NACD

INTERNET SECURITY ALLIANCE

WORLD ECONOMIC FORUM

Principles for Board Governance of Cyber Risk

INSIGHT REPORT

MARCH 2021

In Collaboration with PwC

Cover: Getty Images

Contents

Preface

Digital risk, including cyber risk, is a pervasive and potentially existential concern. Leaders need to understand and take account of cyber risk in their strategic decisions.

Peter Gleason
Chief Executive Officer, National Association of Corporate Directors

Larry Clinton
President, Internet Security Alliance

Sean Joyce
Global and US Cybersecurity, Privacy and Forensics Leader, PwC

Daniel Dobrygowski
Head of Governance and Trust, Centre for Cybersecurity, World Economic Forum

Accelerating digitalization puts new pressures on companies to overhaul their business models and, indeed, fundamentally reimagine how they conduct business. Given that companies are increasingly judged on how well they protect their own information as well as the data entrusted to them by customers and partners, cybersecurity and cyber resilience have become vital concerns for any trustworthy organization.

The growth of our global digital footprint has ensured that cybersecurity will remain a priority for business leaders for years to come. As a result, cybersecurity governance will continue to be a matter of importance for boards of directors. As we are seeing when boards consider environmental, social and governance (ESG) factors,[1] companies that manage the entire portfolio of risks, including cyber, do better in the marketplace.

As a result of a rapidly changing cyber-threat landscape and proliferating regulations, it has become clear that boards, especially, need stronger foundations to govern cyber risks effectively. This report details the work of the leading organizations in this field, the World Economic Forum, the National Association of Corporate Directors (NACD) and the Internet Security Alliance (ISA), along with our global partners and our project adviser, PwC; in it we share our consensus-based, principled approach to delivering successful cyber-risk governance at board level.

There is a need for a cohesive, global, cross-border approach to cyber-risk governance. We therefore convened a group of cybersecurity and functional experts, including senior security, legal and risk officers, business leaders and industry experts, to explore methodologies for boards of directors to follow in improving the cyber-risk position of their organizations regardless of location or industry. These practices and approaches were further validated by members of the boards of some of the most advanced companies in the world. The work that follows represents the collaborative efforts of that group to shape the principles and supporting practices for boards of directors. Their adoption will strengthen cybersecurity and resilience across organizations and environments.

This is an ongoing effort, and we hope that this paper and the accompanying knowledge base that has been and will continue to be developed provide leaders with the guidance necessary to help their organizations achieve the understanding of cyber risk – and their role in governing it – necessary to thrive in the Fourth Industrial Revolution and beyond.

In the NACD Board Survey, **60.5%** of board directors identified cybersecurity as a “very important” or “important” area for improvement over the next 12 months.[2]

Executive summary

This report outlines six globally applicable principles to aid board directors in governing cyber risk.

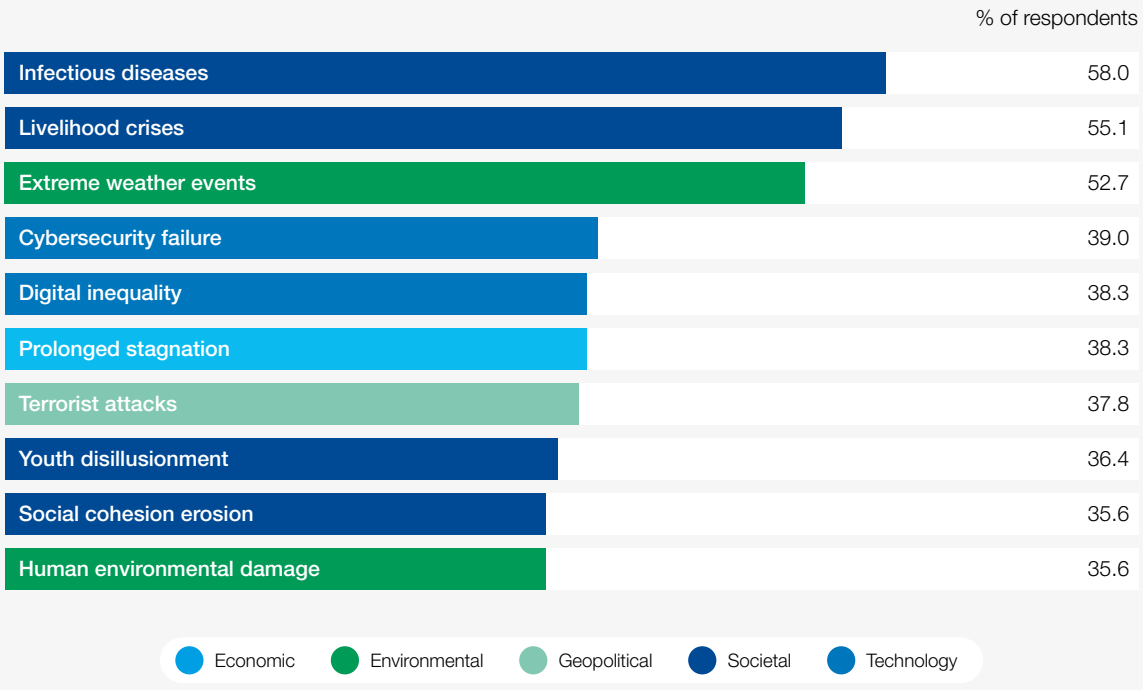
Cyber risk remains among the top risks facing business organizations today. The World Economic Forum's *Global Risk Report 2021* lists cybersecurity failure as a top "clear and present danger" and critical global threat.[3] As with any major enterprise issue, it is important for the board of directors and leadership to set the tone at the top and define how their organizations must address cybersecurity.[4]

This document is the result of collaboration between the World Economic Forum, National Association of Corporate Directors (NACD), Internet Security Alliance (ISA) and a working group of industry professionals, supported by project adviser PwC. These organizations came together to build a set of consensus principles that recognized up-to-date techniques for cyber-risk governance. Building off existing guidance and through an iterative development process, this group developed six consensus principles for cybersecurity board governance.

This paper is designed for corporate directors to reference and follow as they set cybersecurity strategy and engage with stakeholders from across their business and their sector on the issue of cyber risk. In exercising the board's oversight function, we recognize that the best action for the board is to demand, review and analyse management's plans for cyber risks. The contents within provide guidance, examples and critical questions that directors may find useful as they seek to understand their organization's current position, exercise their oversight function and set future goals.

FIGURE 1 **Global risks horizon**

Clear and present dangers
Short-term risks (0–2 years)



Source: Adapted from World Economic Forum Global Risk Report 2021.

Background

Six principles were developed collaboratively by experts on cyber risk in order to integrate and update the leading guidance for directors.

This paper is not the first guidance to be released on the issue of corporate cybersecurity governance. In fact, since 2017, which saw the publication of the original World Economic Forum's *Advancing Cyber Resilience: Principles and Tools for Boards*[5] and the *NACD/ISA Director's Handbook*,[6] numerous resources have been created.[7]

The intention of this work was to find areas of consensus among the leading publications to appeal to a wider, global audience of boards and management teams. The set of principles defined below were developed through the integration of the NACD/ISA 2020 guidance and the World Economic Forum's 2017 publication on the same topic. The principles were then reviewed, discussed and revised in detail by a working group of industry professionals, including representatives of NACD and ISA, with further guidance by non-executive directors of the board from a cross-section of industry-leading companies.

The format of these principles is designed to be easy to digest and aligned with the level of oversight required for corporate directors. Each principle is defined and briefly described, additional perspective being provided in the form of brief implementation guidance statements that demonstrate effective implementation of the principles.

FIGURE 2 **What five trends do you foresee having the greatest effect on your company over the next 12 months?**

Source: National Association of Corporate Directors, 2020-2021 NACD Trends and Priorities of the American Boardroom, pp. 15-20

1

Principles for board governance of cyber risk

The six consensus principles are designed to support board oversight of a cyber-resilient organization while driving strategic goals.

FIGURE 3 **Consensus principles visualized**

Next, this report expands on these principles, with additional context to facilitate adoption and understanding. Additionally, included under each principle are important steps that board directors may take in order to improve cyber-risk governance within the enterprise.

2 The cyber-risk principles in depth

Each principle is defined with additional information and brief guidance to demonstrate effective implementation.

2.1 Cybersecurity is a strategic business enabler

Cybersecurity is more than just an IT issue

Cyberthreats are persistent, strategic enterprise risks for all organizations regardless of the industry in which they operate. Effective organizational cybersecurity directly contributes to both value preservation and new opportunities to create value for the enterprise and larger society. Navigating this risk requires a culture of cybersecurity with leadership commitment to, and modelling of, good cybersecurity decision-making.

Key considerations for the board:

- Hardwire cyber-risk considerations into key operational and strategic decision-making process, including the adoption of cyber risk as a recurring agenda item for full board meetings
- View each major new digital transformation initiative through the lens of cyber risk
- Determine which board committee should have primary oversight of cyber-risk issues
- Analyse cybersecurity issues with respect to their strategic implications and as part of enterprise risk; additionally, analyse business strategy and business model considerations with respect to cybersecurity issues
- Ask executives to identify opportunities to use cybersecurity as a market differentiator/ business driver

In the NACD Board Survey, **70%** of board directors reported viewing cybersecurity as “a strategic, enterprise risk”.[8]

In a survey of more than 400 global companies, conducted by PwC in Q4 2020, 52% of board member respondents reported making significant progress in improving customer trust in the past three years as a result of strengthened cybersecurity practices.

2.2 Understand the economic drivers and impact of cyber risk

Cyber risk remains among the top risks facing business organizations today. However, only 17% of organizations say they are realizing the benefits from better quantification of cyber risk.

Enterprise decision-making requires analysis of the economics of cyber risk

Many business initiatives that drive profitability can also increase cyber risk. In order for organizations to make effective business decisions, risk determinations should focus on the financial impact to the organization, including trade-offs between digital transformation and cyber risk. By using scenario planning, leaders in the organization can consider potential gains and losses relative to other business priorities and obligations. Leaders should also measure cyber risk (empirically and economically) against strategic objectives, regulatory and statutory requirements, business outcomes and cost of acceptance, mitigation or transfer.

Key considerations for the board:

- Review and approve the organization's cyber-risk appetite, or tolerance,[9] in the context of the company's risk profile and strategic goals by ensuring management has:
  - Defined cyber-risk appetite levels in financial terms to inform decision-making and developed key metrics to measure overall cyber-risk management performance
  - Implemented a programme that seeks to identify cyber-risk scenarios that align with the organization's risk profile and establish a risk appetite
  - Provided the board with detailed rationales for the organization's determination of materiality of risk, including cyber risk, based on an indication of the risk's reputational, customer, financial and other relevant impacts as part of its regular risk-management monitoring framework
- Instruct management to establish a consistent framework, using industry-accepted risk quantification models, for calculating the potential economic impact and likelihood of cybersecurity scenarios
- Require continuous examination of comparative measurements and metrics[10] for cyber risk. Industry-accepted frameworks and reporting can guide data-driven decisions, aligning risk appetite with organizational goals and strategy
- Base cyber-risk management decisions on the potential impact and likelihood of risk events and functional loss or exposure

Economic decision-making in the context of cyber risk

Choosing to enter a new market may have substantial business advantages. However, the cyber risks – such as additional network connections, theft of IP and new regulatory exposure – could be just as, or even more, substantial. This is a strategic business decision for the board.

The board needs to consider not just the economic upside of the new market but the economic downside of the cyber risk. Management should provide the board with an empirical and economic assessment of the probable extent of cyber risks versus the probable business advantages using modern risk-assessment techniques that enable such analysis. This analysis also helps determine the appropriate risk-mitigation or risk-transfer mechanisms available to compensate for the risk.[11]

37% of organizations strongly agree that quantifying risks leads to better management of cyber risks against the spend; chief executive officers are more likely to strongly agree.

However, only 17% of organizations say they are realizing the benefits from better quantification of cyber

2.3 Align cyber-risk management with business needs

Boards should understand and assess how to effectively manage cyber risks in the pursuit of business objectives

By focusing on how to treat cyber risks (through avoidance, acceptance, mitigation or transfer), organizations can build a security profile that aligns with business needs and defined risk tolerances or risk appetite. Effective governance of any enterprise requires clear alignment between cyber-risk management and business objectives across every facet of decision-making, including mergers and acquisitions, business transformation, innovation, digitalization, pricing, product development, market expansion etc.

Key considerations for the board:

- Critically review the organization's business strategy and drivers (e.g. digital growth) in the context of their cyber-risk implications
- Require management (i.e. the entire C-suite) to report to the board on the cybersecurity implications of their activities, including relevant cyber risks, risk ownership and alignment to the enterprise risk-management programme, while not neglecting to cover how decisions on cyber risk are tracked
- Require management to report to the board with well-developed, written and tested plans (or roles in the overall plan) to counter adverse cyber events
- Require management to integrate cyber-risk analysis into significant business decisions (e.g. launching a new product or publishing an app), along with effective assurances of the information's quality and comprehensiveness
- Require management to provide the board with roadmaps on how the company makes determinations of risk materiality that inform regulatory obligations[13]

2.4 Ensure organizational design supports cybersecurity

Organizational structure should integrate and support security and strategic goals

Organizations should design an internal governance structure that addresses cybersecurity on an enterprise-wide basis. This includes defining clear ownership, authority and key performance indicators (KPIs) among all internal stakeholders for critical risk management and reporting responsibilities. It also demands the integration of cybersecurity practices into how the business operates and makes decisions.

Key considerations for the board:

- Review the organizational structure to ensure that the cybersecurity function is adequately represented across the business, internal groups and leadership
- Understand the basis for, and challenge the assignment of, important roles and lines of accountability for cybersecurity strategy, policy and execution
- Set expectations that cybersecurity and cyber-risk functions are to receive adequate staffing and funding and monitor the efficacy of these determinations
- Inspire a cybersecurity culture and encourage collaboration between the cybersecurity function and all stakeholders relating to, and accountable for, cyber risk at various levels (e.g. compliance, privacy etc.)
- Ensure an accountable officer[14] has authority and responsibility to coordinate cyber-risk strategy throughout the organization and that the organization has a comprehensive plan for data governance

In a survey of more than 400 global companies, conducted by PwC in Q4 2020, 44% of board member respondents stated that their organizations have made significant progress over the past three years in improving employee experiences with the cyber function.

Meanwhile, 46% of board member respondents reported their companies making significant progress over the same period in more effective alignment between risk management and their organization's cyber programme.

2.5 Incorporate cybersecurity expertise into board governance

Board members must work closely with management to maintain an informed understanding of cyber risks to enable the organization to serve as a responsible party in the broader environment in which the business operates.

Boards need diverse sources of cybersecurity expertise

Boards must avail themselves of external industry and other guidance as well as the cybersecurity expertise of fellow directors, third parties and internal resources to effectively oversee the organization's cybersecurity within an appropriate structure focused on oversight. In light of the rapidly changing cyber landscape, board directors themselves must continually seek to expand their own knowledge of this topic.

Key considerations for the board:

- Build relationships with internal stakeholders who can provide expertise to guide strategic cybersecurity decisions, up to and including ensuring cyber expertise is represented on the board
- Partake in opportunities to increase board directors' base level of knowledge on cyber risk
- Seek out third-party advisers and assessors – who report to the board regularly – to ensure effective oversight of management
- Consider periodic audits, reviews of cybersecurity strength and benchmarking by independent third parties
- Carry out regular sessions with the board to update the group on recent cyber incidents, trends, vulnerabilities and risk predictions. Use external third parties, where necessary, to ensure accuracy and competence

Board allies in cybersecurity

Directors, recognizing that cyber risk is an enterprise-wide concern, should look to a variety of executives and managers in order to ascertain the full impact of cyber risk on the organization. Each member of the management team has a responsibility to understand the impact of cyber risk within her or his remit and can therefore support the board's effort to develop a holistic view. While the chief information security officer (CISO) may be some organizations' foremost cyber-risk expert and main point of contact for the board on cyber-risk issues, the CISO need not work in isolation. Executives who can support the board's understanding of cyber risk include:

- Chief risk officer
- General counsel/chief legal officer
- Chief information officer
- Chief technology officer
- Chief trust officer
- Chief privacy officer

This is a non-exhaustive list of allies the board can call upon to examine the company's cyber risk.

Does the board need a "cyber expert"?

Considering how pervasive cyber risk has become, some companies may seek to recruit board directors with cyber risk or cybersecurity expertise. While the question of how necessary this is arises with greater frequency as digital risk becomes more widely recognized as a feature of modern business, there is no one answer that will fit every company. At the outset, companies should consider whether the board would be better served by increasing the entire board's understanding of cyber risk, rather than relying on a single member. Additionally, the board should consider the interface between cyber-risk management structures already in place with the board as well as the availability of "cyber experts" for recruitment and the specific attributes of expertise necessary in a candidate.[15]

2.6 Encourage systemic resilience and collaboration

Effective cyber-risk strategy includes improving the cyber resilience of industries and sectors

The highly interconnected nature of modern organizations means we run the risk of failures that spread beyond one enterprise to affect entire industries, sectors and economies. It is no longer sufficient just to ensure the cybersecurity of your own enterprise; rather, cyber resilience demands that organizations work in concert. Recognizing that only collective action and partnership can meet the systemic cyber-risk challenge effectively, senior strategic leaders must encourage collaboration across their industry and with public and private stakeholders to ensure that each entity supports the overall resilience of the interconnected whole.

Key considerations for the board:

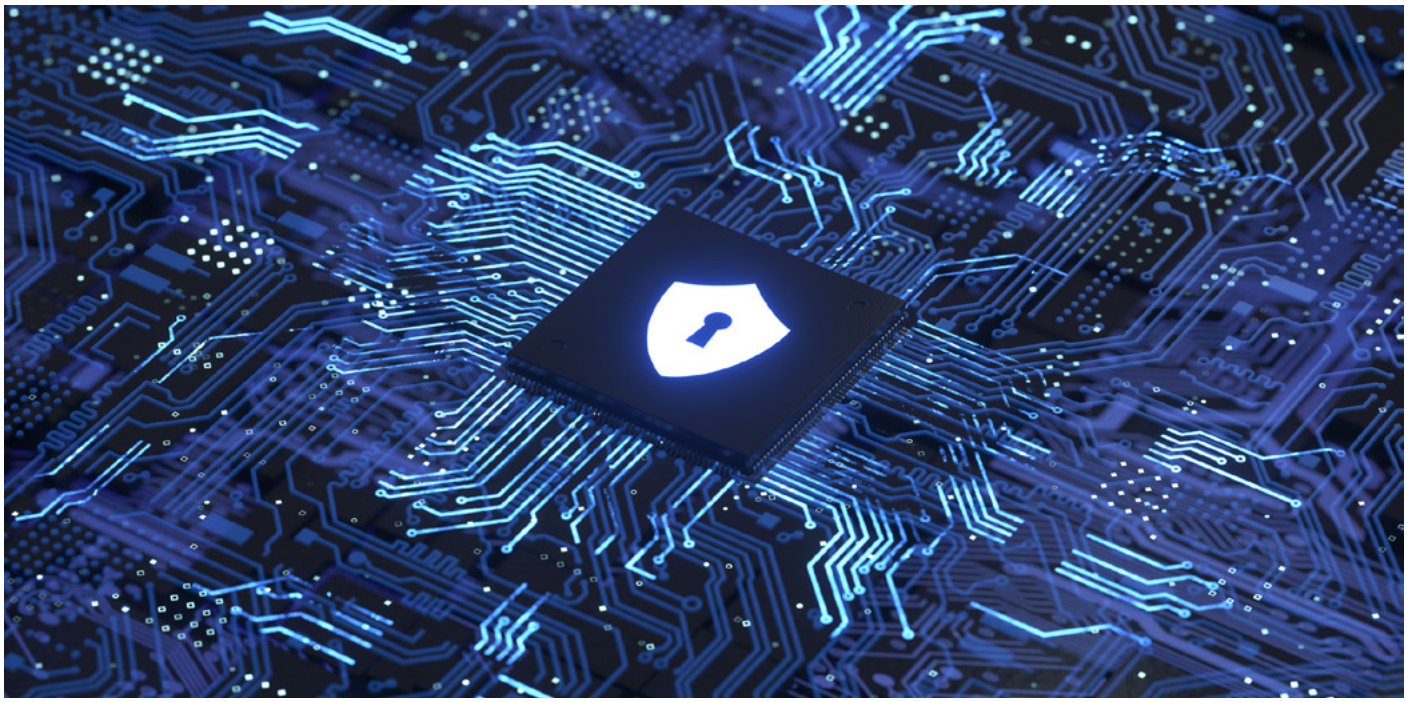
- Develop a 360-degree view of the organization's risk and resiliency posture to operate as a socially responsible party in the broader environment in which the business operates
- Develop peer networks, including other board members, to share best governance practices across institutional boundaries
- Ensure management has plans for effective collaboration, especially with the public sector, on improving cyber resilience
- Ensure that management takes into account risks stemming from the broader industry connections (e.g. third parties, vendors and partners)
- Encourage management participation in industry groups and knowledge and information-sharing platforms

The systemic implications of cyber risk

Cyber risks can arise from a company's network of partners, suppliers and vendors. Although not common, supply-chain attacks can tear through increasingly interconnected companies, passing from vendor to partner, and wreaking havoc on industries and economies.

In 2017, the NotPetya attack spread from a malware-infected system in Ukraine to paralyse global shipping and cause an estimated $10 billion in damages to a wide variety of industries, from pharmaceuticals to construction, from personal care to consumer foodstuffs.[16]

In 2020, malware was uploaded to much of the US federal government, including the Department of Defense, to 425 companies in the US Fortune 500, and to as-yet-untold other customers worldwide, by compromising an update installed by SolarWinds, a US-based technology infrastructure vendor.[17] The extent of the damage likely to follow, or even the purpose of the attack, is still open to speculation.



Conclusion

Board directors should adopt the consensus principles described in this report to form the basis of an effective cyber-risk governance regime.

The board needs to understand cyber risk, and its role in governing this threat, to perform its oversight function effectively. It continues to be important for members of the board of directors and industry professionals to increase their knowledge of how to address cybersecurity within their organizations. This report offers an opportunity for directors to increase their understanding of cyber risk and provides guidance for interactions as board directors more fully embrace their role with regards to cyber risk.

As part of this body of work, the World Economic Forum, NACD and ISA will continue their shared efforts to enhance boards' ability to incorporate cyber-risk planning into overall company strategy. Towards that end, our organizations have embarked on an effort to quantify the efficacy of these principles. What began as an offering of good practices here will soon expand into a research agenda that will help board directors to determine where best to apply their limited time and which aspects of the principles described here are likely to be the most crucial to implement in the shortest time frame. While all of the principles described in this report form the basis of an effective cyber-risk governance regime, soon we will understand what impact adoption of each principle is likely to have.

We ask readers of this report to adopt the principles described, endeavour to understand the impact of cyber risk on business strategy and work together to ensure that every organization is cyber resilient.

Taxonomy

Term	Definition
Accountable officer	A senior executive within the organization who is responsible and accountable to the board for developing and implementing the organization's cyber-risk and resilience programme[18]
Board and board of directors	Corporate fiduciaries responsible for overseeing management strategy, as well as the identification and planned response to enterprise-wide risks affecting a company and its value to stakeholders and shareholders[19]
Cyber resilience	A dimension of cyber-risk management, representing the ability of systems and organizations to develop and execute long-term strategies to withstand cyber events;[20] an organization's ability to sustainably maintain, build and deliver intended business outcomes despite adverse cyber events[21]
Cyber risk	Probable loss event that materializes when a cyberthreat affects an asset of value and results in a material impact on an organization. Cyber risk can be measured as the probable frequency and the probable impact of a loss event[22] Consideration should be given to the following aspects of this risk: – Physical – core technical infrastructure of hardware and software – Informational – content or data at rest or in transit – Cognitive – knowledge, values, beliefs, intentions and perceptions of individuals and groups
Cybersecurity	The set of activities that protect networks, devices and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity and availability of information and proper delivery of services [23]
Systemic cyber risk	The risk that a cyber event (attack[s] or other adverse event[s]) at an individual component of a critical infrastructure ecosystem will cause significant delay, denial, breakdown, disruption or loss, such that not only are services affected in the originating component but consequences also cascade into related (logically and/or geographically) components of the ecosystem, resulting in significant adverse effects to public health or safety, economic security or national security[24]

Contributors

Lead authors

Larry Clinton
President, Internet Security Alliance

Daniel Dobrygowski
Head of Governance and Trust, Centre for Cybersecurity, World Economic Forum

Sean Joyce
Global and US Cybersecurity, Privacy and Forensics Leader, PwC (Project Adviser)

Friso Van der Oord
Senior Vice-President, Content, National Association of Corporate Directors

Advisory team

Nisha Almoula
Project Fellow, World Economic Forum, New York

Clark Andrews
Project Fellow, World Economic Forum, New York

Georges DeMoura
Head of Industry Solutions, Centre for Cybersecurity, World Economic Forum

Chris Hetner
Special Advisor for Cyber Risk, National Association of Corporate Directors

Josh Higgins
Senior Director of Policy and Communications, Internet Security Alliance

Akshay Joshi
Head of Operations and Partner Engagement, Centre for Cybersecurity, World Economic Forum

Jeremy Jurgens
Managing Director, Head of Centre for Cybersecurity, World Economic Forum

Joe Nocera
Leader of Cyber and Privacy Innovation Institute, PwC (Project Adviser)

Independent Board Director Advisory Panel

These independent board directors, who volunteered to share their experience at the board level, contributed knowledge and feedback to this effort in their individual expert capacity.

Keith Alexander
sitting on the board of Amazon

Caroline Dorsa
sitting on the board of Biogen

Lynn Dugle
sitting on the board of State Street

Linda Hudson
sitting on the board of Bank of America

Leslie Ireland
sitting on the board of Citi

Shelley Leibowitz
President, SL Advisory, on the boards of MassMutual and Morgan Stanley

Michael G. Vickers
sitting on the board of BAE Systems

Maggie Wilderotter
sitting on the board of Hewlett Packard Enterprise

Acknowledgements

Working group

Candid Wüest
Vice-President of Cyber Protection Research, Acronis

Tracie Grella
Global Head of Cyber, AIG

Anthony Shapella
Head of Analytics, Cyber Insurance, AIG

Catharina Richter
Global Head of Cyber Center of Competence, Allianz

Shanil Williams
Global Head of Financial Lines. Allianz

Michael Meli
Chief Information Security Officer and Managing Director, Bank Julius Baer

Craig Froelich
Chief Information Security Officer, Bank of America

Kristen Marquardt
Senior Vice-President, Cyber Strategy and Communications Bank of America

John Slavitt
General Counsel, Check Point Software Technologies

Darren Thomson
Head of Cybersecurity Strategy, CyberCube

Pascal Millaire
Chief Executive Officer, CyberCube

Mark Hughes
Senior Vice-President and General Manager of Security, DXC Technology

Nick Sanna
President, FAIR Institute

John Holmes
Chief Legal Officer Forcepoint

Drew Simonis
Vice-President, Deputy Chief Information Security Officer, Hewlett Packard Enterprise

Manoj Kuruvanthody
Group Head – Cybersecurity Strategy and Governance, Infosys

Randy Herold
Chief Information Security Officer, ManpowerGroup

Joram Borenstein
General Manager, Cybersecurity Solutions Group, Microsoft

Paul Calatayud
Chief Security Officer, Americas, Palo Alto Networks

Ryan Gillis
Vice-President, Cybersecurity Strategy and Global Policy, Palo Alto Networks

Janus Friis Bindslev
Chief Digital Risk Officer, PensionDanmark

Swamy Kocherlakota
Executive Vice-President, Chief Information Officer, S&P Global

Jim Alkove
Chief Trust Officer, Salesforce

Mark Engel
Senior Vice-President, Risk Analytics and Cybersecurity, Scotiabank

Joseph Trohak
Vice-President, Cybersecurity and IT Risk, Scotiabank

Mike Wilkes
Chief Information Security Officer, SecurityScorecard

Brett Lancaster
Managing Director, Global Head of Customer Security, SWIFT SCRL

Maya Bundt
Head, Cyber and Digital Solutions, Swiss Reinsurance

Rajiv Singh
Senior Vice-President and Head – Global Cybersecurity Business, Tech Mahindra

Neal Pollard
Chief Information Security Officer, UBS

Jack Freund
Head of Cyber Risk Methodology, VisibleRisk

Derek Vadala
Chief Executive Officer, VisibleRisk

Lee Painter
Global Head of Security Governance, Zurich Insurance Group

Andreas Suberg
Group Head of Digital and Resilience Risk, Zurich Insurance Group

ISA Board

Members of the Internet Security Alliance Board joined this effort in partnership with the working group:

Ryan Boulais
Chief Information Security Officer, AES

Deneen Defiore
Vice-President and Chief Information Security Officer, United Airlines

John Frazzini
President and Chief Executive Officer, Secure Systems Innovation Corporation and X-Analytics

Mike Gordon
Chief Information Security Officer, Lockheed Martin Corporation

Tracie Grella
Global Head of Cyber Insurance, AIG; member of the World Economic Forum's Working Group

Lisa Humbert
Managing Director and Chief Information Risk Officer, MUFG Union Bank.

Gary McAlum
Senior Vice-President and Chief Security Officer, USAA

Tim McKnight
Chief Information Security Officer, SAP

Greg Montana
Corporate Executive Vice-President, Chief Risk Officer, FIS

Richard Spearman
Group Corporate Security Director, Vodafone

Ted Webster
Vice-President, Security Governance, Risk and Compliance, Centene

J. R. Williamson
Senior Vice-President and Chief Information Security Officer, Leidos

ISA also appreciates the support of Kyle Ferguson, Kevin Richards and Robert Vescio of X-Analytics in this effort.

Endnotes

1. World Economic Forum, Measuring Stakeholder Capitalism: Towards Common Metrics and Consistent Reporting of Sustainable Value Creation, September 2020: https://www.weforum.org/reports/measuring-stakeholder-capitalism-towards-common-metrics-and-consistent-reporting-of-sustainable-value-creation (link as of 19/2/21).
2. NACD, 2020–2021 NACD Trends and Priorities of the American Boardroom, pp. 15–20.
3. World Economic Forum, Global Risks Report, 2021: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf (link as of 17/2/21).
4. FAIR Institute, Roundtable – Helping the Board Exercise Proper Cyber Risk Oversight (FAIRCON2020), 2020: https://www.youtube.com/watch?v=cdeWtHJitZs&t=64s (link as of 17/2/21).
5. World Economic Forum, Advancing Cyber Resilience: Principles and Tools for Boards, 2017: http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf (link as of 17/2/21).
6. The latest version can be accessed online – NACD Director's Handbook on Cyber Risk Oversight, 2020: https://www.nacdonline.org/insights/publications.cfm?ItemNumber=67298 (link as of 17/2/21).
7. Federation of European Risk Management Associations, At the Junction of Corporate Governance and Cybersecurity, 2018: https://www.ferma.eu/app/uploads/2017/05/WEB-FERMA-Brochure2017-29-June.pdf; National Cyber Security Centre (UK), Cyber Security Toolkit for Boards, 2019: https://www.ncsc.gov.uk/collection/board-toolkit; Berkeley Center for Long Term Cybersecurity, Resilient Governance for Boards of Directors: Considerations for Effective Oversight of Cyber Risk, 2020: https://cltc.berkeley.edu/2020/01/15/resilient-governance-for-boards-of-directors-considerations-for-effective-oversight-of-cyber-risk/; Carnegie Endowment for International Peace: Cyber Policy Initiative, Board-Level Guide: Cybersecurity Leadership, 2020: https://carnegieendowment.org/specialprojects/fincyber/guides/board-guide (links as of 19/2/21).
8. NACD, 2020–2021 NACD Trends and Priorities of the American Boardroom, pp. 15–20.
9. Risk tolerance or risk appetite (a tolerance level for losses resulting from cyber events on an annualized basis) should be defined by the board with respect to strategic goals and quantification of cyber-event likelihood and impact. Please see World Economic Forum, Advancing Cyber Resilience: Principles and Tools for Boards, 2017, p. 33 for more details: http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf (link as of 17/2/21).
10. These may take the form of internal assessment, external ratings or other tools available to the company.
11. NACD, Cyber-Risk Oversight 2020: Key Principles and Practical Guidance for Corporate Boards, p. 23: http://isalliance.org/wp-content/uploads/2020/02/RD-3-2020_NACD_Cyber_Handbook__WEB_022020.pdf (link as of 19/2/21).
12. PwC, Global Digital Trust Insights 2021, Cybersecurity Comes of Age: https://www.pwc.com/gx/en/issues/cybersecurity/digital-trust-insights.html (link as of 24/2/21).
13. Based, for instance, on an indication of the organization's reputational, customer and financial impact.
14. For more on the accountable officer, please see the Taxonomy section.
15. NACD, Cyber-Risk Oversight 2020: Key Principles and Practical Guidance for Corporate Boards, p.23: http://isalliance.org/wp-content/uploads/2020/02/RD-3-2020_NACD_Cyber_Handbook__WEB_022020.pdf (link as of 19/2/21).
16. Andy Greenberg, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, Wired, 22 August 2018: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (link as of 17/2/21).
17. Jake Williams, What You Need to Know About the SolarWinds Supply-Chain Attack, SANS Institute, 15 December 2020: https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/ (link as of 17/2/21).
18. World Economic Forum, Advancing Cyber Resilience: Principles and Tools for Boards, 2017: http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf (link as of 17/2/21).
19. NACD, Cyber-Risk Oversight 2020, Key Principles and Practical Guidance for Corporate Boards, p. 6: http://isalliance.org/wp-content/uploads/2020/02/RD-3-2020_NACD_Cyber_Handbook__WEB_022020.pdf (links as of 19/2/21).
20. World Economic Forum, Advancing Cyber Resilience: Principles and Tools for Boards, 2017: http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf (link as of 17/2/21).
21. Maya Bundt and Andrea Bonime-Blanc, Cyber Resilience ESG Reporting, SwissRe Institute, 2020, p. 4: https://www.swissre.com/institute/research/topics-and-risk-dialogues/digital-business-model-and-cyber-risk/cyber-resilience-esg-report.html (link as of 17/2/21).
22. Jack Freund and Jack Jones, Measuring and Managing Information Risk: A FAIR Approach, Butterworth-Heinemann, 2014.
23. United States Department of Homeland Security Cybersecurity and Infrastructure Agency (CISA), What Is Cybersecurity? Rev., 14 November 2019: https://us-cert.cisa.gov/ncas/tips/ST04-001 (link as of 17/2/21).
24. World Economic Forum, Understanding Systemic Cyber Risk, October 2016: https://www.weforum.org/whitepapers/understanding-systemic-cyber-risk (link as of 17/2/21).

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org