2:

Command of the subject
Board members receive cyber-resilience orientation upon joining the board and are regularly updated on recent threats and trends, with advice and assistance from independent external experts being available as requested.

Board orientation and regular updates on cyber-resilience should incorporate threats and trends related to cyber-risk and resilience associated with AI. Given the variety of contexts in which an enterprise may use or encounter AI capabilities, the scope of board orientation and updates related to AI should include both existing and future use cases.

Principle 3:

Accountable officer
The board ensures that one corporate officer is accountable for reporting on the organization's capability to manage cyber-resilience and progress in implementing cyber-resilience goals. The board ensures that this officer has regular board access, sufficient authority, command of the subject matter, experience and resources to fulfil these duties.

The board should ensure that the corporate officer accountable for reporting on cyber-risk and resilience considers and incorporates, as appropriate, the organization's use of and interaction with AI capabilities in his or her reporting responsibilities. Given the broad and varied potential use cases for AI, the board should also ensure that the accountable corporate officer has sufficient visibility of all areas of the organization where AI may arise.

Principle 4:

Integration of cyber-resilience
The board ensures that management integrates cyber-resilience and cyber-risk assessment into overall business strategy and into business-wide risk management, as well as budgeting and resource allocation.

The board should ensure that management integrates cyber-resilience and cyber-risk assessment related to the acquisition, use of or interaction with AI into business strategy and business-wide risk management.

Principle 5:

Risk appetite
The board annually defines and quantifies business-risk tolerance relative to cyber-resilience and ensures that this is consistent with corporate strategy and risk appetite. The board is advised on both current and future risk exposure as well as regulatory requirements and industry/societal benchmarks for risk appetite.

In defining and quantifying business risk tolerance relative to cyber-resilience and ensuring consistency with corporate strategy and risk appetite, the board should ensure robust consideration of the potential cyber-risks associated with the organization's current and anticipated use of AI. The board should ensure that risk exposure related to AI is included when it is advised on current and future cyber-risk exposure, regulatory requirements and industry/societal benchmarks for risk appetite.

Principle 6:

Risk assessment and reporting
The board holds management accountable for reporting a quantified and understandable assessment of cyber-risks, threats and events as a standing agenda item during board meetings. It validates these assessments with its own strategic risk assessment using the Board Cyber-Risk Framework.[1]

The board should hold management accountable for including cyber-risks, threats and events related to current and future use of AI in its risk assessment and reporting.

Principle 7:

Resilience plans
The board ensures that management supports the officer accountable for cyber-resilience through the creation, implementation, testing and ongoing improvement of cyber-resilience plans, which are appropriately harmonized across the business. It requires the officer in charge to monitor performance and to regularly report to the board.

The board should ensure that management takes full account of existing use of AI across the organization (including to support the execution of the resilience plans themselves) when creating, implementing, testing and improving the cyber-resilience plans in support of the accountable officer.

Principle 8:

Community
The board encourages management to collaborate with other stakeholders, as relevant and appropriate, in order to ensure systemic cyber-resilience.

The board should encourage collaboration with respect to current and potential enterprise-level use of AI as well as global developments in AI that may affect the broader environments in which the organization operates.

Principle 9:

Review
The board ensures that a formal, independent cyber-resilience review of the organization is carried out annually.

The board should ensure that this annual review includes the organization's use of, and interaction with, AI capabilities.

Principle 10:

Effectiveness
The board periodically reviews its own performance in the implementation of these principles or seeks independent advice for continuous improvement.

In light of the rapid development of AI, the board should consider whether it needs to seek independent advice for continuous improvement of its own performance with respect to cyber-risk and resilience oversight of AI.

Discussion Guide

Principle 1:

Responsibility for cyber-resilience

- Based on the company's current and anticipated future use of and interaction with AI, does the board's existing structure and process for reviewing cyber-risk and resilience provide sufficient oversight of AI?
- What skills and attributes do current and future board members need in order to understand cyber-risk and resilience with respect to AI?
- Do existing board members possess the requisite skills and experience to effectively oversee cyber-risk and resilience with respect to AI?

Principle 2:

Command of the subject

- Does the board receive initial orientation and regular updates on cyber-resilience, including threats and trends related to the current and anticipated future use of AI within the organization?
- Does the board ensure that internal updates regarding the organization's cyber-resilience, risk exposure and risk stance, as well as any independent assessments and benchmarking of the organization's cyber-risk and resilience approach, incorporate the organization's current and anticipated future use of AI?

Principle 3:

Accountable officer

- Is the assigned corporate officer accountable for cyber-risk and resilience also authorized and accountable for reporting on cyber-risk and resilience related to AI?
- Does the corporate officer accountable for reporting on cyber-risk and resilience related to AI have sufficient visibility over all areas of the organization where AI may arise?
- Does the corporate officer accountable for reporting on cyber-risk and resilience related to AI have sufficient visibility over all areas of the organization where AI may arise?

Principle 4:

Integration of cyber-resilience

- Does the board ensure that management integrates cyber-resilience and cyber-risk assessment – as related to the organization's acquisition, use of or interaction with AI – into an overall business strategy and business-wide risk management?
- Does the board review annually the organization's strategic plan, ensuring that cyber-risk and resilience of current or anticipated use of AI is appropriately incorporated and represented in the plan?
- Does the board consider the organization's current and anticipated use of AI in its review of the organization's cyber-resilience strategy, including risk-management options such as insurance?

Principle 5:

Risk appetite

- Does the board have an understanding and visibility of how the organization's cyber-risk appetite is being applied in business decision-making related to AI?
- Is risk exposure related to the organization's current and anticipated future use of AI included when the board is advised on current and future cyber-risk exposure, regulatory requirements and industry/societal benchmarks for risk appetite?

Principle 6:

Risk assessment and reporting

- Does the board hold management accountable for providing balanced reporting regarding the present and future organizational and ecosystem-wide cyber-risk situation – including those affected by the development of AI – as a standing agenda item during board meetings?
- Does the board receive updates from management regarding specific threats and trends associated with the use of AI by third parties?
- Does the board ensure that management's action plans regarding the organization's cybersecurity culture and awareness take into account current or future use of AI?

Principle 7:

Resilience plans

- Does the board ensure that management's cyber-resilience plans – including business continuity, communications, disaster recovery and incident response plans – take full account of the existing use of AI across the organization (including supporting the execution of the resilience plans themselves)?
- What is the organization's policy regarding the board's role in relation to cyber-resilience plans – including those related to the deployment of AI as part of those plans – and has this been clearly and explicitly communicated to the board and executive management?
- Does the board ensure that management has adopted an appropriate approach to cyber-resilience related to the organization's use of and interaction with AI?

Principle 8:

Community

- Does the board encourage management to collaborate with other stakeholders, as consistent with overall business strategy, related to current and potential enterprise-level use of AI as well as global developments in AI that may affect the broader environments in which the organization operates?
- Does the board receive updates from the corporate officer accountable for reporting on cyber-risk and resilience regarding potential opportunities for community collaboration to address cyber-risk and resilience related to AI, as well as the benefits and risks of such collaborations on a broad basis and with respect to specific stakeholders?
- Does the corporate officer accountable for reporting on cyber-risk and resilience ensure internal coordination by all relevant parts of the organization on the cyber-risks arising from AI?

Principle 9:

Review

- Does the board ensure that there is an annual independent cyber-resilience review of the organization that includes the organization's use of, and interaction with, AI capabilities, as overseen by the accountable corporate officer in collaboration with other relevant corporate officers?
- Does the board ensure there is a process in place to evaluate third-party cyber-risk and resilience as related to AI?

Principle 10:

Effectiveness

- Does the board periodically review its own performance in the implementation of these principles?
- In light of the fast-developing potential uses of AI, does the board need to seek independent advice for continuous improvement of its own performance with respect to cyber-risk and resilience oversight of AI?

Endnotes

(Reference as of 24/7/19)

1. The Board Cyber-Risk Framework is detailed in Advancing Cyber Resilience Board Principles.

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Phone: +41 (0) 22 869 1212

San Francisco Centre for the Fourth Industrial Revolution
1201 Ralston Ave, San Francisco, CA 94129,
Phone: (415) 704-8848

contact@weforum.org | www.weforum.org

For more information, contact Kay Firth-Butterfield,
Head of AI and Machine Learning,
Centre for the Fourth Industrial Revolution.

kay.firth-butterfield@weforum.org