the global voice of
the legal profession®

International Bar Association

Presidential Task Force and the Legal Policy & Research Unit

Global perspectives on protecting against cyber risks: best governance practices for senior executives and boards of directors

Purpose: The purpose of this report is to provide first-of-its-kind global perspectives and guidance on best governance practices for senior executives and boards of directors in protecting their organisations from global cyber risks, with a view to harmonising efforts globally for effective protection against cyber attacks. It includes specific recommendations to protect against cyber risks in small, large and global organisations. While the scope of this report is global, it draws, in particular, on reporting sourced from Task Force members spread across ten jurisdictions – Australia, Brazil, Denmark, Germany, India, Israel, Singapore, Uganda, the United Kingdom, and the United States – each of whom has compiled research and analysis on comparative practice across this diverse set of countries.

Contents

Disclaimer: This document is published by the International Bar Association as a result of the Presidential Task Force established in 2021 by the President of the International Bar Association. The findings, interpretations, and conclusions expressed herein are a result of a collaborative process facilitated and endorsed by the Presidential Task Force on Cybersecurity formed by the President of the International Bar Association, but whose results do not necessarily represent the views of the International Bar Association, nor the entirety of its members, partners, or other stakeholders.

The International Bar Association (IBA) is the foremost organisation for international legal practitioners, bar associations and law societies. Established in 1947, shortly after the creation of the United Nations, the IBA was born out of the conviction that an organisation made up of the world's bar associations could contribute to global stability and peace through the administration of justice. In the ensuing 75 years since its creation, the organisation has evolved, from an association comprised exclusively of bar associations and law societies, to one that incorporates individual international lawyers and entire law firms.

The present membership is composed of more than 80,000 individual international lawyers from most of the world's leading law firms and some 190 bar associations and law societies spanning more than 170 countries.

The IBA has considerable expertise in providing assistance to the global legal community, and through its global membership it influences the development of international law reform and shapes the future of the legal profession throughout the world.

The IBA Legal Policy & Research Unit (LPRU) undertakes research and develops initiatives that are relevant to the rule of law, the legal profession and the broader global community. The LPRU engages with legal professionals and institutions to ensure innovative, collaborative and effective outcomes.

I. Foreword

The world is more reliant on technology and digitalisation than ever before. Technology has had a positive impact on economies, societies, public and private entities, as well as human life. But our growing dependence on digital technologies and the convergence of the physical and digital comes with the risk of cyber attacks. Every piece of digital data and connected system represents a point of vulnerability that hackers and cybercriminals can target. Most organisations across the world recognise that it is not a case of 'if' but 'when' their organisation will be impacted by a cyber attack. Such risks are accelerated by geopolitical instability, lack of available talent, and increasing shareholder and regulatory expectations, which – all together – should make cybersecurity a top priority for boards and senior management.

Cyber attacks are among the fastest-growing form of crime worldwide and they are becoming more sophisticated, targeted, widespread and difficult to detect. Senior management, under the oversight of the board of directors, are responsible for managing cybersecurity and broader data security risks within the organisation and, as a result, need to focus their attention on establishing proper cybersecurity risk governance, both before and after a cyber event.

There is a great global need for best practices and standards for corporate and organisational cybersecurity risk governance applicable to boards and management. Cyber attacks are cross-border in nature, and the challenges related to protecting people, businesses and institutions against cyber attacks are similar for organisations across the world. The speed and scale of these evolving risks have resoundingly outpaced the ability of organisations to manage them effectively.

Regulators, too, have struggled to keep pace. The reality is that, in the few places they exist, cybersecurity regulations vary considerably in terms of requirements, level of detail, and the method of supervision and enforcement. Guidance documents are often fragmented, and sector- or country-specific, and there is no globalised approach or set of principles for governance of cybersecurity risks. As a result, there is a lack of structured overview of best practices through which boards and senior management can look at cybersecurity and compliance.

The purpose of this report is to provide first-of-its-kind global perspectives and guidance on best governance practices for senior executives and boards of directors in protecting their organisations from global cyber risks, including with a view to harmonising efforts globally for effective protection against cyber attacks. It includes specific recommendations to protect against cyber risks in small, large and global organisations.

While the scope of this report is global, it draws, in particular, on reporting sourced from Task Force members spread across ten jurisdictions – Australia, Brazil, Denmark, Germany, India, Israel, Singapore, Uganda, the United Kingdom, and the United States – each of whom has compiled research and analysis on comparative practice across this diverse set of countries.

The ultimate target audience of the report is boards of directors and senior management (directly), as well as society at large, including industry bodies, legislators and enforcement agencies (indirectly). But our secondary goal is to inform and empower lawyers to take up the cause of

ensuring strong cybersecurity risk governance by becoming catalysts for change at their firms and organisations, as well as with their clients.

What role do lawyers play in cybersecurity? For many organisations, lawyers play a crucial role in managing risks and advising on sensitive business decisions that carry important legal and reputational consequences. They can drive changes in their organisations when the challenges cut across multiple functions. Thus, the IBA and its members have an important role to play in bringing about the leadership changes needed to address modern cyber risks, and they do not need to be technical experts to do so. Although the IBA's members include some of the most experienced global practitioners within cybersecurity and data protection, others without this specialisation still bring much-needed leadership skills and strong judgement to these challenges. By joining efforts, IBA's members can collect, structure, and present a consolidated view of international best practices within cybersecurity risk governance based on key learnings and experiences from various jurisdictions across the world.

Søren Skibsted

Co-Chair, IBA Presidential Task Force on Cyber Security (Kromann Reumert, Denmark)

Luke Dembosky

Co-Chair, IBA Presidential Task Force on Cyber Security (Debevoise & Plimpton, US)

'There is a real need for leadership and development of international cyber best practices in the intersection of law, public policy and technology. This IBA report sets a global benchmark on best governance practices for corporates in effectively safeguarding their organisations against cyber risks.'

Sternford Moyo, *Scanlen & Holderness, Zimbabwe; IBA President 2021–2022*

II. Executive summary

a. The evolution of cybersecurity as a top priority for organisations

Cybersecurity risks have reached the magnitude of requiring significant attention by senior management and the board of directors. While this is not a new development, many in corporate and organisational leadership remain uncertain about how exactly to engage with these issues. Compliance alone is not enough. Over time, laws and regulatory expectations regarding corporate and organisational governance of cyber risks have expanded to try to keep pace with best practices in a number of jurisdictions, and are beginning to take shape or are expected soon in others. Yet the rapidly evolving nature of cyber risks, technologies, defences and practices easily outpaces the fastest of regulatory regimes, leaving tremendous discretion with corporate and organisational leadership to be responsible stewards of the organisation's systems and information assets. The recent proliferation of generative artificial intelligence (AI) systems is a salient reminder of the need for strong corporate and organisational governance to manage the inherent risks of technological change.[1]

Gone are the days when these risks were deemed the province of the IT department or security vendors. While IT and information security (IS) remain integral to any cyber risk management programme, a holistic, cross-organisational approach to planning, testing and response is now expected in several leading jurisdictions. Beyond their obvious role in compliance, legal counsel is also a vital part of managing cyber risks and responding to significant incidents when they occur.

b. Effective board and senior management governance of cybersecurity risks

Thankfully, there is now a 'playbook' – albeit one that is constantly being updated — for good cyber governance. The emerging components of 'good cyber governance' include active management and board engagement with the issues, including what sort of cyber risk profile the organisation has, what critical systems and data the organisation holds, where this data is held, what security choices are being made to protect it, and whether regular testing is occurring. It is clear that senior leadership and the board need to become conversant enough with the organisation's information assets and risks in order to ask intelligent questions and have an overall understanding of the organisation's cyber programme, without necessarily becoming deep technology experts themselves. Where necessary to understand the risks and decisions involved, the board should avail itself of briefings from outside technical and legal experts.

Once they are satisfied that a carefully considered cyber risk management programme is in place, it is also essential that management and the board ensure it is tested regularly. Testing involves three basic areas of focus: (1) technical testing, such as penetration testing, to find security gaps in technical controls; (2) risk assessments, which involve a broader look not only at systems but other data-related risks, such as whether the organisation is creating unnecessary risk by keeping

1 See, eg, 'Does Your Company Need a ChatGPT Policy? Probably' (Debevoise Data Blog, 7 February 2023), www.debevoisedatablog.com/2023/02/07/does-your-company-need-a-chatgpt-policy-probably/ [accessed 19 June 2023].

more sensitive data than it can justify for business purposes; and (3) response testing, including tabletop exercises and other simulated cyber incidents in which not only first responders, but also management and the board, participate, identify areas for improvement, and ensure follow through to address lessons learned.

We recognise that the exact allocation of responsibilities between senior management and the board of directors may vary somewhat from one jurisdiction to another. In the United States, for example, the board's role is focused on oversight of cybersecurity generally, not on day-to-day management. And although many organisations in the US would discuss a possible ransom payment with their board, the ultimate decision of whether a payment is in the best interests of the organisation would typically be determined by senior management. In other jurisdictions, the answers on these points may be different because of different legal or other expectations regarding the degree to which the board is expected to be involved in actual management of the cyber programme or in specific decisions like that involving a ransom payment. Recognising these differences, readers should of course apply their own jurisdictional lens to the division of duties between management and board. The principles we set forth, however, are the same regardless of that division.

c. How to use this report

We expand on these topics and several others in the main body of the report below. Our goal is not to turn everyone, including top management representatives, into technical experts (although we certainly encourage everyone to become more technically savvy) or to prescribe use of particular technical standards, but rather to give readers a roadmap of the key governance components of a strong cyber risk management programme. To this end, we provide at the end of the report a summary of the top-level best practice recommendations derived from our analysis. These recommendations are to:

1. Understand the cyber risk profile of the organisation: Every organisation faces cybersecurity risks and must understand the sector- and business-specific risks facing their organisations.
2. Understand the key information assets to protect: Decision-making is predicated on understanding the key systems and data of the organisation.
3. Understand significant regulatory requirements: Senior management and boards must understand what regulators expect of their organisations.
4. Determine the appropriate risk tolerance of the organisation: Cybersecurity standards are chosen based on organisation risk profile and a determination of risk tolerance.
5. Understand what cybersecurity standards the organisation is using: Senior management and the board should understand the rationale for the organisation's chosen cybersecurity standard(s).
6. Ensure appropriate risk decisions on protecting key information assets: Make sure senior management and the board understand the organisation's strategy for protecting key systems and data.
7. Ensure periodic risk assessments are conducted: Risk assessments provide insight into the organisation's risk profile and tolerance and produce recommendations to strengthen cybersecurity measures.
8. Understand who 'owns' cybersecurity and cyber risk management: Clear lines of responsibility help increase security and meet regulatory requirements.
9. Ensure the board has sufficient cybersecurity expertise: Meaningful cyber risk management requires sufficient expertise.
10. Ensure management has sufficient cybersecurity expertise: Regulators are increasingly expecting large organisations to have a chief information security officer.
11. Invest sufficient funds to meet cybersecurity goals: Cybersecurity expenditures should correspond with an organisation's size, complexity and risk profile.
12. Understand the cybersecurity testing and training program and review results: Consistent testing and subsequent takeaways are critical to ensuring strong responses to cyber incidents.
13. Ensure senior management and board receive regular updates: Effective oversight requires awareness of risk reduction efforts, technology changes and updates on emerging risks.

14. Ensure appropriate reporting lines so that cyber risks are raised to leadership: Individuals responsible for managing cybersecurity should brief the board to help minimise the risk of cybersecurity risks being suppressed.
15. Assess changes in cyber risk posture caused by business developments: Cyber risks fluctuate due to business developments, so reassessment is critical to understand the organisation's cyber risk posture.
16. Review, understand, and test the organisation's cyber incident response plans: Developing and testing incident response plans are critical measures in strengthening an organisation's cybersecurity.
17. Oversee the response to significant incidents: Senior management and the board should oversee the organisation's response to significant cybersecurity incidents.

If you read only one part of the report, please be sure to focus on the specific recommendations list, which is intended to represent 'actionable' steps that readers can take to strengthen their cyber risk governance, or to confirm that their programme indeed is in keeping with best governance practices in this important area. We are hopeful that this will be a useful tool for everyone to familiarise themselves with important cyber governance issues and to use this knowledge to advance the discussions with organisations with which they are involved.

III. The evolution of cybersecurity as a top priority for organisations

a. Cybersecurity threats in a digitally connected world

Digitalisation creates value. Technology and digitalisation are critical to organisations and businesses and are intrinsically linked to their business model and competitiveness. However, the value of digitalisation comes with inherent cyber and information risks of a massive scale. While growing digital connectivity brings benefits and opportunities, it also exposes organisations (and economies and societies at large) to cyber threats. Cyber attacks are among the fastest-growing forms of crime worldwide. The number, complexity, and scale of cybersecurity incidents are growing and they cross borders at high speed. The coronavirus pandemic has accelerated the digital transformation but, on the other hand, has also contributed to a global rise in cybersecurity incidents. The deployment of cyber attacks in Russia's war against Ukraine has posed the threat of increased state-sponsored, or otherwise politically motivated, cyber activity across the world, and cybersecurity has become an ever-increasing global issue.

The first known cyber attack on a country was launched on Estonia in April 2007, affecting the online services of banks, media outlets and government bodies for weeks. Since then, many other countries and organisations have suffered cyber attacks, including on critical infrastructure. According to a World Economic Forum survey, 91 per cent of all respondents believe that a far-reaching, catastrophic cyber event is at least somewhat likely in the next two years, and 43 per cent of organisational leaders think it is likely that, in the next two years, a cyber attack will materially affect their own organisation.[2] In the first half of 2022, 53.3 million Americans were impacted by a data compromise[3] and 82 per cent of breaches in Verizon's *Data Breach Investigations Report* involved influencing human behaviour through a social attack.[4]

Cybercrime is becoming increasingly monetised, particularly in the case of cyber attacks that use ransomware. Likewise, with payments becoming increasingly cashless, online theft – of money and also of personal data – has been on the rise.[5] According to Verizon,[6] 89 per cent of total breaches committed in 2022 were financially motivated and 11 per cent were motivated by espionage. On average, about 45 per cent of breaches featured hacking, 17 per cent involved malware and 22 per cent involved phishing. This trend is expected to increase further alongside the technological developments, such as 5G networks, quantum computing and devices linked to the Internet of Things (IoT). Over 20 billion

2 *Global Cybersecurity Outlook 2023*, (World Economic Forum, January 2023), 4.

3 *First Half 2022 Data Breach Analysis: Victim Rates Decline as Compromises Target Businesses* (Identity Theft Resource Center, 5 July 2022), www.idtheftcenter.org/wp-content/uploads/2022/07/20220713_H1-2022-Data-Breach-Analysis.pdf [accessed 19 June 2023].

4 *2022 Data Breach Investigations Report* (Verizon, 2022) www.verizon.com/business/resources/T60f/reports/dbir/2022-data-breach-investigations-report-dbir.pdf [accessed 19 June 2023].

5 *European Online Payment Fraud and Security in 2022: E-Commerce Trends in Europe Shift as Fraudulent Activities Increase* (Research and Markets, 17 March 2022), www.prnewswire.com/news-releases/european-online-payment-fraud-and-security-in-2022-e-commerce-trends-in-europe-shift-as-fraudulent-activities-increase-301505254.html [accessed 19 June 2023].

6 *2022 Data Breach Investigations Report* (Verizon, 2022) www.verizon.com/business/resources/T60f/reports/dbir/2022-data-breach-investigations-report-dbir.pdf [accessed 19 June 2023].

IoT devices are expected to be in use by 2024, creating a vastly more expanded attack surface area and further accelerating the need for robust cybersecurity.

In an increasing digitally connected world, the growing challenges in the cybersecurity landscape require organisation leaders to enhance the protection of their businesses against cyber threats and attacks, and to invest more money[7] and resources in making cyberspace safer for themselves and their employees, customers, and business partners at the benefit of economies and societies as a whole.

b. The role of senior management and boards in cybersecurity risk management

When considering an organisation's 'licence to operate',[8] boards and executives will find that the organisation cannot operate without certain critical assets (including systems, data, IP and suppliers) before its survival, integrity, and reputation is severely at risk. Often, executives and board members have a good understanding of financial risks, production risks and supply chain risks, and how to structure a proper risk management programme to address those risks. For example, many organisations follow the 'three lines of defence' approach, wherein management takes ownership of risk, the board supervises, and independent observers provide risk assurance. However, cyber risks have not received the same attention. Rather, the responsibility for managing cyber and information security is often left to the IT department, a chief information security officer (CISO) or an IT vendor. This no longer suffices, both from a licence to operate and a liability perspective.

The fact that digitalisation has come to encompass all significant areas within an organisation means that protecting an organisation's critical business processes, systems and data has become crucial. As a result, cybersecurity is now a major, whole-of-organisation risk requiring senior-level attention, engagement and decisions.

Today, it is expected – and must be considered best practice in corporate and organisational governance – that boards and executives, *at a minimum*, (1) know what is digitally critical for the organisation's operation, integrity, reputation, and compliance, and (2) ensure that policies and plans are in place and tested to protect the critical assets of the organisation. This requires that boards and executives establish a framework for how the organisation will work with digitisation and protection of its digital assets. In other words: *boards and executives are responsible for the organisation's preparation of a comprehensive cyber and information security strategy.*

The issues that boards and executives face when it comes to cybersecurity are:

1. existing legislative, supervisory and enforcement regimes are fragmented, ineffective, and not aligned in terms of rules, standards and expectations regarding cybersecurity;

---

7 When comparing organisations from the EU to their US counterparts, data shows that EU organisations allocate on average 41 per cent less to cybersecurity than their US counterparts. See *NIS Directive has Positive Effect, though Study Finds Gaps in Cybersecurity Investment Exist* (European Union Agency for Cybersecurity, 11 December 2020), www.enisa.europa.eu/news/enisa-news/nis-directive-has-positive-effect-though-study-finds-gaps-in-cybersecurity-investment-exist [accessed 19 June 2023].

8 There is not one, single definition of 'licence to operate.' In this context, it refers to the regulatory, economic, operational, environmental and social management aspects of an organisation's business that can best be described as 'the acceptance and trust of stakeholders and society at large in the legitimacy of an organisation's operations and business conduct which it must seek to retain in order to remain successful in the long term'. Definition from Encyclo.co.uk, see www.encyclo.co.uk/meaning-of-License_to_operate [accessed 19 June 2023].

2. countries do not share all relevant information systematically with one another, eg, in respect of best practices to protect against cyber risks and intelligence about imminent threats generally or within specific industries, with negative consequences for understanding cyber risks and the effectiveness of cybersecurity measures; and

3. there are no generally applicable rules and guidance for senior management to establish a cyber and information security strategy exist at international level.

The coming years will no doubt introduce an abundance of new rules, regulations and guidelines, nationally and internationally, in response to the growing threats posed with digitalisation and the surge in cyber attacks.

Most recently, a new European Union Network and Information Security (NIS2) Directive entered into force on 16 January 2023, and EU Member States have until 17 October 2024 to transpose its measures into national law. NIS2 strengthens and streamlines security and reporting requirements by imposing (1) a risk management approach, which provides a minimum list of basic security elements that must be applied, and (2) a process for incident reporting, content of the reports and timelines. NIS2 also introduces more stringent supervisory measures for national authorities and stricter enforcement requirements. These sanctions include:

- regular and targeted audits;
- on-site and off-site checks;
- request of information and access to documents or evidence;
- binding instructions;
- orders to implement the recommendations of a security audit;
- orders to bring security measures in line with NIS requirements;
- administrative fines up to a maximum of at least €10m or 2 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher; and
- imposition of a temporary prohibition of the exercise of managerial functions by any natural person discharging managerial responsibilities at chief executive officer or legal representative level.

NIS2 imposes obligations on the management bodies of in-scope entities to approve and supervise the implementation of cybersecurity risk management measures. EU Member States must ensure that management bodies can be held liable for infringements by the entity of provisions relating to those measures. Members of management bodies are also required to follow training on a regular basis to gain sufficient knowledge and skills to identify risks and assess cybersecurity risk management practices and their impact on the services provided by the entity. In order to ensure real accountability for the cybersecurity measures at the organisational level, NIS2 introduces provisions on the liability of natural persons responsible for or acting as a legal representative of the entities falling within the scope of NIS2. NIS2 applies to all medium and large-sized organisations in 18 selected sectors.

Although this – and similar – legislation is welcomed in order to increase the level of cybersecurity, the reality is that most legislation serves as a baseline standard, and that there continue to be different, and possibly insufficient and overlapping, regulatory requirements across the world. Accordingly, organisation leaders are left with the responsibility of preparing a strategy and setting up a governance framework for managing cyber risks without an internationally standardised methodology. This remains a key challenge for organisations as well as society at large.

c. Expanding cyber regulations and the role of legal counsel

For well-prepared organisations, legal counsel plays an important role in managing cyber risks. Because compliance alone does not necessarily make organisations secure, risk-based judgements around a range of related issues with legal and reputational implications for organisations requires legal counsel's involvement and judgment. The relatively few cybersecurity regulations in the world primarily establish baselines of conduct and identify risk categories, beyond which it is still essential for the organisation to make important risk and security decisions. Indeed, if regulators were to try to prescribe all of the specifics of a modern cyber programme, most requirements would become obsolete before they could even be drafted.

All of these reasons make clear why today's corporate counsel, supported by outside counsel as needed, are called upon to be leaders within their organisations on cyber risk management. Often working alongside the organisation's risk officer and CISO (or equivalent cybersecurity leader), they should engage in understanding the options and decisions to be made regarding:

- protecting critical systems and data;
- the organisation's preparations should there be a major cyber attack or system outage; and
- the wide range of liability and reputational issues the organisation will face following an incident, and how it will navigate them.

On a 'big picture' level, organisations should also ensure that their senior leadership and boards are engaging on these issues, receiving regular briefings, reviewing risk assessments, participating in testing, and ensuring continuous improvement for their organisations.

IV. Effective senior management governance of cyber risks

a. Leadership and cybersecurity risk

Managing cyber risk is an issue of top business concern. In 2022, the World Economic Forum recognised cyber risk as 'the most immediate and financially material sustainability risk that organisations face today'.[9] Additionally, in its 2023 global risk report, the Word Economic Forum ranked widespread cybercrime and cybersecurity as a top ten risk facing the world over the coming two to ten years.[10]

Although boards of directors are ultimately responsible for an organisation's cybersecurity given their oversight role, in most jurisdictions it is the day-to-day responsibility of management. For example, management will be those tasked with analysing risk and communicating their analysis to the board, the ultimate decision maker; choosing and implementing the cybersecurity standards applicable to their organisation (if not mandated by law or regulation); and ensuring that the organisation is ready to respond effectively to a cybersecurity incident.

To engage effectively with cyber risk issues, senior management needs to fully understand the difference between a risk-based approach and a compliance-based approach to cybersecurity. Often, a risk-based approach will deliver better outcomes, as it provides strategies that are tailored to an organisation's unique operating environment. Senior executives are likely to be the people within the organisation to knit teams together to deliver the multidisciplinary capability which is necessary to deliver effective risk-based cybersecurity.

Mistakes which occur in cyber incident risk management and response are often due to the failure to involve or give weight to the advice provided by certain teams. Senior executives should ensure that their organisations have and regularly test and update cyber incident response plans. Effective incident response is vital to containing an incident and reducing the harms to individuals and markets that can be caused by an incident.

The volume of laws with which organisations must comply is steadily increasing. Non-compliance makes organisations and individuals an easy target for adverse scrutiny. Regulators and courts are also increasingly recognising senior management's responsibilities in cyber governance in a more formal way: holding senior management personally accountable in certain areas, or requiring organisations to make periodic disclosures about management's role in implementing cybersecurity policies.[11] An emerging trend is for organisations to appoint a CISO – a senior executive assigned to lead the organisation's cyber risk management.

---

9 Anna Sarnek and Cristina Dolan, 'Cybersecurity is an environmental, social and governance issue. Here's why' (World Economic Forum (1 March 2022), www.weforum.org/agenda/2022/03/three-reasons-why-cybersecurity-is-a-critical-component-of-esg/.

10 Various authors, *Global Risk Report 2023* (World Economic Forum, January 2023), www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf [accessed 20 June 2023], 6.

11 See: Securities and Exchange Commission proposed rule on cybersecurity risk management, strategy, governance and incident disclosure: www.sec.gov/rules/proposed/2022/33-11038.pdf.

In some jurisdictions, there are well-established frameworks assigning responsibility to senior management for cybersecurity. For example, the United Kingdom's Senior Managers and Certification Regime (SM&CR) introduced a statutory duty of responsibility in financial services organisations, requiring senior executives to take reasonable steps to prevent breaches from occurring or continuing to occur in their area of responsibility. Other jurisdictions (such as Hong Kong and Australia) have similar regimes. In the EU, as from beginning of 2025, the Digital Operational Resilience Act will require senior management to identify and assess the risks associated with their organisation's network and information systems, and to implement direct measures to prevent and mitigate the effects of security incidents. Such a regime makes sense in the financial services sector. As the head of the European Central Bank has warned, a simultaneous cyber attack on important banks could trigger a liquidity crisis that could turn quickly into a systemic crisis threatening regional or even global financial stability.[12]

b. Identifying and prioritising what to protect

It is not possible for an organisation to protect all its assets to the same extent. Effective cybersecurity management is all about risk-based prioritisation, wherein organisations identify the systems that deliver important or critical services, and take steps to protect what matters most. It is the task and responsibility of the board and senior management to ensure such identification, eg, based on the overall strategy of the organisation. Senior management must then brief (and periodically update) the board on the key information assets of the organisation (both systems and data), so that the board can exercise its oversight in understanding the risk-based choices made to protect these assets.

Because cyber threats, cyber regulations and the organisation's information assets are continuously changing, cybersecurity risk management is an ongoing process, which should take the form of an ongoing sequence of policy decisions and prioritisation exercises that result in the continuous improvement of the organisation's overall cybersecurity.[13]

Whereas data laws implemented several years ago, such as the General Data Protection Regulation (GDPR), focused strongly on protecting personal information, the focus has now shifted to building resilient systems that can recover quickly from disruption (whether from malicious or non-malicious causes). For example, some financial sector regulators now focus heavily on cyber-specific business continuity planning in light of the prevalence in recent years of disruptive cyber attacks that go well beyond theft of data in targeting the organisation's very ability to operate.[14]

A tsunami of global laws is aimed at improving resilience – especially in the area of critical national infrastructure – and identifying more services as included in the definition of critical national infrastructure. For example, unlike its predecessor, NIS2 in the EU identifies manufacturers of certain products like pharmaceuticals, medical devices and chemicals as critical, as well as digital services like social networking platforms and data centre services.[15] Other recent laws, such as the

12 Phil Thornton, 'Cyber attacks could cause financial crisis, says ECB chief Christine Lagarde', (*Independent*, 6 February 2020), www.independent.co.uk/news/business/news/cyber-attack-financial-crisis-christine-lagarde-ecb-a9322556.html [accessed 20 June 2023].

13 Romauld Hoffmann et al, *Risk Based Approach in Scope of Cybersecurity Threats and Requirements*, (Elsevier BV, 2020).

14 See, for example, New York Department of Financial Services Cybersecurity Regulation 23 NYCRR Part 500 (2017), section 500.16.

15 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 2 Directive). See www.nis-2-directive.com/ [accessed 20 June 2023].

Security of Critical Infrastructure Act in Australia or the Cyber Incident Reporting for Critical Infrastructure Act of 2022 in the US, take a similar approach.

c. Assessing the primary cybersecurity risks the organisation faces

One of senior management's primary responsibilities in the area of cyber governance is in identifying, analysing, and mitigating cyber risk, and, in turn, briefing the board on these risks. Because cyber risks are constantly evolving, the board (or committees of the board) will need to be briefed on a periodic basis.

A risk-based approach towards cybersecurity (as opposed to a compliance-based approach – see further below) is essential to delivering good outcomes. Risk-based approaches to information security allow organisations to adopt strategies that are tailored to their unique operating environment, threat landscape and business objectives. Risk management is about identifying what might go wrong, understanding what you care about and why, and thinking through how you may be compromised.[16]

For the purposes of cyber governance, organisations should consider which people, information, technologies and business processes are most critical. The task then is to work out how to manage the risks identified – traditionally by either avoiding, reducing, transferring or retaining them. One approach suggested by McKinsey & Company involves the following:

1. identify and map digital assets, including data, systems and applications, across the business value chain;
2. assess risks for each asset, using surveys and executive workshops;
3. identify potential attackers, the availability of assets to users and current controls and security measures protecting the systems through which access can be gained to the assets;
4. locate where security is weakest around critical assets and identify the controls that should be in place to protect them; and
5. create a set of initiatives to address the high priority risks and control gaps.[17]

The scope of cybersecurity differs from country to country, based on the level of that country's development and resources, internet penetration, national-level cybersecurity priorities, stakeholder involvement, provisions of laws, regulations and directives, and guidelines. Public awareness of cybersecurity issues and a country's capability to enforce rules related to cybersecurity also play an important role in mitigating data security risks. Organisations based in countries where internet

16 For example, as Uganda's banking sector has adopted mobile agency banking, ATM bulk note acceptors, and PDQ machines and cards, all of which have been a target for electronic fraud, have been prioritised as critical systems.

17 See Adrian Booth et al, 'Critical infrastructure companies and the global cybersecurity threat', (McKinsey & Company, 11 April 2019), www.mckinsey.com/capabilities/risk-and-resilience/our-insights/critical-infrastructure-companies-and-the-global-cybersecurity-threat [accessed 20 June 2023]; Piotr Kaminski, et al, 'Protecting Your Critical Assets: Not All Systems and Data Are Equal', (McKinsey & Company (31 January 2017), www.mckinsey.com/business-functions/risk-and-resilience/our-insights/protecting-your-critical-digital-assets-not-all-systems-and-data-are-created-equal [accessed 20 June 2023].

connectivity is rapidly expanding can be uniquely susceptible to increasingly sophisticated and frequent cyber attacks.[18]

In some jurisdictions, regulators have begun to mandate how organisations should approach risk-based prioritisation. For example, in Israel, the pending Cyber Defence Bill and Israel National Cyber Directorate requires boards of directors in certain organisations to discuss the following subjects annually:

1. cyber risks;
2. the potential damage that a cyber attack could cause the organisation, customers, assets and vendors, and the probability that an attack could occur;
3. resources directed to preventing cyber attacks;
4. the part of the organisation responsible for cybersecurity, and the authority and resources provided to it; and
5. methods of execution of Israel National Cyber Directorate instructions.[19]

Across organisations, there must be good communication between the people who analyse risk and the people who make decisions based upon that analysis. As the National Cyber Security Centre (NSCS) in the UK says: 'Communication between these two groups must be clear understandable and useful. If the people who make decisions can't interpret the analysis they're presented with, then there is little point in doing risk analysis at all.'[20]

Senior management will often lead the processes described above. In many cases their job will be to communicate clearly to decision makers within the organisation – who may be other senior executives or board members.

d. Selecting and implementing cybersecurity standards appropriate to the organisation (eg, ISO, NIST, others)

Cybersecurity industry standards provide a common language for security across countries and industries. The leading global standards for large organisations are the NIST and ISO standards (such as the information risk management standard, ISO 27001, or the business continuity management standard, ISO 22301). There are also standards for smaller organisations (such as the Information Assurance for Small and Medium Enterprises (IASME) standard). In addition, there are some standards that apply to all organisations regardless of size undertaking a specific activity –

18 For example, Uganda, like many other developing African countries, predominantly has small and medium enterprises (SMEs), richly diversified by ownership, industry and level of development. A lack of awareness of cybersecurity issues, in both the general population as well as among the senior management of these organisations, results in many businesses operating without necessary cybersecurity standards in place. This has contributed to a high level of cybercrime, with malicious actors preying on weak and poorly integrated systems. Fraudulent SIM card registration and SIM card swapping (online fraud), online impersonation of high-profile personality (CEO fraud), unauthorised access (data manipulation), integrator compromise (business email compromise) and remote access vulnerabilities (social engineering, malware) are prevalent throughout Uganda.

19 Amir Cahane, 'The New Israeli Cyber Draft Bill – A Preliminary Overview' (The Federmann Cyber Security Research Center), https://csrcl.huji.ac.il/news/new-israeli-cyber-law-draft-bill [accessed 20 June 2023]..

20 *Risk Management Guidance* (National Cyber Security Centre), www.ncsc.gov.uk/collection/risk-management-collection/essential-topics/fundamentals [accessed 20 June 2023].

such as the Payment Card Industry Data Security Standard (PCI DSS), which pertains to entities that accept, transmit or store any cardholder data.

Increasingly, regulators are mandating baseline cybersecurity standards that must be achieved. For example, in the NIS2 Directive, which is designed to further improve the cybersecurity resilience and incident response capabilities of those operating in critical national infrastructure, there is a list of basic technical and organisational measures which *must* be applied, such as cryptography and encryption.

It is the task and responsibility of senior management to understand the mandatory and supplementary standards that will apply in the organisation, in order to ensure appropriate protection given the circumstances and the strategies of the organisation. While senior executives may not be technical experts, they, and the board, are ultimately responsible for ensuring that the organisation has identified the relevant standards and supplemented them as appropriate. As addressed below, regulators, in turn, understand that unless management and the board can avail themselves of technical expertise, they cannot meaningfully engage with these issues.

e. Ensuring that the organisation has adequate cybersecurity expertise, whether in house or external

Regulators across the globe are starting to ask probing questions about cybersecurity expertise, yet many countries are still at the stage where cybersecurity expertise is in short supply.[21] It is the task and responsibility of senior management to ensure that the organisation has adequate cybersecurity expertise, whether in-house or external, at all times.

Some jurisdictions require organisations to appoint a cybersecurity expert to a senior management role within the organisation. For example, Israel has enacted several laws and regulatory guidelines that require the appointment of a CISO or that require organisations to accept a CISO appointed by the government or military.[22] Additionally, according to the upcoming EU NIS2 Directive, boards of directors must establish effective governance structures to oversee their organisations' cybersecurity activities. This includes appointing a senior executive responsible for cybersecurity and ensuring that cybersecurity risks are regularly discussed at board meetings.

The recent regulatory proposals from the US Security and Exchange Commission (SEC) are a good indicator of emerging trends.[23] It proposes that listed companies disclose the cybersecurity expertise of members of the board of directors, if any. The proposals do not define what constitutes 'cybersecurity expertise,' given that such expertise may cover different experiences, skills and tasks. However, they do include a non-exclusive list of criteria that should be considered in determining whether a director has expertise in cybersecurity:

- whether the director has prior work experience in cybersecurity, including, for example, prior experience as an information security officer, security policy analyst, security auditor, security architect or engineer, security operations or incident response manager, or business continuity planner;

21 See, for example, Owen Hughes, 'Bad news: The cybersecurity skills crisis is about to get even worse', (ZD Net, 1 June 2022), www.zdnet.com/article/bad-news-the-cybersecurity-skills-crisis-is-about-to-get-even-worse/ [accessed 20 June 2023].

22 Protection of Privacy Law, 5741 – 1981, Part 1, 17B; Protection of Privacy Regulations (Data Security) 5777-2017; Israel National Cyber Directorate, *Cyber Defense Methodology for an Organization.*

23 *Commission Statement and Guidance on Public Company Cybersecurity Disclosures* (Securities and Exchange Commission, February 2018), www.sec.gov/rules/interp/2018/33-10459.pdf [accessed 20 June 2023].

- whether the director has obtained a certification or degree in cybersecurity; and
- whether the director has knowledge, skills or other background in cybersecurity, including, for example, in the areas of security policy and governance, risk management, security assessment, control evaluation, security architecture and engineering, security operations, incident handling or business continuity planning.[24]

This is a useful checklist to consider when looking at whether the organisation has adequate cybersecurity expertise within its board and senior management.

The criteria above could be fulfilled by the chief information security officer (CISO) or information technology director (IT Director). Increasingly, one will expect to find cybersecurity expertise in the chief executive officer (CEO), chief financial officer (CFO), general counsel (GC), organisation secretary, head of business continuity, head of legal, head of insurance, or financial crime compliance lead. Dramatic growth in ransomware attacks has led to a greater number of people within organisations acquiring knowledge and skills in cybersecurity, with those fulfilling the above roles closely involved in incident prevention and response.

f. Assigning roles and responsibilities, and ensuring cross-functional collaboration

In cybersecurity, cross-functional collaboration is essential. This is reflected in emerging regulatory guidance. In several sectors, relevant authorities have published guidance detailing the division of responsibilities between the elements within an organisation and their collaboration when managing cyber risks, ensuring cyber and information security, and handling cyber incidents.

The Israel National Cyber Directorate (INCD) published two recommended guidebooks for organisations in which an internal collaboration and division of responsibilities is proposed: (1) *Cyber Defense Methodology for an Organization*; and (2) *Managing Cyber Risks in an Operational Technologies Environment – Board of Directors Guidebook*. In the latter guidebook, INCD recommends that an organisation's board of directors clarify organisational responsibility for managing cyber risks by assigning general responsibility and policy to senior management, execution of which is the responsibility of professional cybersecurity personnel.

In some sectors, authorities have imposed a requirement for organisations to put in place policies and procedures that detail the chain of command and reporting, and that set a clear division of responsibilities in cyber defence scenarios.[25]

Senior management will often be doing the difficult work of knitting together the right expertise into a coherent, high-functioning team. In a ransomware attack, for example, an organisation will need various forms of expertise, including: technical experts to contain the incident and establish the facts; compliance experts to consider notification obligations under various regulatory regimes (data protection and sector specific); insurance experts to ensure that cover is not voided inadvertently;

---

24 *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, (Securities and Exchange Commission, 9 March 2022), www.sec.gov/rules/proposed/2022/33-11038.pdf [accessed 20 June 2023], at 40, n 79.

25 For example, in Israel, the Supervisor of Banks has issued Directive 357 on Information Technology Management and the Capital Market Authority, Insurance and Savings – Ministry of Finance issued Circular Letter 4-9-2010, Managing Information Technology in Institutional Investors (the 2010 CMA Circular).

legal experts to consider whether payment of a ransom might break the law; and communications experts to advise on messaging to various stakeholders.

Senior management will usually be responsible for ensuring that an organisation is equipped to respond to a cybersecurity incident, including that:

- the organisation has a full crisis response plan in place;
- the crisis plan for a cybersecurity incident is integrated with the organisation's wider crisis plans;
- the crisis plan includes all the teams within the organisation who will need to contribute (eg, insurance);
- everyone who will need to apply the plan knows where to find it;
- the plan provides for all notifications to regulators or other bodies that may be required; and
- the plan is rehearsed.

g. Identifying and ensuring compliance with evolving cybersecurity regulatory requirements

It is important to recognise that compliance and cybersecurity are not the same thing. A compliance-based approach tends at most to deliver basic protections – a lowest common denominator of security controls.[26] As NCSC puts it, compliance and cybersecurity 'may overlap, but compliance with common security standards can coexist with, and mask, very weak security practices.'[27]

Senior executives have an important role to play in ensuring compliance with evolving cybersecurity regulatory requirements. Often, a compliance-based approach by itself will not provide adequate protection, but of course is a necessary component of the cybersecurity programme to avoid being an easy target for criticism by regulators and for claims by those harmed by non-compliance.

There is an ever-increasing amount of regulation with which to comply, for example:

- mandates for technical and organisational measures which must be applied;
- stricter notification requirements; and
- increasingly complex supply chains and associated risks.

The financial services sector in the UK is particularly strong in this area; principles from this sector may be extracted and applied to other sectors in the UK and globally. Following the financial crisis of 2007/08, which highlighted a number of risk management shortcomings, the UK implemented a regime to place personal accountability upon senior executives in firms (as did other places, such as Hong Kong and Australia). This regime – the Senior Managers and Certification Regime (SM&CR) – introduces a statutory duty of responsibility, requiring senior executives to take reasonable steps to prevent regulatory breaches from occurring or continuing to occur in their area of responsibility.

---

26 See, for example, 'Why A Compliance-Based Approach to Cybersecurity is Not Enough', (Securicon, 27 July 2020), www.securicon.com/why-a-compliance-based-approach-to-cybersecurity-is-not-enough/ [accessed 21 June 2023].

27 *Risk Management Guidance* (National Cyber Security Centre), www.ncsc.gov.uk/collection/risk-management-collection/essential-topics/fundamentals [accessed 21 June 2023].

Under SM&CR, every senior manager should have a statement of responsibilities which clearly says what they are accountable for. Certain roles (ones where a senior manager's error might cause significant harm to the firm or its customers) require certification – and at least once a year firms need to check and certify that the people holding the role are fit and proper to perform their role. In addition, all senior executives must adhere to the Conduct Rules, which set out the minimum standards of individual behaviour expected in financial services.

The Individual Conduct Rules – in Chapter 2 of the Code of Conduct (COCON) – require individuals to act with due skill, care and diligence and set out the 'reasonable steps' senior executives are required to take when carrying out their roles, including:

- reasonable steps to ensure that the business of the firm for which you are responsible is controlled effectively;
- reasonable steps to ensure that the business of the firm for which you are responsible complies with the relevant requirements and standards of the regulatory system;
- reasonable steps to ensure that any delegation of your responsibilities is to an appropriate person and that you oversee the discharge of the delegated responsibility effectively; and
- a senior manager must also disclose appropriately any information of which the Financial Conduct Authority (FCA) or Prudential Regulatory Authority (PRA) would reasonably expect notice.

A senior manager carrying out the 'chief operations function' (SMF 24) at certain firms is responsible for 'the internal operations and technology of a firm', which will, of course, include cybersecurity. The SMF 24 function is often split between the chief operating officer (COO) and chief information officer (CIO).

The new operational resilience rules, which came into force in the UK on 31 March 2022, as well as similar rules coming into force in other financial centres such as the EU, Hong Kong and Singapore, continue this focus on individual accountability and raise the bar further in relation to regulators' expectations. Operational resilience is the ability to prevent, adapt, respond to, recover and learn from operational disruptions, such as cybersecurity incidents. The rules recognise that disruption is inevitable in an increasingly digitalised and complex world, and expect senior executives to 'connect the dots' across a range of practical risk management and governance activities. Where it exists, the SMF 24 function holds overall responsibility for implementing operational resilience policies and reporting to the board.

In practice, this means that individual senior executives may be directly accountable in regulatory proceedings for inadequate cybersecurity or poor cyber resilience planning, such as failure to properly prepare for crisis events. They will also be directly accountable in relation to incident management – if they fail to keep the regulator informed, put out misleading statements to customers or markets about recovery, or respond slowly or only partially to an incident causing detriment to customers or a negative market impact.

Similarly, NIS2 introduces governance and accountability obligations for management bodies in relation to cybersecurity.

Security of supply chains and other vendor relationships is an area in which organisations will need to exercise particular care (often referred to as third-party risk management). There are two aspects of risks associated with suppliers and other vendors: (1) direct threats to the organisation via the third party as the vector, such as through a compromised supply chain component, or through the compromise of a trusted network access maintained by the vendor; and (2) indirect threats to the organisation where the third party itself is attacked directly, such as through the loss of sensitive organisation data held by the vendor, or where the vendor's operations are disrupted in a ransomware attack and the vendor is unable to provide important services to the organisation as a result.

A highly publicised example of the second category is the Colonial Pipeline incident. Colonial Pipeline is a major pipeline operator that transports gasoline, diesel, aviation fuels and home heating oil throughout the East Coast of the United States. In May 2021, Colonial Pipeline suffered a ransomware attack and lost access to its IT systems until it made a ransom payment to the threat actor.[28] The attack disrupted product deliveries and affected gasoline supplies throughout the East Coast of the United States. For many organisations and for the US Government (not to mention for many individual consumers who ultimately waited in long lines for gasoline), their critical supply was disrupted.

In response to this attack and similar threats, the US Transportation Security Administration has issued security directives meant to strengthen cybersecurity in the pipeline sector. For example, the security directives require pipeline companies to designate a cybersecurity coordinator that can liaise with government agencies, identify critical cyber systems, establish network segmentation policies and controls, and implement access control measures.[29]

Similarly, the European Commission recently presented a Council Recommendation to increase resilience in critical infrastructure that may be vulnerable to cyber attack,[30] while the Australian Cyber Security Centre (ACSC) announced last year that entities responsible for critical infrastructure asset classes must report cybersecurity incidents to the ACSC in order to support Australia's Critical Infrastructure and Systems of National Significance (CISONS).[31] As these regulatory actions indicate, senior management will increasingly be responsible for many such responsibilities and should be aware of sector-wide cyber risks and corresponding regulations that address them.

Other third-party risk challenges stem from the fact that many organisations have moved to cloud infrastructure, software as a service (SaaS) and other new tech solutions. These business decisions offer the promise of flexibility, economies of scale and operational efficiencies, and, if managed correctly, potentially improved security. However, the complexity of many of the technologies/solutions and the speed at which they are evolving means that it is often difficult for organisations to understand and manage the associated risks. These risks are also amplified when the third-party vendors further sub-outsource to 'fourth-party' providers. For many organisations around the world, the rapid growth and scale of third-party dependencies has increased their potential exposure to cyber threats via their third- and fourth-party partners. For example, a report by the Economic

28 Testimony of Joseph Blount, President and CEO, Colonial Pipeline Company to the US Senate Committee on Homeland Security and Governmental Affairs (8 June 2021), www.hsgac.senate.gov/imo/media/doc/Testimony-Blount-2021-06-08.pdf [accessed 21 June 2023].

29 *Pipeline Cybersecurity Mitigation Actions, Contingency Planning and Testing* (Transportation Security Administration, 21 July 2022). www.tsa.gov/sites/default/files/tsa_sd_pipeline-2021-02-july-21_2022.pdf [accessed 21 June 2023].

30 *Proposal for a Council Recommendation on a Coordinated Approach by the Union to Strengthen the Resilience of Critical Infrastructure,* (Eur-Lex, 18 October 2022), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0551 [accessed 21 June 2023].

31 *Critical Infrastructure* (Australian Cyber Security Centre), www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/critical-infrastructure [accessed 21 June 2023].

Commission for Latin America and the Caribbean (ECLAC) identified third-party data risks as one of the greatest concerns around protection of assets.[32]

As a result, regulators are expecting senior management to have a plan to manage supply chain and vendor cyber risks. For example, Brazil's Central Bank issued a resolution that requires covered financial institutions to enter into agreements requiring that third-party providers comply with notification and disclosure requirements.[33] It is a senior management task and responsibility to assess the cybersecurity situation and additional measures, if any, to be taken when onboarding and amending supply chains and supplier relationships.

h. Establishing, updating, and ensuring compliance with cybersecurity policies and procedures

Cybersecurity policies and procedures set out the assets that must be protected, the threats to those assets, and the security controls that exist to protect those assets. Examples include an acceptable use policy for IT assets, a remote access policy, or an access control policy.

Given that cyber laws and regulations often state that appropriate technical and organisational measures to provide cybersecurity should take into account the 'state of the art' (see, for example, Article 32 of the GDPR or Article 13 of the NIS Directive (EU 2016/1148)), there is an expectation that policies and procedures such as those mentioned above will be kept up to date. Maintaining state of the art cybersecurity policies is a task and responsibility of senior management.

i. Implementing periodic training and testing

Cybersecurity training and testing should take place regularly using a risk-prioritised approach, and it is the task and responsibility of senior management to ensure that periodic training and testing are implemented throughout the organisation. For example, in relation to the new operational resilience rules in financial services in the UK, firms are required to have sound, effective and comprehensive strategies to enable them to comply with their obligations, which would include cybersecurity training and testing programmes. The UK's Financial Conduct Authority (FCA) also requires strategies, processes and systems to be comprehensive and proportionate to the nature, scale and complexity of the firm's activities.

Security testing monitors the effectiveness of an organisation's cybersecurity controls and highlights issues which need attention. There are many forms of testing which can reduce the risk of successful cyber attacks. For example:

- vulnerability assessments to search for known vulnerabilities in networks or databases;
- log reviews to check that privileged users are not misusing their privileges;

32 *State of Cybersecurity in Logistics in Latin America and the Caribbean* (Economic Commission for Latin America and the Caribbean, 2021), https://repositorio.cepal.org/bitstream/handle/11362/47655/1/S2100687_en.pdf [accessed 21 June 2023].

33 Resolution CMN 4,658 (Banco Central Do Brasil, 26 April 2018), https://www.bcb.gov.br/ingles/norms/Resolution%204658.pdf [accessed 21 June 2023].

- audits – internal, external and third-party – which aim at demonstrating the effectiveness of controls to a third party;
- tests of users' awareness of risks associated with their use of the organisation's digital assets; and
- penetration tests involving trained security professionals trying to exploit systems.

There is an increased emphasis on audits, including notably in scrutinising audit reports as part of the due diligence process when buying organisations to assess potential liabilities, as well as upon audit rights in contractual arrangements. Specifically, when an organisation is looking to acquire a business, it should carry appropriate cyber due diligence.

Testing cyber incident response plans continues to be important. Effective incident response is vital to containing an incident, and reducing the harms to individuals and markets that can be caused by an incident. Incident response mistakes which occur are often due to the failure to involve or give weight to the advice provided by certain teams.

In the US, UK and many other jurisdictions, it is typical to 'wargame' an incident with all the teams which will be involved in incident response, in order to test that there are no conflicts between an organisation's broader crisis plans and cyber incident response plans. 'Wargames' further ensure that the cyber incident response plans:

- contain everything the teams within the organisation will need in order to respond quickly and effectively;
- contain clear markers of when particular teams need to become involved/handover points; and
- are clear about who will have responsibility for decision-making.

This practice is increasingly evolving into a regulatory requirement. Most notably, the New York Department of Financial Services has proposed regulations that would require covered entities to test its incident response plan with senior officers, including the CEO, at least annually.[34] In the UK, the FCA has, on at least one occasion, fined a bank for failing to respond to a cyber attack with sufficient rigour, skill and urgency.[35]

In terms of frequency, many well-prepared organisations conduct at least one simulated breach response or 'tabletop' exercise per year that includes, at a senior management level, both technical and non-technical functions needed for a significant incident response, such as the legal, compliance, and communications functions. First responders and those whose job functions are specific to cybersecurity will of course take part in more frequent exercises, and understanding how they will classify and escalate incidents up the chain of command and how and when to involve legal and other non-technical functions will be essential to any meaningful exercise.

On a final note, organisations should also be mindful that cybersecurity requires maintaining the availability and integrity of information, as well as confidentiality. Accordingly, they should undertake

34 NYDFS Proposed Amendments to Cybersecurity Regulation, Section 500.16(d)(1).

35 'FCA Fines Tesco Bank £16.4m for Failures in 2016 Cyber Attack', (Financial Conduct Authority, 10 January 2018), www.fca.org.uk/news/press-releases/fca-fines-tesco-bank-failures-2016-cyber-attack [accessed 21 June 2023].

code reviews and tests to discover security, performance or reliability flaws in applications before they go live and negatively impact business operations.

j. Ensuring timely and effective reporting

Two reporting issues are particularly important: (1) senior executives' reporting to the board; and (2) reporting by senior executives or the board to regulators or other parties, such as law enforcement, customers, investors, or counterparties to transactions.

1. Reporting to the board

Boards need timely and clear information to effectively carry out their duties, which include cybersecurity oversight. Senior executives are responsible for providing the board in a timely and effective manner with necessary information for board members to discharge their duties. Such reporting should use non-technical language to help the board understand evolving cybersecurity risk. Reports also frequently include an update on the status of projects to address previously identified risks, information about emerging risks, threats or vulnerabilities, new notable information assets, and significant cyber incidents or incident trends within the organisation. Analysis of how a cyber attack might affect important business services within an organisation are important for the board to receive.

We address in Section V the frequency and format of reporting to the board.

2. Reporting to regulators and other parties

New cybersecurity laws and regulation are expanding reporting obligations and, often, imposing tighter timetables. Even where there is no duty to report incidents prescribed by legislation, many jurisdictions take pains to set out clear reporting expectations.

For example, although Israel has not passed primary legislation with broad application that imposes a duty to report cyber incidents, the Israel Securities Authority (ISA) asserted in *Legal Stance No.105-33: Disclosure in Cyber* that corporations' current duties to report (eg, annual reports) include the duty to report cyber threats and incidents, and the document specifies the degree of detail. Since corporations have a duty to report certain incidents immediately, an outcome of the ISA position is that, where cyber incidents meet the reporting thresholds in other respects, they give rise to a duty to report the incident.

Likewise, in NIS2, the generalised reporting obligation in NIS1 is replaced with a streamlined tiered plan. Incidents having a significant impact upon service will have to be reported to the relevant supervisory authorities within 24 hours at the latest, with an intermediate report and a final report no later than one month after the initial notification.

Similarly, under new Australian rules, responsible entities must report on critical cybersecurity incidents affecting the critical national infrastructure asset within 12 hours and on other cybersecurity incidents within 72 hours of becoming aware of the incident. Further, the proposed

SEC regulations in the US would require a registrant to disclose a material cybersecurity incident within four business days of determining such incident occurred.[36]

The proposed duty about reporting is an ongoing one – so that under the new rules periodic reporting requirements would be amended to obligate a registrant to provide updated disclosures relating to previously disclosed cybersecurity incidents – and to require disclosure where previously undisclosed and individually immaterial cybersecurity incident have become material in the aggregate.

In extreme instances, failing to report a cybersecurity incident may constitute a criminal offence. For example, under the Cybersecurity Act which came into force in 2018 to establish a legal framework for the oversight and maintenance of national cybersecurity in Singapore, the failure of a critical information infrastructure owner to notify the Commissioner of certain cybersecurity incidents within the prescribed period of becoming aware of such an occurrence is an offence under Section 14 of the Act. An owner shall be 'liable on conviction to a fine note exceeding $100,000 or to imprisonment for a term not exceeding 2 years or to both'.

An 'owner' in relation to critical information infrastructure in the Act is 'the legal owner of the critical information infrastructure and, where the critical information infrastructure is jointly owned by more than one person, includes every joint owner'.

k. Establishing a culture of cybersecurity and data protection

Cybersecurity is a business risk that affects the whole organisation. Those at the top of the organisation who are responsible for risk management and for governance should lead on establishing the right culture. Without such a culture, it becomes increasingly difficult in a world of growing cyber risks and regulations to protect the organisation from cyber risk.

Some advocate that organisations should take the same approach towards cybersecurity as many jurisdictions have taken towards health and safety issues. Given the threat landscape, including the volume of threats from nation states and the role that cybersecurity now plays in critical national infrastructure – defined in the broad sense we see in recent legislation – there is a strong argument for this mentality. In any event, senior executives play a vital role – and have a responsibility for – establishing an appropriate and resilient culture of cybersecurity in their organisations.

36 *Fact Sheet: Public Company Cybersecurity; Proposed Rules* (Securities and Exchange Commission) www.sec.gov/files/33-11038-fact-sheet.pdf [accessed 21 June 2023].

V. Effective board governance of cyber risks

This chapter provides guidance for the board of directors in supervising cybersecurity risks. Each section focuses on one facet of a board's supervisory role. Each section is further divided into relevant sub-sections which underline the detailed measures boards can implement pursuant to international best practices and which address examples from specific jurisdictions that have incorporated the relevant best practice in their legal and regulatory frameworks. The examples are followed by practical recommendations for boards to follow, as final decision makers, within their corporations.

a. The board's role: oversight of cyber risk management

Cybersecurity measures can only be successful if implemented throughout the entire organisation from top to bottom: ie, from the supervisory board through all management levels and all employees. The organisation should ensure that all executives and employees are informed (and trained) in cybersecurity to adequately perform their role and responsibility.

This section focuses on the supervisory board as the top-level management board of an organisation, (as opposed to management boards dealing with day-to-day management tasks). In a wide range of jurisdictions, the law affords the supervisory board the ultimate oversight responsibility of (cyber) risk management. Hence, boards have a legal obligation to ensure that cybersecurity is addressed by the organisation, often using senior management as the key instrument to this end. The specific way a board deals with the topic (eg, how much board time is allocated to cyber risks) is, however, not prescribed by law but varies based on the organisation's risk exposure.

This does not mean that boards cannot assign tasks attributable to cybersecurity to one member within the board and, of course, specific tasks can further be delegated to internal or external resources. Frequently, boards will delegate responsibilities for cybersecurity risk to senior management, including through an audit committee, risk committee or, in some organisations, a dedicated technology risk or cybersecurity committee. However, in any event, the supervisory board as a whole bears the responsibility for final decision making in the area of cybersecurity.

By way of example, according to UK governance guidelines[37] and the general principles of German corporate law, the delegation of IT matters to the CIO or equivalent does not free the members of the supervisory board from their obligation to deal with cybersecurity. Similarly, in Australia, a recently enacted Prudential Standard makes the boards of covered entities directly accountable for the oversight of operational risk management, including business continuity plans that set out how the entity would identify, manage and respond to a disruption within approved tolerance levels and are regularly tested with severe but plausible scenarios.[38]

37 *Cyber Security Toolkit for Boards* (National Cyber Security Centre, 2021), www.ncsc.gov.uk/files/board_toolkit_2021.pdf [accessed 21 June 2023].

38 *Prudential Standard 230*, (Australian Prudential Regulation Authority, July 2022), 5.

In most jurisdictions, it is recommended to integrate cyber risk management into an organisation's objectives and risks. According to Singaporean[39] and Australian[40] best practice guides, it is explicitly recommended to establish risk management protocols or information security management systems for this purpose.

In the US, SEC regulations require boards to oversee cybersecurity risks. SEC guidance further suggests that 'the development of effective disclosure controls and procedures is best achieved when an organisation's directors, officers, and other persons responsible for developing and overseeing such controls and procedures are informed about the cybersecurity risks and incidents that the organisation has faced or is likely to face'.[41]

For effective oversight, boards should make sure that they stay informed of the relevant legal, regulatory and threat landscapes. Cybersecurity should be considered as a wider organisational risk (rather than just an IT risk) in all organisation-level strategy and risk discussions. Boards should make sure that management continually communicates cybersecurity objectives to all employees and defines, and explains to the board for its review, what level of risk the organisation can tolerate and the rationale behind it. Assessment of cyber risks should include both quantitative and qualitative means to give a realistic understanding of potential financial exposure. The allocation of responsibilities between the board and senior management should also be a part of the organisation's risk guidelines, which should incorporate regular and robust cybersecurity information exchange between the board and senior management.

This subsection covers the following topics:

- attention to and evaluation of cyber risks at board meetings;
- assessment of cyber risk tolerance;
- understanding the standards management aims to achieve;
- understanding financial and legal risk exposure; and
- receiving regular management reporting.

1. Risk assessment and attention to cyber risks

Supervisory boards are well advised, on a regular basis and often based on material prepared by senior management, to understand and assess cyber risks in the context of:

- the organisation's most important assets and systems, including in the technology landscape, whether they be tangible assets (eg, IT systems), intellectual assets (eg, data and IP) and/or reputation;

39 *Statement of Good Practice Cyber Security Risk Management* (Singapore Institute of Directors, 2020), www.sid.org.sg/images/PDFs/Codes/SGP16.pdf [accessed 21 June 2023], 6.

40 *Cyber Security Policy* (NSW Government, January 2020), www.digital.nsw.gov.au/sites/default/files/NSW-Cyber-Security-Policy-2021-2022.pdf [accessed 21 June 2023].

41 *Commission Statement and Guidance on Public Company Cybersecurity Disclosures* (Securities and Exchange Commission, February 2018), www.sec.gov/rules/interp/2018/33-10459.pdf [accessed 21 June 2023].

- such assets and systems' processing and storage (eg, in the cloud, at an external supplier, and inside or outside of its place of operation);
- the organisation's most important suppliers and partners and their cybersecurity circumstances;[42]
- the organisation's primary vulnerabilities, whether it is pertaining to technology, people or processes;
- the organisation's key threats and the probability of their occurrence, including identification of likely attackers and their goals (eg, financially, IP, information and/or digital identity) and tools they use to achieve these goals (eg, phishing, drive-by exploits, social engineering, distributed denial of service (DdoS) and/or malware); and
- the organisation's potential losses and other consequences associated with a cyber attack (eg, if important values are changed, stolen, leaked, or if critical systems or other IT services are inaccessible for a shorter or longer period of time).

As with other business risks, a robust risk assessment is essential to identify, analyse and evaluate cyber risks. Danish best practice guidelines[43] recommend that the board of directors receives and addresses an updated cyber risk assessment at least twice a year, based on the organisation's most important assets, IT infrastructure, business model, primary vulnerabilities, likely threats and possible losses resulting from cyber attacks.

Directors, just like senior management, need to understand and approach cybersecurity as a strategic enterprise risk and not just an IT risk. There is value to moving cybersecurity outside of the IT department and into enterprise-wide risk and strategy discussions at both management and board levels.[44]

Based on a thorough risk assessment, directors and senior management would be well positioned to push for – and ensure – internal regulations on cybersecurity and to make sure that the cyber-related objectives are continuously and unambiguously communicated to management and employees in order to create sustainable compliance awareness in the organisation with regard to cybersecurity.[45] In this context, directors and management would be able to effectively structure a security policy framework as a hierarchy, with higher level policies supported by underlying standards, guidelines and procedures.[46]

2. Assessment of cyber risk tolerance

In today's interconnected business world, cyber risks cannot be reduced to zero, nor can they be avoided altogether. For example, it will be virtually impossible to prevent an employee with criminal intent to circumvent at least some cyber risk prevention measures. Therefore, it is not surprising that some jurisdictions recommend the creation of a tolerance threshold in relation to cyber risks.

---

42 According to a World Economic Forum survey, 'business executives acknowledge that their organization's cybersecurity risk is influenced by the quality of security across their supply chain of commercial partners and clients'. *Global Cybersecurity Outlook 2023*, January 2023, 4.

43 *Cyber Security for the Board of Directors, Recommendation to Strengthen Cyber Security Competences* (Board Leadership Society Centre of Cybercompetences, December 2022), https://bestyrelsesforeningen.dk/wp-content/uploads/2023/01/Cyber_Bestyrelsesvejledning_-FINAL-December-202246-Skrivebeskyttet.pdf [accessed 21 June 2023], 16 (in Danish).

44 *Cyber-Risk Oversight 2020, Key Principles and Practical Guidance for Corporate Boards*, (NACD, 25 February 2020), http://isalliance.org/wp-content/uploads/2020/02/RD-3-2020_NACD_Cyber_Handbook__WEB_022020.pdf [accessed 21 June 2023], 12–16 and 30–34.

45 See ISO 37301:2021, formerly ISO 19600:2014.

46 *Prudential Practice Guide: CPG 235 – Managing Data Risk* (Australian Prudential Regulation Authority, September 2013), www.apra.gov.au/sites/default/files/Prudential-Practice-Guide-CPG-235-Managing-Data-Risk_1.pdf [accessed 21 June 2023].

Singaporean best practice guides[47] warn against setting a 'zero tolerance' for cyber risks, as this would limit digital innovation. US best practice guides[48] recommend that cyber risks that exceed the risk appetite are escalated to management and that the board or board committee should approve the enterprise-wide risk appetite statement. Furthermore, it states that the risk appetite is to be informed by the institution's role in critical infrastructure.

In general, boards should make sure that management defines specific and clear guidelines on the types and amount of risk an organisation is willing to tolerate, ideally as part of an information security management system, in order to be able to define effective priorities. Danish best practice guidelines recommend that the board of directors, as often as relevant and at least once per year, re-evaluates the organisation's cybersecurity strategy, including cyber risk tolerance, based on a balance between the organisation's general business strategy, business goals, IT infrastructure, security budget and willingness to invest, etc.[49]

The board should establish transparent quantitative means, in addition to traditional qualitative risk assessment approaches, to get a realistic evaluation and understanding of the degree of their organisation's financial exposure to cyber risk. In many jurisdictions, there is no specific legal definition as to how such risk assessment is to be conducted. Hence, whereas organisations do have a clear legal responsibility to conduct a risk analysis on the basis of the facts identified, the decision on how to conduct that risk analysis, and – even more so – the determination of what is an acceptable risk tolerance, remains subject to management's reasonable discretion and the board's oversight.[50]

Risk appetite within cybersecurity may vary depending on the organisation's objectives, digitalisation strategy, risk profile, regulatory framework, IT and security budget, and other circumstances of organisation at any given time. Also, it may vary within different domains relevant to the organisation: risk type, product type, customers, suppliers and objectives. The organisation's risk appetite will inform – and be part of – the overall cyber strategy of the company, and it will need to be implemented as a baseline in internal policies of the organisation, eg, in respect of operational, compliance, market, liquidity and other risks. Overall, it should reflect the risk the board is willing to accept in order to achieve the organisation's strategic objectives.

3. Understanding the standards that management aims to achieve

Boards should make their decisions on a fully informed basis. Again, whereas boards have some level of discretion on decision-making (in many jurisdictions, this is pursuant to the so-called 'business judgement rule') they need to make sure that the relevant underlying facts are properly considered. Hence, a decision which, *ex post*, turns out to be wrong may, in many cases, not trigger a board member's liability. However, if a board did not deal with the issue of cyber risks at all, or has not made sure that it has done so on a fully informed basis, liability is much more likely. For example,

47 *Statement of Good Practice – Cyber Security Risk Management* (Singapore Institute of Directors, 2020), www.sid.org.sg/images/PDFs/Codes/SGP16.pdf [accessed 21 June 2023].

48 See, for example, *Recommended Practices* (Cybersecurity & Infrastructure Security Agency), www.cisa.gov/uscert/ics/Recommended-Practices [accessed 10 January 2023]; and *Cybersecurity Assessment Tool* (FFIEC, May 2017), www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf [accessed 21 June 2023].

49 *Cyber Security for the Board of Directors, Recommendation to Strengthen Cyber Security Competences* (Board Leadership Society Centre of Cybercompetences, December 2022), https://bestyrelsesforeningen.dk/wp-content/uploads/2023/01/Cyber_Bestyrelsesvejledning_-FINAL-December-202246-Skrivebeskyttet.pdf [accessed 21 June 2023], 16 (in Danish).

50 *Risk Management Guide for Information Technology Systems* (National Institute of Standards and Technology, July 2002), www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf [accessed 21 June 2023].

in the US, the SEC has made clear that how a board 'engages with management on cybersecurity issues allows investors to assess how a board of directors is discharging its risk oversight responsibility in this increasingly important area'.[51] Therefore, boards need to ensure they understand the standards that the organisation aims to achieve.

An Israeli best practice guide for banks[52] recommends that management should be responsible for staying updated on cyber risks, coordinating activity and tracking effectivity of the cybersecurity policy.

The relationship, allocation of responsibilities, and constant exchange of information between board and management should be part of the guidelines on cyber risk. Management and staff should be adequately informed about cybersecurity standards and trained where necessary, and as the applicable standards and underlying facts impacting both risk exposure and countermeasures change rapidly, boards are well advised to define reasonably short intervals for dealing for cybersecurity issues on the board level.

4. Understanding financial and legal risk exposure

Similar to understanding relevant standards of risk mitigation measures preventing cyber risks, boards need to be aware of their organisation's financial and legal risk exposure. This presupposes that boards are informed about the applicable regulatory and legal landscape as well as, in particular, the dependency of operating procedures on information processing systems and the value of the data controlled by the organisation.

As such, Singaporean[53] and UK[54] best practice guidelines explicitly recommend consulting external advisers such as lawyers to obtain independent perspectives from outside the organisation.

Although directors are not required to have in-depth knowledge about the increasingly complex area of cybersecurity law, they should be briefed on a regular basis about requirements that apply to the organisation and the organisation's plans to meet them. The understanding of financial and legal risk exposure can be attained by establishing internal teams composed of legal counsels, business experts, and IT personnel to help keep the board abreast on various regulatory and legal developments.

5. Receiving regular management reporting

The obligation of the management to report regularly to the board is generally recommended across all reviewed jurisdictions, sometimes as a derivative of the general recommendation integrating cyber risk management into the organisation's objectives and risks. For example, reporting obligations to

51 *Commission Statement and Guidance on Public Company Cybersecurity Disclosures* (Securities and Exchange Commission, February 2018), www.sec.gov/rules/interp/2018/33-10459.pdf [accessed 21 June 2023].

52 *Directive 357 on Information Technology Management* (Israel Supervisor of Banks).

53 See generally section 2.3, *Statement of Good Practice – Cyber Security Risk Management* (Singapore Institute of Directors, 2020), www.sid.org.sg/images/PDFs/Codes/SGP16.pdf [accessed 21 June 2023].

54 *Cyber Security Toolkit for Boards* (National Cyber Security Centre, 2021), www.ncsc.gov.uk/files/board_toolkit_2021.pdf [accessed 21 June 2023], 31.

the board are explicitly recommended in India[55] and Germany.[56] For certain sectors, such as banking in the US, reporting to the board is required by law.[57]

The right cadence and length of periodic reporting to the board in cybersecurity matters will necessarily vary from organisation to organisation. For larger organisations, in the absence of specific regulatory guidance, it is typical to hold at least two significant cybersecurity updates per year to the full board, and at least quarterly updates to the responsible committee of the board. In Denmark, best practice guidelines recommend that the board has cybersecurity on the agenda at every meeting, and that prior to the meeting, the board receives relevant reporting from management addressing current threats, security incidents, results of security tests, awareness activities and audit reviews, and proposals for additional measures.[58]

Provided the topics are adequately covered at board level, the format of such reports is usually left to the organisations and should depend on the size and risk vulnerability of the organisation. Many US organisations use an issue tracking chart or similar 'dashboard' approach, indicating progress on ongoing cybersecurity initiatives, but also including any new or otherwise unplanned cybersecurity matters, such as incidents of note or key regulatory developments. In any case, boards should ensure that the organisation promotes an effective corporate and organisational environment where significant cyber developments are readily and swiftly reported by the management.

b. Approval and periodic review of key programme documents

Cybersecurity policies and structures should be integrated at all levels of an organisation based on a proper risk assessment and the risk appetite of the organisation. Proper threat assessments must be conducted and the board can accordingly adopt relevant cybersecurity guidelines (possibly on the basis of standards that have been published by regulators or industry groups). Appointing a data compliance officer or a cybersecurity officer can ensure that all policies are up to date. It would also be useful and typically necessary to design incident management plans that are repeatedly exercised within the organisation. This subsection covers the following topics:

- policies, guidelines and standards;
- controls and procedures; and
- cyber crisis management plans.

1. Policies, guidelines and standards

Good cybersecurity does not solely depend on an organisation's IT department, but requires everyone in an organisation to play their part in ensuring that cybersecurity measures are properly executed.

---

55 Information and Cyber Security Guidelines, 2023 (Insurance Regulatory and Development Authority of India, 24 April 2023), https://irdai.gov.in/document-detail?documentId=3314780 [accessed 21 June 2023].

56 ISO 37301:2021, formerly ISO 19600:2014.

57 For an example of federal regulations, see 12 CFR Part 30, App B, wherein federal agencies require financial institutes to maintain information security programmes. For an example of a state regulation, see Cybersecurity Regulation 23 NYCRR s 500.04(b), wherein the New York State Department of Financial Services requires covered organisations to report on their cybersecurity programs.

58 *Cyber Security for the Board of Directors, Recommendation to Strengthen Cyber Security Competences* (Board Leadership Society Centre of Cybercompetences, December 2022), 16, https://bestyrelsesforeningen.dk/wp-content/uploads/2023/01/Cyber_Bestyrelsesvejledning_-FINAL-December-202246-Skrivebeskyttet.pdf [accessed 21 June 2023] (in Danish).

Therefore, cybersecurity measures should be integrated into an organisation's day-to-day functions, and all members of the organisation should be accountable for its implementation. Correspondingly, it is crucial that supervisory boards provide clear guidelines to management to provide oversight and accountability on:

- cybersecurity risks that should be managed;
- keeping abreast of technological and risk developments; and
- ensuring that an organisation's cybersecurity measures adequately address the cybersecurity risks identified.

Policy documents and management structures such as committees with designated cybersecurity functions can play an important role in establishing processes that will facilitate on-going compliance with cybersecurity requirements. Such policy documents and structures can also help organisations define and communicate to their staff members baseline requirements to be addressed.

These measures should also be proportionate to the sensitivity of the data handled by the organisation, as well as the criticality of the infrastructure.

In this regard, best practices guidelines across many jurisdictions have various common themes. For example:

- Boards should either conduct a risk assessment themselves to identify the possible weaknesses in their organisation's information security systems, or direct management to do the same.
- Following the risk assessments, organisations should then formulate appropriate treatment plans, IT security policies or other cybersecurity frameworks to address these threats.[59]
- To ensure that cybersecurity measures are well integrated into an organisation's functions, guidelines from the board should address both the technical aspect of cybersecurity risk management, and the people/behavioural aspect of cybersecurity risk management.[60]

Accordingly, boards should ensure that the organisation conducts the necessary risk assessments to identify weaknesses within their cybersecurity programmes, and should also provide management with guidelines to create a positive cybersecurity culture within the organisation to ensure that everyone plays their part in upholding cybersecurity standards. In Germany, for example, aside from ensuring that a thorough analysis of the cybersecurity risks an organisation faces is carried out, there is also an emphasis on creating a positive cybersecurity culture within an organisation.[61] This includes creating sustainable compliance awareness within the organisation through continuous messages from the board to its management and employees,[62] and developing IT security policies and processes that focus not only on technical solutions but also organisational framework conditions.[63]

---

59 *Cyber Security Toolkit for Boards* (National Cyber Security Centre, 2021), www.ncsc.gov.uk/files/board_toolkit_2021.pdf [accessed 21 June 2023], 25.

60 *Ibid*, 28.

61 *BSI-Standard 200-1 Information Security Management System (ISMS)* (Bundesamt Für Sicherheit in der Informationstechnik, October 2017), www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2001_en_pdf.pdf?__blob=publicationFile&v=2 [accessed 21 June 2023], 26.

62 *Ibid*, 22.

63 *Ibid*, 5.

As a result, it is advisable that the board ensures that cyber risks are addressed appropriately – and based on a proper risk assessment and identification of the organisation's risk appetite – in policies and processes for IT and physical security as well as digital behaviour, and that the board ensures that such policies are understood by the entire organisation and made an integral part of the culture of the organisation.

2. Controls and procedures

Boards must have at least a high-level understanding of the controls and procedures that are necessary to ensure that their organisations take to protect the key information assets and to ensure compliance with the necessary laws and/or regulations in relation to certain aspects of cybersecurity, like data protection or the protection of critical information infrastructure.

With regard to data protection, legislation across various jurisdictions has generally set out the following requirements:

- designate a data protection officer;
- develop and implement data protection policies and practices to demonstrate compliance with the relevant legislations or regulations; and
- establish procedures to ensure the relevant individuals and/or authorities are duly notified of data breaches.

Similarly, in relation to the protection of critical information infrastructure, relevant organisations must take appropriate and proportionate measures to ensure the security of their network and information systems. These organisations are also under an obligation to notify the relevant authorities in the event of a security breach. Senior management and the board are ultimately responsible for ensuring the entity has these policies and procedures in place and is following them.

The board should ensure that the organisation has designated a data protection officer or a cybersecurity officer to oversee the organisation's compliance with the relevant legislation and/or regulations. This officer should be involved in briefing senior management and the board on these issues. The data protection officer or cybersecurity officer should have relevant training and expertise, so that they may carry out their functions more effectively.

The board should make clear its expectation that management establish review cycles and feedback loops to ensure that policies and procedures are kept up to date to address new developments and changes to risk profile.

3. Cyber crisis management plan

As addressed above, it is essential that organisations have a cyber incident response or crisis plan and that they practice it in simulations. Cybersecurity incidents can often have a huge impact on an organisation's operations and reputation, such that the board should understand the organisation's response plan and either participate in or be briefed on the results of such response testing.

For example, in Singapore, it is recommended that these incident management plans should be practised in the presence of independent observers, so that they may provide feedback on areas of improvement.[64] In the UK, it is recommended that the board participates in these exercises, so that they can better understand how an incident can possibly impact their organisation.[65]

Whether or not the board participates directly in response testing, it should understand when it will be notified of an incident or suspected incident, and what its role will be related to the response. For example, regarding the potential payment of a ransom in a ransomware attack, many boards expect to be briefed on, and ask questions about, such a significant decision for the organisation, but do not believe it is the board's role ultimately to decide whether it is in the organisation's best interest to make a payment. Others may disagree strongly, or may operate in a very different regulatory environment in that regard. Either way, it is important that the board and management decide these lines of authority in preparation for, rather than during, an actual incident.

c. Board cyber expertise

Having a qualified cyber expert as a part of the board can improve the overall cybersecurity standing of an organisation. Alternatively, the board can engage with external experts who can help curate a bespoke cyber risk management plan for the organisation. Another useful measure can be appointing a cybersecurity or IT steering committee. This subsection covers the following topics:

- board member(s) with expertise;
- access to experts (external/independent); and
- appointment of steering committees.

1. Board member(s) with expertise

For effective and timely management of cybersecurity risks, corporate and organisational boards need relevant expertise to understand the critical impact on their businesses. However, there are concerns about:

- the availability of a very small pool of qualified candidates to draw from around the world; and
- whether a candidate with deep technical experience and focus could productively perform board service and associated duties without blurring the line between governance and management.

There are guidance documents and best practices from key jurisdictions that recommend boards of directors of organisations to have relevant expertise on cybersecurity:

- In Singapore, the Monetary Authority of Singapore recommends that boards consider including members with cybersecurity experience, since it might be difficult to involve an external party for all types of cybersecurity-related issues.[66] Alternatively, boards could also consider involving

64 *Statement of Good Practice – Cyber Security Risk Management* (Singapore Institute of Directors, 2020), www.sid.org.sg/images/PDFs/Codes/SGP16.pdf [accessed 21 June 2023].

65 *Cyber Security Toolkit for Boards* (National Cyber Security Centre, 2021), www.ncsc.gov.uk/files/board_toolkit_2021.pdf [accessed 21 June 2023].

66 *Technology Risk Management Guidelines* (Monetary Authority of Singapore, January 2021), www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf [accessed 21 June 2023].

individuals with the relevant expertise in sub-committees, like the audit or risk committee, to facilitate information reporting to the full board for further deliberation.

- In the US, best practice guides and handbooks recommend that the board or an appropriate board committee recruit cybersecurity/digital/IT expertise or engage additional experts to assist with oversight responsibilities. The NACD ISA Handbook references the example of a global organisation where the board-level technology committee includes directors who are experts in privacy and security from a customer perspective.[67] Another interesting development in the US is that the proposed draft Cybersecurity Disclosure Act of 2021 requires publicly traded companies to disclose in their mandatory annual reports to investors whether they have a cybersecurity expertise or experience on their board of directors and, if not, provide an explanation for why not.

Boards should consider having relevant cyber expert(s) on the boards or relevant committees, to set the right 'tone at the top' to help reduce cyber exposure by design. A cyber expert can understand the overall cyber landscape and probe the organisation's cyber compliance posture. If the board does not have such expertise, it should ensure – and be prepared to document – how it avails itself of sufficient outside expertise to advise on issues relevant to its oversight duties.

Other suggestions to consider range from developing an annual cyber curriculum of cyber briefings to providing ongoing training as well as using third-party assessments.[68]

2. Access to experts (external/independent)

The common theme emerging from surveyed jurisdictions indicates a positive attitude towards engaging with external, independent experts on cybersecurity-related matters. According to a World Economic Forum survey, '[s]tructured interactions between cyber and business leaders are becoming more frequent – 56 per cent of security leaders now meet monthly or more often with their board.'[69]

However, this consensus is marked by differing degrees to which such engagement is envisioned, in each jurisdiction.

Best practice guidelines across various jurisdictions have generally been established as follows:

- boards may consider engaging external independent experts on an ad hoc or retainer basis to brief the board on relevant issues, or to provide an independent perspective on the cybersecurity matters presented to the board;[70]
- expert engagement may comprise seeking expert opinion of external auditors, if the board considers that the internal audit's coverage, skills, capacity and capabilities is insufficient[71]; and

67 *Cyber-Risk Oversight Handbook* (NACD ISA, 2020), https://isalliance.org/isa-publications/cyber-risk-oversight-handbook publicly traded companies, 23.

68 Advanced Cyber Security Center Staff, *Leveraging Board Governance for Cybersecurity* (January 2019), https://www.acscenter.org/_files/ugd/75caa5_ba2f6d7768244a2c82a238fd91f4f3f6.pdf.

69 *Global Cybersecurity Outlook 2023* (World Economic Forum, January 2023), 4.

70 *Statement of Good Practice – Cyber Security Risk Management* (Singapore Institute of Directors, 2020), www.sid.org.sg/images/PDFs/Codes/SGP16.pdf [accessed 21 June 2023], 4–5.

71 *Prudential Practice Guide* (Australian Prudential Regulation Authority, June 2019), www.apra.gov.au/sites/default/files/cpg_234_information_security_june_2019_0.pdf [accessed 21 June 2023], 7 and 28.

- expert engagement may also take the form of technical experts formulating a bespoke cyber risk management plan.

Nevertheless, there are some challenges that hinder boards from working with external, independent experts. One may be that there is a severe shortage of cybersecurity professionals with requisite expertise,[72] thus experts are in short supply. This is more the case for developing countries like Uganda, where access to experts may be difficult as the area of cybersecurity is still developing. Another may be the challenges of cyber leaders to present security issues in terms that board-level executives can understand to allow business leaders to engage in operational cyber requirements to advance their organisations' overall cyber capabilities.

Even in the absence of any specific regulations or best practices in this regard, cooperation with external experts often will be necessary due to the board's obligation to make fully informed decisions.

3. Appointment of steering committees

An IT or cybersecurity steering committee is a group of high-level stakeholders overseeing and providing strategic guidance on how best to address cybersecurity threats and effectively govern the institution towards its stated vision and business objectives. In principle, the idea of appointing a steering committee is uncontroversial. However, across all ten surveyed jurisdictions (with the exceptions of India and Israel), there are no formal laws or best practice guidance on the appointment of steering committees.

In Israel, the finance ministry recommends that all institutional investors in Israel establish a steering committee on cybersecurity risk management. The committee is to convene quarterly to discuss the work plan and its execution, results of risk assessments and ways to reduce risks, draw conclusions from cyber incidents, and report the findings to the board.[73] The committee is headed by the CEO. Other members of the committee include the chief of IT, chief risk management officer and chief cyber defence officer (in small organisations, the CEO will replace the committee).[74]

In India, delegated legislation mandates the formation of an information security steering committee (ISSC) for an organisation which is declared by the state as crucial for the critical information infrastructure of the country. The committee comprises of higher management officials of the organisation, tasked with performing information security audits, approving information security policies, and planning, developing and reviewing remedial actions to mitigate and recover from malicious cyber incidents.[75] It is chaired by the CEO/managing director. Most interestingly, other members include a representative of the National Critical Information Protection Centre

---

72 Emil Sayegh, 'As the End of 2020 Approaches, the Cybersecurity Talent Drought Gets Worse', (*Forbes*, (24 September 2020), www.forbes.com/sites/emilsayegh/2020/09/22/as-the-end-of-2020-approaches-the-cybersecurity-talent-drought-gets-worse/?sh=23255a625f86; Robert Ackerman, 'Too Few Cybersecurity Professionals Is a Gigantic Problem for 2019' (*TechCrunch*, 27 January 2019), techcrunch.com/2019/01/27/too-few-cybersecurity-professionals-is-a-gigantic-problem-for-2019/ [accessed 21 June 2023].

73 *Institutional Entities Circular 2016-9-14, Cyber Risk Management in Institutional Entities* (Department of Capital Market, Insurance and Savings, Israeli Ministry of Finance)

74 Tal Kaplan et al, 'Israeli Ministry of Finance Issues Circular on Cyber-Security Risk Management' (Lexology, 22 September 2016), www.lexology.com/library/detail.aspx?g=8d60392f-a130-4c6b-b64e-334bd8ba7a51 [accessed 21 June 2023].

75 NCCIIPC Notification Rules, rule 2(1)(g) (Ministry of Electronic and Information Technology, 22 May 2018), www.meity.gov.in/writereaddata/files/NCIIPC-Rules-notification.pdf [accessed 21 June 2023].

(the national nodal agency for critical information infrastructure),[76] an official of the government, in every such steering committee. Further, the organisation may also nominate experts to the committee. The Rules provide an elaborate set of roles and responsibilities for the steering committee.[77]

Even absent formal regulatory requirements, management and boards should consider appointing a steering committee and establish a mechanism for timely communication of cyber incidents and share results of information security audits and compliance.

Management and boards can consider placing a cybersecurity group within a critical business activity or operation where significant cyber risks are involved. The placement can consider overall organisational structure, functions, interests and incentives for an effective determination of cyber risks.

Management and boards can consider developing in-house cyber expertise within their business operating units where there is greater risk in executing the business functions.

d. Ensuring adequate financial investment by the organisation in cybersecurity

While certainly a shared responsibility with management, the board should ensure that the organisation is making sufficient financial investments in cybersecurity. This subsection outlines some key measures relating to financial investment that organisations should consider implementing to achieve effective protection. Some recommendations include: earmarking a budget for cybersecurity that is distinct from the IT budget; training employees regularly on digital technologies and outsourcing; and having a clear understanding and internal awareness about potential expenses that can arise out of cybersecurity incidents.

Although no jurisdiction currently requires organisations to mandatorily earmark a specific budget for implementing cybersecurity initiatives,[78] when financial investment by the organisation in cybersecurity is lumped together with the IT budget, this often leads to vagueness in exact intended investment under the above-mentioned two areas.

1. Investment in training employees and culture

Employees are essential to ensure a high level of security. The explosive growth of phishing emails, malware and ransomware targeting management and employees calls for proper digital behaviour throughout the organisation.

Regarding investment in cyber awareness and training employees, best practice guidelines across various jurisdictions have generally established the following:

---

76 Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules 2013, rule 3(1), (Ministry of Electronic and Information Technology) https://www.meity.gov.in/writereaddata/files/GSR_19%28E%29_0.pdf [accessed 21 June 2023].

77 NCCIIPC Notification Rules rule 3(2) (Ministry of Electronic and Information Technology, 22 May 2018), www.meity.gov.in/writereaddata/files/NCIIPC-Rules-notification.pdf [accessed 21 June 2023].

78 While not a requirement, guidance by the Federal Reserve Bank in New York suggests that the board should devote sufficient attention to cybersecurity as it would to traditional financial market shocks such as liquidity shortages. See, for example, 'Thoughts on Cybersecurity from a Supervisory Perspective' (speech by Kevin Stiroh, Executive Vice President, Federal Reserve Bank of New York, 12 April 2019), www.newyorkfed.org/newsevents/speeches/2019/sti190412 [accessed 21 June 2023].

- Adequate and regular training of key personnel, as necessary, is a common recommendation found across many of the jurisdictions surveyed.[79] For this, businesses should identify what needs can be met in house *versus* what can or should be outsourced to third parties.[80]
- Training may include briefings, training sessions, workshops and e-learning modules, as well as reporting procedures for misconduct (whistleblowing systems) and suggestions for improvements to the compliance system (employee feedback).[81]

In the UK, a cybersecurity toolkit recommends: (1) training existing staff; (2) engaging external expertise; and (3) conducting outreach to students to develop future staff through trainings, apprenticeships or sponsorships.[82]

In Singapore, best practices highlight the importance of investing in training management and employees in relevant cybersecurity and digital skills. This helps to realise the full potential of technological gains and minimises cyber risks to the organisations.[83]

In Denmark, best practices guidelines highlight that the organisation's investment in cybersecurity training of the organisation's employees is one of the most important sources to a better cybersecurity culture and a higher level of cybersecurity.[84]

In the US, best practice guidance advocates for a separate cybersecurity budget as opposed to the traditional model of including it into the IT budget.[85]

As a result, it is advisable that the board ensures that the organisation maintains a training programme for members of the board, directors and other employees in relation to security and awareness training, and that the board – together with the executive management – actively contributes to a positive and appropriate cybersecurity culture in the organisation, where:

- a common security language is adopted throughout the organisation;[86]
- security can be discussed openly; and
- employees can report mistakes and security breaches if and as they may happen.

---

79 For the US, see New York Department of Financial Services Cybersecurity Resolution 23 NYCRR Part 500 (2017), section 500.10, and more importantly section 500.14, at www.governor.ny.gov/sites/default/files/atoms/files/Cybersecurity_Requirements_Financial_Services_23NYCRR500.pdf [accessed 22 June 2023]; and FTC's Red Flag Rules (CFR s 681.1), section (e)(3), www.ecfr.gov/current/title-16/chapter-I/subchapter-F/part-681/section-681.1 [accessed 22 June 2023]. For India, see *IRDAI Information and Cyber Security Guidelines* (2023), https://irdai.gov.in/document-detail?documentId=3314780 [accessed 22 June 2023].

80 *The Financial Impact of Cyber Risk* (American National Standards Institute, 2008), https://isalliance.org/publications/the-financial-impact-of-cyber-risk-50-questions-every-cfo-should-ask [accessed 22 June 2023], as referenced in the *NACD ISA Cyber-Risk Oversight Handbook* (2020), https://isalliance.org/isa-publications/cyber-risk-oversight-handbook [accessed 22 June 2023], 26–27.

81 In Germany, ISO 19600's recommendations mention elements of cybersecurity governance and, more particularly, employee training.

82 *Cyber Security Toolkit for Boards* (National Cyber Security Centre, 2021), www.ncsc.gov.uk/files/board_toolkit_2021.pdf [accessed 22 June 2023].

83 *Statement of Good Practice – Cyber Security Risk Management* (Singapore Institute of Directors, 2020), www.sid.org.sg/images/PDFs/Codes/SGP16.pdf [accessed 22 June 2023].

84 *Cyber Security for the Board of Directors, Recommendation to Strengthen Cyber Security Competences* (Board Leadership Society Centre of Cybercompetences, December 2022), https://bestyrelsesforeningen.dk/wp-content/uploads/2023/01/Cyber_Bestyrelsesvejledning_-FINAL-December-202246-Skrivebeskyttet.pdf [accessed 22 June 2023], 48 (in Danish).

85 See, for example, *The Financial Impact of Cyber Risk* (American National Standards Institute, 2008), https://isalliance.org/publications/the-financial-impact-of-cyber-risk-50-questions-every-cfo-should-ask, as referenced in the *NACD ISA Cyber-Risk Oversight Handbook* (2020), https://isalliance.org/isa-publications/cyber-risk-oversight-handbook [accessed 22 June 2023], 26–27.

86 According to a World Economic Forum survey, 'Building a security-focused culture requires a common language based on metrics that translate cybersecurity information into measurements that matter to board members and the wider business'. *Global Cybersecurity Outlook 2023*, January 2023, 4.

2. *Investment in technology*

Businesses should update or replace outdated systems and regularly update software security to ensure it remains compliant with the information security policy framework.[87] Also, businesses should invest in updating or replacing old legacy systems and legacy IT infrastructure.[88]

For example, in the US, best practice guides and reports recommend adapting and adopting new technologies like AI, cloud configuration, blockchain, the IoT, or quantum computing.[89] In Singapore, boards are also advised to invest in automated technology to increase the efficacy of security operations.[90]

In the EU, the upcoming NIS2 Directive will require a wide range of organisations to take 'appropriate and proportionate measures' to manage the risks to their network and information systems. This includes allocating appropriate resources to cybersecurity, including funding, staffing and technology investments.

Earmarking a specific percentage of the organisation's expenditure towards cybersecurity, distinct from the IT budget, may be desirable for organisations of a particular size and for those operating in particular sectors such as financial and banking sectors, etc.

Management and boards may consider establishing a set process to formally discuss and estimate potential expenses associated with cybersecurity incidents as part of the budgeting process. Also, a budget process for requesting additional cybersecurity staff to the cybersecurity strategy may be warranted.[91]

87 For an example from Australia, see *Prudential Standard 234*, (Australian Prudential Regulation Authority, July 2019), www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf [accessed 22 June 2023], 17–18. For an example from the US, see *Leveraging Board Governance for Cybersecurity* (Advanced Cyber Security Center, 2019), For an example from the United States, see Advanced Cyber Security Center Staff, *Leveraging Board Governance for Cybersecurity* (January 2019), p. 23, https://www.acscenter.org/_files/ugd/75caa5_ba2f6d7768244a2c82a238fd91f4f3f6.pdf, p. 25.

88 *Leveraging Board Governance for Cybersecurity* (Advanced Cyber Security Center, 2019), Advanced Cyber Security Center Staff, *Leveraging Board Governance for Cybersecurity* (January 2019), https://www.acscenter.org/_files/ugd/75caa5_ba2f6d7768244a2c82a238fd91f4f3f6.pdf.

89 Principle 4, *Cyber-Risk Oversight Handbook* (NACD ISA, 2020), https://isalliance.org/isa-publications/cyber-risk-oversight-handbook/ [accessed 22 June 2023].

90 *Statement of Good Practice – Cyber Security Risk Management* (Singapore Institute of Directors, 2020), www.sid.org.sg/images/PDFs/Codes/SGP16.pdf [accessed 22 June 2023].

91 *Cybersecurity Assessment Tool* (FFIEC, May 2017), www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf [accessed 22 June 2023].

VI. Trends in national and sectoral governance requirements

Beyond the 'best practices' described above, there are several notable regulatory trends in cyber governance.

Common themes of these requirements include the designation of a particular individual to be ultimately responsible for managing cybersecurity risks of the organisation. For example, the highly influential New York Department of Financial Services' Cybersecurity Regulation, one of the first comprehensive cybersecurity regulations in the world, requires that the entities it regulates 'shall designate a qualified individual responsible for overseeing and implementing the covered entity's cybersecurity programme and enforcing its cybersecurity policy (for purposes of this Part, chief information security officer or CISO)'.[92]

Similarly, following the Colonial Pipeline cyber incident discussed above, the US imposed specific requirements on pipeline operators to designate a 'Cybersecurity Coordinator' to be available to regulators.[93] This trend is beginning to take root outside of the US as well. In Singapore, for example, the Monetary Authority has issued guidelines providing that '[t]he board of directors and senior management should ensure a Chief Information Officer, Chief Technology Officer, or Head of IT, *and a Chief Information Security Officer* or Head of Information security ... are appointed.'[94]

Reflecting another trend, the same New York cyber regulation requires that the chief information security officer report in writing at least annually to the regulated entity's board of directors or equivalent governing body regarding the entity's cybersecurity programme and material cybersecurity risks, including the overall effectiveness of the cybersecurity programme. A senior officer or the board of the organisation must then annually certify the organisation's compliance with the regulation.[95] An expectation by regulators of upward reporting of cyber risk management issues to senior management and the board is therefore another trend of note.

Since at least 2018 when it issued guidance on the subject, the SEC has indicated it expects board involvement in the oversight of material cyber risks faced by public companies.[96] Although the guidance was couched in terms of required disclosure of material cybersecurity risks, the SEC's mention of requiring companies to disclose the extent of the board's role in overseeing material cyber risks to public companies made its expectation clear on this point. Similarly, the Australian Prudential

92 Cybersecurity Requirements for Financial Services Companies, 23 NYCRR Section 500.4(a).

93 *DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators* (Department of Homeland Security, 27 May 2021), www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators [accessed 22 June 2023].

94 *Technology Risk Management Guidelines* (Monetary Authority of Singapore, January 2021), www.mas.gov.sg/-/media/mas/regulations-and-financial-stability/regulatory-and-supervisory-framework/risk-management/trm-guidelines-18-january-2021.pdf [accessed 22 June 2023] (emphasis added).

95 Cybersecurity Requirements for Financial Services Companies, 23 NYCRR Section 500.17 and Appendix A.

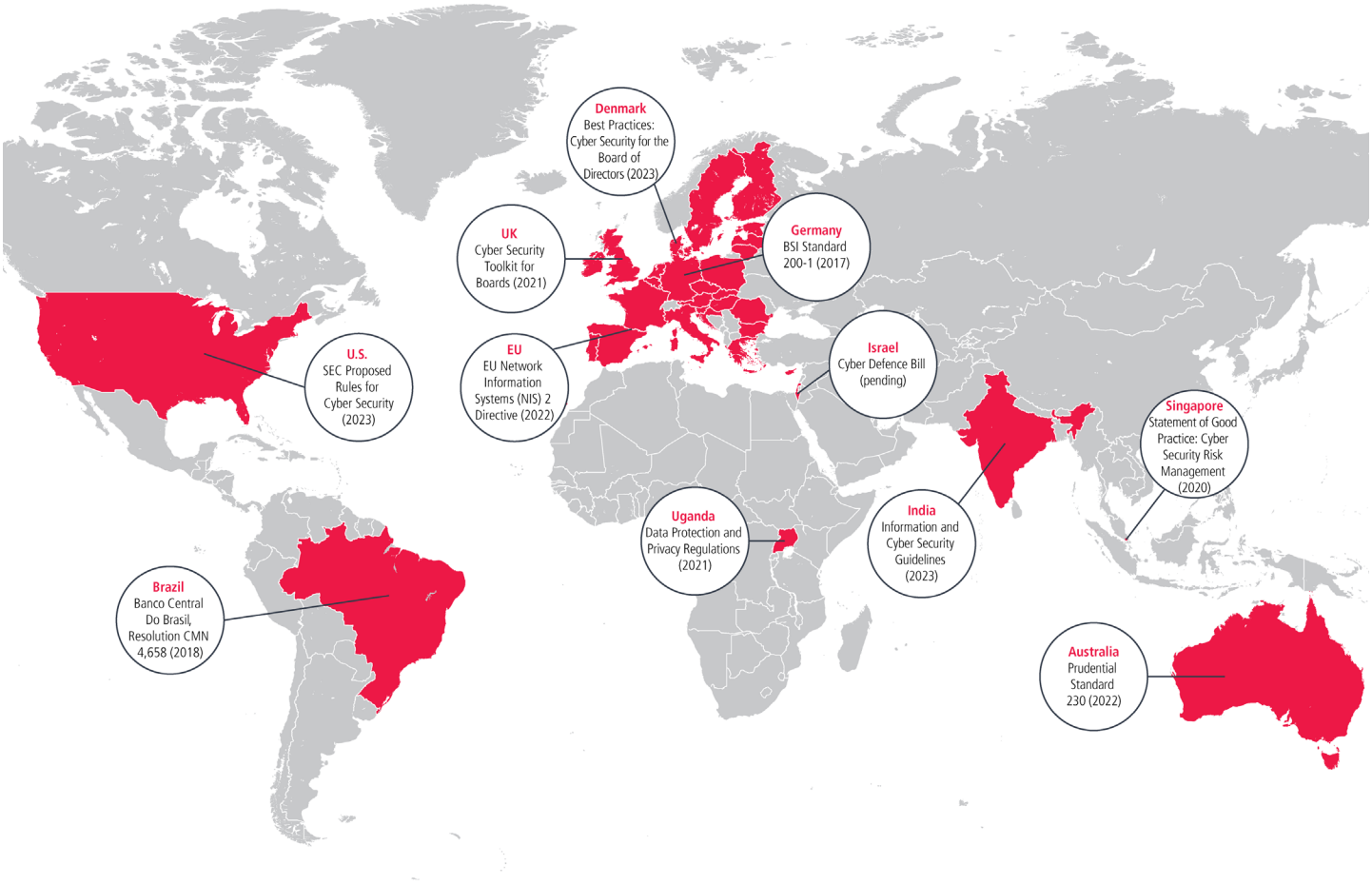
96 *Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release Nos. 33-10459; 34-82746* (Securities and Exchange Commission, 21 February 2018), 17–18.

Regulation Authority issued Information Security Standards that make it the responsibility of the board of a regulated entity to ensure the entity maintains information security policies.[97]

We summarise below a much more detailed list of suggested senior management and board practices regarding managing cyber risks, and this list is informed in part by the changing regulatory landscape on these issues.

97 Prudential Standard 234 (Australian Prudential Regulation Authority, July 2019), www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf [accessed 22 June 2023].

Key cybersecurity law/regulation/guidance from selected jurisdictions represented in the Task Force



Australia: Prudential Standard 230 (2022) Makes boards of covered entities directly accountable for oversight of operational risk management.

Brazil: Banco Central Do Brasil, Resolution CMN 4,658 (2018) Requires covered financial institutions to enter into agreements requiring third-party providers comply with notification and disclosure obligations.

Denmark: Best Practices: Cybersecurity for the Board of Directors (2023) Recommends boards receive and address an updated cyber risk assessment based on the company's most important assets.

European Union: Directive (EU) 2022/2555, also known as Network Information Systems (NIS)2 Directive (2022) Aims to create a higher common level of cybersecurity. EU Member States have until 17 October 2024 to incorporate NIS2 Directive into national law. Directive (EU) 2016/1148, also known as the NIS1 Directive (2016), has been repealed by NIS2 Directive. **EU Regulation 2022/2554, known as the Digital Operational Resilience Act (DORA)** Creates a cybersecurity regulatory framework in the financial services sector for the EU and will be applicable from 17 January 2025.

Germany: BSI Standard 200-1 (2017) Provides management principles, including key duties of management in achieving information security.

India: Information and Cyber Security Guidelines (2023) Provides that boards must approve the overall framework of cybersecurity policy and strategy.

Israel: Cyber Defence Bill (pending) Requires boards in certain organisations to discuss cyber risks, resources, and governance.

Singapore: Statement of Good Practice Cyber Security Risk Management (2020) Recommends establishing risk management protocols for information security management systems.

Uganda: Data Protection and Privacy Regulations (2021) Establishes a Personal Data Protection Office and obligations for data controllers.

UK: Cyber Security Toolkit for Boards (2021) Recommends boards participate in incident response exercises.

US: SEC proposed rules for cybersecurity (2023) Requires registrants to disclose material cybersecurity incidents within four business days.

Figure 1. Key cybersecurity law/regulation/guidance from selected jurisdictions represented in the Task Force.

VII. Trends in liability risks to directors and officers

The threat of individual liability of directors and senior executives for failure to institute or maintain adequate cybersecurity is at most just starting to emerge. Due to a lack of specific laws in many jurisdictions addressing cyber and information security obligations of organisations, one of the ways directors may be found liable for poor cybersecurity governance (whether constituting a breach of other legislation or otherwise) is through a breach of general directors' duties.

In Australia, for example, the Corporations Act 2001 (Cth) imposes broad duties on directors and officers to exercise powers with due care and diligence, act in the best interests of the organisation, and ensure they do not improperly use information. However, it is not explicit in the legislation whether these duties extend to cyber and information security risks. Most countries have a similar 'Companies Act,' which contains directors' duties with similar wording. While a failure to ensure an organisation adequately addresses cybersecurity risks may result in a breach of such duties, uncertainty remains.

Another potential avenue for directors to be personally liable is through a breach of a director's supervisory duties, particularly when organisations have specific obligations to establish security measures against cybercrime. In Germany and Denmark, a representative of a business or organisation may commit an administrative offence if they intentionally or negligently fail to put in place the supervisory measures required for preventing illegal conduct in the organisation or by the organisation (section 130(1)–(3) *Administrative Offence Act* (OWiG)). As the laws and regulations dealing with cyber and information security frequently do not impose specific requirements on how senior management should address cyber risks, a breach of such duties is harder to establish.

Many countries, such as Israel and India, are also beginning to adopt international cyber and information security standards. As a result, corporations operating in those countries may be liable for a failure to have systems and processes in place to manage cyber and information security incidents even in the absence of primary legislation. Such standards are arguably sufficient to make specific organs, such as the board, liable for not following through with responsibilities listed in secondary legislation and guidelines.

a. Closest liability scenarios thus far

Most cyber and information security legislation that does exist provides for enforcement mechanisms (such as powers of investigation) by the relevant authority. The legislation may also set out offences in respect of breaches of particular provisions. Across the various laws and regulations, liability of directors can result in administrative fines, as well as criminal convictions in more serious cases. The personal liability which may be imposed on directors depends on the specific legislation in each country.

Administrative fines are the most common forms of liability for directors, as is the case in the EU. However, criminal liability can also arise in some circumstances. In Singapore, for example, the Personal

Data Protection Act 2012 (No 26 of 2012) (PDPA) does not provide any offences for which directors will be liable that arise from cybersecurity incidents. Directors do, however, have a duty to cooperate with the Commissioner when it exercises its investigatory powers following a cyber and information security incident. If directors do not comply with their duty to co-operate, personal liability can arise. Consequently, either a fine or imprisonment can be imposed (section 51(3)–(4) of the PDPA).

While there is the potential for fines, penalties and imprisonment to be imposed on directors, there are very few instances where they have been applied in practice. One reason is that current regulations primarily target the entities themselves. It is not until organisations are found to be in breach that individual directors and officers are scrutinised. There is, however, a general trend towards imposing greater responsibility on directors.

In the US, in a recent shareholder derivative suit brought against Marriott and its board in connection with a 2018 data breach, a Delaware court granted the defendant's motion to dismiss, but, in doing so, strongly endorsed the notion that directors were responsible for cybersecurity oversight, stating that '[t]he corporate harms presented by non-compliance with cybersecurity safeguards increasingly call upon directors to ensure that organisations have appropriate oversight systems in place'.[98] More generally, non-cyber case law from Delaware indicates that if the board does not engage in good faith with a particular risk issue, it may lose the benefit of the doubt that it exercised its duty of care (under the US 'business judgment rule' in *Caremark*). For example, where the board fails to ensure the establishment of a compliance programme or, once one is established, fails to oversee and ensure ongoing compliance, it may lose protection of the business judgment rule.[99]

In addition, while US regulators have mostly brought enforcement actions in connection with cybersecurity-related failures and misconduct against the organisation itself,[100] regulators are beginning to impose greater responsibility on directors and senior officers themselves. For example, the New York State Department of Financial Services (NYSDFS), an influential state-level regulator of financial services, requires that the boards or senior officers of covered organisations certify that their institution is in compliance with cybersecurity requirements set out by the NYSDFS.[101]

b. Other practical implications of a governance failure

In addition to legal liability, there are practical implications for not being compliant or sufficiently engaged with issues of cyber and information security. For example, businesses may experience increased rates, reduced coverage terms, and even non-renewals from insurers who want to reduce

98 *In re Marriott International Inc.*, CA No 2019-0965-LWW (Del Ct Chancery, 5 October 2021).

99 For example, in *Marchand*, a Delaware court reinstated shareholder derivative claims against the directors of an ice cream company who allegedly failed to implement an adequate compliance system for monitoring and reporting 'mission critical' issues (in that case, food safety). *Marchand v Barnhill*, 212 A 3d 805 (Del 2019). Similarly, in *Clovis*, the board of an oncology company faced a shareholder derivative suit alleging their breach of fiduciary duty for failure to adequately oversee clinical trials and public disclosures related to a new lung cancer drug. The Delaware court denied the defendants' motion to dismiss, holding that directors 'must make a good faith effort to implement an oversight system and then monitor it.' *Clovis Oncology, Inc. Derivative Litigation*, CA No 2017-0222-JRS, Memorandum Opinion (1 October 2019). The case ultimately settled.

100 See, for example, the cease and desist order from *In the Matter of Atlaba Inc., f/d/b/a Yahoo! Inc.*, Admin Proc No 3-18448 (24 April 2018) (the SEC imposed a $35m penalty on Yahoo! successor Altaba, for failing to timely disclose a data breach) and the consent order from *In the Matter of Capital One*, AA-EC-2015-48 (insight into how the US Treasury Office of the Comptroller of the Currency expects regulated entities to implement 12 CFR, Part 30).

101 23 NYCRR 500, Cybersecurity Requirements for Financial Services Companies (New York State Department of Financial Services, March 2017), www.governor.ny.gov/sites/default/files/atoms/files/Cybersecurity_Requirements_Financial_Services_23NYCRR500.pdf [accessed 22 June 2023].

their cyber incident risk.[102] Cyber insurance underwriters now have a focus on data security controls when evaluating risk, and are likely to require evidence of at least some preventive controls such as multi-factor authentication (MFA), remote desktop protocol (RDP), data backup practices, segregation of networks, encryption, patch management, privileged account management (PAM), employee training and a host of others. Businesses lacking these preventative controls may face carriers refusing to quote on insurance cover, or to demand significant rate increases, limited capacity and possible coverage restrictions.

The different approaches that countries have taken in regards to liability of directors for cyber and information security largely depends on the level of technological advancement and the extent to which cyber attacks have been experienced in the relevant country. For example, Uganda has made limited progress in developing a cybersecurity governance framework[103] (and consequently holding directors responsible for cyber incidents). While technological limitations are partly responsible for this, it is predominantly due to inadequate capacity of investigatory authorities, the judiciary, and the government bodies charged with addressing cybersecurity risks.

c. Emerging themes related to director and officer responsibilities for cybersecurity

1. Directors and officers need to be more proactive

Jurisdictions are increasingly focused on requiring directors to be proactive in addressing cyber risks. Common actions taken by organisations and directors are reactive – for example, mitigating harm and loss after a cyber attack. Regulators are increasingly looking for organisations to enact measures and strategies to prevent cyber attacks from occurring and allow organisations to keep up with the evolving nature of cyber risks. As a result, directors will not only face potential liability for an organisation's failure to adequately address a cyber incident when it occurs, but may face liability for a failure to ensure the organisation regularly updates its processes to safeguard against future risks. This may require directors to ensure cyber risk assessments are regularly undertaken along with other preventative steps such as penetration tests. Additionally, many countries are seeking to place obligations on directors and officers to ensure the organisation develops a culture of data protection and cyber and information security awareness.

2. Inadequate cyber expertise

A further limitation expressed across all jurisdictions is that directors and officers frequently do not possess adequate cyber expertise. Public awareness of cyber and information security threats is increasing due to media coverage on the growing threat of cyber attacks. As a result, more organisations are setting up cyber risk management systems. There is still, however, a need for many organisations to outsource or use external cyber experts to assist in managing cyber and information security.

---

102 Robyn Adcock. 'Cyber Risks, Business Insurance & Risk Market Update' (Gallagher, 31 May 2022), www.ajg.com/au/news-and-insights/2022/may/adapting-your-risk-management-protections-to-match-evolving-cyber-cover/ [accessed 22 June 2023].

103 See, for example, Uganda's Data Protection and Privacy Regulations (2021), https://pdpo.go.ug/media//2022/03/Data_Protection_and_Privacy_Regulations-2021.pdf [accessed 22 June 2023].

3. *Lack of clear regulation and case law*

Finally, there is very little case law and jurisprudence that can assist in expressly identifying directors' and officers' duties or responsibilities in relation to cybersecurity. Case law has often focused on addressing issues that arise in an isolated manner, and therefore does not provide a solid and unified understanding about the subject. One of the biggest questions that is yet to be settled is whether breaching a binding guidance can lead to a breach of a statutory duty and consequent civil liability for directors. Most class actions following cyber incidents are founded primarily on breaches of privacy and data protection legislation and on negligence theories of liability.

Further, most litigation addressing breaches of cyber-related legislation has been brought against the organisations themselves and not against individual directors. An exception is the US, where there have been several cases brought under the *Caremark* standard seeking to hold directors personally liable for failure to monitor and prevent data breaches.[104] While none of the cases have yet survived the motion to dismiss phase, courts have acknowledged that, while not enough to meet the *Caremark* standard of 'consciously failing to act,' boards in certain cases 'probably should have done more' to defend against data breaches.[105]

Therefore, based on judgments so far, liability is rarely attributed to directors and officers for a failure to address cyber risks, provided they act according to the description of their duties (which often do not include express obligations in relation to cyber and information security).

104 See, for example, *Palkon v Holmes*, No 2:14-CV-01234, 2014 WL 5341880 (DNJ, 20 October 2014); *In re The Home Depot Inc.*, 2016 WL 6995676 (ND GA, 30 November 2016).

105 *In re The Home Depot Inc.*, 2016 WL 6995676, at 18 (ND GA, 30 November 2016).

VIII. Summary of recommendations

Our analysis of the laws, guidance, and best practices in various jurisdictions leads to a series of key considerations for senior executives and boards of directors, summarised here in as actionable a format as possible. We encourage lawyers to become advocates for a strong cybersecurity risk governance programme at their firms and when advising their clients. We hope that this list will prove useful to them, their senior management colleagues, and ultimately to the board of directors, in deciding where to focus these efforts.

- Understand the cyber risk profile of the organisation:
    - Senior management and board should receive briefings on the significant internal and external cybersecurity risks to the key information assets of the organisation.
    - Briefings should take into account sector- and business-specific risks, as well as jurisdictional and geopolitical risks.
    - It is important also to understand key supply chain and other third-party risks, even if the impact to the organisation is indirect.
    - Larger organisations should maintain a 'risk register' or similar chart of significant cyber risks to the organisation and what controls are in place or planned to counter each such risk.
    - Briefings should periodically be conducted by outside experts, who may bring a broader range of experiences than the internal team.
    - Larger organisations should consider joining sector-specific threat intelligence sharing organisations, as well as receiving law enforcement cyber risk alerts.
    - Larger organisations should consider threat monitoring services, including dark web monitoring, to try to identify emerging threats to their organisations before they materialise.
- Understand the key information assets to protect:
    - Senior management and the board need to know what the key systems and data are of the organisation, in order to assess the risk choices regarding their protection. Developing and implementing a data governance framework is a critical means to reducing cyber risk.
    - Assessment of key assets must include third parties holding sensitive data, or operating or accessing important systems of the organisation.
    - Information assets change with business acquisitions, technology migrations, significant new software changes and other important developments; they should therefore should be reassessed when significant changes occur. The age and health of IT infrastructure should also be monitored.
- Understand significant regulatory requirements:

- It is imperative that senior management and the board understand what regulators expect of the organisation, in the form of both regulations and guidance.
- Compliance alone will not ensure adequate cybersecurity: compliance is just one foundational component of the cyber risk management programme.
- The organisation's investments in cybersecurity should be informed by regulatory trends to future-proof efforts where possible, and to maximise the value of investments made in the cyber programme.
- Specialised legal expertise around cybersecurity and data protection laws, often separate from data privacy expertise, is increasingly in demand for many organisations, so that senior management and board should ensure they have the right expertise available to address evolving legal demands in this area.

- Determine the appropriate risk tolerance of the organisation:
  - There is no one cybersecurity standard that is appropriate for all organisations; instead, standards are chosen based on risk profile and a determination of risk tolerance.
  - Senior management and the board should consider, among other things, the reputational risks associated with a cybersecurity incident; the expectations of customers, regulators, and other stakeholders; and how the organisation wants to be positioned in the market vis-à-vis competitors.
- Understand what cybersecurity standards the organisation is using:
  - Senior management and the board should understand the rationale for the organisation's chosen cybersecurity standard(s), to ensure that they are appropriate based on the nature of the business, regulatory requirements and other risk considerations.
  - The choice of cybersecurity standards should be assessed from time to time as standards and expectations evolve; each periodic cyber risk assessment is a good opportunity to assess whether the existing standards are appropriate.
- Ensure appropriate risk decisions on protecting key information assets:
  - Senior management and the board should receive an explanation from the senior technical leadership regarding the organisation's strategy for protecting key systems and data.
  - Risk decisions should account for third-party cyber risks, including supply chain risks.
- Ensure periodic risk assessments are conducted:
  - The organisation should conduct regular cyber risk assessments including assessments led by outside experts who can provide an independent point of view.
  - Assessments should be customised to the organisation's risk profile and risk tolerance, as well as the chosen cybersecurity standard(s) to which it adheres.
  - Assessments should also benchmark against competitors or other similar organisations based on size, complexity and risk profile.

- It is essential that recommendations arising from a risk assessment be appropriate and realistic for the organisation, and that the organisation documents which recommendations it will follow and, for those it will not, why it believes they are unnecessary based on risk profile, compensating controls, or other factors.

- Understand who 'owns' cybersecurity and cyber risk management:
  - It should be clear who is responsible for managing cybersecurity at the organisation; increasingly, regulators expect organisations to have a chief information security officer or equivalent senior 'first line' role.
  - For larger organisations, there is often a 'second line' risk management role, such as a chief risk officer, whose responsibilities include assessing and tracking cyber risks to the organisation.
  - Likewise, larger organisations typically have a 'third line' audit function to confirm adherence to policies and procedures.
  - Legal and compliance personnel also have an important role in cyber risk management, and increasingly rapid regulatory reporting requirements concerning cyber incidents means that compliance, legal and information security must be in close coordination in the early stages of an incident.
- Ensure the board has sufficient cybersecurity expertise:
  - The board cannot meaningfully oversee cyber risk management of the organisation without sufficient expertise to understand and assess the issues.
  - Regulators increasingly require boards either to have cyber expertise directly on the board through at least one or two directors, or to avail itself of outside experts in supplement its knowledge as needed.
- Ensure management has sufficient cybersecurity expertise:
  - For many organisations, it is not enough that the 'IT department' also handle cybersecurity issues; larger organisations are generally expected to have a separate information security function devoted to such issues.
  - As noted above, regulators increasingly expect that larger organisations have a chief information security officer responsible for all cybersecurity issues for the organisation.
  - Management and the board must ensure that the person responsible for cybersecurity for the organisation has the right mix of technical and leadership skills for such a demanding role.
  - Beyond cybersecurity leadership personnel, the organisation should have sufficient depth and breadth of expertise in other cyber-related functions, including sufficient specialised vendor resources, identified to supplement the internal cyber team as needed in an incident or with large technical projects.

- As noted above, specialised cybersecurity and/or data protection legal counsel are increasingly needed, whether in-house or through outside counsel, and senior management and board should ensure the organisation has these resources identified as needed.

- Invest sufficient funds to meet cybersecurity goals:
  - Senior management and the board should ensure that cybersecurity expenditures are appropriate for the size, complexity, and risk profile of the organisation.
  - Periodic cyber risk assessments, as noted above, should include benchmarking relative to expenditures by similar organisations, to the extent possible.
  - Cyber insurance, although typically expensive, should at least be seriously considered by management and the board as they assess the organisation's particular cyber risks and what investment in the cyber programme is needed to offset them.
- Understand the cybersecurity testing and training programme and review results:
  - Senior management and the board should understand the types of cybersecurity testing that the organisation is conducting and be briefed periodically on the results of significant tests.
  - Testing should include periodic incident simulations, such as 'tabletop' exercises in which the organisation practices its response to a cyber incident. Senior management and the board should be briefed on the results of these exercises and should participate in them periodically.
  - Senior management and board should also ensure that all employees and contractors with access to systems and data of the organisation receive at least annual cybersecurity training, and are periodically tested through 'phishing tests' and other simulations to ensure they are being careful and vigilant.
- Ensure senior management and board receive regular updates:
  - The board may delegate initial responsibility for cyber risks and risk initiatives to a committee of the board, but the full board should be briefed at least periodically on these issues.
  - The board should, for example receive updates on the progress of risk reduction efforts and technology changes (such as a migration to a cloud environment), as well as updates on emerging cyber risks.
- Ensure appropriate reporting lines so that cyber risks are raised to leadership:
  - Cyber briefings to the board should be done directly by the individual(s) directly responsible for managing cybersecurity, such as the chief information security officer, rather than being filtered through a non-security role.
  - Regulators increasingly expect reporting lines that minimise the risk of cybersecurity risks being suppressed or under-represented in reporting to the board.
- Assess changes in cyber risk posture caused by business developments:
  - Because cyber risks are constantly fluctuating, it is important that management and board ensure these risks are reassessed appropriately as significant changes occur.

- New business ventures, mergers and acquisitions, new cyber infrastructure, and significant regulatory and geopolitical changes are examples of developments that may warrant reassessment of the organisation's cyber risk posture.

- Review, understand, and test the organisation's cyber incident response plans:
  - Senior management and board should ensure that the organisation has an actionable cyber incident response plan (IRP) at the enterprise level.
  - Rather than mere technical playbooks, the enterprise cyber IRP should include the roles of other functions related to cyber incidents, including legal, communications, compliance, and senior leadership and the board.
  - The cyber IRP should include classification and escalation procedures for particular cyber incidents or suspected incidents, and should clearly define roles and responsibilities of the various response teams.
  - The organisation should periodically practice responding to mock cyber incidents, using its cyber IRP, and should adjust its response plans as needed.
  - With the rise of ransomware and other cyber attacks that cause operational disruptions beyond the breach of data, management and board should ensure that the organisation has appropriate cyber-specific business continuity and disaster recovery plans, including backups of its data, contingency plans for its business operations, and alternative communications methods in case needed.

- Oversee the response to significant incidents:
  - Senior management and board should oversee the response to significant cybersecurity incidents. This should be reflected in the organisation's cyber incident response plan.
  - What types of incidents and at what levels of severity should be raised to senior leadership will depend on the particular organisation, but these considerations should be discussed, agreed upon and reflected in the incident response plan.
  - For lower-level incidents not escalated to senior leadership, senior management and board may wish to receive periodic statistical reports concerning the number of such incidents and any overall trends of note to the organisation.

IX. Contributions and acknowledgements

The IBA Presidential Task Force on Cyber Security is pleased to present the report *Global perspectives on protecting against cyber risks: best governance practices for senior executives and boards of directors.*

The report is made possible through the efforts and expertise of the Co-Chairs and globally situated Members of the IBA Presidential Task Force on Cyber Security. Their active engagement enabled cross-country data collection and facilitated in-depth comparative analysis and resulting conclusions. The Task Force's significant contribution to the report is sincerely acknowledged.

Members of the IBA Presidential Task Force on Cyber Security:

Søren Skibsted, Co-Chair (Kromann Reumert, Denmark)

Luke Dembosky, Co-Chair (Debevoise & Plimpton, US)

Sara Carnegie (IBA Legal Policy & Research Unit, UK)

Anurag Bana (IBA Legal Policy & Research Unit, UK)

Kate Macmillan (Herbert Smith Freehills, UK)

Marc Hilber (Oppenhoff, Germany)

Harriet Pearson (Hogan Lovells, US)

Anne-Marie Allgrove (Baker McKenzie, Australia)

Anthony Borgese (Minter Ellison, Australia)

Chung Nian Lam (Wong Partnership, Singapore)

Arye Schreiber (MyEDPO, Israel)

Olive Nancy Kwaga (CTI Africa, Uganda)

Thiago Sombra (Mattos Filho, Brazil)

Christel Teglers (Kromann Reumert, Denmark)

Special thanks to Ned Terrace and Michael Pizzi of Debevoise & Plimpton (US), for their invaluable efforts in consolidating and reviewing the report.

Special thanks to the IBA Legal Policy & Research Unit for driving the project, and to its Legal Interns – Sushant Khalkho, Charlotte White, Harriet Watson and Amna Shabbir – for their important contributions through their research work on this project.

Sincere gratitude and appreciation to Robert Silvers (US Department of Homeland Security) as the keynote speaker and to the panellists Justin Greis and Brian Kelly (McKinsey & Company), Jordan Kelly (FTI Consulting), Ian Paul McDougall (LexisNexis) and Brenton Steenkamp (EY Advisory), who participated and contributed in the cybersecurity showcase session at the IBA 2022 Annual Conference in Miami.

Special mention to Andy Serwin and Ross McKean (DLA Piper), Ahmed Baladi and Stephenie Handler (Gibson Dunn), Paul Pittman and Detlev Gabel (White & Case), Marcy Wilder (Hogan Lovells), Nazar Chernyavsky (Sayenko Kharenko), Alexis Collins (Cleary Gottleib) and Martin Schirmbacher (Haerting) for their participation and contribution in the brainstorming sessions in preparation for the project initiative.

Sincere thanks to Peter Bartlett, the immediate past chair of the Legal Practice Division for initiating and supporting the project and to the Technology Law Committee for their support throughout.

This report is an important tool, and a meaningful statement of the IBA's commitment to the issues of corporate and organisational cybersecurity. In this context, immense gratitude to the immediate past IBA President Sternford Moyo for establishing the Task Force, and to his successor as President, Almudena Arpón de Mendívil Aldama, for supporting its work and mission.

Appreciation and gratitude also to the various teams at the IBA London Office who assisted with this project in various forms: Divisions; Content; Production; Marketing; Membership and the Press Office.

the global voice of
the legal profession®

International Bar Association

Chancery House, 53-64 Chancery Lane,
London WC2A 1QS, United Kingdom
Tel: +44 (0)20 7842 0090
Website: www.ibanet.org