INTERNET SECURITY ALLIANCE

ecoDa The European Voice of Directors

AIG

Cyber-Risk Oversight 2020

Key Principles and Practical Guidance for Corporate Boards in Europe

Cyber Risk Governance

WHY A CYBER-RISK OVERSIGHT HANDBOOK FOR EUROPEAN CORPORATE BOARDS?

In 2019, the European Union Agency for Network and Information Security (ENISA) reported the past year saw "significant changes in the cyberthreat landscape."

Cybersecurity is the fastest growing, and perhaps most dangerous, threat facing organisations today. Boards are increasingly focused on addressing these threats.

In 2014, the Internet Security Alliance (ISA) and the National Association of Corporate Directors (NACD) created the first Cyber-Risk Oversight Handbook for Corporate Boards to provide a coherent approach to deal with the issue at Board level. In 2018, the Internet Security Alliance published editions of the handbook for Boards of Directors in the United Kingdom, Japan and Latin America.

The cyber-risk handbooks are an attempt to provide Board members with a simple and coherent framework to understand cyber risk, as well as a series of straight-forward questions for Boards to ask management to assure that their organisation is properly addressing its unique cyber-risk posture.

Independent research on previous editions of the cyber-risk oversight handbook – focused on the same core principles – has shown that use of these principles results in better cybersecurity budgeting, better cyber-risk management, increased alignment of cybersecurity with business goals, and helps create a culture of security.

This handbook has been put together by cybersecurity experts from multiple governments and industry sectors, working together on a voluntary basis. It remains generic and general" and non-sector-specific. No one is being paid to contribute to this effort and there is no charge for the handbook.

This handbook—developed in partnership between ISA, ecoDa and AIG —will promote continued adoption of uniform cybersecurity principles for corporate Boards not only in Europe but across the globe.

Table of Contents

Acknowledgements

The following professionals are acknowledged for their contributions to the development of this Handbook through participation in project meetings, workshops, tele-conferences, and content creation:

INTERNET SECURITY ALLIANCE

Larry Clinton, President & CEO, Internet Security Alliance

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

Dan Lips, Assistant Vice President, Internet Security Alliance

Celeste Lowery, Administrative Assistant to Larry Clinton, President & CEO, Internet Security Alliance

AIG

Mark Camillo, Head of Cyber, EMEA, AIG

Sebastian Hess, Cyber Risk Advisor, AIG

ecoDa

Jan Wesseldijk, Chair, ecoDa

Michel de Fabiani, Chair, Policy Committee, ecoDa

Béatrice Richez-Baum, Director General, ecoDa

Cisco Systems

Santiago Solanas, Vice president EMEAR South and France, Cisco Systems

DLA PIPER

Jim Halpert, Partner, Co-Chair, Global Cybersecurity Practice, Co-Chair, Global Data Protection, Privacy and Security Practice, DLA Piper

Armin Hendrich, Partner, DLA Piper

Prof. dr Patrick Van Eecke, Partner, Co-Chair, Global Cybersecurity Practice, Co-Chair, Global Data Protection, Privacy and Security Practice, DLA Piper

THE BALTIC INSTITUTE OF CORPORATE GOVERNANCE

Rytis Ambrazevičius, President, Baltic Institute of Corporate Governance, Professional Board member

DIRECTORS' INSTITUTE FINLAND

Juhani Strömberg, Senior Advisor, Directors' Institute Finland

GUBERNA

Wouter Avondstondt, Co-founder and manager at Toreon - Information Security

Yves Poullet, Independent Board Member, Guberna Certified Director

NEDCOMMUNITY

Carolyn Dittmeier, Scientific Committee, Nedcommunity

THE SWEDISH ACADEMY OF BOARD DIRECTORS

Katja Severin Danielsson, Partner at PwC Sweden, Board member INSEAD SE Chapter

Per-Arne Molin, Partner at PwC, Sweden

Carl Thorn, Manager Cyber Security at PwC Sweden

THE SWISS INSTITUTE OF DIRECTORS

Michael Hilb, Professor, University of Fribourg, and Member of the Board of Trustees, Board Foundation

Foreword

Organisations across Europe are on notice.

It is no longer a question of whether an organisation will be hacked. It is a simply a question of when.

In coming years, all organisations across Europe will face a range of increasing cybersecurity threats—including traditional cyber-crime, data theft, economic or industrial espionage, ransomware, and disruptive cybersecurity attacks[1].

The *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013)* clearly described the challenge we face:

"For cyberspace to remain open and free, the same norms, principles and values that the EU upholds offline, should also apply online. Fundamental rights, democracy and the rule of law need to be protected in cyberspace. Our freedom and prosperity increasingly depend on a robust and innovative Internet, which will continue to flourish if private sector innovation and civil society drive its growth. But freedom online requires safety and security too."

Ensuring that cyberspace remains free and open will require the government and private sectors to work together to defend our shared values. The European Confederation of Directors Associations (ecoDa) presents this handbook as a tool for corporate directors to use to do their part to ensure internet safety and security. The recommendations elaborated in this paper aim to fit into the overall strategic risk management concepts, they should be considered in an integrated approach and they should help fill the gap between board members' needs and their perceived current knowledge. In any case, it does not prevent board members to tailor make the recommendations to the specific characteristics of their companies. The recommendations do not pretend to be a one-size-fits-all approach.

[1] See recent discussions at the World Economic Forum in January 2020: www.weforum.org/agenda/2020/01/what-are-the-cybersecurity-trends-for-2020/

Executive Summary

This handbook is intended to promote sufficient knowledge by Board members, in any corporate structure, to allow the Board as a whole to respect its mandate for oversight and strategy of information security by evaluating the effectiveness of the risks their organisation is facing, in a full and comprehensive manner, and how it is mitigating those risks.

Five principles have been identified for Boards to follow in addressing and ensuring oversight of cyber risk.

> Principle 1 - Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
>
> Principle 2 - Directors should understand the reputational and legal implications of cyber risks as they relate to their company's specific circumstances.
>
> Principle 3 - Boards should ensure adequate access to cybersecurity expertise, with appropriate reports at both Board and Committee level.
>
> Principle 4 - Board directors should ensure that management establishes an enterprise-wide cyber-risk management framework which encompasses culture, preventive, detective and response capabilities, monitoring and communication at all levels. Resources should be adequate and allocated appropriately on the basis of strategies adopted.
>
> Principle 5 - Board discussions about cyber risk should include strategies on their management (mitigation, transfer through insurance or partnerships, acceptance, etc).

These principles were developed and are applicable to, and important for all directors, including members of unitary (one-tier) Boards, two-tier Boards, and Nordic boards[2]. Every organisation has valuable data and related assets that are under constant threat from cyber-criminals or other adversaries.

This handbook promotes the principles of strategic risk management.

Principle 1 sets the ground for a strategic risk governance by the Board. The Principles 2 and 3 further guide the Board in assessing the risks and determining appropriate strategies. Principles 4 and 5 offer guidance for what the board should expect of management to address cybersecurity as an enterprise-wide risk management issue.

The five principles for effective cyber-risk oversight detailed in this handbook are presented in a relatively generalised form in order to encourage discussion and reflection by Boards of directors. Naturally, directors will adapt these recommendations based on their organisation's unique characteristics; including size, life-cycle stage, strategy, business plans, industry sector, geographic footprint, culture, and so forth.

[2] "A Guide to Corporate Governance Practices in the European Union," ecoDa and International Finance Corporation, 2015, at: www.ifc.org/wps/wcm/connect/c44d6d0047b7597bb7d9f7299ede9589/CG_Practices_in_EU_Guide.pdf?MOD=AJPERES (4 June 2019).

To support the practical implementation of the five principles, a number of tools ("Toolkits") have been provided in the annex of the handbook, mostly providing good questions for directors to ask when reviewing the vast amount of information they will access:

- **Toolkit A - Possible points to include in Board Review or Self-Assessment regarding "Cyber Literacy" and Cybersecurity Culture**

  It is common practice for Boards to adopt an annual review of its performance. It is thus quite appropriate to include in this review, and in particular in its tools provided of questionnaires and structured interviews, questions on cybersecurity literacy and culture at Board level.

- **Toolkit B - Questions for the Board to Ask Management About Cybersecurity**

  In the context of an integrated risk management approach, the possible questions for Board members to ask range from strategic issues, organisational governance, preventive measures and operational controls, threat intelligence, capacity for incident management and recovery. The questions are thus many and may be posed in the context of the various meeting both at Committee level and Board level.

- **Toolkit C - Board-Level Cybersecurity Metrics**

  Metrics cannot be standardised. That is why the Board members can raise the right questions, with the help of this toolkit, to promote a proper quantification of the risks themselves, and of the entity's processes designed to mitigate those risks. These metrics should fall into a proper reporting process to the Board, its committees and management.

- **Toolkit D - Cybersecurity Considerations During M&A Phases**

  Cybersecurity diligence during M&A calls for a two-pronged approach. 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. In addition, all parties involved in the deal process need to be aware of the increased potential for a cyber-attack during the transaction process itself and should diligently maintain their cybersecurity efforts. Applying this approach during M&A will serve to ultimately protect stakeholder value.

- **Toolkit E - References to international standards**

  Finally, this guide summarises references to significant frameworks that assist the Board in having a concrete reference for purposes of an ongoing comprehensive assessment of the cyber security framework of the enterprise.

Introduction

Every day, A.P. Moller-Maersk carries millions of tons of cargo across a network of more than 300 ports in more than 120 countries, or about one-fifth of the world's freight.[3] But on the afternoon of June 27, 2017, the Danish company suffered one of the most damaging cyber-attacks in history. Computer screens across the company's offices went black. Some computers warned users that their files were encrypted and demanded a bitcoin payment. Within hours, the firm's entire global information technology system was offline.

A.P. Moller-Maersk was one of the companies around the world affected by the NotPetya ransomware attack. The attack was estimated to cost the Danish company more than 250 million EURO.

Earlier that year, the WannaCry ransomware affected the U.K. National Health Service (affecting nearly a third of National Health Service trusts), France's Renault, Spain's Telefonica, Portugal Telecom and Deutsche Bahn. According to EUROPOL, the WannaCry and NotPetya attacks "were of an unprecedented global scale, affecting an estimated 300,000 victims, in over 150 countries, with the WannaCry attacks alone estimated to have cost global economies in the region of USD 4 billion."

In 2019, the Cambridge Centre for Risk Studies, in partnership with Lloyd's of London and others, analysed hypothetical scenarios and estimated that "the economic damage to the world economy from a concerted global cyber-attack propagated via malicious email may range between $85 billion and $193 billion." (76 billion EURO and 173 billion EURO)

This sobering estimate highlights the significant risk European companies face from cyber threat.

World Economic Forum

The World Economic Forum listed large-scale cyber-attacks as one of the top five biggest risks facing the world in 2019 Leading companies view cyber risks in the same way they do other critical risks – in terms of a risk-reward trade-off. It is not the responsibility of the Board to become IT experts, but the Board must provide the necessary leadership to protect the organisation from cyber-attacks. The vast majority of cyber incidents are economically motivated, with targets including personal data; financial data; business plans etc…

Due to the immense number of interconnections among data systems, it is no longer adequate for organisations to only secure "their" network; as vendors, suppliers, partners, customers, or any entity connected with the company electronically, can potentially become a point of vulnerability.

Government agencies have focused primarily on defending the nation's critical infrastructure, including power and water supplies and communication and transport networks, from cyber-attacks. There is consensus in the cybersecurity field that cyber-attacks are well ahead of the corporations that must defend against them. Cyber-attacks are relatively inexpensive yet highly profitable, and the resources and skills necessary to launch an attack are quite easy to acquire. Thus, it is no surprise that many observers believe that cyber-risk defence tends to lag a generation behind the attackers.

[3] Maersk, at: https://www.maersk.com/ (3 June 2019)

Trends in corporate cybersecurity: increasing threats, rising complexity

The EY Center for Board Matters and the PwC Governance Insights Center both identified cybersecurity and data privacy as a top priority for European Boards for 2019.[4]

According to the PwC Global Annual CEO survey, based on interviews with 1581 CEO's in 83 countries and presented at the World Economic Forum in Davos January 2020, the top threats on CEOs' radar are over-regulation, trade conflicts, uncertain economic growth, cyber threats and policy uncertainty.

Cyber Security continues to be a top threat in 2020 with a higher ranking on a global basis[5]. Leading companies view cyber risks in the same way they do other critical risks – in terms of a risk-reward trade-off. This is especially challenging in the cyber domain for two reasons.

First, the complexity of cyber threats has grown dramatically. Corporations now face increasingly sophisticated events that outstrip traditional defences. As the complexity of these attacks increases, so does the risk they pose to corporations. The potential effects of a data breach, ransomware attack, business interruption or other cyber incident are expanding well beyond information loss or disruption. Cyber-attacks can have a severe impact on an organisation's reputation and brand, which may be affected more by tangential factors like timing or publicity than the actual loss of data. Companies and directors may also incur legal risk resulting from cyber-attacks.

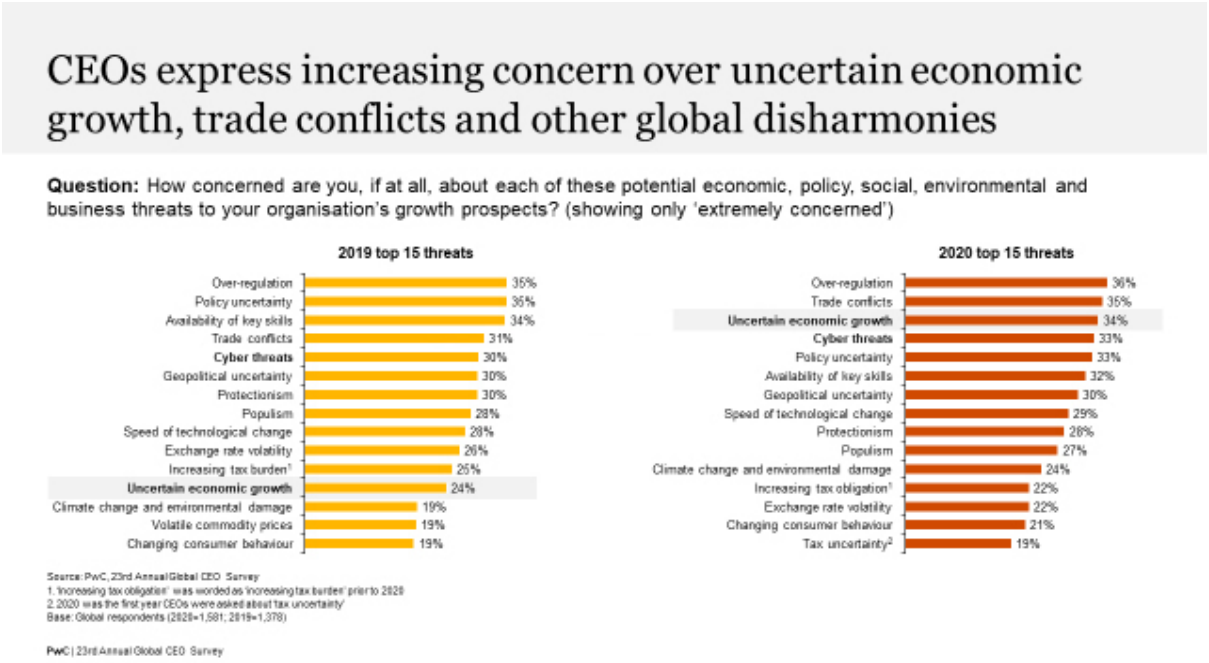
At the same time, the motivation to deploy new and emerging technologies in order to lower costs, improve customer service, and drive innovation is stronger than ever.

These competing pressures on corporate staff and business leaders mean that conscientious and comprehensive oversight at the Board level is essential. As a result, managing and mitigating the impact of cyber risk requires strategic thinking that goes beyond the IT department and into the boardroom.

Although many smaller and medium-sized companies have historically believed that they were too insignificant to be targets, that perception is wrong. In fact, the majority of small and medium-sized businesses have been victims of cyberattacks. In addition to being targets in their own right, smaller firms are often an attack pathway into larger organisations via customer, supplier, or joint-venture relationships, making vendor and partner management a critical function for all interconnected entities.

[4] EY Center for Board Matters, "Board agenda 2019: Top priorities for European boards," at: https://www.ey.com/gl/en/issues/governance-and-reporting/center-for-board-matters/ey-top-eight-priorities-for-european-boards-in-2019 (5 June 2019) and PwC Governance Insights Center https://www.pwc.com/us/en/services/governance-insights-center.html

[5] https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2020.html



Balancing cybersecurity with profitability

Like other critical risks organisations face, cybersecurity cannot be considered in isolation. Members of management and the board must strike the appropriate balance between protecting the security of an organisation and mitigating losses, while continuing to ensure profitability and growth in a competitive environment.

Many technical innovations and business practices that enhance profitability can also undermine security. For example, many technologies, such as mobile technology, cloud computing, and "smart" devices, can yield significant cost savings and business efficiencies, but they can also create major security concerns if implemented incorrectly. Properly deployed, they could increase security.

Similarly, trends such as BYOD (bring your own device), 24/7 access to information, the growth of sophisticated "big data" analytics, and the use of long international supply chains may be so cost-effective that they are essential elements in order for a business to remain competitive. However, these practices can also dramatically weaken the security of the organisation.

It is possible for organisations to defend themselves while staying competitive and maintaining profitability. However, successful cybersecurity methods cannot simply be "bolted on" at the end of business processes. **Cybersecurity needs to be woven into an organisation's key systems and processes from end to end; and when done successfully, it can help build competitive advantage**.

The benefits of basic cybersecurity hygiene

According to PwC Digital Trust Insights, “only 27% of the board members feel ‘very comfortable’ that the board is getting adequate reporting on metrics on cyber and privacy risk management[6] . This doesn’t mean that reasonable security is unachievable, it just means that cybersecurity needs to be more than simply IT-based perimeter security.

As attacks have become more sophisticated, defences must become more sophisticated too. Many cyber threats and attacks can be avoided based on a disciplined basic IT security, and such disciplined basic IT security is moreover a foundation to be able to guard against more sophisticated attacks or breaches. Greater attention should be given to the ability of organisations to make wise investments in cyber security.

Cyber security is gaining an increasing share of the total IT budget, but many organisations make the wrong priorities and invest without actually knowing how it affects the cyber risks to which they are exposed.

Companies should involve the Cyber security aspect in an early stage of the Digital Transformation Journey. According to the Fall 2018 Digital Trust Insights, PwC , "91% of enterprise-wide digital transformation include security and/or privacy personnel as stakeholders, and 53% include proactive management of cyber and privacy risks by design in the project plan and budget “fully from the start” .

[6] Fall 2018 Digital Trust Insights, PwC https://www.pwc.fr/fr/assets/files/pdf/2018/11/pwc-en-journey-to-digital-trust.pdf

The worker…

.. as first line of defence

Workers are on the frontline of an organisation's defence against cybersecurity threats. They can prevent many breaches simply by recognising and avoiding phishing attacks and ensuring that software patches are regularly updated. In this respect, employees are an organisation's first firewall and a critical aspect of an organisation's cyber resilience.

According to ENISA citing the U.K. government, "around 80% of cyber-attacks are the result of poor cyber habits within the victim organisations."[7] Management is responsible for ensuring that employees receive adequate cyber hygiene training and are held accountable to follow the organisation's security policies and practices.

However, board members have an opportunity to set the tone for the entire organisation through leading by example and overseeing how management identifies, prioritizes and monitors cyber risk. According to PwC, there are seven key areas of focus:

1. Address cyber as an enterprise-wide business issue, not an IT issue
2. Have an oversight approach with access to cyber expertise
3. Understand legal and regulatory requirements
4. Discuss the adequacy of the cyber strategy and plan
5. Engage in discussions with management about cyber risk appetite
6. Get the right information to monitor the cyber and privacy programme
7. Monitor cyber resilience[8].

… as enemy in your camp

According to McKinsey, insider threats are present in half of all cyber breaches.[9] This highlights the need for a strong and adaptable security programme, equally balanced between external and internal cyber threats. **Organisations can't deal with advanced threats if they are unable to stop low-end attacks.** Contract workers and employees, whether disgruntled or merely poorly trained, present at least as big an exposure for companies as attacks from the outside. (Toolkit B includes a discussion of insider threats.)

The vast majority of cyber incidents are economically motivated.[10] Cyber-attackers routinely attempt to steal, corrupt or encrypt all manner of data. Typical targets include personal information, financial data, business plans, trade secrets, and intellectual property. However, any data of value, or essential information system can be a target for attack.

---

[7] ENISA, "Review of Cyber Hygiene Practices," December 2016, at: https://www.enisa.europa.eu/publications/cyber-hygiene (16 July 2019).

[8] "How Boards can better oversee Cyber", PwC https://www.pwc.com/us/en/services/governance-insights-center/library/risk-oversight-series/overseeing-cyber-risk.html

[9] Tuckery Bailey, Brian Kolo, Karthik Rajagopalan, and David Ware, "Insider threat: the human element of cyberrisk," McKinsey & Company, September 2018, at: www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk (August 2, 2019).

[10] Verizon, *2016 Data Breach Investigations Report*, p. 7.

Cybersecurity Trends in the European Union

- "Mail and phishing messages have become the primary malware infection vector."[11] – ENISA
- "Ransomware is still overtaking banking Trojans in financially-motivated malware attacks, a trend anticipated to continue," according to the Internet Organized Crime Threat Assessment 2018.[12] -- IOCTA
- Distributed-Denial-of-Service attacks are one of the most common attack vectors: "ENISA reports that over a third of organisations faced a DDoS attack in 2017, compared to just 17 % in 2016." [13] -- ENISA
- "State-sponsored agents increasingly target banks using attack-vectors utilized in cyber-crime."[14] – ENISA
- "The emergence of IoT environments will remain a concern due to missing protection mechanisms in low-end IoT devices and services. The need for generic IoT protection architectures/good practices will remain pressing."[15] – ENISA

[11] ENISA Threat Landscape Report 2018, January 28, 2019, at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 (3 June 2019).
[12] Internet Organized Crime Threat Assessment 2018, at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment (June 3, 2019).
[13] Internet Organized Crime Threat Assessment 2018, at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment (June 3, 2019).
[14] ENISA Threat Landscape Report 2018, January 28, 2019, at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 (3 June 2019).
[15] ENISA Threat Landscape Report 2018, January 28, 2019, at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 (3 June 2019).

Greater connectivity, greater risk

In a December 2018 speech on best practices, Prof. Dr. Udo Helmbrecht, Executive Director of ENISA, discussed how new technologies are reshaping the cybersecurity landscape and increasing risk. [16]

"In the last few years, there have been many new developments in the cyber world. We continue to witness the digitalisation of our daily lives, the development of new technologies, new threats and new stakeholders," Prof. Dr. Helmbrecht commented, adding: "From a technical perspective, we have new technologies changing the cyber landscape. The Internet of Things/Internet of people is now being deployed with an estimated 20 Billion devices expected to be operational before 2020. Industry 4.0, Robotics, Artificial Intelligence, Quantum Computing, and BlockChain technologies are emerging as disruptive technologies and are beginning to affect our daily lives."

Although 70% of respondents to a PwC's survey say AI is critical to at least some of their business, only 31% are very comfortable they are building sufficient digital trust controls into their adoption of AI. The most effective controls are built during the design and implementation phase [17] .

Due to the immense number of interconnections among data systems, it is no longer adequate that organisations secure only "their" network. Vendors, suppliers, partners, customers, or any entity connected with the company electronically can become a potential point of vulnerability. The growing interconnected nature of traditional information systems and non-traditional systems such as security cameras, copiers, video-gaming platforms and cars (the so-called Internet of Things, or IoT) has resulted in an exponential increase in the number of potential points of entry for cyber-attackers; and thus, the need for organisations to expand their thinking about cyber-risk.

As Prof. Dr. Helmbrecht warned: "Europe and its digital single market need to be ready to adapt and reap the benefits of these technologies in a safe and secure cyber environment. Traditional approaches to security will have to be adapted in order to cope with these new challenges." According to PwC, 81% say IoT is "critical" to at least some of their business but only 39% are "very comfortable" they are building sufficient digital trust controls into adoption of IoT and 30% say they plan to invest in IoT security over the next 12 months". [18]

[16] https://www.enisa.europa.eu/publications/ed-speeches/cybersecurity-best-practices
[17] PwC, "Accelerating innovation: How to build trust and confidence in AI", 2017.
[18] Fall 2018 Digital Trust Insights, PwC

Cybercrime on the rise

Government agencies have focused primarily on defending the nation's critical infrastructure (including power and water supplies, communication and transportation networks, and the like) from cyber-attack. According to PwC, "only about half of medium and large businesses in key sectors say they are building resilience to cyberattacks and other disruptive events to a large extent. And fewer than half of them say they are very comfortable their company has adequately tested its resistance to cyberattacks" [19]. While such attacks are technically possible and could have very serious consequences, EUROPOL reports that "a significant portion of cybercrime is carried out by financially motivated criminals."[20]

ENISA warns that, "[in] 2018, Cyber-criminals remained the most active threat agent group in cyber-space," and assessed this threat group was "responsible for over 80% of the incidents." Cyber-attackers routinely attempt to steal all manner of data, including personal information from customers and employees, financial data, business plans, trade secrets, and intellectual property. Increasingly, cyber-attackers are employing tactics that encrypt an organisation's data, effectively holding it hostage until they receive a payment – so-called "ransomware."

According to EUROPOL, "While it is difficult to provide reliable estimates, some industry reports suggest that the global cybercrime costs are in the hundreds of billions of euros per year."[21]

Although many smaller and medium-sized companies have historically believed that they were too insignificant to be targets, that perception is wrong. According to the Hiscox Cyber Readiness Report 2019, which is based on a survey of more than 5,300 in Europe and the United States, "smaller firms, with fewer than 50 employees, reported an increase in cyber-attacks from 33% to 47%. Similarly medium sized firms, employing 50 – 249 people, also reported a sharp increase from 36% to 63%."[22] In addition to being targets in their own right, smaller firms are often an attack pathway into larger organisations via customer, supplier, or joint-venture relationships, making vendor and partner management a critical function for all interconnected entities.

What is at Stake?

	Top 10 most valuable information to cyber criminals	Top 10 biggest cyber threats to organisations
1.	Customer information (17%)	Phishing (22%)
2.	Financial information (12%)	Malware (20%)
3.	Strategic plans (12%)	Cyberattacks (to disrupt) (13%)
4.	Board member information (11%)	Cyberattacks (to steal money) 12%
5.	Customer passwords (11%)	Fraud (10%)
6.	R&D information (9%)	Cyberattacks (to steal IP) (8%)
7.	M&A information (8%)	Spam (6%)
8.	Intellectual property (6%)	Internal attacks (5%)
9.	Non-patented IP (5%)	Natural disasters (2%)
10.	Supplier information (5%)	Espionage (2%)

Source: EY Global Information Security Survey 2018-19.

[19] idem
[20] Internet Organised Crime Threat Assessment IOCTA 2017, at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017 (4 June 2019).
[21] EUROPOL, European Cybercrime Centre – EC3, at: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (4 June 2019).
[22] Meera Narendra, "Cyber-attacks reported by 61% of US and European firms over past year," PrivSecReport, 29 April 2019, at: https://gdpr.report/news/2019/04/29/cyber-attacks-reported-by-61-of-us-and-european-firms-over-past-year/ (4 June 2019).

The Upside-Down Economics of Cyber Security

There is consensus in the cybersecurity field that cyber-attackers are well ahead of the corporations that must defend against them.

To begin with the Internet is designed as an "open system" with little thought to security. Cyber-attacks are relatively inexpensive yet highly profitable, and the resources and skills necessary to launch an attack are quite easy to acquire. It is no surprise that many observers believe cyber-risk defence tends to lag a generation behind the attackers.

It is difficult to demonstrate return on investment (ROI) for cyber-attack prevention, and successful law enforcement response to such attacks is virtually non-existent. For instance, a review of cybersecurity prosecutions in the United Kingdom found that "less than one percent of cyber-crime incidents are prosecuted."[23]

This does not mean that defence is impossible, indeed the sections covering Principles 4 and 5 describe how organisations can now make economically based assessments for cyber risk and management. However, it does mean that **Board members need to ensure that management is fully engaged in making the organisation's systems as resilient as economically feasible**. This includes developing defence and response plans that are capable of addressing sophisticated attack methods, as well as preparing a communications plan in the event of a cyber incident.

But to be effective, cyber strategy must be more than reactive. Leading organisations also employ a proactive, forward-looking posture that includes generating intelligence about the cyber-risk environment and anticipating where potential attackers might strike. This includes subjecting their own systems and processes to regular and rigorous testing to detect vulnerabilities.

[23] Stephen White, "Less than 1 percent of cyber crime incidents are prosecuted," PrivSecReport, at: https://gdpr.report/news/2019/05/28/less-than-one-percent-of-cyber-crime-incidents-are-prosecuted/ (17 July 2019).

Corporate Directors Should Lead by Example

The European Union Agency for Network and Information Security wrote: “Organisations should strive for adherence (active participation) rather than compliance – rapidly emerging threats require employees who are engaged and willing to step up. Organisational leadership has a key role in developing effective and workable security—by helping security specialists to fit security into the business, breaking down silos and leveraging other organizational capabilities (safety, HR, communications) – but not least by setting the tone and leading by example. Measures to improve security behavior should be an ongoing, iterative process – the human factor in cyber-security is never ‘solved’, and there is no simple ‘solution,” but human skills and knowledge, rather than vulnerabilities, can be made to work in favour of an organisation’s defensive cybersecurity.”

“Lead by example: always follow security policies (you are a high-value target) and commit a portion of your time to work with security specialists and staff to finding workable solutions in your areas of expertise.”

- ENISA, “Cybersecurity Culture Guidelines: Behavioral Aspects of Cybersecurity,” December 2018.

The OECD recommended 8 organisational principles to promote the development of a robust cyber risk management framework. These principles emphasised, among other things, building a cyber aware corporate culture, indication and designation of risk owners, compliance with human rights and fundamental values, cooperation and breaking down barriers, strategical and operational approaches including a three-step risk assessment, technical and organisational innovation , the importance of culture in preparedness and resilience capabilities.

- Digital Security Risk Management for Economic and Social Prosperity- OECD Recommendations and Companion Document (2015)

Principle 1

Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

Key recommendations:

- Information security should not be considered as purely a technical issue left to the IT department;
- Cybersecurity has to be perceived as an enterprise-wide risk management issue through the whole life cycle of the company;
- The risk-oversight should be a function of the full board;
- The board should not rely on a one-size-fits-all approach, they have to define their own tailor-made plans;
- The board should develop the right culture inside the company to ensure that all employees take cybersecurity as a serious matter;
- The management's duty is to make information related to the prevention, detection and response capabilities and knowledge of the maturity scale in which the company operates, available to the board. In doing so, the management should not consider only the organisation's own networks but its larger ecosystem.

Tool Kits:

- Toolkit A for suggested questions to include in the Board Review & Self-Assessment to help assess the Board's level of understanding of cybersecurity issues or cyber literacy;
- Toolkit B for a list of cybersecurity questions that directors can ask management on issues such as strategy, risk assessment, prevention measures, incident, incident response, and post-breach response and communication;
- Toolkit C for related questions that directors can ask to promote optimal performance metrics and reporting;
- Toolkit D for cybersecurity considerations related to mergers and acquisitions.

In detail:

Historically, corporations have categorised information security as a technical or operational issue to be handled by the information technology (IT) department. This misunderstanding was fed by siloed corporate operating that left functions and business units within the organisation feeling disconnected from responsibility for the security of their own data or protecting against other forms of cyber-attacks which can affect the entire organisation. Instead, this critical responsibility is handed off to IT, a department that in most organisations is strapped for resources and budget authority. **Furthermore, deferring responsibility to IT inhibits critical analysis and communication about security issues, and hampers the implementation of effective security strategies.**

In an increasingly inter-connected ecosystem, every business is a technology business where IT creates and adds value. Most companies invest heavily in IT innovation and making technology

infrastructures increasingly central to overall business strategy and operations. Depending on their sector and the services they provide, some companies rely more inherently on IT than others.

The 2015 *Digital Vortex* study found that digital disruption "has the potential to overturn incumbents and reshape markets faster than perhaps any force in history"[24]. All companies are digital companies, whether they recognize it or not.

Over the last several years, the business community's level of awareness of the importance of information security in general, and the cross-functional nature of cybersecurity in particular, has grown a great deal – fueled in part by the constant stream of headlines about cyber incidents[25].

But while progress has been made, many management teams and boards still hold dated views about cybersecurity. The 2018-19 NACD Governance survey noted that a majority of board members continue to regard cyber as an area for improvement and expect cyber-attacks to have a major impact on their business in the next 12 months. The EY 2018 global information security survey found that, "77% of organisations are still operating with only limited cybersecurity and resilience, while 87% of organisations warn they do not yet have sufficient budget to provide the levels of cybersecurity and resilience they want"[26].

Ideally cyber risks should be evaluated in the same way an organisation assesses the security of its human, intangible and physical assets and the risks associated with their potential compromise. In other words, **cybersecurity is an enterprise-wide risk management issue that needs to be addressed from a strategic, cross-departmental, and economic perspective**.[27] It is not just an IT (or technology) issue, but also about business processes, people, and value.

Cyber risk and the business ecosystem

Cyber-attacks can take on many different forms and have evolved beyond traditional hacking. Some of the highest-profile data breaches or cyber-attacks to date have had little to do with traditional hacking. For example, spear phishing (a common e-mail attack that targets specific individuals) is a leading cause of system compromise. Activities such as product launches or production strategies that use complex supply chains that span multiple countries and regions can magnify cyber risk. Similarly, mergers and acquisitions requiring the integration of complicated systems, often on accelerated timelines and without sufficiently allocating resources to perform comprehensive due diligence, can increase cyber risk.

Another obstacle companies face in creating a secure system is how to manage the degree of connectivity that the corporate network has with partners, suppliers, affiliates, and customers. Several significant and well-known cyber-breaches did not actually start within the target's IT systems, but instead resulted from vulnerabilities in one of their vendors or suppliers, as the examples in the section, Greater connectivity, greater risk," reflect. It is important to implement a TPRM (Third Party Risk Management) from several perspectives including sourcing, continuously monitoring and exit plans.

---

[24] Global Center for Digital Business Transformation, "Digital Vortex: How Digital Disruption is Redefining Industries," An IMD and Cisco Initiative, June 2015, at: https://www.cisco.com/c/dam/en/us/solutions/collateral/industry-solutions/digital-vortex-report.pdf (16 July 2019).

[25] NACD's 2018-19 Governance Survey noted that 81% of directors believe their understanding of the cyber threat has increased over the past three years, and 50% now feel their companies are properly secured from cyber attack (up from 37%). Of course, that means 50% of directors also don't feel their organizations have been properly secured.

[26] EY, Global Information Security Survey, 2018, at: https://www.ey.com/en_gl/giss (August 22, 2019).

[27] Internet Security Alliance and American National Standards Institute, *The Financial Management of Cyber Risk: An Implementation Framework for CFOs,* 2010.

In addition, organisations are investigating new ways to manage data, (e.g., having some data residing on external networks or in public "clouds"), which can increase their risk. **By outsourcing their data storage, the company have limited ability to secure the data.** As a result, organisations using these, often cost effective, methods, should evolve methods to assure adequate risk management is undertaken by the provider.

As a result, **directors should ensure that management is assessing cybersecurity not only as it relates to the organisation's own networks, but also regarding the larger ecosystem in which it operates**. Progressive boards will oversee these activities and engage management in a discussion of the varying levels of risk that exist in the company's ecosphere and understand how they are taken into consideration as the organisation's leaders make about how they calculate the appropriate cyber-risk posture and tolerance for their own corporation of the organisation.[28].[29] Board members also should understand what highly sensitive data and business operations the company needs to protect most, and ensure that management has a protection strategy that addresses these priorities. The board should instruct management to consider not only the highest-probability attacks and defences, but also low-probability, high-impact attacks that would be catastrophic attack scenarios that have a low probability of occurrence but would have an existential impact on the organisation.

The overall spectrum of a cyber enterprise- wide risk management system at Board level must cover several capacities, with the aid of the adoption of a specific framework allowing for comprehensive assessment and oversight of all areas, including;

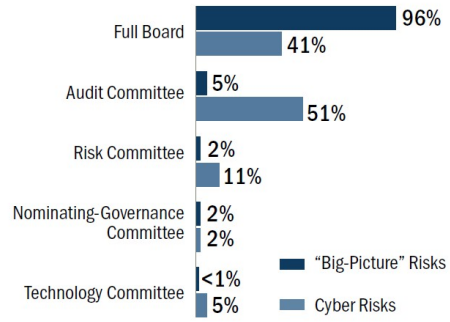
- Governance & organisation
- Strategy in line with objectives
- Risk analysis
- Steps taken regarding all phases of prevention, detection and response capabilities

A comprehensive assessment of all capacities is necessary to ensure truly effective global risk management. Reference to international frameworks is included in Toolkit E of the handbook.

Figure 2

Governance and cyber-risk oversight responsibility at the Board level

To which group has the board allocated the majority of tasks connected with the following areas of risk oversight? (Partial list of response choices; multiple selections permitted)



Source: *2016–2017 NACD Public Company Governance Survey*

[28] NACD, et al., *Cybersecurity: Boardroom Implications* (Washington DC: NACD, 2014)(an NACD White paper).
[29] NACD, et al., *Cybersecurity: Boardroom Implication* (Washington, DC: NACD, 2014) (an NACD white paper).

How to organise the Board to manage the oversight of cyber risk, and enterprise-level risk more broadly, is a matter of considerable debate. Cyber-risk can be mitigated and minimised significantly if approached as an enterprise-wide risk management issue. However, as with traditional risks, cyber risks cannot be eliminated entirely, and Boards need to understand the nature of their company's threat environment. The NACD Blue Ribbon Commission on Risk Governance recommended that risk oversight should be a function of the full Board.[30] NACD research finds this to be true at most public-company Boards with so-called "big picture risks" (i.e. risks with broad implications for strategic direction, or discussions of the interplay among various risks). Yet most Boards assign the majority of cybersecurity-related risk-oversight responsibilities to the Audit committee (Figure 2), which also assumes significant responsibility for oversight of financial reporting, internal control and compliance risks. However, European Boards may consider other factors, including the difference in corporate board governance structure, across European countries.

There is no single approach that will fit every Board: some 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. **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.** The full Board should be briefed on cybersecurity matters at least semi-annually and as specific incidents or situations warrant. **Committees with designated responsibility for risk oversight (and for oversight of cyber-related risks in particular) should receive briefings on at least a quarterly basis.**

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 meet together once a year for a discussion that includes a "deep dive" on cybersecurity.[31]

While including cybersecurity as a stand-alone item on Board and/or committee meeting agendas is now a widespread practice, the issue should also be integrated into full-board discussions involving 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.

The culture of a company tends to flow from the top down and Boards should take a vigorous approach to cybersecurity to show employees that cyber risk must always be an important consideration. Effective governance structures should then be implemented to underpin that culture and ensure the company is properly focused on managing these risks. **It is also advisable for directors to participate in cyber-breach simulations to gain exposure to the company's response procedures in the case of a serious incident to mitigate against its potential impact**, and to practice for a potential scenario that requires the board to make an important decision.

[30] NACD, *Report of the Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward* (Washington, DC: NACD, 2009).
[31] Adapted from Robyn Bew, "Cyber-Risk Oversight: 3 Questions for Directors," *Ethical Boardroom*, Spring 2015.

To facilitate this, Boards should consider having access to IT-expertise at the Board level, rather than simply relying on other parts of the business, and a transparent allocation of responsibility for oversight of cybersecurity. This is discussed further in Principle 3.

See Toolkit A for suggested questions to include in the Board Review & Self-Assessment to help assess the Board's level of understanding of cybersecurity issues or cyber literacy.

Comprehensive assessment and oversight by the Board of cyber risk is not 'one-size fits all'

In addition to the many Governance issues, the Board must obtain from management a comprehensive assessment of all prevention, detection and response capabilities, and knowledge of the maturity scale in which the organisation currently operates, and targets.

In order to do this, the true awareness of risk specific to the entity is fundamental. As noted in most governance and control issues, "one size does not fit all".

The strategic awareness is threefold

- Know the wide sphere of threats, to continually update for emerging risks;
- Realize the extent of the business "ecosystem", where connectivity extends within and outside the entity;
- Understand and agree on the more and less critical assets of the enterprise subject to cyber risk.

The sphere of threats widens: Some of the highest-profile data breaches or cyber-attacks to date have had little to do with traditional hacking. For example, spear phishing (a common e-mail attack that targets specific individuals) is a leading cause of system compromise. Product or production strategies that use complex supply chains that span multiple countries and regions can magnify cyber risk. Similarly, mergers and acquisitions requiring the integration of complicated systems, often on accelerated timelines and without sufficient due diligence, can increase cyber risk.

The business ecosystem: **another obstacle companies face in creating a secure system is how to manage the degree of connectivity that the corporate network has with partners, suppliers, affiliates, and customers.** Several significant and well-known cyber-breaches did not actually start within the target's IT systems, but instead resulted from vulnerabilities in one of their vendors or suppliers. Furthermore, an increasing number of organisations have data residing on external networks or in "clouds," which they neither own nor operate and have little inherent ability to secure. Many organisations are also connected with elements of the national critical infrastructure, raising the prospect of cybersecurity at one company or institution becoming a matter of public security, or even affecting national security.

As a result, directors should ensure that management is assessing cybersecurity not only as it relates to the organisation's own networks, but also regarding the larger ecosystem in which it operates. Companies should perform a maturity assessment related to security aspects of third parties in the ecosystem. This also needs to be addressed in the context of the organisations threat profile. Advanced Persistent Threats may target a subcontractor multiple links in the supply chain from the main target.

Progressive Boards will engage management in a discussion of the varying levels of risk that exist in the company's ecosystem and account for them as they calculate the appropriate cyber-risk posture and tolerance for their own corporation.[32] They should also understand what highly sensitive data and business operations the company needs to protect most, and ensure that management has a protection strategy that addresses these priorities. The Board should instruct management to consider not only the highest-probability attacks, but also low-probability, high impact attacks that would be catastrophic.[33]

Awareness of the critical assets: identifying highly sensitive categories of data and critical business operations is essential to determining a strategy and requires regular updates with management

- What are our company's most critical data assets? The importance of the company's assets as it refers to cyber risk vary immensely between companies and must be assessed as to priority.
    - Customer information or passwords;
    - Financial information;
    - Intellectual property, patented or non-patented;
    - R&D information;
    - Strategic plans or M&A information;
    - Board member and employee information;
    - Supplier information.
- What highly sensitive data does the company hold? (e.g. sensitive personal data)
- What is the backbone of the business and what are the IT infrastructures in use to run the business?
- Where do they reside? Are they located on one or multiple systems?
- How are they accessed? Who has permission to access them?
- How often have we tested our systems to ensure that they are adequately protecting our data?

Once the strategic risk identification is in the hands of the Board, it is then able to evaluate and discuss the programme of defence proposed by management.

See Toolkit B for a list of cybersecurity questions that directors can ask management on issues such as strategy, risk assessment, prevention measures, incident response, and post-breach response and communication.

See Toolkit C for related questions that directors can ask to promote optimal performance metrics and reporting.

See Toolkit D for cybersecurity considerations related to mergers and acquisitions.

[32] NACD, et al., *Cybersecurity: Boardroom Implication* (Washington, DC: NACD, 2014) (an NACD white paper).
[33] Ibid. See also: KPMG Audit Committee Institute, *Global Boardroom Insights: The Cyber Security Challenge*, Mar. 26, 2014.

Principle 2

Directors should understand the reputational and legal implications of cyber risks as they relate to their company's specific circumstances.

Key recommendations:

- Cybersecurity is not just about reputational issues, it is also about liability of board members;
- Board members should have a good knowledge of the existing legislations be it at European or national level, or even Industry-specific in order to exercise properly their duty of care.

In detail:

A 2018-19 survey on public governance found that 48.9 percent of directors surveyed identified "changes in the regulatory climate" as a "top trend having the greatest effect over the next 12 months," higher than "economic slowdown," "cybersecurity threats," or "geopolitical volatility."[34]

The legal and regulatory landscape with respect to cybersecurity, including required disclosures, privacy and data protection, information-sharing, infrastructure protection and more, is complex and constantly evolving.

Boards should stay aware of both reputational and liability issues faced by their organisations – and, potentially, by directors on an individual basis. For example, high-profile attacks may result in lawsuits, including (for public companies) shareholder derivative suits accusing the organisation of mismanagement, waste of corporate assets, and abuse of control. Plaintiffs may also allege that the organisation's board of directors neglected its fiduciary duty by failing to take sufficient steps to confirm the adequacy of the company's protections against data breaches and their consequences. Exposures can vary considerably, depending on the company's or organisation's sector and operating locations.

The business judgment rule may protect directors, so long as the board takes reasonable investigation steps following a cybersecurity incident. Other considerations include maintaining records of boardroom discussions about cybersecurity and cyber risks; staying informed about industry-, region-, or sector-specific requirements that apply to the organisation; and determining what to disclose in the wake of a cyberattack. It is also advisable for directors to participate in one or more cyberbreach simulations, or "table-top exercises," to gain exposure to the company's response procedures in the case of a serious incident.

[34] NACD Risk Oversight Advisory Council, "Current and Emerging Practices in Cyber-Risk Oversight," 2019.

Legal Landscape in the EU

Legal challenges to organisations include overlapping and conflicting rules and requirements, lack of coordination among rulemaking and legislative authorities, and different priorities driving the development of new regulations. While directors do not need to have deep knowledge about this increasingly 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 or not the organisation is adequately addressing these potential legal risks.

There are three key trends emerging from both EU cyber laws:

1. A broad legal requirement to maintain "appropriate" security standards, informed by the nature of the data requiring protection;
2. Greater transparency requirements, including obligations to notify data breaches to regulators (and in some cases affected individuals) within very short timescales; and
3. Much tougher sanctions for non-compliance and greater risk of private claims.

Data protection: rules for data controllers and data processors[35]

Within the European Union, the General Data Protection Regulation (GDPR) sets out various obligations for "controllers" (organisations with control over why certain personal data must be collected and used, and how) and "processors" (organisations collecting or using personal data in accordance with the controller's instructions). In particular, it requires the implementation of *"appropriate technical and organisational 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 organisation 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).

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.[36] ICO also recently fined international hotel company Marriott $123 million for a breach in the loss of more than 300 million customers' information.[37]

The GDPR is also relevant for non-EU organisations, as many other European countries have adopted similar legislation, or simply by virtue of the wide territorial reach of the GDPR.

[35] Regulation (EU) 2016/679
[36] 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).
[37] 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).

Industry-specific requirements

Next to the GDPR, industry-specific legislation might require an organisation 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 organisations. The ones with the broadest scope[38] at the time of writing of this handbook include the following:

1. **Essential services**: The Network and Information Systems ('NIS') Directive[39] contains requirements for 'operators of essential services' (critical infrastructure) and certain 'digital service providers' that serve essential service providers. These rules include obligations in relation to cybersecurity and notification of incidents with a certain level of impact on the continuity of the services in question. According to cybersecurity expert Melissa Hathaway writing for the Centre for International Governance Innovation, "Companies that suffer a significant breach or service outage must notify the relevant national authority within 48 hours and include the following data points: duration of incident, number of affected parties (for example, customers, vendors, and so on), geographic spread; extent of disruption of service, and impact on economic (calculated in GDP terms) and societal activities."[40]

   These rules apply to the following organisations and industries:

   a) Operators of essential services: energy *(electricity, natural gas, petrol)*, transport *(air transport, rail transport, water transport and road transport)*, finance *(financial institutions, financial trading platforms)*, healthcare *(healthcare institutions, including hospitals and private clinics)*, water *(drinking water supply and distribution)*, digital infrastructures *(IXP [internet exchange points], DNS service providers, top-level domain name registries)*;

   b) Digital service providers serving operators of essential services: online marketplaces, online search engines, cloud computing services.

2. **Telecommunications**: specific security and breach notification obligations also apply to providers of public electronic communications networks or of publicly available electronic communications services. In relation to the latter, for instance, the e-Privacy Directive[41] and Regulation 611/2013/EC provide for a specific breach notification obligation in case of any (i) personal data breach (with a deadline of 24 hours, 'where feasible') or (ii) breach of the security of the network. The new European Electronic Communications Code[42] also provides

[38] There are also EU-wide rules in relation to more specific sectors, such as trust service providers (Regulation (EU) No 910/2014 - "eIDAS Regulation").
[39] Directive (EU) 2016/1148
[40] Melissa Hathaway, "Patching Our Digital Future is Unsustainable and Dangerous," Centre for International Governance Innovation, at: https://www.cigionline.org/articles/patching-our-digital-future-unsustainable-and-dangerous (19 June 2019).
[41] Directive 2002/58/EC
[42] Directive (EU) 2018/1972, to be implemented in national law by EU Member States by 21 December 2020

for an obligation for providers of public electronic communications networks and providers of publicly available electronic communications services to notify "without undue delay" any security incident that has had a significant impact on the operation of networks or services.

3. **Financial sector**: in addition to the NIS Directive, the revised Payment Services Directive[43] (PSD2) contains notification obligations for payment service providers, as well as obligations regarding the management of operational and security risks. Regulators such as the European Banking Authority (EBA) and the European Central Bank (ECB) have also published guidance and documentation on security incident reporting in the banking and payment sectors[44].

4. **Publicly traded companies**: finally, publicly traded companies are subject to general disclosure obligations[45], and Boards of publicly traded companies should be aware that the existence of a cybersecurity breach could constitute inside information and might need to be disclosed to the market. Key considerations will be whether the information is: precise, not generally available, and likely to have a significant effect on the company's share price if made public.

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. On 13 September 2017, the European Commission adopted a cybersecurity package, building on existing instruments and presenting new initiatives to further improve EU cyber resilience and response.[46] One proposal was to charge The European Union Agency for Network and Information Security with new responsibilities to support Member States, EU institutions and businesses in key areas, including the implementation of the NIS directive. The 2017 package also included a blueprint for rapid response to establish a well-rehearsed plan in case of a large-scale cross-border cyber incident or crisis to enhance cooperation between EU Member States and Institutions.

The Commission also proposed setting up an EU certification framework with ENISA at its heart. In March 2019, the European Parliament adopted the safety certification scheme for products, processes and services, while expressing its concern over the Chinese technological threat. This text creates the first European cybersecurity certification scheme to ensure that products, processes and services sold in EU countries comply with cybersecurity standards.[47] In addition to EU and European countries' laws and regulations, organisations must also understand global cybersecurity laws and regulations and the implications for their company's cyber risk. For example, companies should understand the legal requirements of the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018. This law clarifies the legal obligation to comply with a search warrant applies to organisations

[43] Directive (EU) 2015/2366

[44] 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

[45] Article 7, 17 of Regulation (EU) No 596/2014 (the Market Abuse Regulation)

[46] European Commission, "Cybersecurity package 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'," 19 September 2017, at: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-package-resilience-deterrence-and-defence-building-strong-cybersecurity-eu (19 June 2019).

[47] Irene Kostaki, "European Parliament adopts Cybersecurity At to counter Chinese IT threat," New Europe, 13 March 2019, at: https://www.neweurope.eu/article/european-parliament-adopt-cybersecurity-act-asking-for-countermeasures-to-chinese-it-threat/ (19 June 2019).

under U.S. jurisdiction regardless of whether the communication is located beyond the United States.[48] Companies should understand the legal requirements of this law and its relation to the European Union's GDPR.

Board Minutes

Boards should consider how they: maintain records of discussions about cybersecurity and cyber risks; stay informed about industry, region, and sector-specific requirements that apply to the organisation; analyse evolving risks in relation to business resilience and response plans; and, determine what to disclose (and to whom) in the wake of a cyberattack.

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 programme and the integration of technology with the organisation's strategy, policies, and business activities.

[48] Matthias Artzt, Walter Delacrus, "How to comply with both the GDPR and the CLOUD Act," International Association of Privacy Professionals, 29 January 2019, at: https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act/ (19 June 2019).

Principle 3

Boards should ensure adequate access to cybersecurity expertise, with appropriate reporting, at both Board and Committee level.

Key recommendations:

- Board members should employ the same principles of inquiry and constructive challenge as for strategic decisions;
- The board has the duty to precisely specify its expectations to the management and be directive in the type of information they wish to receive;
- Even if Cybersecurity is entrusted to a specific committee, the full board should feel concerned and get at least quarterly debriefings from the management;
- Cybersecurity should not be treated as a stand-alone topic; it has to be embedded in all dimensions of the company's strategy.

Tool Kits:

- Toolkit B for aspects on the cyber risk management team and organisations
- Toolkit C for possible questions on and examples of cyber-risk reporting metrics and dashboards

In detail:

As the cyber threat has grown[49], the responsibility (and expectations) of board members has grown. **Directors need to do more than simply understand that threats exist and receive reports from management. They need to employ the same principles of inquiry and constructive challenge that are standard features of Board-management discussions about strategy and company performance**.

As discussed in Principle 1, leading boards now understand that cyber security is not simply an independent item to be addressed for a few minutes at the end of a board meeting. Rather, cyber security is an essential element of many board level business decisions and needs to be integrated into discussions on issues like mergers, acquisitions, new product development, strategic partnerships and the like at an early stage. As a result, boards need to be accessing information not simply from IT and technical operations but from a wide range of sources including human resources, finance, PR, legal/compliance and others. Several models for implementing such a process are discussed in Principle 4.

[49] NACD Risk Oversight Advisory Council, "Current and Emerging Practices in Cyber-Risk Oversight," 2019. According to 2018-2019 survey of corporate directors, "roughly 83 percent of public company directors and 68 percent of private company directors reported that the quality of cyber-risk information provided by management has improved in the past two years." However, the study also learned that more than 90 percent of directors were "looking to improve cybersecurity oversight across the coming year." These findings highlight that while cybersecurity risk reporting is improving, many Boards continue to seek ways to improve oversight over their organization's cyber-risk.

Over the past decade, boards have become more active in overseeing cybersecurity and requiring information from management[50]. Despite these signs of progress, more than 90 percent of directors of public and private companies surveyed "are looking to improve cybersecurity oversight across the coming year."[51] Only about 14 percent of directors believe their board has a "high" level of knowledge of cybersecurity risks. Only 15% of organisations say their information security reporting currently fully meets their expectations."[52] According to Fall 2018 Digital Trust Insights, PwC "80% say the board has been provided a cyber risk management strategy, but only "27% say they are "very comfortable" the board is getting adequate reporting on metrics on cyber and privacy risk management.[53] When asked to assess the quality of information provided by the board to senior management, information about cybersecurity was rated lowest, with nearly a quarter of public-company directors reporting that they were dissatisfied or very dissatisfied with the quality of information provided by management about cybersecurity. Less than 15 percent said they were very satisfied with the quality of the information they received, as compared with an approximately 64 percent high-satisfaction rating for information about financial performance.[54]

Finally, even in organisations that have implemented good board education programmes on cyber security, leading directors recognize that this education needs to be regularly refreshed. NACD's 2018/19 Public company Governance Survey found that a majority of boards see cyber security as "an area where board knowledge can grow quickly stale. Since threats are nearly limitless and constantly mutate. Directors must assume their current understanding of cyber risks has an expiration date."

[50] Jody R. Westby, Carnegie Mellon University, *Governance of Enterprise Security: CyLab 2012 Report*, (Pittsburgh, PA: Carnegie Mellon University, 2012), p. 7 and p. 16. The 2012 survey found that fewer than 40 percent of boards regularly received reports on privacy and security risks, and 26 percent rarely or never received such information. Since then, boardroom practices have changed dramatically. In an NACD survey of public-company directors, "81 percent now believe their boards' understanding of cyber risk has improved in the last two years." Nearly 90 percent of public-company directors say their boards discuss cybersecurity issues on a regular basis and receive information from a range of management team members (Figure 4). A majority of boards have reviewed 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. In fact, more than 75 percent of boards reviewed their company's current approach to securing its most critical assets against cyber-attacks within the past year.

[51] NACD, *Current and Emerging Practices in Cyber Risk Oversight*, (Washington, DC NACD 2019), p.1.

[52] "Is cybersecurity about more than protection," EY Global information Security Survey, at: https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf (August 16, 2019).

[53] Fall 2018 Digital Trust Insights, PwC https://www.pwc.fr/fr/assets/files/pdf/2018/11/pwc-en-journey-to-digital-trust.pdf

[54] NACD, *2016–2017 NACD Public Company Governance Survey* (Washington, DC: NACD, 2016), p. 28.

How Can Boards Access the Cyber Security Information They Need?

Board members should set clear expectations with management about the format, frequency, and level of detail of the cybersecurity-related information they wish to receive in reviewing reports from management. This should begin with using the cybersecurity expertise within the company to enhance their knowledge. For example, the organisation's Chief Information Security Officer, or other senior management official responsible for overseeing security, can help the Board better understand cybersecurity.

However, directors should be mindful that there might be an inherent bias on the part of management to downplay the true state of the risk environment. Many boards find the scope of cybersecurity reporting insufficient[55].

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. The full board should be briefed on cybersecurity matters at least quarterly and as specific incidents or situations warrant. Committees with designated responsibility for risk oversight— and for oversight of cyber-related risks in particular—should receive briefings on at least a quarterly basis.

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 meet together once a year for a discussion that includes a "deep dive" on cybersecurity.[56]

While including cybersecurity as a stand-alone item on board and/or committee meeting agendas is now a widespread practice, **the issue should also be integrated into a wide range of issues to be presented to the board including discussions on 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 assets, virtually all major business decisions before the board will have cyber components to it. In many ways cyber is now a cross-cutting issue similar to legal and finance. Just as virtually every business decision needs to be considered from a financial and legal perspective, so too, in the digital age, is the case with cyber security. Effective boards approach cybersecurity as an enterprise-wide risk management issue[57].

Boards can, and ought to, consider augmenting their in-house expertise by using a variety of methods to integrate independent expert assessments. These include:

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

---

[55] Sean Martin, "Cyber Security: 60% of Techies Don't Tell Bosses About Breaches Unless It's 'Serious,'" *International Business Times*, April 16, 2014. The study found that 60 percent of IT staff do not report cybersecurity risks until they are urgent—and more difficult to mitigate—and acknowledged that they try to filter out negative results. This potential bias can be mitigated if boards implement one of the enterprise-wide team structures discussed in Principle 4.

[56] Adapted from Robyn Bew, "Cyber-Risk Oversight: 3 Questions for Directors," *Ethical Boardroom*, Spring 2015.

[57] Directors may refer to the Toolkits at the end of this handbook to explore recommendations for how to approach key issues related to cybersecurity oversight, ranging from how to address issues related to crisis management, including incident response, and evolving security challenge, such as supply chain risks and insider threats..

- Leveraging the board's existing independent advisors, such as external auditors and outside counsel, who will have a multiclient and industry-wide perspective on cyber-risk trends.
- Participating in relevant director-education programmes, 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 programmes with fellow board members.

According to one study, 54 percent of companies world-wide employ a Chief Information Security Officer (CISO).[58] Another survey found that organisations with CISOs in place were more likely to have dedicated incident-response teams and plans, and were more confident about the strength of their company's defences against threats such as malware.[59] Where there is no CISO, it will be the security team that carries the responsibilities for cybersecurity.

The Board and top management should assess the appropriateness of the reporting line of the CISO, if present, and the alternative accountability system if absent.

The Question of Adding a "Cyber Expert" to the Board

How to organize the board to manage the oversight of cyber risk—and, more broadly, enterprise-level risk oversight—is a matter of considerable debate. Some recent research has 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 agendas of key committees, depending on how risks are allocated."[60] Additional research found that over half of boards assign the majority of cybersecurity-related risk-oversight responsibilities to the audit committee (Figure 2), which also assumes significant responsibility for oversight of financial reporting and compliance risks.

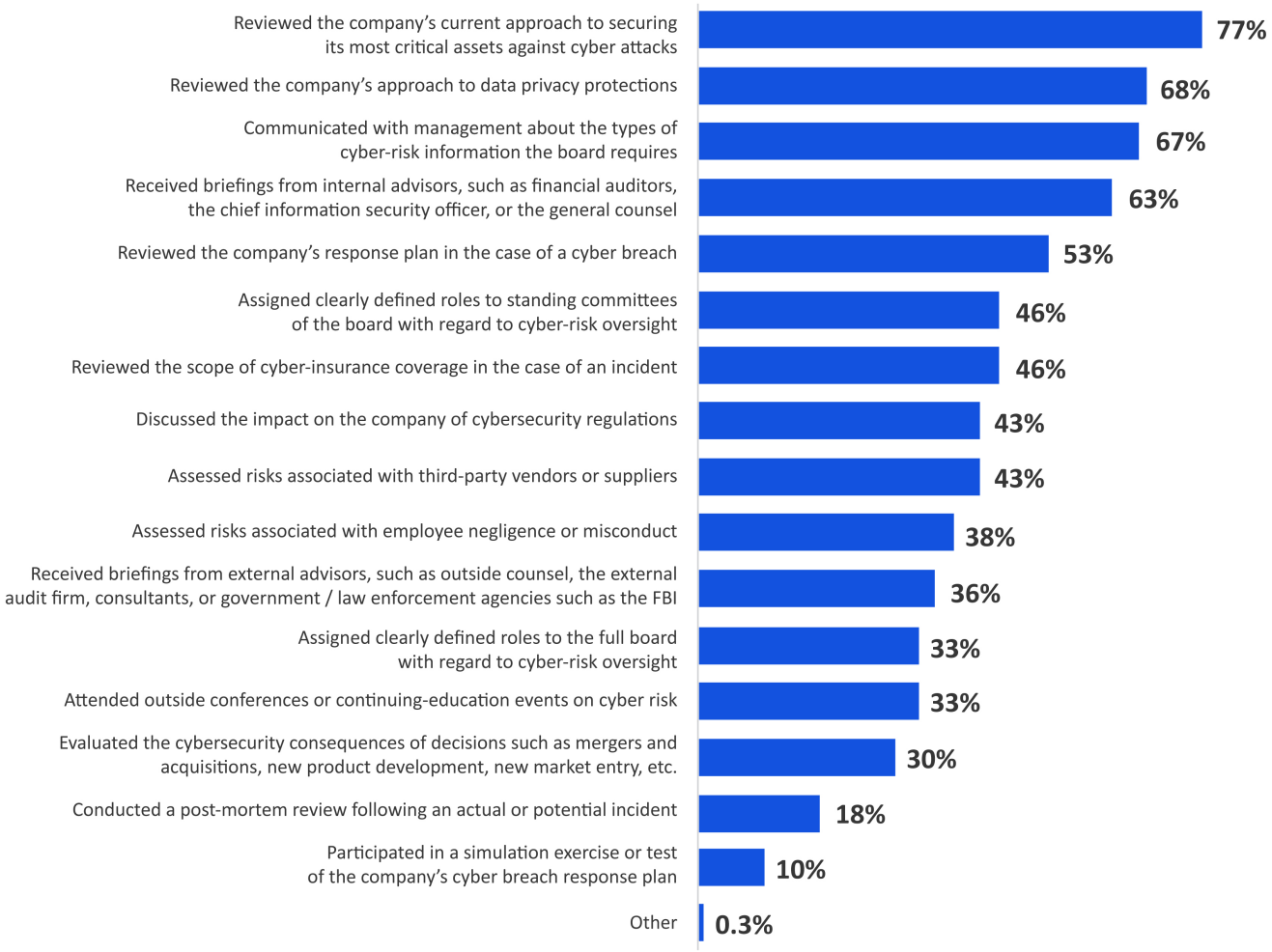
Some companies are considering whether to add cybersecurity and/or IT security expertise directly to the Board via the recruitment of new directors. While this may be appropriate for some companies or organisations, there is no one-size-fits-all approach that will apply everywhere (see "A Cyber expert on Every Board?"). At an NACD roundtable discussion between directors and leading investors, participants expressed concerns about calls to add so-called "single-purpose" directors, whether narrowly specialized in cybersecurity or other areas, to all Boards. As one participant put it, "It can signal risk aversion, a concern that the Board will be sued, so we need one of X, Y, and Z – all the [management] skills du jour. But Board directors aren't running the company"[61].

[58] PwC, Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security Survey 2016 (New York, NY: PwC, 2015), p. 26, and see Paul Solman, "Chief information security officers come out from the basement," *Financial Times,* Apr. 29, 2014.
[59] Kris Monroe, "Why are CISOs in such high demand?", *Cyber Experts Blog*, Feb. 8, 2016.
[60] NACD, *Report of the NACD Blue Ribbon Commission on Adaptive Governance: Board Oversight of Disruptive Risks* (NACD, 2018), p. 13.
[61] Discussion at a joint meeting of the NACD Advisory Councils for Audit Committee Chairs and Nominating and Governance Committee Chairs, Oct. 5, 2016.

Figure 3

Which of the following cyber-risk oversight practices has the board performed over the last 12 months?

Cyber-risk oversight practices performed by the board over the past year
(Select all that apply)



Source: *2018-2019 NACD Public Company Governance Survey*

Directors Can Improve Cyber Risk Oversight Expertise by Completing Training Programme

See Toolkit C for examples of cyber-risk reporting metrics.

The Swiss Institute of Directors	Workshops on cybersecurity are organised as part of the curriculum of the programme without certification.
Luxembourgish Institute of Directors (ILA)	ILA offers a non-certificate training programme on cyber security: Cyber Security for the Board "How to manage Cyber Security risks in the Digital age" https://www.ila.lu/training-1
Board Leadership Society of Denmark	The Cyber Security for Boards Project builds upon the unique competence development and training platform for Board Directors https://boardleadershipsociety.com/5288-2/ In Danish: https://bestyrelsesforeningen.dk/styrkelse-af-strategiske-cyberkompetencer/
Dutch Association of executive and non-executive Directors (NCD)	NCD facilitates colleges and intervision for their members regarding IT and digital issues and dilemmas at board of directors level. For more information contact the NCD service team (www.ncd.nl).

See Toolkit B for aspects on cyber risk management team and organisations
&
Toolkit C for possible questions on cyber-risk reporting metrics.

Principle 4

Board directors should ensure that management establishes an enterprise-wide cyber-risk management framework which encompasses culture, preventive, detective and response capabilities, monitoring and communication at all levels. Resources should be adequate and allocated appropriately on the basis of strategies adopted.

Key recommendations:

- The management should establish both an enterprise-wide technical framework (mobile devices, AI...) as well as a systematic framework (with a forward-looking approach) that will facilitate board oversight of cyber risk;
- The management should have an integrated approach to cyber risk in order to establish a clear accountability framework, clear processes and communication guidelines;
- The management should opt for a bottom-up aggregation approach;
- The board and the management should set the tone at the top and develop the right culture and raise awareness to develop Cyber resilience.

In detail:

Principles 4 and 5 of the Cyber Risk Handbook differ in some respects from the first three principles in that the first three principles focused specifically on what the board should be doing itself and these principles focus more on what the board should be expecting from management.

Technology integrates modern organisations, whether workers are across the corridor or halfway around the world. But, the reporting structures and decision-making processes at many companies are legacies of a siloed and unintegrated past, where each department and business unit makes decisions relatively independently, and without fully taking into account the digital interdependency that is a fact of modern life.

Directors should seek assurances that management is taking an appropriate enterprise-wide approach to cybersecurity by establishing both an enterprise-wide technical framework as well as a management framework that will facilitate board oversight of cyber risk.

Directors should set the expectation that, in developing the company's cyber-risk prevention and response plans, management has considered appropriate cybersecurity framework(s) specific to the organisation and the jurisdictions in which it operates.

Culture and accountability at all levels of the organisation are essential elements.

The European Union Agency for Network and Information Security (ENISA) recommends "a model of awareness, analysis and intervention for organisations to systematically plan and implement changes to address human aspects of cybersecurity."[62]

[62] ENISA, "Cybersecurity Culture Guidelines: Behavioral Aspects of Cybersecurity," December 2018, at: www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity (June 5, 2019).

The Technical Control Framework for Cyber-Risk Management

Modern cyber systems are immensely complicated. Moreover, business and competitive pressures demand that organisations continually adapt and update these systems integrating mobile devices, AI, cloud configurations, blockchain, Internet of Things, quantum computing and surely many more technical innovations and business practices. Clearly directors cannot be expected to fully track and understand all these changes. However, boards should seek assurances from management that they are tracking the cyber systems the enterprise relies on using a framework that has been thought through and is appropriate to the organisation's business needs – including security.

An organisation should start with an assessment of its unique risk profile and threat environment. The ability of an organisation to implement an effective cybersecurity framework starts with a clear understanding of the risk environment it operates in, its unique risk appetite, and the resources needed to mitigate the potential cyber risks. See toolkit E that describes the international framework.

As discussed further in Principle 1, the importance of the company's assets as it refers to cyber risk vary immensely between companies and must be assessed as to priority.

Organisations can use one of the independent, international cybersecurity frameworks to inform a comprehensive assessment of their cybersecurity risk posture, including a gap analysis. This comprehensive assessment can lead to the development of a mitigation plan that the organisation can use to manage progress in implementing controls or other measures to increase security. Such a mitigation plan can incorporate simulations and other mechanisms to ensure that the organisation is reducing its cybersecurity risk as discussed in the Principle 2 section. (Toolkit C addresses board-level cybersecurity metrics, including a discussion on new economic models for managing cyber risk.)

Fortunately, there has been a continual evolution, not only of technologies, but organized frameworks that enable practitioners to better understand, track and manage these complex systems. **Although some organisations choose to largely adopt one such framework, more typically organisations 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 a security perspective (possibly due to the vast variance in cyber-attack methods) but increasingly tools are being developed that map to various frameworks and will enable management to determine and in some cases quantify security management of the systems they choose to use. Greater detail on this process is discussed in Principle 5.

International frameworks exist for cybersecurity technical controls, such as ISO/IEC 27001, developed by the *Organisation Internationale de Normalisation*. Within the European Union, there has been an increase in legislators' interest in these norms, which can sometimes be used to demonstrate compliance[63]. At the European level, the European Union Agency for Network and Information Security (ENISA) has also issued advice and recommendations on information security best practice. In September 2017, the European Commission proposed to reform ENISA and establish a voluntary certification framework that will provide a comprehensive EU industry-wide set of rules, technical requirements, standards and procedures on cybersecurity[64].

[63] See e.g. Belgian implementation of the NIS Directive, which specifically states that ISO/IEC 27001 certification creates a presumption that an organisation's security policy is compliant with the Belgian NIS security requirements.
[64] ENISA. (2017, September 13). European Commission proposal on a Regulation of the European Parliament and of the Council on the future of ENISA [Press release].

In the United States, the National Institute of Standards and Technology (NIST) published a voluntary cybersecurity framework in 2014 and continues to update the framework to reflect best practices for implementing security controls. [65] Released in 2014, the NIST Cybersecurity Framework is a set of standards, methodologies, procedures, and processes that aligns policy, business, and technological issues to address cyber risks. The framework seeks to provide a common language for senior corporate management to use within the organisation in developing an enterprise-wide approach to cyber-risk management. The framework is framed around five key functions, including identify, protect, detect, respond, and recover.[66]

The Framework suggests that to start their cybersecurity review, corporations engage in a risk-management process that will determine where the organisation sits on a four-tier scale: (1) partial, the lowest tier; (2) risk informed; (3) repeatable; and (4) adaptive, the highest tier. This level of management may be beyond the practical ability of all organisations, but some elements are available to all companies. In 2019, NIST published an analysis discussing how the framework was being used internationally.[67]Among the other most commonly used Frameworks management can select and adapt are:

- The International Organisation for Standardization (ISO) created the ISO/IEC 27000 standards for information security.[68] ISO explains that "using this family of standards will help your organisation manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties." [69]

- SANS. The Center for Internet Security's "CIS Controls" includes a list of 20 different security controls for organisations, categorized as "basic," "foundational," or "organisational."[70] These controls range from establishing an inventory of hardware and software assets to penetration testing and red team exercises.[71]

- The Payment Card Industry (PCI) Data Security Standards set "operational and technical requirements for organisations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions."[72]

Directors should set the expectation that, in developing the company's cyber-risk defence and response plans (and related communications plans), management has considered appropriate cybersecurity framework(s) specific to the organisation and the jurisdictions in which it operates.

---

[65] See: The National Institute of Standards and Technology, "Cybersecurity Framework," at: https://www.nist.gov/cyberframework (16 July 2019).
[66] NIST, Cybersecurity Framework 1.1, 16 April 2018, at; https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (16 July 2019).
[67] NIST, "Picking up the Framework's Pace Internationally," at: https://www.nist.gov/cyberframework/picking-frameworks-pace-internationally (16 July 2019.
[68] International Organization for Standardization, "ISO/IEC 27001 Information Security Management," at: https://www.iso.org/isoiec-27001-information-security.html (September 3, 2019).
[69] International Organization for Standardization, "ISO/IEC 27001 Information Security Management," at: https://www.iso.org/isoiec-27001-information-security.html (September 3, 2019).
[70] Center for Internet Security, "The 20 CIS Controls & Resources," at: https://www.cisecurity.org/controls/cis-controls-list/ (September 3, 2019).
[71] Center for Internet Security, "The 20 CIS Controls & Resources," at: www.cisecurity.org/controls/cis-controls-list/ (September 3, 2019).
[72] PCI Security Standards Council, "Maintaining Payment Security," at: https://www.pcisecuritystandards.org/merchants/process (September 3, 2019).

Establishing a Management Framework for Cyber Security

Consistent with the understanding that cyber security is broader than simply an "IT" issue is the realisation that cyber risk management should not be left to the province of the IT experts. As we discuss elsewhere, most attacks are not really the result of technical failure but are commonly human error of some sort. From a board perspective, one of the areas of concern regarding cyber-attacks is the reputational risk which strongly suggests the PR department ought to be involved in cyber risk management. Similar arguments can be made for including legal, finance, compliance, R&D and others in the overall cyber risk process.

There is no one model of structural framework that will apply perfectly to all organisations. However, **a multi-stakeholder approach is almost certainly something boards should consider having management implement**. Recognizing that organisations will want to adapt to their unique needs we offer two alternative models which can be used as a starting point.

ISA- ANSI Integrated Approach to Managing Cyber Risk

One of the first multi-stakeholder 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*. This rudimentary model stresses not only that multi stakeholders ought to be involved but advocates for an identified leader – not from IT – who has cross organisational authority. It also advocates for a separate cyber security budget as opposed to the traditional model of folding cyber security into the IT budget.

An Integrated Approach to Cyber Risk Management

1. 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. This would include assessing the organisation's current threat landscape and risk picture. Then, clearly establishing its risk appetite. Identifying potential risk to the organisation, as well as its risk threshold, will help the cyber-risk team assess which systematic framework aligns most appropriately with its mission and goals. The framework should bring clarity as to prevention, detection and response processes, in addition to accountability.

Accountability

2. **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. Accountability at all levels should be clear and transparent.
3. Appoint a **cross-organisation cyber-risk management team**. All substantial stakeholder departments must be represented, including business unit leaders, legal, internal audit and compliance, finance, HR, IT, and risk management.
4. Define roles in relation also to the Three Lines of Defence concepts [73]

[73] See FERMA – ECIIA Cyber Risk Governance Report published on 11 September 2017 https://www.ferma.eu/publication/ferma-eciia-cyber-risk-governance-report

Culture & Awareness

5. Foresee adequate training of employees to promote safe practices and awareness of all types of threats.
6. Ensure an adequate “tone at the top” which promotes awareness and proactivity.
7. Be aware that **cybersecurity laws and regulations** differ significantly across jurisdictions (among U.S. states, between the United States 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 organisation, especially as some countries aggressively expand the scope of government involvement in the cybersecurity arena.

Communication

8. Take an **integrated approach to developing reports** to employees, management and the Board. Executives should be expected to track and report metrics that quantify the business impact of cyber threats and associated risk-management efforts. These reports should strike the right balance between too much detail and what is strategically important to report to the Supervisory Board.
   Evaluation and monitoring of cyber-risk management effectiveness and the company’s cyber-resiliency should be conducted as part of the internal audit plan and other management reviews and relative reports should be circulated to all relevant parties, which will ensure continuous improvement.
   Develop and adopt an organisation-wide cyber-risk management plan and internal communications strategy across all departments and business units. While cybersecurity obviously has a substantial 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.
9. External communication must also be addressed, especially to address the phase of response and recovery from an incident.

Operational design of processes

Operational design must address both the prevention measures of the identified risks and the ability to identify, respond and recover from an incident.

The areas to be considered are many:

- Asset management
- Host security
- Identity and Access management
- Network security
- Software security
- Policies and Procedures
- Threat intelligence

A second conceptual model has emerged over the past few years largely originating in the financial services space but increasingly being adopted by leading organisations in various sectors. This, "Three Lines of Defence" model stresses multiple independent operations within the organisation having varied and increasing roles in assessing and checking cyber risk management. The model may be summarized as:

- First Line of Defence – operates the business, owns the risk designs and implements operations
- Second Line of Defence – defines policy statements & defines the Risk Management framework. Provides a credible challenge to the first line. Evaluates risk exposure for board to determine risk appetite
- Third Line of Defence – commonly internal audit is responsible for independent evaluation of the first and second lines

Roles for each level of defense can be further detailed as:

First Line of Defence

- Provide a thorough exam of line one's work—is the business doing enough? Each business line defines the cyber risk they face & weaves cyber risk and self-assessment into fraud, crisis management and resiliency process.
- Business lines need to actively monitor existing and future exposures, vulnerability threats and assess what impact cyber risk has on new tech deployment, client relationships, and business strategies.

Second Line of Defence

- Should be independent functions with monitoring and/or control responsibilities. Manages enterprise cyber risk appetite and RM framework within overall enterprise risk –challenges the first line. Determines how to appropriately measure cyber risk and integrates into a risk tolerance statement for the firm.
- Focus of first and second tiers needs to be on effectively managing risk – not regulatory compliance – although they can integrate compliance.

Third Line of Defence

- Internal audit provides independent objective assessment and assurance of firm's framework and process across lines one and two with focus on proper risk management and operational effectiveness and efficiency. Internal Audit relies on international frameworks however will take into account the firms' need to develop their own to adapt to enhanced threats.
- Internal audit performs independent tests and assessments of both internal processes and third-party risks. It must be ensured of adequate professional competencies with a continuous professional education which allows it to stay abreast of constantly evolving technology and threat intelligence.

Source: Internet Security Alliance[74]

[74] Adapted from Internet Security Alliance and American National Standards Institute, *The Financial Management of Cyber Risk: An Implementation Framework for CFOs* (Washington, DC: ANSI, 2010). See also Internet Security Alliance, *Sophisticated Management of Cyber Risk* (Arlington, VA: ISA, 2013).

Principle 5

Board discussion about cyber risk should include strategies on their management (mitigation, transfer through insurance or partnerships, etc.).

Key recommendations:

- The board should consider the return on cyber investments and shift to a risk-based approach;
- Cybersecurity must be conceptualised as a measure of future loss.

In detail:

Perfect cybersecurity is an unrealistic goal. Cybersecurity - as with security in general - is a continuum, not an end state. Moreover, compliance is not the equivalent of security and security is not the equivalent of compliance.

Management teams need to determine where, on a spectrum of risk, they believe the firm's operations and controls have been optimised, and how this relates to the overall business strategy. As with other areas of risk, an organisation's cyber-risk tolerance must be consistent with its strategy and, in turn, its resource allocation choices ("Defining Risk Appetite" is discussed later in this principle).

Traditional risk assessment models have had difficulty fulfilling these requirements. Historically cyber risk assessment tended to be based on long check lists of control requirements – often 500 or more. However, as Doug Hubbard pointed out in his classic book *How to Measure Anything in Cyber Security*, "*There is not a single study indicating that the use of such methods actually reduces risk*".

Several authors have outlined difficulties with these check-the-box methods asking if all 500 items needed to be checked in order to improve security? Or was security improved (and by how much) if you only checked 250 items? 251? Or possibly you just needed to start at number 250 and check through 500.

Most problematic for management and corporate boards, these traditional methods did not put cyber risk assessment in quantitative economic terms. Fortunately, there has been in the past few years a useful evolution in cyber risk assessment that moves cyber risk assessment a bit closer to the empirical methods boards are more comfortable with in assessing other risks such as financial risk. These more contemporary methodologies, such as X-Analytics or Factor Analysis of Information Risk tend to view cyber risk not as categories (e.g. supply chain or insiders) but as a quantity.

By conceptualizing cyber risk as a measure of future financial loss from a given scenario over time, management can provide boards with a much clearer assessment of how much money they need to spend to lower their risk to an acceptable level consistent with their risk appetite and business plan.

At a conceptual level, the board should consider questions such as the following:

- **What data, systems and business operations are we willing to lose or have compromised?** Discussions of risk tolerance will help to identify the level of cyber risk the organisation is willing to accept as a practical business consideration. In this context, distinguishing between mission-critical or highly sensitive data and critical business operations and other data or systems that are as important, but less essential or sensitive, is a key first step. However, data compromise is not the only component of cyber risk. Legal implications, including regulatory sanctions for data breaches, could exist that far exceed the actual value of the data, and reputational risk from bad publicity may correspond more to external factors than the actual value of the systems compromised.

- The importance of the company's assets was discussed at a strategic level in Principle 1. Once macro-analysis is made, then a further drill down of where the data is located and who are the owners is necessary.

However, data compromise is not the only component of cyber risk. Legal implications, including regulatory sanctions for data breaches could exist that far exceed the actual value of the data, and reputational risk from bad publicity may correspond more to external factors than the actual value of the systems compromised.

- **How should our cyber-risk mitigation investments be allocated among basic and advanced defences?** Most organisations typically apply security measures equally to all data and functions. However, protecting low-impact systems data from sophisticated threats could require greater investment than the benefits warrant. For those lower-priority assets, organisations should consider accepting a greater level of security risk than higher-priority assets, as the costs of defence will likely exceed the benefits. Boards should encourage management to frame the company's cybersecurity investments in terms of Return On Investment (ROI), and probability of occurrence associated with exploitation. They should also reassess probability of occurrence and reassess ROI regularly, as the costs of protection, the company's asset priorities, and the magnitude of the threat will change over time.

- **What options are available to assist us in mitigating certain cyber risks?** Organisations of all industries and sizes have access to end-to-end solutions that can assist in reducing some portion of cyber risk. They include a battery of preventative measures such as reviews of cybersecurity frameworks and governance practices, employee training, IT security, expert response services and managed security services. Beyond coverage for financial loss, these tools can help to mitigate an organisation's risk of suffering property damage and personal injury resulting from a cyber-breach. Some solutions also include access to proactive tools, employee training, IT security, and expert response services, to add another layer of protection and expertise. The inclusion of these value-added services proves even further the importance of moving cybersecurity outside of the IT department into enterprise-wide risk and strategy discussions at both the management and board levels. However, management needs to keep the Board informed of the rapidly changing cyber risk landscape and be agile enough to adjust to quickly changing technologies and cyber-attack scenarios such as data theft, data corruption, and even the use of security mechanisms (e.g. encryption) as attack methods (e.g., ransomware).

- **What options are available to assist us in transferring certain cyber risks?** Cyber insurance is a control and exists to provide financial reimbursement for unexpected losses related to cybersecurity incidents. This may include accidental disclosure of data, such as losing an unencrypted laptop, or malicious external attacks, such as phishing schemes, malware infections, or denial-of-service attacks. Determining when this control makes economic sense requires the ability to quantify the return that control provides versus other competing controls. Cyber insurance would not be the first control chosen but it is practical when the risk reduction it achieves versus the cost is a better value than the risk reduction a competing set of controls would provide. When choosing a cyber-insurance partner, it is important for an organisation to choose a carrier with the breadth of global capabilities, expertise, market experience, and capacity for innovation that best fits the organisation's needs. Insurers frequently conduct in-depth reviews of company cybersecurity frameworks during the underwriting process and policy pricing can be a strong signal that helps companies understand their cybersecurity strengths and weaknesses providing a potential path to improve their cybersecurity maturation. Many insurers, in partnership with technology companies, law firms, public relations companies and others, also offer access to the preventative measures discussed above.

- **How should we assess the impact of cybersecurity incidents?** Conducting a proper impact assessment can be challenging given the number of factors involved. To take just one example, publicity about data breaches can substantially complicate the risk evaluation process. Stakeholders—including employees, customers, suppliers, investors, the press, the public, and government agencies—may see little difference between a comparatively small breach and a large and dangerous one. As a result, reputational damage and associated impact (including reactions from the media, investors, and other key stakeholders) may not correspond directly to the size or severity of the event. The board should seek assurances that management has carefully thought through these implications in devising organisational priorities for cyber-risk management.

Defining Risk Appetite

Risk appetite is the amount of risk an organisation is willing to accept in pursuit of strategic objectives. Thus, it should define the level of risk 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 capitalising on opportunities.

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 they willing to bear, and to what level?
- Capacity – What resources are required to manage those risks?
- Financial – Are we able to adequately quantify our risks and harmonise our spending on risk controls?
- Measurement – Can we measure and produce reports to ensure proper monitoring, trending and communication in reporting is occurring?

Source: PwC, *Board oversight of risk: Defining risk appetite in plain English* (New York, NY: PwC, 2014), p. 3.

Designing an effective cyber risk appetite for an institution starts at the Board of Directors level. Once the Board-level cyber risk appetite is established, the statements and metrics can be cascaded to lower levels of the institution.

A cyber risk appetite statement can be useful in clarifying the importance of certain risks over others. It grants insight for the whole organisation into what the teams shouldering this risk need to prioritize for the enterprise to function. A Cyber risk appetite statement gives insight into the enterprise organisation's risk approach as a whole. Specifically, the statement highlights critical risks that are necessary to accept to participate in the industry and the risks specific to given business sectors.

Two examples follow:

Example 1
The organisation has a tolerance for risk, allowing it to achieve its business objectives in a manner that is compliant with the laws and regulations in the jurisdiction in which it operates.

The organisation has a low-risk appetite for the loss of its business and customer data. The organisation has a medium risk appetite for physical information security assets and will track assets greater than US$2,000. Information assets will be protected per the organisation's data classification framework. The organization has a high-risk appetite for access controls. All access to the organizations mission-critical systems will be controlled via biometric authentication.

Example 2
<The Bank> faces a broad range of risks in its responsibilities as a central bank. Acceptance of some risk is often necessary to foster innovation and efficiencies within business practices. The risks arising from our policy responsibilities can be significant. These are managed through processes emphasizing the importance of integrity, maintaining quality staff and public accountability.

<The Bank> is also exposed to some significant financial risks, mainly due to it holding foreign exchange reserves. In terms of operational risks, we have a low appetite for risk and make resources available to control operational risks to acceptable levels. <The Bank> recognises that it is not possible or necessarily desirable to eliminate some of the risks inherent in its activities.

Source: Security Bloggers Network » Contextualize Quantified Cyber Risk With A Risk Appetite Statement

Basic Method for Economically Assessing Cyber Risk

Basic steps toward competent cyber risk management may include:

- Using best available data management to make probabilistic assessments of possible attack scenarios;
- Management should focus on scenarios that are probable and would yield an expected loss significant enough to matter to the business;
- Calculate the best case, worst case and most likely case of attack and identify what degree of loss is acceptable (risk appetite);
- Determine the investment required to mitigate, or transfer, risk to an acceptable level
- Option: run multiple scenarios using methods such as Monte Carlo simulations to more accurately define risk and mitigation costs to various scenarios.

The European Union Agency for Network and Information Security (ENISA) recommends "a model of awareness, analysis and intervention for organisations to systematically plan and implement changes to address human aspects of cybersecurity"[75]. The Board's role is to bring its judgement to bear and provide effective guidance to management, in order to ensure the company's cybersecurity strategy is appropriately designed and sufficiently resilient given its strategic imperatives and the realities of the business ecosystem in which it operates.

[75] ENISA, "Cybersecurity Culture Guidelines: Behavioral Aspects of Cybersecurity," December 2018, at: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity (June 5, 2019).

Toolkit A

Possible points to include in Board Review & Self-Assessment regarding "Cyber Literacy" and Cybersecurity Culture[76]

Even prior to a Board meeting, directors may do well to self-assess if they have considered various aspects of cybersecurity beyond the technical and operational aspects. In particular, boards should be thinking of cybersecurity in business terms, and considering if they are preparing their organisation on a strategic level. Among the questions, directors may want to ask are the following:

1. Does the CEO encourage open access between and among the Board, external sources, and management about emerging cyber threats?
2. Are we considering the cybersecurity aspects of our major business decisions, such as M&A, partnerships, new product launches, etc., in a timely fashion?
3. Do we know the maturity scale of our cyber risk programme?
4. Are we spending appropriately on cybersecurity tools and training? Do we know if our spending is cost effective? Are we actually improving security or just completing compliance requirements?
5. Who is managing our cybersecurity? Do we have the right talent and clear lines of accountability/communication for cybersecurity?
6. Have we considered how we would manage our communications in the case of a cyber event, including communicating with the public, our shareholders, our regulators, our rating agencies? Do we have segmented strategies for each of these audiences?
7. Does our organisation participate in any of the public or private sector ecosystem-wide cybersecurity and information-sharing organisations?
8. Is the organisation adequately monitoring current and potential cybersecurity-related legislation and regulation?[77]
9. Does the company have adequate insurance, including Directors and Officers, that covers cyber events? What exactly is covered?[78] Are there benefits beyond risk transfer to carrying cyber insurance?[79]

This toolkit will help directors identify what questions to ask senior management and also provides a numerical scale to assess the board's culture[80]. See also PwC publication on "How can Boards better oversee Cyber risk" which includes an appendix with relevant questions for the Board to ask[81]

Directors wishing to incorporate a cybersecurity component into their board's self-assessment can use the questions in the table below as a starting point.

---

[76] National Association of Corporate Directors, 2018-2019 NACD Public Company Governance Survey, p. 17. The *NACD 2018-2019 Public Company Governance Survey* found that, "More than half of directors, 52 percent, are now confident that they personally have the understanding to provide effective cyber risk oversight, and 58 percent "believe their boards collectively know enough about cyber risk to provide effective oversight."

[77] Ibid.

[78] StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, "Board Oversight."

[79] Ibid.

[80] Report of the NACD Blue Ribbon Commission on Board Evaluations: Improving Director Effectiveness (Washington, DC; NACD, 2010), p.7. NACD has defined boardroom culture as "the shared values that underlie and drive board communications, interactions, and decision making. It is the essence of how things really get done."

[81] www.pwc.com/us/en/services/governance-insights-center/library/risk-oversight-series/overseeing-cyber-risk.html

Use the numerical scale to indicate where the Board's culture generally falls on the spectrum shown below. <---------->			Action Item
We classify cyber risk as an IT or technology risk	1 2 3 4 5 ☐ ☐ ☐ ☐ ☐	We classify risk as an enterprise wide risk	
Our cybersecurity discussions with management focus primarily on reviews of past events (e.g. historical breach data)	1 2 3 4 5 ☐ ☐ ☐ ☐ ☐	Cybersecurity is incorporated into forward-looking discussions with management (e.g. new product/service development, M&A/joint ventures, market entry)	
Our Board relies on management to assess critical assets, major threats, and overall risk assessment	1 2 3 4 5 ☐ ☐ ☐ ☐ ☐	Our Board has participated in a strategic risk assessment critical assets, major threats, and overall risk assessment, in order to promote an enterprise – wide risk management strategy	
The board receives information about cybersecurity exclusively from management	1 2 3 4 5 ☐ ☐ ☐ ☐ ☐	The board receives first-hand information about cybersecurity from non-management sources	
Information about emerging cyber threats or potential issues is filtered through the CEO	1 2 3 4 5 ☐ ☐ ☐ ☐ ☐	The CEO encourages open access and communications between and among the board, external sources and management about emerging cyber threats	
Our Board does not expect management to uniquely assess and manage cyber risks.	1 2 3 4 5 ☐ ☐ ☐ ☐ ☐	Our Board expects management to provide it with a clear analysis of what our cyber risks are, which to accept, what we can mitigate, and what we can transfer consistent with our business goals	
Our Board is not supported by a Committee with sufficient knowledge of cyber risk management	1 2 3 4 5 ☐ ☐ ☐ ☐ ☐	Our Board is sufficiently supported by a Committee with sufficient knowledge of cyber risk management	

Questions Directors Can Ask to Assess the Board's Cyber Literacy

1. What do we consider our most valuable assets? How does our IT system interact with those assets? What would it take to feel confident that those assets were protected?

2. Are we considering the cybersecurity aspects of our major business decisions, such as M&A, partnerships, new product launches, etc., in a timely fashion?

3. Who is in charge? Do we have the right talent and clear lines of accountability/responsibility for cybersecurity?

4. Does our organisation participate in any of the public or private sector ecosystem-wide cybersecurity and information-sharing organisations?

5. Is the organisation adequately monitoring current and potential cybersecurity-related legislation and regulation? Does the company have insurance that covers cyber events, and what exactly is covered? Is there Director and Officer exposure if we don't carry adequate insurance? What are the benefits beyond risk transfer of carrying cyber insurance?

Case Studies

Lax Security Culture Allowed North Korean Hackers to Penetrate a Multinational Corporation and Entertainment Industry Leader

In 2014, a multinational entertainment industry corporation reported a "brazen attack" on the company. Hackers penetrated the company's information systems, stole data, and leaked sensitive information online, including copies of unreleased films and embarrassing emails. The attackers also used malware to erase assets within the company's information systems. The U.S. government blamed the North Korean government for the attack.

At the time, former employees stated that the company's lax security practices contributed to the attack. One former employee called the company's information security team "a complete joke." The employee added: "We'd report security violations to them and our repeated reports were ignored." Another former employee explained. "The real problem lies in the fact that there was no real investment in or real understanding of what information security is."

The U.K. National Health Service and the WannaCry Attack

On 12 May 2017, hundreds of thousands of computers around the world were victimized by the WannaCry Ransomware Attack. In the United Kingdom, the National Health Service (NHS) suffered significant disruptions—including 19,000 health appointments canceled. The attack cost the NHS an estimated £92 million; 139 of the appointments involved potential cancer referrals.
These disruptions and losses would have been avoidable, if the NHS had a stronger cybersecurity culture as an organization. Investigators later determined that the NHS was using old operating systems, including Windows XP, with known vulnerabilities.

The National Audit Office (NAO) evaluated the incident and reported that the Department of Health was warned about the risk of a cyber attack on the NHS a year earlier. "The WannaCry cyber attack had potentially serious implications for the NHS and its ability to provide care to patients," NAO head Amyyas Morse commented. "It was a relatively unsophisticated attack and could have been prevented by the NHS following basic IT security best practices."

The National Audit Office concluded: the Department and NHS national bodies need to, "ensure that organisations, boards, and their staffs are taking the cyber threat seriously, understand the direct risks to front-line services, and are working proactively to maximize their resilience and minimize impacts on patient care."

Sources: Matthew Field, "WannaCry cyber attack cost the NHS £92m as 19,000 appointments canceled," *The Telegraph*, 11 October 2018; National Audit Office, "Investigation: WannaCry cyber attack and the NHS," October 17, 2017.

Case Study: International Banking System Exhibits Strong Leadership in Response to Breach

In 2016, an Asian bank experienced a major cyber attack, resulting in millions of dollars being transferred through the international SWIFT banking network. Although the SWIFT network was not compromised through this breach, SWIFT leadership proactively took action to preserve its reputation and delivered a message to all its clients that weaknesses in their systems would no longer be tolerated. SWIFT also created the Customer Security Programme following this incident. This programme led to the establishment of a customer security control framework providing a variety of mandatory and suggested criteria for SWIFT clients. This framework established a security baseline for all of the 11,000 banking institutions that use SWIFT. As a result of this programme, by 2018, 94% of SWIFT clients had attested to their compliance with the framework.

Source: www.centralbanking.com/fintech/4397726/cyber-security-provider-swift

Toolkit B

Questions for the Board to Ask Management About Cybersecurity

Of all the cybersecurity risk issues for an organisation to worry about, perhaps the greatest challenge is mitigating the insider threat. The cyber insider threat encompasses employers, contractors, vendors, and others who have legitimate access to the network, systems, and/or data of the organisation to some degree. Verizon's Data Breach Report identified five types of cyber insider threats[82]:

- **Careless Workers:** Employees or partners who non-maliciously misappropriate resources, break acceptable use policies, mishandle data, install unauthorized applications or use unapproved workarounds.
- **Inside Agents:** Insiders recruited, solicited, or bribed by external parties to exfiltrate data.
- **Disgruntled Employees:** Insiders recruited, solicited, or bribed by external parties to exfiltrate data.
- **Malicious Insiders:** Actors with access to corporate assets who use existing privileges to access information for personal gain.
- **Feckless Third Parties:** Business partners who compromise security through negligence, misuse, or malicious access to or use of an asset.

Case Study:
Insurance Company Insider Steals Customer Data

In 2017, an employee of a private global health insurance company accessed the firm's customer database to steal the personal data of more than 500,000 people. The information included customers' names, birthdays, email addresses and nationalities. The company insider later tried to sell the information on the dark web.

The U.K. Information Commissioner's Office fined the company £175,000 for failing to implement adequate security measures to protect customers' information. "[The company] failed to recognize that people's personal data was at risk and failed to take reasonable steps to secure it," said ICO Director of Investigations Steve Eckersley.

[82] Verizon Insider Threat Report, "Out of sight should never be out of mind," undated but released in 2019, p. 5

This toolkit will help boards of directors ask senior management the right questions to ensure that these wide-ranging cyber insider threats are being properly mitigated.

Questions Boards Should Ask Senior Management on Insider Threats

Strategy and Comprehensive Risk Assessment

1. What are the frameworks we align to, and has the organisation completed a gap analysis?
2. Do we have a systematic framework or ISO in place to address cybersecurity and to assure adequate cybersecurity risk management?
3. What are our critical business services and processes? How do they map to legal entities, regulators' perspectives, IT departments, and suppliers?
4. What is important to protect, and how many times have we seen these assets compromised?
5. Do we have appropriately differentiated strategies for general cybersecurity and for protecting our mission-critical assets?
6. Have we prioritised the company's cybersecurity risks, and identified the strategy to manage these risks?
    a. Do we have a list of most critical IT systems and an inventory of all IT systems?
    b. Have we identified our more likely adversaries and cyber threats, both internally and externally?
    c. Have we considered all aspects of connectivity with the external environment?
7. In management's opinion, what are the most serious vulnerabilities related to cybersecurity (including within our IT and technology systems, personnel, or processes)?
8. Have we considered obtaining an independent, third-party assessment of our cybersecurity risk management programme?

Risk Strategy and Business Evolution

1. What kind of business strategy decisions have an impact on cyber risk?
2. What is our insurance coverage for cyber? Is it adequate and what kind do we have? Why do we have that sort of insurance?
3. What is our strategy to address cloud, BYOD, and supply-chain threats?
4. How are we addressing the security vulnerabilities presented by an increasingly mobile workforce?
5. Are we growing organically or buying companies? Are they mature companies or start-ups? Where are we geographically?

Organisation

1. Do we have an enterprise-wide, independently budgeted **cyber-risk management team**? Is the budget adequate? How is it integrated with the overall enterprise risk management process?
2. How is the cyber-risk management team composed? Have all appropriate functions been considered? For example
    i. Steering committee composed of a range of management members with
    ii. Information security function
    iii. Physical security function
    iv. Information technology
    v. Legal
    vi. Compliance
    vii. Operations
    viii. Shared services
    ix. Business units

To initiate a dialogue about cyber risk governance in your organization, consider the following:

- Leverage opportunities to gain bottom up support/cooperation from 1st and 2nd lines of defence
- A strong champion is critical- it could be the CISO, CSO, CRO or another influential leader
- It also helps to have a top down support /mandate from the Board/top management
- Start small- invite other leaders to existing steering committee/governance/key project meetings and look for ways to help each other meet objectives

Source: Ferma- At the Junction of Corporate Governane & Cybersecurity 2019

3. How effective is the cyber risk management team, including the information-security team, in collaborating between departments and corporate functions on cybersecurity-related matters? For example, as regards:
    - Business development regarding due diligence on acquisition targets and partnership agreements;
    - Internal audit regarding the evaluation and testing of control systems and policies;
    - Human resources on employee training and access protocols;
    - Purchasing and supply chain regarding cybersecurity protocols with vendors, customers, and suppliers; and/or
    - Legal regarding compliance with regulatory and reporting standards related to cybersecurity as well as data privacy?
4. Does the cyber risk management team have the necessary skills? Do they receive continuing professional education?
5. What role does each member of the cyber risk management play in the organisation's enterprise risk management (ERM) structure and in the implementation of ERM processes?
6. How is the risk ownership decided?
7. What support does the cyber risk management team receive from the CEO, CIO, and senior management team?
8. How is the organisation's cybersecurity budget determined? Comparing this figure with industry spending trends is probably the best way to gain context over the adequacy of funding. What is its size (e.g., percentage of total IT/Technology spending), and how does this figure compare with leading practice in our industry and generally? What role does the security team play in cybersecurity budget allocation and investment decisions? Which security tools or other investments were below the "cut" line in the budget?

With particular regard to the information security function:

9. What is the information security function's scope of authority in terms of resources, decisions, rights, budget, staffing and access to information? How does this compare to leading practice in our industry and generally?[83]
10. What is the information security function's administrative reporting relationship (e.g., CIO, CISO, CTO, COO, Head of Corporate Security, other)? Does it differ from the functional reporting relationship?
11. What protocols are in place to ensure that the information security function has an independent channel to escalate issues and to provide prompt and full disclosure of cybersecurity deficiencies?[84]
12. What role, if any, does the cyber risk management team and the information security function play beyond setting and enforcing cybersecurity policies and related control systems?
    - For example, does the information security team provide input on the development process for new products, services, and systems or on the design of partnership and alliance agreements, etc., such that cybersecurity is "built in" rather than "added on" after the fact?
13. What are the arrangements in place to be able to scale up the information security function, in case of a crisis? Do we have the right relationships with suitable third parties?
14. How is the information security team's performance evaluated? Who performs these evaluations, and what metrics are used?
15. How does the information security team develop and maintain knowledge of the organisation's strategic objectives, business model, and operating activities?
    - For example, in companies that are actively pursuing a "big-data" strategy to improve customer and product analytics, to what extent does the security team understand the strategy and contribute to its secure execution?
16. Where do management and our cyber risk management team teams disagree on cybersecurity?

Prevention measures and Operations

1. How do our operational controls, including access restrictions, encryption, data backups, monitoring of network traffic, etc., help protect against insider threats?
2. How have we adapted our personnel policies, such as background checks, new employee orientation, training related to department/role changes, employee exits, and the like, to incorporate cybersecurity?
3. Do we have an insider-incident activity plan that spells out how and when to contact counsel, law enforcement and/or other authorities, and explore legal remedies?
4. Do we have forensic investigation capabilities?
5. What are the leading practices for combating insider threats, and how do ours differ?

[83] See, for example, Marc van Zadelhoff, Kristin Lovejoy, and David Jarvis, *Fortifying for the Future: Insights from the 2014 IBM Chief Information Security Officer Assessment* (Armonk, NY: IBM Center for Applied Insights, 2014).

[84] A 2014 study of global information security issues found that organizations with CISOs reporting outside the CIO's office have less downtime and lower financial losses related to cybersecurity incidents as compared with those who report directly to the CIO. See Bob Bragdon, "Maybe it really does matter who the CISO reports to," *The Business Side of Security* (blog), June 20, 2014.

6. How do key functions (IT, HR, Legal, and Compliance) work together and with business units to establish a culture of cyber-risk awareness and personal responsibility for cybersecurity? Considerations include the following:
    a. Written policies which cover data, systems, and mobile devices should be required and should cover all employees.
    b. Establishment of a safe environment for reporting cyber incidents (including self-reporting of accidental issues).
    c. Regular training on how to implement company cybersecurity policies and recognise threats.
7. What are we trying to prevent by protecting against insider threats?

Prevention measures - Supply-Chain/Third-Party Risks

1. What do we currently do and what will need to be done to fully include cybersecurity in our current supply-chain risk management?
2. How much do we know about our supply chain regarding cyber-risk exposure and controls? What due diligence processes do we use to evaluate the adequacy of our suppliers' cybersecurity practices (both during the on-boarding process and during the lifetime of each contract)? Which departments/business units are involved? Are there appropriate contingency arrangements in place in the event of a major problem with critical third-party suppliers?
3. Does the business carry out appropriate strategic monitoring of third-party suppliers?
4. What providers do we use for the cloud? Which critical business functions have we outsourced to third parties, such as cloud security?
5. How do we balance the financial opportunities (lower costs, higher efficiency, etc.) created by greater supply-chain flexibility with potentially higher cyber risks?
6. How are cybersecurity requirements built into vendor agreements? How are they monitored, and are we doing our due diligence to enforce contracts? Contracts can be written to include minimum cybersecurity requirements, including for example:
    a. Written cybersecurity policies.
    b. Personnel policies, such as background checks, training, etc.
    c. Access controls.
    d. Encryption, backup, and recovery policies.
    e. Detailed requirements regarding data held by the third party.
        i. Retention and deletion requirements for data held.
        ii. Clear inventories of types of data held.
        iii. Clarity on what is stored, moved, processed, etc.
    f. Secondary access to data.
    g. Countries where data will be stored.
    h. Notification of data breaches or other cyber incidents.
    i. Communication plans for incident reporting and response.
    j. Incident-response plans.
    k. Audits of cybersecurity practices and/or regular certifications of compliance.
7. Do we allow our suppliers to subcontract the delivery of any part of the contract? If so, what level of control/scrutiny do we exercise over the subcontracting arrangements? How do we monitor changes to subcontracting arrangements through the lifetime of the contract?

8. Do we have technology in place to profile suppliers and partners from the cybersecurity point of view to identify potential vulnerabilities and actively manage third party risk?
9. Are we indemnified against security incidents in our supply chain? What is the financial strength of the indemnification?
10. How difficult/costly will it be to establish and maintain a viable cyber-vulnerability and penetration-testing system for our supply chain?
11. How difficult/costly will it be to enhance monitoring of access points in the supplier networks?
12. Do our vendor agreements bring incremental legal risks or generate additional compliance requirements (e.g., GDPR, etc.)?

Response capability-Planning for a Potential Incident, Crisis Management and Response

1. Are we members of information sharing communities? If so, what are the lessons learned from our peers who have experienced breaches
2. How capable is management in "threat intelligence" by always updating its full knowledge of threats and adversaries, given the wide range of sources:
    - Phishing
    - Malware
    - External cyberattacks to disrupt, to expropriate funds, to steal IP
    - Internal attacks to disrupt, to expropriate funds, to steal IP
    - Fraud
    - Spam
    - Natural disasters
    - Espionage
3. When was the last time we conducted a penetration test or an independent external assessment of our cyber defences? What were the key findings, and how are we addressing them? What is our maturity level?
4. Were we told of cyber-attacks that have already occurred and how severe they were?
5. What is our ability to protect, detect and respond to incidents? How does it compare with others in our sector?
6. In the context of our business, has a material cybersecurity breach been defined to ensure proper escalation?
7. At what point is the board informed of an incident? What are the criteria for reporting?
8. What is known about the intent and capability of the attacker? What do we know about how the attacker might use the data?
9. Does our organisation have an appropriate methodology in place for assessing the risk in case of an incident and determining whether any notifications are legally required?
10. Are we clear as to who must be notified and when? What are the timetables and strategy considerations for reporting incidents to customers? Regulators/relevant government entities? Law Enforcement? Vendors/partners? Internally? Peers? Investors? What timetables are mandated by laws and regulations and what is at the company's discretion?
11. How will management respond to a cyberattack? Does the company have a validated incident-response plan?[85] Are we adequately exercising our cyber-preparedness and response plan?

[85] Ibid.

12. Do we have a crisis management plan in place? For significant breaches, how good is our communication plan (both internally and externally) as information is obtained regarding the nature and type of breach, the data impacted, and the ramifications to the company and the response plan?[86]
13. What are we doing to avoid making the problem worse for our organisation? How do we ensure we have appropriate legal advice in the incident and crisis management teams? Are the legal teams integrated in the incident and crisis plans?
14. What external communication strategies have been developed to manage reputational risk during the incident?

Recovery capability- After a Cybersecurity Incident

1. How did we learn about the incident? Were we notified by a third party, or was the incident discovered internally?
2. What do we believe was the motive for the incident? What was the impact, and how do we measure it? Have any of our operations been compromised?
3. Is our cyber-incident/crisis response plan in action, and is it working as planned?
4. What is the response team doing to ensure that the incident is under control and that the attacker no longer has access to our internal network?
5. What were the weaknesses in our system that allowed the incident to occur and why had they not been identified or remediated?
6. Has the security team checked for associated vulnerabilities across all company systems/networks, not just the affected systems or services? Have they checked what happened against the controls framework and made the necessary changes to both security controls and business controls?
7. What steps can we take to make sure this type of event does not happen again? How do we ensure that lessons are learned and remediation actions tracked?
8. What can we do to mitigate any losses caused by the incident?
9. Does the incident alter the risk tolerance of the business? Has this been discussed and have any changes been captured?
10. What external communication strategies have been developed to manage reputational risk after the incident?

Monitoring

1. What cybersecurity performance measures and milestones have been established for the organisation as a whole?
2. If we answer to regulatory authorities, can we be subject to a regulatory audit?
3. Does our external auditor indicate we have cybersecurity-related deficiencies in the company's internal controls over financial reporting? If so, what are they, and what are we doing to remedy these deficiencies

Adapted from NACD, et al., *Cybersecurity: Boardroom Implications* (Washington, DC: NACD, 2014) (an NACD white paper).

[86] StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, "Board Oversight."

Toolkit C

Board-Level Cybersecurity Metrics

Which cybersecurity metrics should be included in a board-level briefing? This question is deceptively simple. Similar to virtually every other division and function within the organisation, the cybersecurity function collects and analyses a tremendous volume of data and there is little consensus on which are the critical few pieces of data that should be shared with a board audience. Adding to the challenge is the fact that cybersecurity is a relatively new domain, with standards and benchmarks that are still developing or evolving.

Ultimately, directors will need to ask members of management to define the cybersecurity information, metrics, and other data that is most relevant to them given the organisation's operating environment – including industry or sector, regulatory requirements, geographic footprint, and so on. More often than not, boards see a high volume of operational metrics which provide very little strategic insight on the state of the organisation's cybersecurity programme. Metrics that are typically presented include statistics such as "number of blocked attacks," "number of unpatched vulnerabilities," and other stand-alone, compliance-oriented measures, that provide little strategic context about the organisation's performance and risk position.

As a starting point, directors can apply the same general principles used for other types of Board-level metrics to cybersecurity-related reporting.

The following recommendations provide a starting point for the types of cybersecurity metrics that board members should consider requesting from management.

1. Have we developed metrics based on cyber-risk appetite?
   Definition of risk appetite is discussed in Principle 4. In addition, Principle 2 points out the importance of reputational risk and legal risk which helps focus on some potentially important aspects affecting risk appetite.
   Metrics on risk appetite is a fundamental question for the Chief Information Security Officer (CISO) and the Chief Risk Officer (CRO)—and other appropriate officials with these responsibilities. This type of collaboration can produce qualitative and quantitative data points for presentation to the board that provide context around cyber-risk appetite.

   "Linking relevant quantitative metrics to well-designed qualitative statements is important to measure the level of compliance of the institution with the risk appetite statement. Often more than one indicator is needed to adequately reflect a given risk appetite statement. The metrics selection process should ensure that (a) the metrics have a clear link to the statement, (b) data required to measure the metrics are available or can be collected in a timely fashion, (c) the metrics are measuring risk (rather than pure performance) and the design of the metrics is forward looking where possible, and (d) the metrics are simple and easy to interpret for an audience less familiar with the topic. The limited availability of internal (and external) historic data for potential cyber risk metrics makes the calibration of thresholds challenging. Therefore, alternative calibration approaches need to be used to establish meaningful thresholds."[87]

[87] Oliver Wyman, When The Going Gets Tough, The Tough Get Going Overcoming The Cyber Risk Appetite Challenge, April 2018

2. What Value chain metrics do we have that indicate risk to the company? One organisation has implemented a cybersecurity risk "index" which incorporates several individual metrics covering enterprise, supply chain, and consumer-facing risk, depending on the materiality of the issue or asset.

   For example,

   - If a company is dealing with a large customer base, risk indexes may focus, among other things, on customer risk.
   - If the company is dealing also with a large supplier group or partnerships, risk indexes may move in the direction of supplier vulnerabilities.
   - If intangible assets are a major value to the company, a cyber risk index can focus on the asset protection.

   Thus, it is fundamental to ascertain what values are at risk from Cyber-attacks and the potential losses, whether financial or reputational: Cyber Value-at-Risk and Cyber scenario losses can be assessed on this basis and are part of the fundamentals of developing risk appetite.

   Value chain relationships typically pose increased risk for companies given the degree of system interconnectivity and data-sharing that is now part of everyday business operations.

   - How do we assess the cyber-risk position of our suppliers, vendors, JV partners, and customers?
   - How do we conduct ongoing monitoring of their risk posture?
   - How many external vendors connect to our network or receive sensitive data from us? This is a borderline operational metric, but it can help support discussions with management about residual risk from third parties.
   - There are service providers within the cybersecurity marketplace that provide passive and continuous monitoring of companies' cybersecurity postures. A growing number of firms use these services to assess their high-risk third-party relationships as well as their own state of cybersecurity.

3. Metrics on **budget utilisation** may be useful.

   - How much of our IT/technology budget is being spent on cybersecurity-related activities?
   - How does this compare to our competitors/peers, and/or to other outside benchmarks? These metrics will support conversations about how management determines "how much spending is enough," and whether increasing investments will drive down the organisation's residual risk. Additional follow-on questions include these:
     - What initiatives were not funded in this year's budget? Why?
     - What trade-offs were made?
     - Do we have the right resources, including staff and systems, and are they being deployed effectively?

4. Metrics on the effectiveness of the organisation's cybersecurity programme and how it compares to those of other companies is clearly of interest at board level.
    - Board-level metrics should include the reporting of the several aspects composing the maturity scale of the cybersecurity programme.
    - Board-level metrics should highlight changes, trends and patterns over time, show relative performance, and indicate impact.
    - External penetration-test companies and third-party experts may be able to provide an apples-to-apples comparison within industry sectors.

5. While operational metrics are the domain of the IT/Security team, it may be beneficial for directors to understand the breadth and depth of the company's cybersecurity monitoring activities for the purposes of situational awareness.
    - What operational metrics are routinely tracked and monitored by our security team?
    - How many data incidents (e.g., exposed sensitive data) has the organisation experienced in the last reporting period?
    - How timely has the identification and resolution of those incidents been?

    These metrics will assist conversations about trends, patterns, and root causes.

6. What metrics do we use to evaluate **cybersecurity awareness** across the organisation?
    - Data about policy compliance, the implementation and completion of training programmes, and the like will help to inform about insider risks at various seniority levels and in various regions and divisions.

7. Metrics on incident management and reputational risk.
    - Did an incident have a reputational impact causing loss of customers or sales?

8. How do we track **the individuals or groups that are exempt from major security policies**, activity monitoring, etc.? These measures will indicate areas where the company is exposed to additional risk, opening the way for discussions about risk/return trade-offs in this area.

Developing Cyber Economic Metrics

Cyber risk is now clearly a board-level issue. The challenge, however, is how to effectively and precisely communicate the financial impact of cyber incidents to the board. Before boards can make informed decisions on how to manage cyber risk, they must first have the ability to translate cybersecurity data into financial metrics. Board directors will need to work with management to outline the most relevant cybersecurity information given the organisation's operating environment, including industry or sector, regulatory requirements, geographic footprint, and so on. To get started, the following board-level cyber risk recommendations provide a starting point that boards should consider requesting from management:

- What are **our quarterly expected loss ratio** metrics related to our cyber-risk condition across our various business units and operating environments?
- What is the **financial impact** related to our cyber risk **worst-case** scenario?
- How are we measuring and prioritizing our **control-implementation activities and cybersecurity budgets** against our financial exposure to cyber risk? Have we adopted operational metrics such as number of incidents, time of response, measured full impact of incident, etc?
- Have we connected our control implementation strategy and cybersecurity programmes, including budgets, with our cyber-risk transfer strategy?
- Based on our financial performance targets, how can cyber risk impact our financial performance? What is our **annual cyber risk expected loss value**?
- What is our cyber risk remediation plan to achieve our target expected loss tolerance level? Is our plan producing a net positive financial return?
- How does our cybersecurity programme align cyber risk based expected loss ratio analysis and expected loss tolerance targets? How are we measuring, tracking, and demonstrating how our **cybersecurity investments** are **reducing our financial exposure** to cyber incidents and delivering cybersecurity **return on investment**?
- How are we measuring and aligning our cyber risk based expected loss ratio analysis and cybersecurity planning with our cyber insurance risk-transfer plan?
- How do we measure the effectiveness of our organisation's cybersecurity programme and how it compares to those of other companies?

Source: Secure Systems Innovation Corporation (SSIC) and X-Analytics

Toolkit D

Cybersecurity Considerations During M&A Phases

Companies involved in transactions are often prime targets for hackers and cybercriminals, because the value of confidential deal-related information is high, and the short timelines, high-pressure environment, and significant workloads associated with transactions can cause key players to act carelessly and potentially make mistakes. Cybersecurity vulnerabilities exploited during a transaction can pose risks to the deal's value and return on investment:

Short-term risks

- Paralysed operations as a result of ransomware or malware.
- Transaction period might be used by threat actors to gain entry and conduct reconnaissance, an event which often is not detected until well after the deal closes.
- Theft of inside information, including valuations, bids, etc.
- Warranty claims, a change of deal terms, or a reduction in the deal's value.
- Forensic investigations related to a data breach.

Long-term risks

- Exposure to risk from regulatory and other lawsuits.
- Regulatory investigation and penalties.
- Loss of customers, and associated impacts on sales and profit.
- Reputational damage.
- Loss of market share to competitors without a known data breach.

Directors should ask management to conduct a cyber-risk assessment for each phase of the transaction's lifecycle to confirm that systems and processes are secure, and to quantify the risks that may impact the company after the deal closes, including revenues, profits, market value, market share, and brand reputation.

Strategy and Target Identification Phase

The risk of attack starts even before an official offer or merger announcement is made. Law firms, financial advisors, consultants and other associated firms are attractive to hackers because they hold trade secrets and other sensitive information about corporate clients, including details about early-stage deal exploration that could be stolen to inform insider trading or to gain a competitive advantage in deal negotiations. A company therefore needs to have an understanding of the controls and security in place at all of the third parties assisting it during the M&A process and a thorough understanding of how sensitive data is to be shared between parties.

Attackers look for hints that a company is considering a merger, acquisition, or divestiture. They may be tipped off by industry gossip, a slowdown in a company's release cycle, staff reductions, or data leakage through social media channels. There are four primary ways that information is at risk:

- A hacker enters the network through gaps in its defences, starting with a company's Internet-facing computers.
- A hacker launches a social engineering attack against a company employee.

- Company insiders (employees, contractors, vendors) release sensitive data and information, either intentionally or as a result of negligence. The risk of insider threats heightens significantly in an M&A.
- Information is exposed through vulnerabilities in third-party vendors or service providers.

During this phase, management should gain an understanding of cyber risks associated with the target company and model the impact of those risks to compliance posture, financial forecasts, and potential valuations. Management can perform the following analysis even before direct engagement with the target company begins:

- Conducting "dark web"[88] (difficult-to-access websites favoured by hackers) searches about the target, their systems, data, and intellectual property. This helps identify whether the company is already on hackers' radar, if systems or credentials are already compromised, and if there is sensitive data for sale or being solicited. Management will need to consider the lawfulness of such searches with reference to the information being accessed.
- Profiling the target company from the cybersecurity point of view, while implementing relevant technology.
- Researching malware infections in the target company and gaps in their defences visible from the outside. This information is publicly available and can be used to compare one company to another, allowing management to save time and energy by not pursuing companies whose risk profile is unacceptably high.
- Modelling the financial impact of identified cyber risks. These risks may not only impact a company's return on invested capital, but also result in loss of competitive advantages, costly remediation, fines, and possibly years of litigation, depending on what was stolen. An initial estimate of the impact may be material enough to encourage strategy teams to alter a deal trajectory. The estimate can be refined as the transaction process continues and as risks are mitigated.

Due Diligence and Deal Execution Phases

During these phases, the company should perform confirmatory cybersecurity due diligence. Significant problems would call for negotiation of a reduction in purchase price to cover costs of necessary remediation. Depending on the risks identified, the Board may want to defer approving the transaction until remediation is complete or decide to back out of a transaction if the risks that are identified warrant such action. Identification of cybersecurity risks during the diligence phase can be accomplished by performing cybersecurity diligence that is tailored to discover these risks:

- Identify insufficient investments in cybersecurity infrastructure, as well as deficiencies in staff resources, policies, etc.
- Identify lax cultural attitudes toward cyber risk.
- Determine cybersecurity-related terms and conditions (or, the lack thereof) in customer and supplier contracts that have a potential financial impact or result in litigation for noncompliance.

[88] The Dark Web is a general term describing hidden Internet sites that users cannot access without using special software such as TOR ("The Onion Router"). While the content of these sites may be accessed, the publishers of these sites are concealed. Users access the Dark Web with the expectation of being able to share information and/or files with little risk of detection.

- Discover noncompliance with data protection laws or other applicable cyber-related regulations and requirements.
- Identify recent data breaches or other cybersecurity incidents, and response thereto.

Effective due diligence on cybersecurity issues demonstrates to investors, regulators, and other stakeholders that management is actively seeking to protect the value and strategic drivers of the transaction, and that they are aiming to lower the risk of a cyber-attack before integration. These risks and upsides can then be factored into the initial price paid and into performance improvement investments that will raise the transaction value, enabling a robust transaction proposal to be presented to shareholders for approval.

Integration Phase

Post-deal integration poses a range of challenges related to people, processes, systems, and culture. Cyber risks add another dimension of complexity and risk to this phase of the transaction. Hackers take advantage of the inconsistencies that exist between the platforms and technology operations of the company and the newly-merged or acquired entity at this phase.

Integration teams need to have the expertise to explore and delve into the smallest of details to identify and mitigate cyber risks such as the following:

- Security gaps identified during preceding phases.
- Prioritization of remediation activities based on potential impact of identified gaps.
- Prioritization of integration activities.
- Employee training on newly integrated systems.

Post-Transaction Value Creation Phase

After a transaction is completed, continued monitoring of cyber risks by management will create numerous opportunities for portfolio improvement and growth.

Management should continue to evaluate the cyber maturity of the merged or acquired entity by benchmarking it against industry standards and competition, just as they do with the core business. Low maturity could impact growth projections and brand reputation due to cyber incidents and possible fines. A breach or compliance issue could cause regulators to investigate, leading to a financial loss or stalling of post-transaction exit plans. Cyber issues can also lead to legal action by customers and suppliers causing value loss and lower returns.

A View from the Sell Side

Many of the same risks impacting the acquiring company that are described herein will of course equally apply to the seller side. In the post transaction valuation creation phase, the seller is particularly exposed to breach disclosures that may impact the deal price / timing and even the ongoing operations of the selling entity if the transaction falls through. Accordingly, a thorough understanding of existing risk vectors prior to deal execution will better inform the nature of warranties made by the selling corporation and reduce exposure.

Information flow to directors of selling companies may be more limited in its nature and frequency as time passes after deal announcement and directors should establish the thresholds and nature for any breach communications in the post announcement period.

Toolkit E

References to International Standards

As also discussed in Principle 4, there are a number of international standards and regulatory bodies that deal with security of information and the systems that handle and process it. This is by no means to be an exhaustive list and represent for the most part the primary references. Other references to authoritative guidance may be cited earlier in this document.

The NIST Cyber Security Framework was designed with the intent that individual businesses and other organisations use an assessment of the business risks they face to guide their use of the framework in a cost-effective way. The framework is divided into three parts: The Framework Core, Framework Implementation Tiers and Framework Profiles:

- The Framework Core is a set of activities, outcomes and references that detail approaches to aspects of cyber security. The core comprises five functions, which are subdivided into 22 categories (groups of cyber security outcomes) and 98 subcategories (security controls).
- Framework Implementation Tiers are used by an organisation to clarify for itself and its partners how it views cyber security risk and the degree of sophistication of its management approach.
- A Framework Profile is a list of outcomes that an organisation has chosen from the categories and subcategories, based on its business needs and individual risk assessments.

Core functions, categories, subcategories and informative references

The five Framework core functions are:

- Identify – Develop the organisational understanding to manage cyber security risk to systems, assets, data and capabilities.
- Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- Detect – Develop and implement the appropriate activities to identify the occurrence of a cyber security event.
- Respond – Develop and implement the appropriate activities to take action regarding a detected cyber security event.
- Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired because of a cyber security event.

Each function is divided into categories – groups of cyber security outcomes that relate to particular activities. Examples include: Asset Management, Access Control and Detection Processes.

Subcategories further divide a category into specific outcomes of technical and/or management activities (security controls). Examples include: External information systems are catalogued, Data-at-rest is protected, and Notifications from detection systems are investigated.

ISO-International Organisations for Standardisation

- **ISO 27000** series to address standards that enable organisations to implement processes and controls that support the principles of information security.

- **ISO/IEC 27001 (2013)** is the international standard for information security management. It is a rigorous and comprehensive specification for protecting and preserving the confidentiality, integrity and availability of an organisation's information assets. The Standard offers a set of 114 best-practice security controls that can be applied based on the risks you face, and implemented as part of a broad organisational structure to achieve externally assessed and certified compliance.

- **ISO 17799 (2005)** a Code of Practice for Information Security management, is intended to serve as a single reference point for identifying the range of controls needed for most situations where information systems are used in industry and commerce.

OECD Guidelines for the Security of Information Systems (2002)
The Organisation for Economic Co-operations and Development's (OECD's) *Guidelines for the Security of Information Systems* is designed to assist countries and enterprises to construct a framework for security of information systems.

COBIT® - Control Objectives for Information and related Technology, developed and promoted by the IT Governance Institute (ITGI)

- **COBIT® 4.0 (2005)** starts from the premise that IT needs to deliver the information that the enterprise needs to achieve its objectives. In addition to promoting process focus and process ownership, COBIT looks at fiduciary, quality and security needs of enterprises and provides seven information criteria that can be used to generically define what the business requires from IT: effectiveness, efficiency, availability, integrity, confidentiality, reliability and compliance.

  COBIT further divides IT into 34 processes belonging to four domains (Plan and Organise [PO], Acquire and Implement [AI], Deliver and Support [DS], and Monitor and Evaluate [ME]). The COBIT framework addresses information security issues of concern in more than 20 processes. However, the four processes that are most directly related to information security are:

  • PO6—Communicate management aims and directions.
  • PO9—Assess and manage IT risks.
  • DS4—Ensure continuous service.
  • DS5—Ensure systems security.

  For each process, a high-level control objective is defined: Identifying which information criteria are most important in that IT process; Listing which resources will usually be leveraged; Providing considerations on what is important for controlling that IT process.

  COBIT further provides more than 200 detailed control objectives for management and IT practitioners who are looking for best practices in control implementation, as well as management guidelines and maturity models building on these objectives.

COBIT includes a management and governance layer, providing management with:

- Performance measurement elements (outcome measures and performance drivers for all IT processes)
- A list of key activities that provides succinct, non-technical best practices for each IT process
- A maturity model to assist in benchmarking and decision making for control over IT

- **COBIT Security Baseline (2004)**
  Also published by ITGI, it addresses security in addition to the risks of the use of IT. Using the COBIT framework, the guidance focuses on the specific risks of IT security useful for all users—home, small to medium enterprises, and executives and board members of larger organisations.

National Association of Corporate Directors (NACD) (U.S.)
NACD Director's Handbook on Cyber-Risk Oversight
The NACD Director's Handbook on Cyber-Risk Oversight is built around five core principles that are applicable to board members of public companies, private companies, and nonprofit organisations of all sizes and in every industry sector. The Handbook was the first non-government resource to be featured on the U.S. Department of Homeland Security's US-CERT C3 Voluntary Programme website.

European Banking Association
Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP)
These Guidelines are addressed to competent authorities and are intended to promote common procedures and methodologies for the assessment of the Information and Communication Technology (ICT) risk under the supervisory review and evaluation process (SREP), referred to in Article 97 of Directive 2013/36/EU1, as regards the banking sector.
In particular, these Guidelines drawn up pursuant to Article 107(3) of Directive 2013/36/EU, supplement and further specify criteria for the assessment of ICT risk as part of operational risk put forward in the EBA Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP)2 (from here on 'EBA SREP Guidelines').

ISA- ANSI Integrated Approach to Managing Cyber Risk
One of the first multi-stakeholder 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*.

Standard of Good Practice for Information Security (2005)
The Information Security Forum's (ISF's) *Standard of Good Practice for Information Security* is based on research and practical experience of members. 'The standard addresses information security from a business perspective, providing a practical basis for assessing an organisation's information security arrangements. It focuses on the arrangements that should be made by leading organisations to keep the business risks associated with critical information systems under control'. Each area is broken down into a number of detailed sections, totaling 135 appropriate controls.

About the Contributors

The Internet Security Alliance

The Internet Security Alliance (ISA) is an international non-profit trade association, founded in 2000, that is focused exclusively on cybersecurity. The ISA Board consists of the primary cybersecurity personnel from international enterprises, representing virtually every sector of the economy. ISA's mission is to integrate economics with advanced technology and government policy to create sustainably secure cyber systems. In 2014, ISA produced the first Cyber-Risk Oversight Handbook, specifically addressing the unique role corporate boards play in managing cyber risk. In their annual Global Information Security Survey, PricewaterhouseCoopers (PwC) reported that the Handbook was being widely adopted by corporate boards and that its use resulted in better cybersecurity budgeting, better cyber risk management, closer alignment of cybersecurity with overall business goals, and helping to create a culture of security in organisation that use it. For more information about ISA, visit www.isalliance.org.

AIG

American International Group, Inc. (AIG) is a leading global insurance organisation. Founded in 1919, today AIG member companies provide a wide range of property casualty insurance, life insurance, retirement products, and other financial services to customers in more than 80 countries and jurisdictions. These diverse offerings include products and services that help businesses and individuals protect their assets, manage risks and provide for retirement security. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange.

Additional information about AIG can be found at www.aig.com | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance www.twitter.com/AIGinsurance | LinkedIn: www.linkedin.com/company/aig.

ecoDa

ecoDa operates as the European Voice of Board Members. ecoDa is an independent actor and a unique umbrella organisation representing the main national institutes of directors in Europe. Its member institutes cover in total about 50,000 individual directors across 22 countries, sitting on the board of companies of all sizes and sectors. All its member institutes are well recognized in their country and are well-recognised market players in regard to Corporate Governance. www.ecoDa.org


CGI
ALBANIA
CORPORATE GOVERNANCE INSTITUTE


armenian institute
of directors


ASOCIATIA
ADMINISTRATORILOR
INDEPENDENTI


BALTIC
INSTITUTE
OF CORPORATE GOVERNANCE


BOARD LEADERSHIP SOCIETY
Boardwork for Value Creation and Good Governance


Directors'
Institute
Finland


GUBERNA
INSTITUUT VOOR BESTUURDERS
INSTITUT DES ADMINISTRATEURS


ICA
Instituto de
Consejeros-Administradores
Asociación Española de Consejeros


IFA
Institut Français des Administrateurs


Institut Luxembourgeois
des Administrateurs


INSTITUTE OF
DIRECTORS – MALTA


IOD
CYPRUS


IOD
Inspiring business


NCD


nedcommunity
amministratori non esecutivi ed indipendenti


SLOVENIAN
DIRECTORS' ASSOCIATION
for effective Corporate
Governance


styreinstitutt


STYRELSEAKADEMIEN


Swiss Institute of Directors


VRD
VEREINIGUNG DER
AUFSICHTSRÄTE IN DEUTSCHLAND e.V.