INTERNET SECURITY ALLIANCE

ecoDa
The European Voice of Directors

CYBER SECURITY RISK HANDBOOK

KEY PRINCIPLES

AND PRACTICAL GUIDANCE
FOR CORPORATE BOARDS IN EUROPE

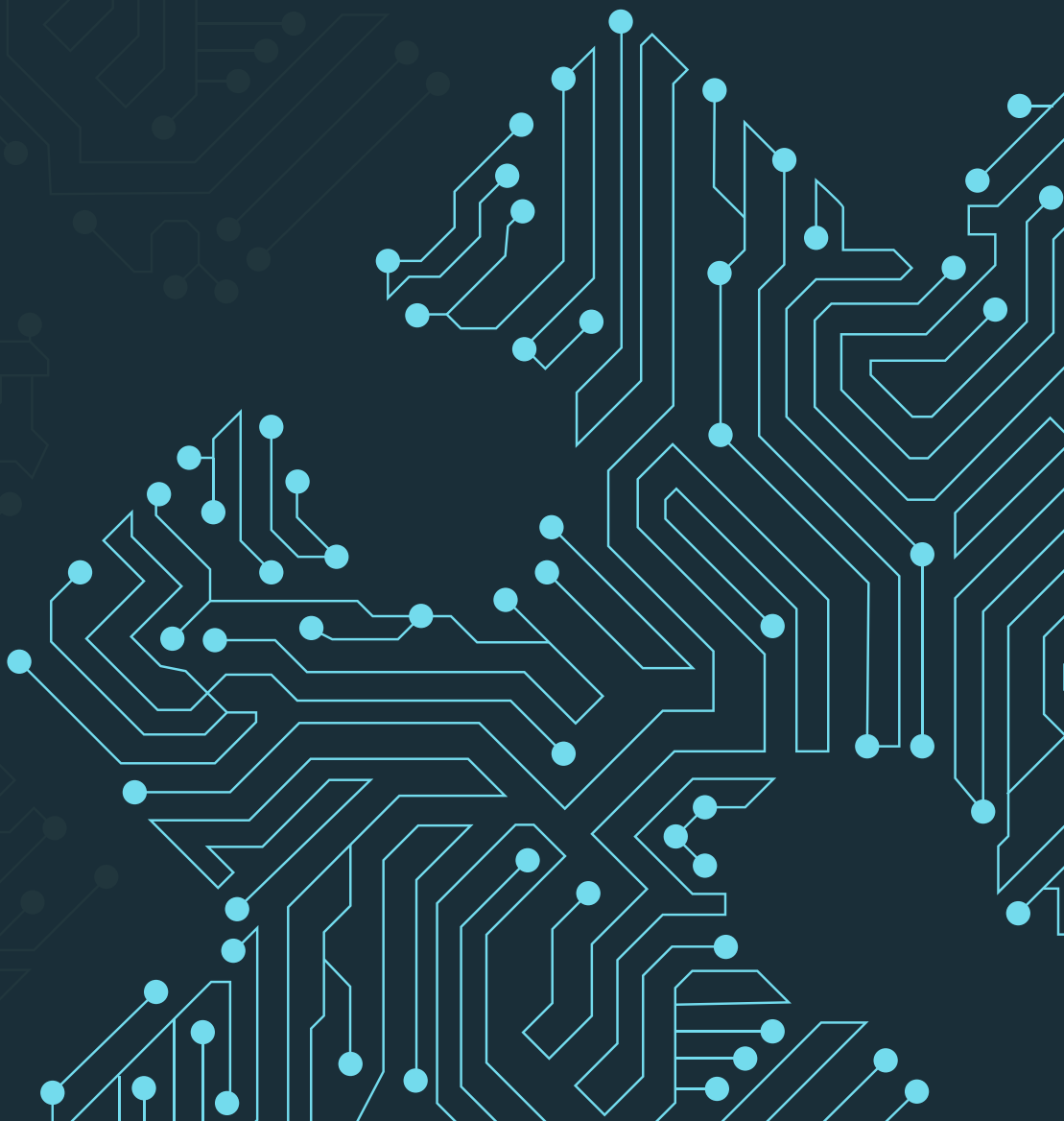


TABLE OF CONTENTS

Principle 1

CYBERSECURITY AS A STRATEGIC RISK 05

INTERNAL CYBERSECURITY STRATEGY AND MANAGEMENT 06

CYBER RISK AND THE BUSINESS ECOSYSTEM 07

KEY CONSIDERATIONS FOR THE BOARD 07

Principle 2

LEGAL AND DISCLOSURE IMPLICATIONS 10

LEGAL LANDSCAPE IN THE EU 10

DATA PROTECTION: RULES FOR DATA CONTROLLERS AND DATA PROCESSORS 10

INDUSTRY-SPECIFIC REQUIREMENTS 11

WHO IS PAYING ATTENTION 12

UNDERSTAND THE CONSEQUENCES 12

KEY CONSIDERATIONS FOR THE BOARD 13

Principle 3

BOARD OVERSIGHT STRUCTURE AND ACCESS TO EXPERTISE 15

HOW CAN BOARDS ACCESS THE CYBERSECURITY INFORMATION THEY NEED? 15

THE QUESTION OF ADDING A "CYBER EXPERT" TO THE BOARD 18

INFORMATION EXCHANGE BETWEEN THE BOARD MEMBERS AND THE MANAGEMENT 19

KEY CONSIDERATIONS FOR THE BOARD 19

Principle 4

21 AN ENTERPRISE FRAMEWORK FOR MANAGING CYBER RISK

21 THE TECHNICAL FRAMEWORK

22 ESTABLISHING A MANAGEMENT FRAMEWORK FOR CYBERSECURITY

23 ISA—ANSI INTEGRATED APPROACH TO MANAGING CYBER RISK

25 KEY CONSIDERATIONS FOR THE BOARD

Principle 5

27 CYBERSECURITY MEASUREMENT AND REPORTING

31 KEY CONSIDERATIONS FOR THE BOARD

33 ENCOURAGE SYSTEMIC RESILIENCE AND COLLABORATION

34 RESILIENCE AND COLLABORATION AMONG THE EU MEMBER STATES

35 KEY CONSIDERATIONS FOR THE BOARD

Principle 1

- CYBERSECURITY AS A STRATEGIC RISK
- INTERNAL CYBERSECURITY STRATEGY AND MANAGEMENT
- CYBER RISK AND THE BUSINESS ECOSYSTEM
- KEY CONSIDERATIONS FOR THE BOARD

CYBERSECURITY AS A STRATEGIC RISK

Historically, instead of individual departments and functions being responsible for the security of data and other digital assets they handled, the responsibility for information security was relegated to Information and Communication Technology (ICT) Department: a department that is in its widest sense responsible of the technological infrastructure, resources and tools used to communicate, create, organize, disseminate, store, and manage company's information. Primarily, ICT departments have the responsibility of continuous operation of the IT infrastructure, which can conflict with security requirements. Furthermore, deferring responsibility for security to ITC departments creates a conflict of interest by putting together the operations, oversight, supervision, and surveillance in one department, and thus jeopardizes the adoption of effective, organization-wide security strategy.

Over the past several years the business community's increased level of awareness of the importance of information security in general, and the cross-functional nature of cybersecurity in particular, have helped to break down siloes and operationalize management of cyber risks as strategic risks. On the 16th December 2020, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new EU Cybersecurity Strategy[1] as a key component of Shaping Europe's Digital Future[2], the Recovery Plan for Europe[3], and the EU Security Union Strategy[4]. The EU Cyber security strategy addresses both cyber and physical resilience of critical entities and networks to ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools. Already in 2021, the joint report from the World Economic Forum, NACD, and the Internet Security Alliance found that "cyber threats are a persistent strategic enterprise risk for all organizations regardless of the industry in which they operate"[5]and recent developments in the cybersecurity field strengthen this statement even further. Effective organizational cybersecurity directly contributes to strategic value preservation and new opportunities for long-term value creation.

Given the value of sustaining and creating potential of embedding cybersecurity into all corners of the enterprise, boards are dedicating increased attention towards cyber risk oversight practices. A 2022 survey found that over 80 percent of board members surveyed either somewhat or strongly agreed that their understanding of cyber risk has "significantly improved" over the past two years[6]. Furthermore, the majority of respondents indicated they were incorporating cyber risk oversight practices into their board's governance structures and meetings at more frequent intervals. This increased awareness and energy directed towards board-level cyber risk is evidence that board members and business leaders are confronting the challenges posed by digital and technological transformation.

Executives and board members now recognize that cybersecurity is an integral element in the critical and challenging transformations required of their organization to grow and compete in the digital age. The key questions for the board are no longer limited to how technological innovation can enable business processes, but how to balance digital transformation with effective management of cyber risks that may compromise long-term strategic interests. And the smartest companies are including security by design as part of their strategic value proposition.

Proper oversight begins with understanding that cyber risk is not limited to narrow technical domains but stretches throughout the enterprise and directly impacts key business outcomes. This includes discussing how the organization will strike the right balance between protecting digital assets and driving digital innovation. In one recent study, 79 percent of CEOs said that investments in long-term value creation initiatives were supported by investors[7].On the other side of the same token, institutional investors and proxy advisors have turned a keen eye on disclosures about cybersecurity controls and governance, and are expecting companies

1 European Commission, "EU Cybersecurity Strategy," Digital Strategy 2020

2 European Commission, "Shaping Europe's Digital Future," European Commission - European Commission, 2020

3 European Commission, "Recovery Plan for Europe," European Commission - European Commission, 2020

4 European Commission, "European Security Union," European Commission - European Commission, 2020

5 World Economic Forum, Internet Security Alliance, and NACD, Principles for Board Governance of Cyber Risk (Arlington, VA: NACD, 2021), p. 7.

6 NACD, 2022 NACD Public Company Board Practices and Oversight Survey (Arlington, VA/ NACD, 2022), p. 6.

7 EY, The CEO Imperative: Will bold strategies fuel market-leading growth?, EY.com, January 10, 2022.

to mitigate cyber risks both as a strategic enabler and as a means to retain and continue long-term value creation[8]. There is a risk that organizations will fall into the trap of letting near-term risks dominate boardroom conversations, but resilient business leaders and boards are increasingly focused on the concept of long-term value maximization and recognize that this strategy is paired with near-term risks and potential missed opportunities[9].

Boards and management teams should acknowledge the potential tension between the need for strategic innovation— increasingly fuelled by digital transformation—and the imperatives of preserving security and trust. Recognizing the high stakes of successful digital transformation, we believe that cybersecurity should now be viewed as a means for a company to execute its strategy—digital or not. At its best, cybersecurity enables companies to create long-term value and sustain trust with their customers and other key stakeholders. *After all, brakes don't slow us down but allow us to go faster.*

INTERNAL CYBERSECURITY STRATEGY AND MANAGEMENT

Boards should understand and review the cybersecurity strategy and management processes that are applicable to the sustainability of their organizations. Board members should know which digital assets (data, algorithms, applications, infrastructure, etc.) are most important for the company. They must protect them and ensure that management has vetted and understands a clear plan to prevent, deter, detect, respond, and recover from physical and cyber-attacks. While protection should start with the digital assets most critical to the organization, boards should also ask management about the process for identifying and measuring cyber risks across the enterprise, business verticals (product lines) and supply chain to help identify material vulnerabilities. These less obvious risks can still pose great threats to the integrity and security of business due to the interconnected nature of modern organizations.

In our digital age, technology is pervasive, it is part of our private and professional lives all the time and everywhere. Furthermore, technology is constantly evolving, with increasingly shorter maturity cycles. Hence the importance of evolving the company's technology and protecting the value it brings us in real time. Organizations need to be prepared to manage a wider set of security exposures related both to technology obsolescence and to emerging disruptive technologies such as AI and quantum computing. It is becoming more critical for boards and management to continually evaluate the validity of their cybersecurity. It is worth noting that emerging technologies and security challenges can be met with emerging cybersecurity best practices such as embracing and implementing zero-trust architecture. On the other hand, legacy technologies may at the same time become vulnerable to new cyber risks and have compliance issues with evolving requirements and regulations. It's up to management to ensure the adoption of the right approaches are paired with emerging technologies that will drive value creation. (For a definition of zero-trust architecture).

Defining zero-trust

The zero-trust concept was developed by Forrester Research in 2012[10] and has since become a leading approach to cybersecurity being adopted across a variety of industries. By 2022, a Forrester survey found over two-thirds of European organizations were in the process of developing a zero-trust strategy[11].

By removing implicit trust to all actors, organizations must emphasize the effectiveness and robustness of their identity and access management programs to establish the necessary roles, information access, and credentialing to appropriately monitor and govern access across the enterprise.

8 Harvard Law School Forum on Corporate Governance, "Building Effective Cybersecurity Governance", by *Orla Cox and Hetal Kanji, FTI Consulting*, November 10, 2022.

9 World Economic Forum, "Global Security Outlook Report 2023", 2023.

10 Forrester, "The Definition of Modern Zero Trust", Forrester.com, January 24, 2022.

11 Nexus Group, "Why Europe is Prioritizing Zero Trust", 2023.

In leading organizations, management teams and boards are starting to integrate the adoption of emerging technologies and data capabilities into discussions about key strategies that cut across the entire organization. Cybersecurity must be part of the same dialogue. One means to do this is to address cybersecurity as an always-present aspect of strategic risks. Nearly a third of boards address cyber risk oversight at the full-board level, rather than singular committees or groups[12].Some organizations are choosing to adapt committees exclusively to address cyber risk[13]. This evolution is consistent with the realization that cybersecurity should be seen as an enterprise-wide strategy- and risk-management issue that should be addressed holistically and proactively when the board is making major strategic decisions.

CYBER RISK AND THE BUSINESS ECOSYSTEM

The EU Commission and ENISA encourage organizations to move beyond a purely IT-centric view of cybersecurity. They advocate for a comprehensive, organization-wide approach that integrates cybersecurity into the overall business strategy. This approach helps organizations build resilience against cyberattacks and protect their valuable assets. Here's some evidence of this stance:

* **EU Cybersecurity Strategy:** The 2020 EU Cybersecurity Strategy emphasizes the importance of a "whole-of-society" approach to cybersecurity. This means all stakeholders, including governments, businesses, and individuals, have a role to play.

* **ENISA Risk Management Guidelines:** ENISA provides various resources and guidelines to help organizations develop and implement cyber risk management strategies. These resources highlight the importance of leadership buy-in and aligning cybersecurity efforts with organizational objectives.

Activities such as product launches or production strategies that use complex supply chains spanning multiple countries and regions can magnify cyber risk. Similarly, mergers and acquisitions regularly require the integration of complicated information systems, often on accelerated timelines, and without sufficient time allocated to perform comprehensive due diligence.

The resulting interplay between the new systems and legacy technology systems, most of which were developed without cybersecurity in mind, needs to be considered as a part of the enterprise-wide risk management strategy. PwC's 2023 Global Risk Survey found that oftentimes mergers, acquisitions, and organizational restructuring add layers of complexity to managing legacy technologies that "limit a holistic view of risk."[14] A year later, almost half the Directors surveyed planned to devote significant cyber budgets to optimizing existing cybersecurity technologies and investments with nearly one-fifth of Directors specifically concerned with consolidating cyber systems.[15]Clinton suggests companies must conduct rigorous due diligence on the target company's cyber risks and assess their related business impact throughout the deal cycle to protect the transaction's return on investment and the entity's value post-transaction.[16]

Another obstacle companies face in creating a secure system is the degree of interconnection that the organization's networks have with its partners, suppliers, affiliates, and customers. Initiatives to exchange trade and logistics business data electronically abound all over the world with the objective of increased data interoperability and productivity and additional information security issues are the cost of such increased productivity. Several significant cyberattacks do not actually start within the target's IT systems, but instead result from vulnerabilities in one of their vendors or suppliers. This requires partnerships across management teams and various departments, who must pressure suppliers and vendors to provide increased transparency and security for their products and services.

12 Forrester, "The Definition of Modern Zero Trust", 2022 p7.

13 Heidrick and Struggles, "Board Monitor Europe 2023" 2023.

14 Price Waterhouse Cooper "From Threat to Opportunity: PwC's Global Risk Survey 2023," 2023.

15 Price Waterhouse Cooper "2024 Global Digital Trust Insights Survey," 2024.

16 Larry Clinton (ed), *Cybersecurity for Business: Organization-Wide Strategies to Ensure Cyber Risk is Not Just an IT Issue* (1st edition, Kogan Page, 2022).

In addition, organizations are adopting new ways to manage data, (e.g., having some data residing on external networks or in the public cloud), which can improve cost-effectiveness and efficiency, but also introduce new risks. The hybridized work culture that was created out of necessity during the COVID-19 pandemic has remained durable, as off-premises, cloud-centred business operations have gained a permanent foothold. By outsourcing data storage, companies have limited their ability to secure the data on their own terms. Companies are subject to service-level agreements made in partnership with the cloud provider that merit careful due diligence against corporate security policies in the contract negotiation phase. Boards need to have sufficient oversight to determine that their management teams are monitoring these services and performing adequate risk-management steps, such as understanding the security controls and monitoring provided by the cloud provider and the results of any third-party audits. (For more on security in the cloud see Tool K in the Toolkit).

KEY CONSIDERATIONS FOR THE BOARD

* Hardwire cyber risk considerations into key operational and strategic decision-making processes including the adoption of cyber risk as a recurring agenda item for full board meetings in alignment with other business and strategy risks.
* View each major new digital transformation initiative through the lens of cyber risk.
* Ask for the cybersecurity of legacy infrastructure and systems. Do they need an update/upgrade to resist a modern attack?
* Analyse cybersecurity issues with respect to their strategic implications and as part of the enterprise risk.
* Analyse business strategy and business model considerations with respect to cybersecurity issues.
* Ask executives to identify opportunities to use cybersecurity as a market differentiator and business driver.

Principle 2

- LEGAL AND DISCLOSURE IMPLICATIONS
- LEGAL LANDSCAPE IN THE EU
- DATA PROTECTION: RULES FOR DATA CONTROLLERS AND DATA PROCESSORS
- INDUSTRY-SPECIFIC REQUIREMENTS
- WHO IS PAYING ATTENTION?
- UNDERSTAND THE CONSEQUENCES
- BOARD MINUTES
- KEY CONSIDERATIONS FOR THE BOARD

LEGAL AND DISCLOSURE IMPLICATIONS

The web of legal issues and disclosure requirements tied to cybersecurity grows more complex yearly, and refinement appears unlikely. Directors overseeing cybersecurity should be prepared to navigate a broad range of sophisticated and evolving legal and regulatory risks. Boards, individual board members, and relevant executive officers should stay informed about the current compliance and liability issues facing their organizations and the specific industries within which they operate.

LEGAL LANDSCAPE IN THE EU

In spite of the legal challenges to organizations due to the development of new regulations, EU Acts are similar in all EU member states whereas EU Directives become effective with national legislations that may differ. In the EU, cybersecurity is one element of and lens to EU's Digital Europe strategy. EU Commission and ENISA are important in the execution of cybersecurity. They guide, support, and monitor EU member states' cybersecurity authorities and actors.

While directors may not be be constantly in position to have deep knowledge of complex area of law, they should be briefed by internal or external counsel on a regular basis about requirements that apply to the company. Reports from management should enable the Board to assess whether the organization is adequately addressing these potential legal risks. For more detail about the legal landscape of cybersecurity in EU, refer to note with the list of relevant regulation at the time of writing this handbook.

There are three key trends emerging from EU cyber laws:

* A broad legal requirement to maintain "appropriate" security standards, informed by the risk assessments that analyse the nature of the assets requiring protection and thus ensuring a higher level of cyber resilience;

* Greater transparency requirements, including requirements to have written cybersecurity policies and clear obligations to report data breaches to regulators (and in some cases affected individuals) within defined timescales; and

* Much tougher sanctions for non-compliance and greater risk of private claims.

DATA PROTECTION: RULES FOR DATA CONTROLLERS AND DATA PROCESSORS[1]

Within the European Union, the General Data Protection Regulation (GDPR) sets out various obligations for "controllers" (organizations with control over why certain personal data must be collected and used, and how) and "processors" (organizations collecting or using personal data in accordance with the controller's instructions). In particular, it requires the implementation of "appropriate technical and organizational measures to ensure a level of security appropriate to the risk". The GDPR also introduces an enhanced notification obligation to disclose any breaches (i) to the affected controllers (where the organization is a processor) or (ii) to the relevant supervisory authority and possibly even to affected individuals (depending on the level of risk), without undue delay (and where feasible within 72 hours). If it fails to notify a breach and cannot invoke any of the limited exceptions to this obligation, a company can be fined up to 4% of its annual worldwide turnover. In addition, supervisory authorities enjoy wide investigative and corrective powers and the GDPR makes it considerably easier for individuals to bring private claims (even as class actions where local legislation allows that). In Europe there are cases where the authorities have decreed the precautionary closure of operations or services while the failures are not corrected.

Recent enforcement actions highlight the cost of failure to comply with GDPR. For example, the United Kingdom's Information Commission's Office (ICO) fined British Airways$230 million following a breach that resulted in a half million customers' information being stolen[2].18 ICO also recently fined international hotel company Marriott $123 million for a breach in the loss of more than 300 million customers' information[3].

The GDPR is also relevant for non-EU organizations, as many other European countries

have adopted similar legislation, or simply by virtue of the wide territorial reach of the GDPR.

INDUSTRY-SPECIFIC REQUIREMENTS

Next to the GDPR, industry-specific legislation might require an organization to take appropriate measures from a cybersecurity perspective, and even to notify security incidents (whether they concern personal data or not).

There are already EU-wide cybersecurity rules (typically Directives, which are then implemented at national level) in relation to many industries or categories of organizations. The ones with the broadest scope[4] at the time of writing of this handbook include the entities falling into the following:

a. **Sectors of High Criticality (essential entities):** energy (electricity, district heating and cooling, oil, gas and hydrogen), transport (air, rail, water and road), banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, ICT service management (business-to-business), public administration, and space.

b. **Other Critical Sectors (important entities):** Postal and courier services; waste management; manufacture, production, and distribution of chemicals; production, processing and distribution of food; manufacturing (of certain specific items); digital providers (online marketplaces, online search engines and social networking services platforms); research organizations.

These are being addressed from multiple angles - through the Directive on measures for a high common level of cybersecurity across the Union (˝NIS2˝, EU 2022/2555), the e-Privacy Directive[5] and Regulation 611/2013/EC, the digital operational resilience act for the financial sector (DORA, EU 2020/0266) and the revised Payment Services Directive[6] (PSD2) and many others. Regulators such as the European Banking Authority (EBA) and the European Central Bank (ECB) with their financial supervisory authority (FSA) units also publish guidance and documentation on security incident reporting in the banking and payment sectors[7].

Additional EU cybersecurity policies and regulations are in development or under consideration, which may lead to new legal or regulatory requirements for companies across Europe.

The implication to a board is similar in many of these; follow the rapid development of cybersecurity, build cybersecurity resilience, and ensure the sufficient engagement of management in cybersecurity risk management and other related activities.

1 Regulation (EU) 2016/679

2 Michael Grothaus, "British Airways just got hit with a massive $229 million GDPR fine", Fast Company, 9 July 2019, at: https://www.fastcompany.com/90373254/british-airways-just-got-hit-with-a-massive-229-million-gdpr-fine (16 July 2019).

3 Catalin Cimpanu, "Marriot faces $123 million GDPR fine in the UK for last year's data breach", ZDnet, 9 July 2019, at: https://www.zdnet.com/article/marriott-faces-123-million-gdpr-fine-in-the-uk-for-last-years-data-breach/(16 July 2019).

4 There are also EU-wide rules in relation to more specific sectors, such as trust service providers (Regulation (EU) No 910/2014 - "eIDAS Regulation").

5 Directive 2002/58/EC.

6 Directive (EU) 2015/2366.

7 For example, The "Guidelines on security measures for operational and security risks under the PSD2" were published by EBA in December 2017, developed in close cooperation with the European Central Bank (ECB), and are in support of the objectives of PSD2, such as strengthening the integrated payments market in the EU, mitigating the increased security risks arising from electronic payments: The EBA guidance on breach major incidents reporting under PSD2 or ESCB incident reporting framework was published in July 2017.

WHO IS PAYING ATTENTION?

Cybersecurity requirements across the EU are in flux with the implementation of the new Directives and acts. There is always a danger that high-profile attacks may spawn lawsuits, but the new Directives and acts represent a break from past cybersecurity legislation by assigning personal liability to corporate executives. Directors need to be cognizant of the increased liability they face and act accordingly.

In the US, investors have not shied away from initiating cyber risk focused suits. High profile suits brought on by the Security and Exchange Commission against SolarWinds Corporation's CISO Tim Brown allege SolarWinds and Brown "defrauded investors" by failing to communicate the extent of SolarWinds' cybersecurity problems. Brown himself was charged with "fraud and internal control failures relating to allegedly known cybersecurity risks and vulnerabilities[8]." This marks the first time that a CISO has been singled out in a US court of law as a result of a cybersecurity incident. The trend indicates that lack of effective cybersecurity oversight and appropriate board structures, practices, and responsibilities presents an opportunity for both regulators and investors to target boards.

Investors also expect companies to be transparent about their cybersecurity processes in public filings and disclosures. The Council of Institutional Investors, a group that represents public, union, and corporate benefit plans, endowments, and foundations, has stated that, "Investors will have greater confidence that [a] company is not withholding information if it proactively communicates the process by which it assesses damage caused by a cyber incident and the methodology it uses to account for cyber incidents affecting data and assets. Communicating such a process will not reveal sensitive information about a company's cybersecurity efforts[9]." In response, some public companies are increasing their voluntary disclosures, in the proxy statement and elsewhere, about how the board is educated on, informed about, and structured for cyber risk oversight.

(See Tool I in the Toolkit - Enhancing Cybersecurity Disclosures—10 Questions for Boards.)

As these requirements are enacted and challenged in court, the definitions within them may evolve. For example, in August 2022, the European Union's top court expanded the definition of sensitive information under GDPR[10]. Some of these requirements now include governance structures, rapid notification of incidents, oversight of third-party vendors, disclosure of material cyber risks, and adequacy of controls. A growing list of nations are enacting laws similar to GDPR, including Australia, Brazil, South Africa, India, and Argentina, among others[11]. Furthermore, comparable court practice development is possible for the new cybersecurity regulations as the sanction structure is similar to that of GDPR.

UNDERSTAND THE CONSEQUENCES

Aside from strong governance and adoption of the best practices outlined in this handbook, there are other practices that can shield organizations from the negative consequences of legal and regulatory enforcement actions. The lead director and corporate secretary should maintain records in appropriate detail of boardroom discussions about cybersecurity and cyber risks (See "Board Minutes"). The board itself should be tasked with staying informed about industry-, region-, or sector-specific requirements that apply to the organization. And, most importantly, the board should work in advance to understand and plan for what must be disclosed in the wake of a cyberattack, and what timing is required to do so. It is also advisable for directors to participate with management in one or more cyberbreach simulations, or "tabletop exercises," to better understand their roles and the company's response process in the case of a serious incident.

8 Securities and Exchange Commission, "SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures", 2023 https://www.sec.gov/news/press-release/2023-227.

9 Council of International Investors, "Prioritizing Cybersecurity: Five Investor Questions for Portfolio Company Boards", 2016, https://www.cii.org/files/publications/misc/4-27-16%20Prioritizing%20Cybersecurity.pdf p4.

10 Catherine Stupp, "EU Court Expands Definition of Sensitive Data, Prompting Legal Concerns for Companies", Wall Street Journal, August 2022, https://www.wsj.com/articles/eu-court-expands-definition-of-sensitive-data-prompting-legal-concerns-for-companies-11660123800?mod=djemCybersecruityPro&tpl=cy

11 "Data Protection Laws of the World", DLA Piper, 2024, https://www.dlapiperdataprotection.com/.

Board Minutes

Board minutes should reflect the occasions when cybersecurity was present on the agenda at meetings of the full board and/or of key board committees, depending on the allocation of oversight responsibilities. Discussions at these meetings might include updates about specific risks and mitigation strategies, as well as reports about the company's overall cybersecurity program and the integration of technology with the organization's strategy, policies, and business activities. Further, board minutes should reflect the disclosure of cybersecurity related incidents, including a summary of how and whether to make disclosures consistent with reporting requirements. Regulators are unable to credit good-faith discussion and oversight of this risk if there is no documentation showing that it happened. Board minutes are one tool for documenting just what was discussed and at what point in time—and one tool that may mean the difference between a painful lawsuit or an easier resolution. Having cybersecurity as a regular part of management, compliance, and internal audit reporting increases the probability of meaningful board discussions related to cybersecurity.

KEY CONSIDERATIONS FOR THE BOARD

* Carry out regular sessions with the board to update the group on legal, regulatory, or contractual trends and recent developments, including compliance assessment updates.
* Consider if any new business endeavours or partnerships generate new and differing legal obligations.
* Assure that management has developed the appropriate level of relationships and line of communications with relevant regulatory and enforcement entities.
* Assure the internal legal team has relationships with outside counsel to aid in special events such as incident response.
* Define the governance structure for disclosing material risks and actual incidents to regulatory authorities.
* Ensure cyber-security is covered in the board meetings and reflected in the meeting minutes.
* Verify eligibility of the company to be subject to NIS2 and other potential Directives.

Principle 3

BOARD OVERSIGHT STRUCTURE AND ACCESS TO EXPERTISE

HOW CAN BOARDS ACCESS THE CYBERSECURITY INFORMATION THEY NEED?

THE QUESTION OF ADDING A "CYBER EXPERT" TO THE BOARD

INFORMATION EXCHANGE BETWEEN THE BOARD MEMBERS AND THE MANAGEMENT

KEY CONSIDERATIONS FOR THE BOARD

BOARD OVERSIGHT STRUCTURE AND ACCESS TO EXPERTISE

Given the breadth of threats facing organizations, directors need more than to understand that threats exist and receive related reports from management. Rather, boards need to employ the same principles of inquiry and constructive challenge that are standard features of board-management discussions about strategy and company performance and include cybersecurity oversight into boardroom operations planning.

As discussed in Principle 1, leading boards now understand that cybersecurity is not a discussion item to be addressed for a few minutes at the end of a board meeting. Rather, cybersecurity is an essential element of board-level oversight and needs to be integrated into business management, risk, compliance, and internal audit reporting and into discussions about issues such as budget, culture, risk appetite, mergers, acquisitions, new product development, geographic expansion, and strategic partnerships—and it should be addressed at an early stage in all these endeavours.

Cybersecurity awareness on corporate boards has risen dramatically. EY's 2023 Global Board Risk Survey found Directors see cyberattacks/data breaches as the third biggest risk in 2023, up from fifth the year before[1]. Most boards have reviewed their company's response plans, received briefings from internal advisors, reviewed the company's data privacy protections, and communicated with management about cyber risk oversight over the past year. More than 70 percent of boards reviewed their company's current approach to securing its most critical assets against cyberattacks within the past year. (See the chart, Cyber Risk Oversight Practices Performed Over the Past 12 Months).

Boards and directors are elevating their understanding and education on the topic of cybersecurity, but there still exists a disparity between the board's ability and understanding and that of management's that slows enterprise-wide oversight of cyber risks. A recent survey by the Global Network of Director Institutes found a majority of directors "considered their boards lacked sufficient expertise" in cyber risk[2]. To bridge this gap, boards need to access information not simply from IT and technical operations but from a wide range of sources including human resources, finance, public relations, legal/compliance, and others. This is the practical outcome of Principle 1, according to which cybersecurity is a strategic not just an IT issue. Several models for soliciting a wide range of perspectives and inputs are discussed in Principle 4.

HOW CAN BOARDS ACCESS THE CYBERSECURITY INFORMATION THEY NEED?

There is no single approach that will fit the cyber risk oversight needs of every company and board, but there are some common best practices for getting, understanding, and using the information needed. From the time that a board member joins a new board or committee, their onboarding should include cybersecurity-specific briefings relevant to the oversight role they are serving. To bring a new director up to speed on the state of cybersecurity within the organization, as well as the board's oversight approach, the board can:

* Schedule a one-on-one briefing between the new director and the organization's CISO, or equivalent officer responsible for cybersecurity.
* Provide a walk-through of the board's cybersecurity and crisis response playbooks.
* Have the new director attend a relevant committee's meeting, where the company has delegated cyber risk to a specific committee.
* A board can also schedule time with the new director and the relevant committee chair for an in-depth discussion on the specific areas of cybersecurity oversight mandated by the committee's charter.

1 EY, "Explore why boards must improve their resilience", 2023, p.30 Explore why boards must improve their resilience | EY - Global

2 GNDI, "The future of board governance - Survey Report", 2022-2023, https://ecoda.eu/wp-content/uploads/2019/08/gndi_future_of_board_governance_survey_report_2022-2023.pdf

Full-board operations will vary based on the organization type, regulatory requirements, their cyber risk oversight needs, and how they wish to operate within the confines of their charters. Some boards choose to conduct all cyber risk-related discussions at the full-board level; others assign specific cybersecurity-related oversight responsibilities to one or more committees (audit, risk, technology, etc.); and still others use a combination of these methods. According to a 2022 survey of publicly traded company directors, 47 percent of boards delegate cybersecurity oversight tasks to the audit committee, while 32 percent oversee the risk as a full board and 13.5 percent delegate it to a risk committee[3].

Whatever the operational model chosen by the board, clear and measurable expectations should be set with management about the format, frequency, and level of detail of the cybersecurity-related information they wish to receive. This should begin with using the cybersecurity expertise within the company to enhance directors' knowledge. For example, the organization's chief information security officer (CISO), or other senior management officials responsible for overseeing security, can help the board better understand cybersecurity via regularly scheduled briefings and meetings. This leader will be able to bridge high-level strategic goals and metrics with board-appropriate information about the intricacies involved with the company's security approach.

While the board looks to these leaders for information, it is still the director's job to practice healthy scepticism. Directors should be aware of inherent bias on the part of management to downplay the true state of the risk environment—and especially if they are not being held accountable to an objective and comprehensive enterprise risk management framework and reporting structure (for more on this matter, see Principle 4). Directors who build a strong relationship with their CISOs should look to the executive for help and should trust but verify their statements and assessments.

The nominating and governance committee should ensure the board's chosen approach is clearly defined in committee charters to avoid confusion or duplication of effort. Committees with designated responsibility for risk oversight—and oversight of cyber-related risks in particular—should receive briefings on at least a quarterly basis. Depending on the board's cyber risk oversight approach, the full board may also be briefed no less than once a quarter and as specific situations warrant.

In order to encourage knowledge-sharing and dialogue, some boards invite all directors to attend committee-level discussions on cyber risk issues or make use of cross-committee membership. For example, one global company's board-level technology committee includes directors who are experts on privacy and security from a customer perspective. The audit and technology committee chairs are members of each other's committees, and the two committees hold a joint meeting once a year for a discussion that includes a deep dive on cybersecurity.

Effective boards approach oversight of cybersecurity as an enterprise-wide risk-management issue. While including cybersecurity as a stand-alone item on board and/or committee meeting agenda is now a widespread practice, the topic should also be integrated into a wide range of issues to be presented to the board including discussions of new business plans and product offerings, mergers and acquisitions, new market entry, deployment of new technologies, major capital investment decisions such as facility expansions or IT system upgrades, and the like. As corporate assets have increasingly become digital or managed and controlled digitally/remotely, virtually all major business decisions before the board will have cybersecurity components to them. Emerging new technologies like artificial intelligence will continue the digitalization of corporate assets and thus increase the need for cybersecurity risk management.

Management, risk, compliance, and internal auditing reporting to the board on relevant cybersecurity matters should be flexible enough to reflect the changing threat environment, as well as evolving company circumstances and board needs.

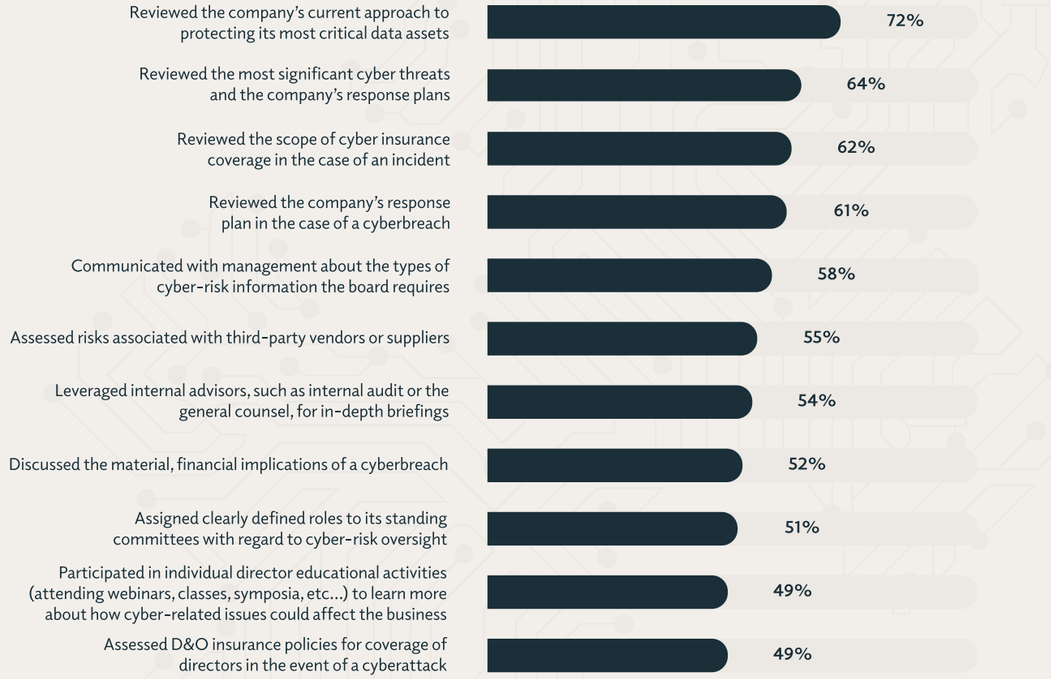
Directors may refer to the tools in the Toolkit to explore recommendations for how to approach key issues

3 *Ibid*

PRINCIPLE 3

CYBER-RISK OVERSIGHT PRACTICES BY THE BOARD

N = 315



SOURCE: 2022 NACD PUBLIC COMPANY BOARD PRACTICES AND OVERSIGHT SURVEY

related to cybersecurity oversight, ranging from how to address issues related to crisis management, including incident response, to evolving security challenges, such as supply-chain risks and insider threats.

Boards should consider augmenting their in-house expertise by using a variety of methods to integrate independent expert assessments.

Those methods include:

* Scheduling deep-dive briefings or examinations from independent and objective third-party experts validating whether the cybersecurity program is meeting its objectives.

* Leveraging the board's existing independent advisors, such as external auditors and outside counsel, who will have a multi-client and industry-wide perspective on cyber risk trends.

* Participating in relevant director-education programs, whether provided in-house or externally. Many boards are incorporating a "report-back" item on their agendas to allow directors to share their takeaways from outside programs with fellow board members.

THE QUESTION OF ADDING A "CYBER EXPERT" TO THE BOARD

How best to organize the board to carry out oversight of cyber risk—and, more broadly, enterprise-level risk oversight—is a matter of considerable debate. The *Report of the NACD Blue Ribbon Commission on Adaptive Governance* recommended that cybersecurity, along with other disruptive risks, "[should] be a component of strategy discussions at the full-board level and may also appear on the agenda of key committees, depending on the way in which risk-oversight responsibilities are allocated[4]."As noted earlier in this principle, 47 percent of surveyed companies said that cybersecurity oversight was allocated to the audit committee—the committee which most often oversees complex audits of financial and compliance matters. As the mandate of this committee expands and the complexity increases, organizations are seeking other means for oversight of this risk.

Some companies in recent years have considered whether to add cybersecurity and/or IT security expertise directly to the board via the recruitment of new directors. The Global Network of Director Institutes' 2023 *Future of Board Governance Survey* found that "83% of directors believe that technological advancements will require changes to board structures for 2030 and beyond, with the results indicating an urgent need to close the gap in cyber skills[5]."

Government bodies in the EU and the US have begun deliberating regulatory action to mandate a designated cyber expert on corporate boards although no mandate has been passed at this time.

An earlier version of the US Securities and Exchange Commission's controversial Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies that went into effect in late 2023 would have compelled companies to recruit someone with cybersecurity expertise onto their board. The final version of the rule dropped that provision after firm pushback from industry.

Some EU member countries have published non-binding guidelines. Spain published the Good Governance Code on Cybersecurity (GGCC) in July 2023, which recommends at least one director per board have a cybersecurity background.

The issue full-board versus committees could be perceived from the both-and rather than the either-or perspective facilitating full-board discussions on strategic issues and more detailed in-depth discussions in committees. Leaving aside that there simply are not enough "cyber experts" to populate every board, and hence the degree of expertise among board candidates may vary considerably, there are several questions posed below that a board should consider before opting for this strategy.

SHOULD YOU HAVE A CYBER EXPERT ON THE BOARD?

* *How are we defining a "cyber expert"? The first principle in this handbook is that cybersecurity is not just an "IT" issue, but rather a strategy related enterprise-wide risk-management issue. Such an expert needs competencies to discuss all board issues, rather than cyber risks only. So, is the board looking to add an expert in enterprise-wide cybersecurity issues? A former CISO? Consider the company's needs and align them accordingly.*
* *Is this strategy really deferring to one individual a responsibility that the full board should undertake? Might it be more appropriate for the full board to increase their understanding of cybersecurity systems in a way that is similar to the understanding that non-lawyers and nonfinancial experts have with these respective issues?*
* *How does having a single cyber expert on the board mesh with the cross-functional cyber-management structures that are becoming increasingly common? (Consider reviewing the "Three Lines" model).*
* *Does placing a cyber expert on the board set a precedent for assigning seats to other specialized oversight areas?*

4 NACD Blue Ribbon Commission, "Adaptive Governance", 2018

5 GNDI, "Future of Board Governance Report", 2023 The GNDI Future of Board Governance Report 2023 (iod.com)

It may take a longer time to address specific cybersecurity issues without a cyber expert. On the other hand, when board members understand the issue, the impact is probably long-lasting and well aligned with business strategy and enterprise risk management. The board also has the option to include internal management level cyber expert to speed up learning or to use external services.

INFORMATION EXCHANGE BETWEEN THE BOARD MEMBERS AND THE MANAGEMENT

Board Members should serve as an example of best practice when handling company information. Numerous Boards resort to usage of their personal email addresses when discussing Board meetings and information pertaining to the company. Also, personal email addresses are being used to access cloud drives where documents are stored. This poses a threat to the company data and makes Board members guilty of cyber risk.

Board Members should always use secure mailboxes with prudent identification protocols created in the company domain and secured from third-party access.

Directors Can Improve Cyber Risk Oversight Expertise by Completing Training Programs, at their local Institute of Non-Executive Directors, Business Schools, IT Universities and basic cybersecurity programs and ad hoc training for board members.

KEY CONSIDERATIONS FOR THE BOARD

* Establish key cybersecurity structures, committee assignments, and cadence for review of information, and ensure that cybersecurity oversight is a topic integrated into the onboarding of new directors.
* Ensure that the board has access to the appropriate expertise from inside and outside the company to help it perform oversight duties with confidence.
* Establish a cybersecurity culture from the boardroom and encourage collaboration across all stakeholders relating to and accountable for cyber risks.
* It is highly recommended to ask the management team to role-play a cyber-attack at least once per term. In an organization where cybersecurity is truly strategic, all company units should appear in the role-playing game: from the IT department to external communications, passing through all operational and support units (such as manufacturing, sales operations and Human Resources).
* Take great care when considering the addition of a cybersecurity expert to the board that this person is not or doesn't become the sole repository for risk oversight of the topic.
* Induction and training sessions to know the "full picture" (what is cybersecurity, most common attacks, frameworks and compliance regulations) to understand the company posture.
* The board's oversight must ensure alignment between the company's security policies and the different levels of control with special emphasis on real-time surveillance systems (Audits and scheduled simulations of breaches and attacks are NOT sufficient for effective monitoring.)

Principle 4

- AN ENTERPRISE FRAMEWORK FOR MANAGING CYBER RISK
- THE TECHNICAL FRAMEWORK
- ESTABLISHING A MANAGEMENT FRAMEWORK FOR CYBERSECURITY
- ISA–ANSI INTEGRATED APPROACH TO MANAGING CYBER RISK
- THREE LINES MODEL
- KEY CONSIDERATIONS FOR THE BOARD

AN ENTERPRISE FRAMEWORK FOR MANAGING CYBER RISK

In order for boards to engage in effective oversight of cyber risk, they need to fully understand the responsibilities that lie in the hands of management. The top sets the tone, and this begins with determining the board's own comfortability with discussing cyber risk issues and if necessary, bringing in cyber expertise. Board members need to be fluent enough in their organization's cyber risk profile to ensure that management is adequately supported. As digital technologies increasingly underpin growth strategies, management has taken on the role of deploying, managing, and securing new digital capabilities across the organization. However, cyber risk reporting structures and decision-making processes continue the legacy of siloed operating models. Management can no longer afford simply to delegate cyber risk management to IT, or to each department and business unit independently.

Directors should seek assurances that management is taking an appropriate enterprise-wide approach to managing cybersecurity risk. Specifically, boards should assess whether management has established both an enterprise-wide technical framework as well as a management framework that will enable effective governance of cyber risk. An integrated risk model should consider cyber risk not just as a technical problem unique and separate from other business risks, but rather as part of a comprehensive enterprise-risk management program.

On the other side, management should seek assurances from the board that cybersecurity practitioners are able to maintain independence while assessing cyber risks. Management needs to be able to inform the board about holes in the organization's cybersecurity posture without fear of retribution. It is in the board's best interest to be fully informed about cybersecurity vulnerabilities that leave the organization open to serious reputational and financial damage.

THE TECHNICAL FRAMEWORK

Complexity is an inherent feature of modern digital technology systems. As business and competitive pressures change, organizations demand that these complex systems be continually adapted and updated. This could mean adopting emerging technologies such as artificial intelligence (AI) and machine-learning (ML), cloud, blockchain, the Internet of Things, or quantum computing to improve business practices and unleash innovation and growth (see Tools K and M in the Toolkit). Directors cannot be expected to fully track and understand all these technologies and their implications for cyber risk. Regarding legacy systems, boards should supervise from board perspective the conduct of annual or bi-annual cyberattack simulations to assess the organization's cyber posture and authorize the necessary budget to avoid cyber risks due to technological obsolescence. Boards should expect from management that they implement and use an appropriate technical cybersecurity framework to defend the organization's digital technology systems that the enterprise has come to rely on. Emerging technologies tend to be much safer, but they require new digital talent profiles and the training of all employees. As maturity is reached in the exploitation of new technologies, the company will be exposed to new threats. There are a broad set of specific cybersecurity applications, tools, and services for new technologies. The board should aim to ensure that the company knows its security posture every time and everywhere for both legacy and new systems. Multiple technical frameworks have been developed by various standards and industry organizations and act as sets of best cybersecurity practices. These frameworks vary in levels of granularity as they list best practice activities along the various steps of the cyber risk management process. Some organizations choose to adopt a single technical cybersecurity framework, while others will select specific aspects of various frameworks and adapt them to their unique business needs. To date, no one framework has been empirically demonstrated as superior from an effectiveness perspective.

Once a cybersecurity framework has been adopted by the organization, directors should request regular updates on the progress made in implementing the selected set of best practices. Various tools have emerged that can help organizations demonstrate progress in implementing a cybersecurity framework:

* Some tools are more focused on technical implementation, helping track the progress of implementing various technical best practice activities along various scales of maturity and deployment.

* Other financially oriented tools measure the effectiveness of those best practices in reducing risk and can be used to prioritize those risks based on business impact.

Greater detail on cybersecurity management and reporting is discussed in Principle 5. Among the most used technical frameworks management can select, adopt, and adapt are these:

* The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), which consists of "standards, guidelines, and best practices to manage cybersecurity risk." The NIST CSF's risk management process includes six key functions (govern, identify, protect, detect, respond, and recover) and over one hundred cybersecurity best practice activities[1].

* The International Organization for Standardization (ISO), together with the International Electrotechnical Commission (IEC) created the ISO/IEC 27000 family of standards as a series of best practices to help organizations improve their information security, through security controls, within the context of an overall Information Security Management System, similar in design to management systems for quality assurance[2]. In EU and Europe, ISO/IEC 27000 family of standards are often used as national standards by national standardization organizations.

* The Centre for Internet Security's CIS Critical Security Controls include a list of 18 security controls with a prioritized set of actions to protect organizations and data from cyber-attack vectors. These controls range from establishing an inventory of enterprise and software assets to incident response management and penetration testing[3].

ESTABLISHING A MANAGEMENT FRAMEWORK FOR CYBERSECURITY

Principle 1 stressed the importance of viewing cybersecurity as a strategic and integrated enterprise risk. Directors should expect the implementation of an effective management framework for cybersecurity that requires the involvement of all relevant stakeholders across multiple business functions, to ensure that all proper cyber risk management activities are covered. While each organization will have unique operations, functions, and departments to account for, some examples of enterprise activities that can be part of a holistic cyber risk management program follow[4].

Information Technology. While this department covers many functions, including managing operational technology (OT), information security in many organizations still falls under IT. The security function is tasked with protecting the organization through the gathering of threat intelligence and the implementation of cybersecurity controls.

* **Risk** — Many organizations also have a risk function. This part of the organization is tasked with assessing their top cyber risk and insuring against catastrophic events.

* **Legal and Compliance** — The legal department or outside counsel can help organizations address regulatory and shareholder obligations and concerns related to cyber risks.

* **Human Resources** — The world of cyber security and privacy is constantly changing. Employees that have access to critical assets of an organization have become primary targets of cyber-attacks. Those that have access to technology and organizational assets are also responsible for the protection of those assets. The Human Resources department addresses questions such as: Are our employees fit and proper to handle this responsibility? Do they have the awareness and skills necessary to meet these expectations? Does the company have the right risk and cyber culture/knowledge?

1 NIST, "Cybersecurity Framework", 2024 https://www.nist.gov/cyberframework

2 ISO/IEC, Information technology — Security techniques — Information security management systems —Overview and vocabulary, 2018 https://www.iso.org/standard/73906.html

3 CIS, "The 18 CIS Critical Security Control", 2024 https://www.cisecurity.org/controls/cis-controls-list

4 For more detailed examples, look to Larry Clinton (ed), *Cybersecurity for Business: Organization-Wide Strategies to Ensure Cyber Risk is Not Just an IT Issue* (1st edition, Kogan Page, 2022).

* **Line-of-Business Executives** — Research and development, marketing, and other line-of-business executives may also need to be represented. They are critical to cyber risk mitigation as they create and use digital data with accountability for data content, plan to launch new digital products and need to understand how to achieve the right balance between enabling better, value-driving customer experiences and protecting the business.

* **Finance** — The finance team likewise has a role to play as businesses assess the acceptable level of risk that they can tolerate against the cybersecurity investments needed to achieve and maintain them. Finance may also play a critical role in assessing the financial impact and materiality of potential or actual cybersecurity events.

* **Physical Security** — Through the adoption of the Internet of Things (IoT) and Industrial Internet of Things (IIoT) devices, the world is becoming increasingly interconnected. This mesh of cyber-physical systems (CPS) expands the attack surface, making physical and digital security essential to prevent cyber physical attacks. Incidents involving the convergence of cyber and physical security fall into two main categories: "Cyberattacks on Physical Systems" and "Physical Systems Used in Cyberattacks".

No one cyber risk model representing various functions and stakeholders will apply perfectly to all organizations. Recognizing that organizations will want to tailor their approach to fit their needs, we offer two different models which can be used as a starting point.

ISA–ANSI INTEGRATED APPROACH TO MANAGING CYBER RISK

One of the first multistakeholder models developed was created by the Internet Security Alliance (ISA) and the American National Standards Institute (ANSI) in their joint 2008 publication, *The Financial Management of Cyber Risk: 50 Questions Every CFO Should Ask*[5]. This basic model stresses not only that multiple stakeholders ought to be involved but also advocates for an identified leader—not from IT—who has cross-organizational authority. It also advocates for a separate cybersecurity budget as opposed to the traditional model of folding cybersecurity into the IT budget. The ISA-ANSI framework outlines the following seven steps:

1. Establish ownership of cyber risk on a cross-departmental basis. A senior manager with cross-departmental authority, such as the chief financial officer, chief risk officer, or chief operating officer (not the chief information officer), should lead the team.

2. Appoint a cross-organization cyber risk management team. All substantial stakeholder departments must be represented, including business unit leaders, legal, internal audit and compliance, finance, human resources, IT, information security, and risk management. If these roles do not exist in the organization, then their equivalents or the appropriate designee should be included.

3. The cyber risk team needs to perform a forward-looking, enterprise-wide risk assessment, using a systematic framework that accounts for the complexity of cyber risk—including, but not limited to, regulatory compliance.

4. Be aware that cybersecurity regulation differs significantly across jurisdictions (between the EU members and other countries, and from industry to industry). As noted in Principle 2, management should dedicate resources to tracking the standards and requirements that apply to the organization, especially as some countries aggressively expand the scope of government involvement into the cybersecurity arena.

5. Take a collaborative approach to developing reports to the board. Executives should be expected to track and report metrics that quantify the business impact of cyber threats and associated risk-management efforts. Evaluation of cyber risk management effectiveness and the company's cyber resiliency should be conducted as part of quarterly internal audits and other performance reviews.

6. Develop and adopt an organization-wide cyber risk management plan and internal communications strategy across all departments and business units. While cybersecurity obviously has a substantial

5 ISA & ANSI, "The financial management of cyber risk" https://webstore.ansi.org/info/cybersecurity

IT component, all stakeholders need to be involved in developing the corporate plan and should feel "bought in" to it. Testing of the plan should be done on a routine basis.

7. Develop and adopt a comprehensive cyber risk budget with sufficient resources to meet the organization's needs and risk appetite. Resource decisions should consider the severe shortage of experienced cybersecurity talent and identify what needs can be met in-house versus what can or should be outsourced to third parties. Because cybersecurity is important across the enterprise, the budget for cybersecurity should not be exclusively tied to one department. Examples include allocations in areas such as employee training, tracking legal regulations, public relations, product development, and vendor management.

Three Lines Model[6]

A conceptual model was created by the Institute for Internal Audit in 2013 called the Three Lines of Defence Model[7]. The model, updated in 2020, stresses multiple independent functions within the organization having separate and complementary roles in assessing, managing, and governing risk. The update eliminated the term "Defence" from its title, an indicator that the current model is focused more on the opportunities and value potential posed by risks[8]. The Three Lines Model moved beyond three defined lines of risk management and instead adopted a principle-based approach inclusive of governance structures.

In the first line, management owns the risk design, implements operations, and maintains a constant dialogue with the management lead for cyber (typically the CISO). Each business line defines the cyber risk they face and weaves cyber risk into risk, fraud crisis management, and resiliency process.

Line two defines policy statements and the risk management framework. It provides a credible challenge to line one and is responsible for evaluating risk exposure, so that the board can determine risk appetite. Line two should be established as a separate, independent function under management and maintain communication with both the cyber risk lead, compliance, and internal audit. Cyber risk management specialist could also be an independent level two professional supporting all three levels.

Line three is internal audit. It is responsible for independent evaluation of both line one and line two, including assessment of roles and processes across lines one and two.

The current model identifies six key principles that were not included in the previous model:

1. *Having the right structures and processes to ensure that cyber risk is appropriately managed through governance.*
2. *Assuring that responsibility for cyber risk is appropriately delegated by the governing body and management has the tools it needs.*
3. *Management's role is within both lines one and two. Second line roles can be assigned to specialists (e.g., a penetration tester) to challenge the first line.*
4. *Internal audit provides assurance and advice on the adequacy and effectiveness of governance and risk management.*
5. *The internal audit's independence is critical to its objectivity, authority, and credibility.*
6. *There must be collaboration among all roles to assure success.*

6 Larry Clinton (ed), *Cybersecurity for Business: Organization-Wide Strategies to Ensure Cyber Risk is Not Just an IT Issue* (1st edition, Kogan Page, 2022).

7 Global Association of Risk Professionals, Three Lines of Defense: A New Principles-Based Approach, 2021 https://guidehouse.com/insights/financial-services/2021/public-sector/garp-three-lines-of-defense?lang=en#:~:text=The%20three%20lines%20of%20defense%20represent%20an%20approach%20to%20providing,relationship%20bet ween%20those%20different%20areas.

8 Jaclyn Jaeger, Analysis: Comparing the IIA's new 'Three Lines Model' to the old one, Compliance Week, 2020 https://www.complianceweek.com/risk-management/analysis-comparing-the-iias-new-three-lines-model-to-the-old-one/29252.article

KEY CONSIDERATIONS FOR THE BOARD

* Boards should expect management to incorporate cyber risk into an enterprise risk management approach.
* In order to provide full oversight of cyber risks, management should adopt both technical and management frameworks, including informing the board about the frameworks.
* There are several technical and management frameworks that can be adopted and adapted for the unique needs of an organization.
* Encourage management to keep up to date with EU cyber information network, research and regulation. They may reinforce the implementation of the two frameworks mentioned above.
* Depending on the type of company, it might be worth to run the cybersecurity self-assessment tools and questionnaires developed by ENISA. They covered a broad range of use cases from small and medium-sized enterprises to national cybersecurity competences through critical sectors like ports.

Principle 5

CYBERSECURITY MEASUREMENT AND REPORTING

NACD's 2022 Public Company Board Practices and Oversight Survey found that only 52 percent of boards are reviewing the material, financial implications of a cyberbreach on their companies—this compared to 72 percent reviewing the company's approach to protecting its most critical assets, for instance[1]. These findings support the claim that in most cases, management still reports on cybersecurity with imprecise scorecards such as "heat maps," where cyber risk is measured in colours or in high-medium-low terms, security "maturity ratings," and highly technical data that are out of step with the metric-based reporting that is common for other enterprise risks.

These legacy practices do not allow management and the board to understand the materiality of cyber events and to properly assess the adequacy and cost-effectiveness of risk mitigation initiatives[2]. According to a NIST publication focused on integrating cybersecurity into enterprise risk management practices, "While qualitative methods are commonplace, companies may benefit from considering a quantitative methodology with a more scientific approach to estimating likelihood and the impact of consequences. This may help to better prioritize risks or prepare more accurate risk exposure forecasts[3]." This does not absolve the board from gaining a basic understanding of the technical aspects of cybersecurity, which helps validate management assumptions in quantifying the risk.

While cyber risk management is a relatively young discipline compared to other forms of enterprise risk, expectations for mitigating and reporting on it should not be reduced. Management should deliver reports that are:

* **Transparent about performance**, with economically focused results based on easily understood methods.
* **Benchmarked**, so directors can see metrics in context to peer companies or the industry.
* **Decision-oriented**, so the board can provide oversight of management's decisions weighed against the defined risk appetite, including resource allocation, security controls, and cyber insurance.

As discussed in Principle 1, cyber risk should be discussed in terms of strategic objectives and business opportunities. In this context, every key performance and risk indicator should be tracked against a target performance or risk appetite, as proposed by management, and approved by the board. Risk appetite statements should be defined in as objective, clear, and measurable a way as possible, while also accounting for subjective factors such as the economic environment in which the appetite was initially decided within.

While this level of reporting is still aspirational for some companies, directors can drive their organizations forward by asking the following five questions and demanding answers backed by the sort of metrics and reports that we suggest in this principle and in Tool F in the Toolkit. In EU, cybersecurity regulations include requirements on cybersecurity measurements and metrics that go beyond heat maps and other similar measures.

1 NACD, "Public Company Board Practices and Oversight Survey", 2022 2022 NACD Public Company Board Practices and Oversight Survey (nacdonline.org)

2 Jack Jones, "'Understanding Cyber Risk Quantification: The Buyer's Guide'", FAIR Institute, https://www.fairinstitute.org/resources/understanding-cyber-risk-quantification-the-buyers-guide-by-jack-jones.

3 Kevin Stein et al., "NISTIR 8286 - Integrating Cybersecurity and Enterprise Risk Management (ERM)", NISTIR 8286 - Integrating Cybersecurity and Enterprise Risk Management (ERM) § (2020), p. ii-74. https://csrc.nist.gov/publications/detail/nistir/8286/final

1. How are we measuring the threat environment that we face and our readiness to face it?

The chief information security officer or chief risk officer should paint a picture of the threat environment (cybercriminals, nation-states, malicious insiders, etc.) that describes what's going on globally, in our industry, and within the organization. Examples of good metrics and reports include:

* Global cyber-related financial and data losses;
* New cyber breach attempts, successful breaches and lessons learned;
* rends in the types of hacker tactics (e.g., ransomware, leveraging zero-day vulnerabilities, etc.), and new attack patterns; recognized on the basis of knowledge and learned from detected attempts in the organization; and
* Cyber threat trends from information sharing and analysis centres (ISACs)[4].

2. What is our cyber risk profile as defined from the outside looking in?

Boards should get cyber risk assessments from independent sources. Useful sources of information include:

* Independent security ratings of the company, benchmarked against peers;
* Third-party and fourth-party risk indicators; and
* Independent security assessments (e.g., external consultants and auditors) perform periodic real-time monitoring/surveillance to ensure continuous security validation. If the company can't afford a breach and attack simulation (BAS) tool, there are several specialized software-as-a-service providers which can meet the budget restrictions and deliver the detailed cyber posture of the company (software, infrastructure, applications, and employees).

3. What is our cyber risk profile as defined by management?

Management should provide assessments with tangible performance and risk metrics on the company's cybersecurity program that spans across departments and functions, which may include:

* Framework-based program maturity assessment conducted by a third-party;
* Compliance metrics on basic cyber hygiene (the five P's): passwords, privileged access, patching, phishing, and penetration testing;
* Percentage of critical systems downtime and time to recover;
* Mean time to detect and remediate cyber breaches;
* Capital at risk, as a typical metric used in the finance sector.

4. What is our cyber risk exposure in economic terms?

The central question here is: what is the company's loss exposure to cybersecurity events? In the past 30 years, we have seen that question answered in economic terms in every risk discipline in ERM: interest rate risk, market risk, credit risk, operational risk, and strategic risk. Now we need to address that question for cyber risk. This expectation can also be found in the U.S. Securities and Exchange Commission's guidance on cybersecurity disclosures and its focus on quantitative risk factors[5].

4 National Council of ISACs, https://www.nationalisacs.org/

5 Securities and Exchange Commission, "Commission Statement and Guidance on Public Company Cybersecurity Disclosures", 2018 https://www.sec.gov/rules/interp/2018/33-10459.pdf

PRINCIPLE 5

CRQ Approaches and Methods

As cyber risk quantification adoption and effectiveness increases several models have emerged for calculating cyber risk in economic terms. Many of these approaches rely on two primary quantification methodologies: asset-based quantification and actuarial based quantification. Both methods attempt to objectively quantify in economic terms a company's cyber risk exposure, likelihood of risk event, and potential loss magnitude of a given incident.

***Asset-Based CRQ:** These models leverage an approach to cyber risk management developed by several leading risk management frameworks such as ISO/IEC 27005 and FAIR. These models mostly perform risk analysis via an asset register alongside a risk register to then quantify a company's cyber risk exposure in economic terms. While robust at the asset level, these models do not always evaluate organizational and ecosystem risks.*

***Actuarial-Based CRQ:** This approach leverages historical actuarial data related to breach and loss events to calculate the cyber risk exposure, potential loss magnitude, and likelihood of risk event. Cyber insurance actuarial data in this space is highly variable[6]. Additionally, this model is unable to account for zero-day attacks and newly discovered vulnerabilities as, by definition, they lack historical actuarial data on those methods of attack.*

Boards should work with the Management in their companies to determine which approach works best for their specific company's cybersecurity goals as both methods have strengths and weaknesses. Some questions to ask to understand whether or not the CISO and their team have made the right choice for the organization follow.

* *Does the chosen CRQ model have any weaknesses? How is the cyber risk management team mitigating what the model doesn't cover?*
* *Is the chosen model flexible enough that we are regularly adding and accounting for new vulnerabilities and recent cybersecurity events within it?*
* *Is the approach we are using in line with our sector and industry peers?*

Multiple cyber risk quantification (CRQ) models have emerged that allow cyber risk professionals to assess a company's cyber loss exposure in financial terms. Frameworks such as Factor Analysis of Information Risk (FAIR)[7], X-Analytics, and other cyber risk quantification models have been adopted by a large number of companies and vendors, following new applied research in the domain[8]. Companies should select the cyber risk quantification method, tools and services that best meet their needs and that can provide defensible results. (See "CRQ Approaches and Methods," for definitions of CRQ methods and questions directors can ask to assess the choice their organization has made.)

In the current environment, directors should demand more robust reporting on metrics such as:

* Value of enterprise digital assets, especially the company's "crown jewels";
* Probability of cyber event occurrence and potential loss magnitude;
* Potential reputational damage and impact on shareholder value;
* Costs of developing and maintaining the cybersecurity program;
* Costs of compliance with regulatory requirements (e.g., the EU's General Data Protection Regulation).

6 Unal Tatar, Omer Keskin, Hayretdin Bahsi and C. Ariel Pinto, "Quantification of Cyber Risk for Actuaries An Economic-Functional Approach", 2020 https://www.soa.org/globalassets/assets/files/resources/research-report/2020/quantification-cyber-risk.pdf

7 The FAIR Institute

8 Notable CRQ publications include: D. Hubbard, R. Seiersen. (2016) 'How to Measure Anything in Cybersecurity Risk', Wiley; J. Jones, J. Freund (2015) 'Measuring and Managing Information Risk: A FAIR Approach', Butterworth-Heinemann; Ruan, K. (2017). Introducing cybernomics: A unifying economic framework for measuring cyber risk, Computers & Security, Volume 65, p 77-89, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2016.10.009.

5. Are we making the right business and operational decisions?

As stated in Principle 1, cybersecurity is not just a technology, security, or even a risk issue. Rather, it is a business issue and a "cost of doing business" in the digital economy. On the opportunity side, advanced technologies and digital innovations can help companies offer new products and services, delight their customers, and streamline or disrupt the supply chain. As a top strategic issue, management should provide the board with risk and return metrics that can support effective oversight of business and operational decisions, such as:

* Risk-adjusted profitability of digital businesses and strategies (including M&A);
* Return on investment of cybersecurity controls; and
* Cyber insurance versus self-insurance.

Board-management discussions about cyber risks should include identification and quantification of financial exposure to cyber risks and which risks to accept, mitigate, or transfer, such as through insurance, as well as specific plans associated with each approach[9].

Defining Risk Appetite

"Risk appetite" is the amount of quantifiable risk an organization is willing to accept in pursuit of strategic objectives. Thus, it should define the level of risk, through measurement, at which appropriate actions are needed to reduce risk to an acceptable level. When properly defined and communicated, it drives behaviour by setting the boundaries for running the business and capitalizing on opportunities. A 2022 commission on the future of board practices also found that it is critical to risk oversight that the board and management "have an agreed and clearly defined risk appetite which provides guardrails for risk activity[10]."

A discussion of risk appetite should address the following questions:

* ***Corporate values** – What risks will we not accept?*
* ***Strategy** – What are the risks we need to take?*
* ***Stakeholders** – What risks are stakeholders willing to bear, and to what level?*
* ***Capacity** – What resources are required to manage those risks?*
* ***Financial** – Are we able to adequately quantify the effectiveness of our risk management and harmonize our spending on risk controls?*
* ***Measurement** – Can we measure and produce reports to ensure proper monitoring, trending and communication is reporting is occurring?*

"Risk appetite is a matter of judgment based on each company's specific circumstances and objectives. There is no one-size-fits-all solution."

Source: PwC, Board oversight of risk: Defining risk appetite in plain English

9 See Securities and Exchange Commission, "Commission Statement and Guidance on Public Company Cybersecurity Disclosures", 2018 https://www.sec.gov/rules/interp/2018/33-10459.pdf, Section 2. Risk Factors, p13; and Jack Jones, 'Understanding Cyber Risk Quantification: The Buyer's Guide'," FAIR Institute

10 NACD, The Future of the American Board Report: A Framework for Governing into the Future, 2022 https://www.nacdonline.org/insights/publications.cfm?ItemNumber=74136

PRINCIPLE 5

KEY CONSIDERATIONS FOR THE BOARD

* When quantified and measured over time with robust tested methods, risk reporting can lead to improved cybersecurity outcomes and cost savings for the organization.
* Heat maps and other imprecise metrics are better than nothing but inferior to quantified metrics and may not meet the requirements of evolving cybersecurity regulations.
* Boards and management should come to an agreement on a cyber risk appetite, related metrics included.
* It is important for cyber risk to be measured, benchmarked, and reported in objective terms to the board in the language of business.
* Make sure that the company's insurance policies include (at least) compensation to third parties and own remediation for damages caused before, during and after the date/times of a cyber-attack.
* Make sure the decisions and actions of the board and its members on cybersecurity matters are covered by Directors and Officers (D&O) liability insurance.

Principle 6

ENCOURAGE SYSTEMIC RESILIENCE AND COLLABORATION

RESILIENCE AND COLLABORATION AMONG THE EU MEMBER STATES

KEY CONSIDERATIONS FOR THE BOARD

PRINCIPLE 6

ENCOURAGE SYSTEMIC RESILIENCE AND COLLABORATION

In 2021 NACD, ISA, and the World Economic Forum collaborated to unify their support for the previous five principles outlined in this handbook. The three organizations also agreed that corporate governance had evolved in recent years and that a new principle was necessary to encourage systemic resilience and collaboration around cybersecurity. The three organizations declared:

> *"The highly interconnected nature of modern organizations means we run the risk of failures that spread beyond the enterprise to effect entire industries, sectors, and economies. This means that 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 risk challenge effectively senior leadership must actively encourage collaboration across industry and government.[1]"*

This principle is consistent with over-arching trends in corporate governance best practice such as the ESG movement which calls on organizations to understand their responsibilities to consider the environmental, social, and governance impacts of their actions on a broader range of stakeholders. In 2019, the Business Roundtable issued a purpose statement that called on companies to go beyond shareholder primacy and consider the interests and expectations of other key stakeholders like employees, customers, and suppliers[2]. Given the interconnected nature of cyber risk spanning disparate companies and industries operating on the insecure structure of the Internet, it is incumbent upon each organizations to be their brother's keeper, so to speak—much in the same way that the "E" in ESG relies on companies to come together to improve our ecological environment, for instance.

The defining characteristic of the Internet is the massive interconnection of multiple systems. Built by default without security in mind, this interconnection has been exploited since its inception and has in the past decade created effects that extend well beyond individual entitles. In 2017, the NotPetya attack spread from a malware-infected system in Ukraine to paralyze 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. 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. The extent of the damage likely to follow, or even the purpose of the attack, is still open to speculation.

While the number of these systemic cyberattacks is still comparatively small some of the most sophisticated risk managers in the world are predicting that these events are merely the "canary in the coal mine" and the emerging expansion of technologies such as 5G mobile communications will likely enhance the opportunity and potential impact of systematic cyber events. Given the breadth of type of victims that were the point of entry in recent systemic attacks, it is imperative for all organizations to secure themselves to secure the system at large.

The board of directors' oversight responsibility is to see that management provides an effective cyber risk strategy including improving the cybersecurity and resilience of not only their organization's systems, but also the security and viability of the cyber eco-system that they are a part of. Board and the management should consider cyber risks of services purchased from external service providers, such as outsourcing, cloud, data exchange, data operator and other similar services, and address them with the means of regular risk management audits and similar activities. Much in the same way that effective cybersecurity risk management required the breaking down of siloes within the organization, truly effective systemic cyber resilience can only be achieved by breaking down the barriers that exist to information sharing between organizations, law enforcement, regulators, and communities. Boards can explore ways that the company and its management can cooperate with information-sharing organizations and law enforcement within various tools in the Toolkit.

1 NACD, "Principles for Board Governance of Cyber Risk", 2021 https://www.nacdonline.org/insights/publications.cfm?ItemNumber=71795

2 Business Roundtable, Statement, 2020, https://www.businessroundtable.org/business-roundtable-redefines-the-purpose-of-a-corporation-to-promote-an-eco nomy-that-serves-all-americans

RESILIENCE AND COLLABORATION AMONG THE EU MEMBER STATES

EU countries agreed on the necessity to have strong government bodies that supervise cybersecurity in their country and that work together with their counterparts in other Member States by sharing information. The Directive on security of network and information systems (NIS Directive), which all countries have now implemented, ensures the creation and cooperation of such government bodies. This Directive was reviewed at the end of 2020, published in the Official Journal of the European Union in December 2022 and entered into force on 16 January 2023. The 21 Member States will have to incorporate the provisions into their national law on 17 October 2024.

European Legislation and certification to encourage resilience and collaboration among the EU Member States includes:

* The cybersecurity agency. ENISA (European Union Agency for Cybersecurity) is the EU agency that deals with cybersecurity. It provides support to Member States, EU institutions and businesses in key areas, including the implementation of the NIS Directive.

* The Cyber Resilience Act. The proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act, bolsters cybersecurity rules to ensure more secure hardware and software products. It is under strong debate and could make the EU a leader on cybersecurity and change the rules of the game globally.

* The Cybersecurity Act strengthens the role of ENISA. The agency now has a permanent mandate and is empowered to contribute to stepping up both operational cooperation and crisis management across the EU. It also has more financial and human resources than before. On 18 April 2023, the Commission proposed a targeted amendment to the EU Cybersecurity Act.

* The EU Cyber Solidarity Act, to improve the response to cyber threats across the EU. The proposal will include a European Cybersecurity Shield and a comprehensive Cyber Emergency Mechanism to create a better cyber defence method.

* The EU-wide certification framework for having a single common scheme for cyber certification of IT products and services within the EU.

PRINCIPLE 6

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 a broader environment in which the business operates.

* Ensure that risks arising from the use of third-party service providers are integrated with the enterprise risk management framework.

* Develop peer networks including other board members to share best governance practices across institutional boundaries.

* Ensure management has plans for effective collaboration and information sharing, especially with the public sector on improving security and resilience.

* Ensuring that management takes into account risk stemming from broader industry considerations (e.g. third-party vendors and partners - see Tool D in the Toolkit for further details).

* Encourage management participation in industry groups and knowledge and information sharing platforms such as sector specific information sharing and analysis centres (ISACs) and/or cross sectoral information sharing organizations (ISOs).

* Encourage management to ensure that their cyber security providers belong to Computer Security Incident Response Teams ('CSIRTs'), also known as Computer Emergency Response Teams ('CERTs'). These teams provide deal with cybersecurity incidents and risks in practice. They cooperate with each other at EU level and has access to the latest cybersecurity technologies and practises.

MEMBERS OF THE WORKING GROUP

Key writers:

Larry Clinton
President/CEO
Internet Security Alliance (ISA)

Parker Phillips
Manager for Policy and Government Affairs
ISA

Advisors:

Tomi Dahlberg
Ph.D (Econ), Board professional, ISS Professor at Turku School of Economics (ret.), Senior Advisor
Directors' Institute Finland (DIF)

Tanja Dreilich
M.Econ, MBA CFO, Supervisory Board Member, Financial and ESG Expert Former CEO
NEMTF

Kasia Kazior
AI Digital Transformation Executive, Supervisory Board Member
Benefit Systems SA (WSE: BFT)

Beatriz Lara Bartolome
NED at UniCredit S. p. A.
Chair of Chapter Zero Spain

Uroš Žust
Partner IT Assurance & Advisory
Forvis Mazars

Béatrice Richez-Baum
Director General
ecoDa

ADDITIONAL CONTRIBUTORS

JR Williamson
Sr, Leidos

Tracie Grella
AIG

Jon Brickey
Mastercard

Deneen DeFiore
United Airlines

Dimitrios Stratakis
BNY Mellon

Kris Lovejoy
Kyndryl

Kelly Bissell
Microsoft Services Group

Brad Maiorino
RTX

Tim Held
US Bank

Ted Webster
Centene

Patrick Hynes
Ernst and Young

Niall Brennan
SAP

Greg Touhill
Carnegie Mellon University

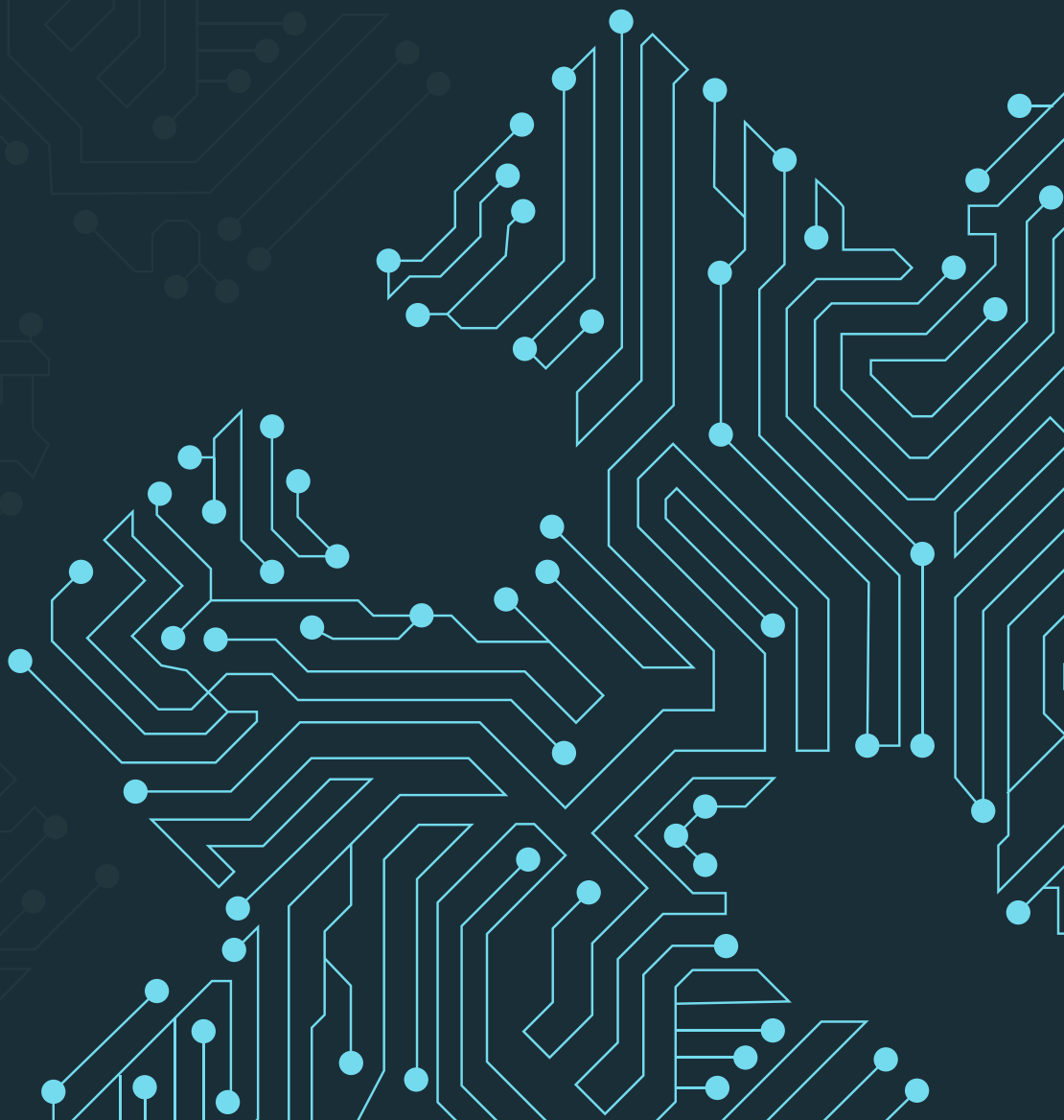
Franck Journoud
National Association of Manufacturers

Richard Rocca
Bunge Limited

Ryan Boulais
AES Corp

Patrick Reidy
GE Aerospace

Michael Higgins
L3 Harris



ecoDa
Avenue des Arts 41
1040 Brussels
Belgium
T: 32 (0) 2231 58 11
contact@ecoDa.eu