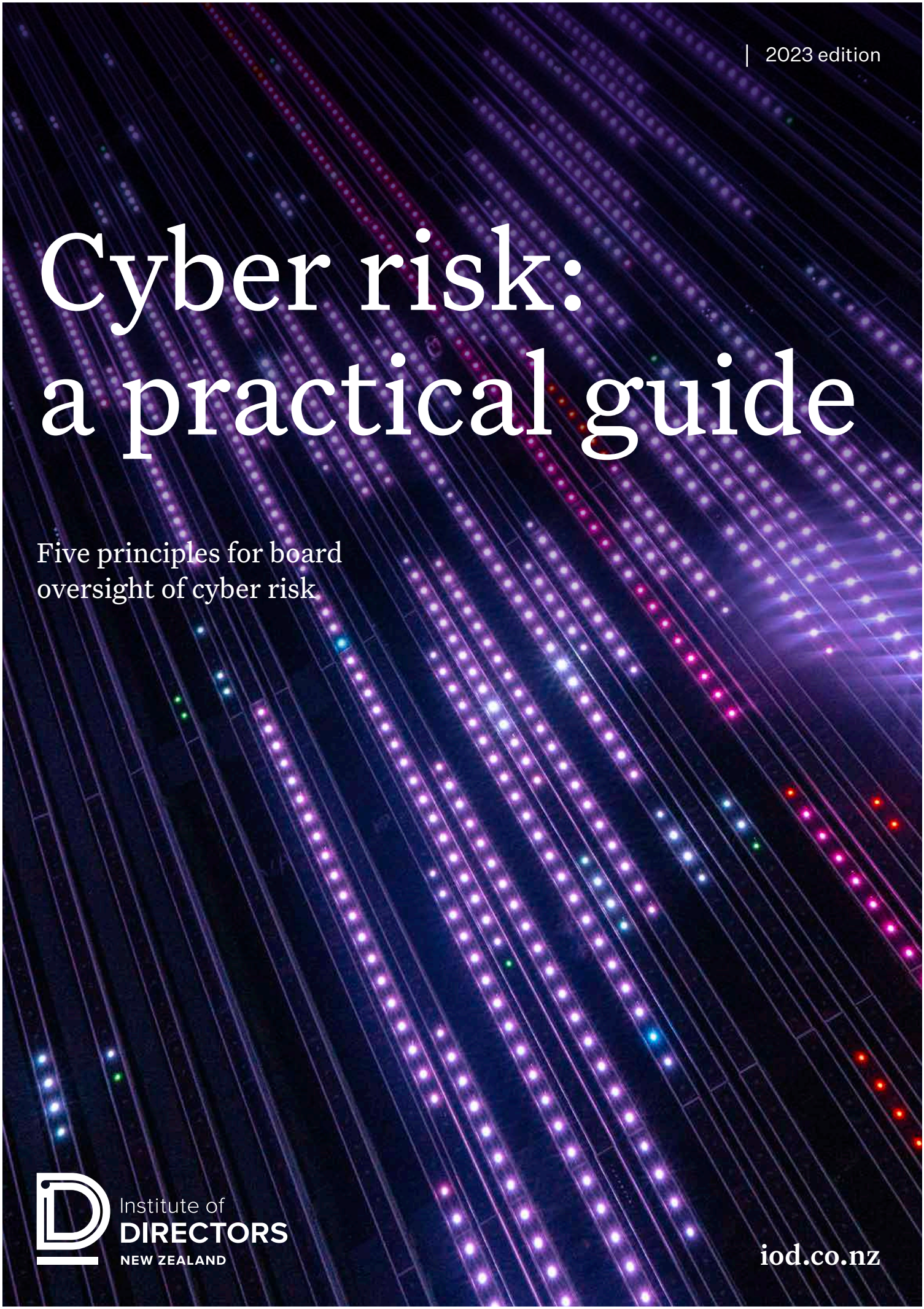
| 2023 edition

Cyber risk: a practical guide

Five principles for board oversight of cyber risk



Institute of DIRECTORS NEW ZEALAND

iod.co.nz

Life for most of us is a state of permanent digital connectivity. Wherever we are and whatever we do, it is undeniably a part of the fabric of our lives. We are dependent and we are vulnerable – and this vulnerability is a big risk for many organisations because it is no longer a question of 'if' you will be subject to a cyberattack, it is a question of 'when'.

Cyber risk, like any other business risk, requires board level attention and response. The magnitude of cybercrime is staggering and its threat is ever-present. It is estimated that cybercrime will cost businesses worldwide $10.5 trillion annually by 2025, while in New Zealand CERT NZ has seen losses of over $39m in the past two years.[1] It is no wonder that these days cybersecurity is high on many board agendas and needs to be given regular and sufficient attention. There have been changes in privacy laws and changes in the technology landscape that mean boards have to be more aware and vigilant.

To keep pace and fulfill their responsibilities, directors must build their cyber competency and the ability to lead organisations in a digital world.

This guide includes five core principles to help boards understand and approach cybersecurity in their organisations.

Acknowledgement: We are grateful to Kordia for their assistance in updating this guide.

ISBN 9789514596957

Five core principles

There are five core principles for board oversight of cyber risk:

1 Take a complete approach

Approach cybersecurity as an enterprise-wide risk, not just an IT issue.

2 Establish an enterprise-wide cyber risk management framework

Ensure that an enterprise-wide cyber risk management framework is established.

3 Give cybersecurity regular attention on the agenda

Cybersecurity needs regular and adequate time on the agenda. Boards should also continue to build their cyber competency and ensure they have access to external expertise.

4 Understand the legal environment

It is essential that directors understand their legal responsibilities and the implications of cyber risk relevant to their organisation.

5 Categorise and address the risks

Board and management discussion of cyber risks should include identification of which risks to *avoid*, which to *accept*, and which to *mitigate or transfer* through insurance, as well as specific plans associated with each approach.

Principle 1.
Take a complete approach

Approach cybersecurity as an organisation-wide risk issue, not just an IT issue.

Historically, cybersecurity has been treated as an operational or technical matter and was overseen by members of the IT team, or specialised staff.

Cybersecurity is now viewed as an enterprise-wide risk management issue. It is also a strategic business enabler that directly contributes to both value preservation and new opportunities to create value for organisations.[2]

Don't dismiss cybersecurity issues as something that only affects other people.

Some organisations feel that because they are relatively small or don't hold substantial amounts of sensitive consumer data, such as credit card numbers or medical information, they are unlikely to be the victims of a cyberattack. The reality is that any organisation that connects to the internet and conducts business activities online, should be mindful of how they manage cyber security risks.

Cyber criminals target organisations of all sizes and from every industry, seeking anything that may have value, including:

- employee log-in credentials
- staff and customer data (Personally Identifiable Information (PII))
- payment information
- business plans, including merger or acquisition strategies and bids
- contracts with customers, suppliers, distributors and joint venture partners
- information about company facilities, including plant and equipment, designs, maps, and future plans
- R&D information, including new products or services in development
- information about key business processes
- source code
- lists of employees and other stakeholders.

Rather than stealing information, some cyber criminals will lock up an organisation's website or network rendering it unusable until a ransom is paid.

Principle 2. Establish an enterprise-wide cyber risk management framework

Ensure that an enterprise-wide cyber risk management framework is established.

Boards have a responsibility to hold management to account in establishing a fully integrated organisational approach to cybersecurity. This is also about staying competitive in a highly dynamic marketplace.

The World Economic Forum's Principles of board governance of cyber risk states that the organisational structure should integrate and support security and strategic goals. It also sets out the following key considerations for boards:[3]

- review the organisational structure to ensure that the cybersecurity function is adequately represented across the business, internal groups and leadership
- understand the basis for, and challenge the assignment of, important roles and lines of accountability for cybersecurity strategy, policy and execution
- set expectations that cybersecurity and cyber risk functions are to receive adequate staffing and funding and monitor the efficacy of these determinations
- inspire a cybersecurity culture and encourage collaboration between the cybersecurity function and all stakeholders relating to, and accountable for, cyber risk at various levels (eg compliance, privacy etc)
- ensure an accountable officer (eg the CISO) has authority and responsibility to coordinate cyber risk strategy throughout the organisation and that the organisation has a comprehensive plan for data governance.

A cyber team, containing representation from across the organisation, should regularly review the cyber risk management plan, quantifying the impact of cyber risk management efforts, producing metrics to explain the outputs and reporting to the board. Internal audits should be conducted on the effectiveness of cyber risk management.

Principle 3. Give cybersecurity regular attention on the agenda

Cybersecurity needs regular and adequate time on the agenda. Boards should also continue to build their cyber competency and ensure they have access to external expertise.

In the 2022 IoD/ASB Director Sentiment Survey, just 54% of directors reported their boards regularly discuss cyber risk and are confident their organisations have the capacity to respond to a cyberattack or incident.

Boards can be flexible in how they oversee cybersecurity. Some may see it as the responsibility of the full board. Others may use an audit and/or risk committee or establish a specific technology committee. The answer requires board discussion and will differ across organisations.

The greater the dependence on technology, the greater the priority and time must be for engaging on cyber issues.

Despite the increasing risk of exposure to cyber threats, executing a comprehensive strategic response continues to be a challenge for directors. Specialist cybersecurity expertise is not overly common on boards and many directors are still building their cyber competence.

Cyber competency

Directors don't need to be cyber experts. However, they do need a sufficient level of understanding to stay on top of key risks and issues to provide leadership and fulfil their obligations. This includes getting to grips with terminology, concepts, and the landscape. All directors need to play their part even if there is a cyber-specialist on the board. Cybersecurity should be factored into board composition, succession planning, and director development.

Reporting from management

Management reporting underpins and enables board oversight of cybersecurity. However, only 39% of directors in the 2022 IoD/ASB Director Sentiment Survey agreed that their board received comprehensive reporting from management about data breach risks and incidents. It is essential that the board has a complete picture of the organisation's current security position to ensure it is prepared for, rather than, surprised by an attack. It is also vital that the board has a strong relationship with and is able to trust the company's Chief Information Security Officer (CISO), or equivalent.

Quality reporting evolves over time to adapt to the changing needs of the organisation and the board. Where the board's information requirements are not being met by management, this should be raised as a priority. *Is management reporting regularly with quality information? Is there robust discussion?*

Guidance to improve reporting

Reporting cybersecurity to boards (by the IoD and Kordia) provides guidance on how to improve cybersecurity reporting and includes:

- guiding principles on reporting to boards
- questions to ask in developing metrics
- sample dashboards.

External expertise

Boards can consult external expertise in the same way that they would on other key risk issues, for example:

- seek briefings from cybersecurity firms, government agencies and industry associations, which can be useful sources of information
- leverage current independent advisors such as auditors and solicitors who offer multi-client and industry-wide perspectives
- find and access director education programmes.

Beyond this, there are benefits in networking with peers and sharing information about the dynamic nature of sophisticated cyber threats and attacks. This is especially important in an environment where information can be scarce beyond what is released in public reports and media.

The bottom line is simple. The board needs to be informed about the company's context and position with regard to cyber risks to provide authentic oversight and to effectively approve management's plans and initiatives.

Questions to ask management

- *Is there meaningful engagement between the IT department and the board? Do we understand each other?*
- *What cyberattacks have occurred in the past and what effect did they have?*
- *What are the organisation's key cybersecurity risks (internal and external) and how are they being managed?*
- *What is management's response plan regarding cyberattacks? What disclosure obligations exist for the organisation? Are these plans and obligations regularly tested and checked for effectiveness?*
- *Has the organisation conducted a penetration test, external assessment or cybersecurity audit? What were the results and what has changed/improved since then? Where are the priorities?*

- *Is a framework in place to address cybersecurity to ensure adequate cyber hygiene?*
- *Secure by design? How are new IT applications checked or accredited before implementation?*
- *Where does security fit in IT procurement considerations?*
- *Does the organisation have access to external cyber expertise?*
- *Is management aware of the threats and who may see our organisation as a target, as well as their methods and motivations?*

A useful approach can be to put the organisation in the shoes of an attacker. *Where are the vulnerabilities in the organisation's systems? Where could cyber criminals cause the organisation the most damage and how?*

Principle 4. Understand the legal environment

It is essential that directors understand their legal responsibilities and the implications of cyber risk relevant to their organisation.

Director obligations span from fundamental fiduciary duties to responsibility for ensuring privacy law is complied with.

It is critical that the board and management understand their organisation's legal framework and potential liability implications of cyber risk. Some organisations may have extensive obligations (eg having regard to their size, industry and operations).

Stakeholder expectations and requirements are also highly important, for instance, regulators and insurers may require notification and/or investigation of cyber incidents.

The domestic and international regulation of cybersecurity, from the prosecution of cyber criminals to company disclosure of cyber breaches, is still evolving. Directors must be vigilant and may need to seek external advice in some circumstances. Clear and reflective board minutes should be kept as a record of the board's engagement in cybersecurity risk management.

Privacy breach notification

In 2020 New Zealand introduced mandatory reporting of privacy breaches under the Privacy Act 2020 (which replaced the Privacy Act 1993). This requires organisations to report to the Privacy Commissioner and affected individuals when there has been a harmful (or potentially harmful) privacy breach. It is an offence for an organisation, without reasonable excuse, to fail to notify the Commissioner (with fines of up to $10,000).

It is essential that organisations have policies and processes in place to deal with and respond to cyber and privacy issues. Boards should be kept informed about breaches and the potential impact for their organisation. For more information, see The new Privacy Act – key resources for directors on the IoD's website.

The European Union's General Data Protection Regulation (GDPR) came into force in May 2018. This applies to all organisations processing the personal data of European Union residents. Some New Zealand organisations will need to ensure they are GDPR compliant.

CERT NZ and the National Cyber Security Centre[4]

New Zealand's Computer Emergency Response Team (CERT NZ) launched in 2017, is a dedicated government cybersecurity agency tasked with making online New Zealand a safer place. CERT NZ, which is part of a global network of CERT organisations, supports businesses, organisations and individuals affected by cybersecurity incidents, and provides information and advice. Cybersecurity issues and incidents can be reported through the CERT NZ website.

The National Cyber Security Centre (NCSC) is part of the Government Communications Security Bureau and it helps significant public and private sector organisations protect their information systems. Cyber incidents relating to critical national infrastructure are currently reported to the National Cyber Security Centre (NCSC) on a voluntary basis.

The NCSC assists organisations to respond to and recover from high-impact cyber security incidents. The NCSC's response supplements support from commercial providers, and can include:

- On-site incident handling assistance
- Digital forensics and technical analysis
- Incident Response Communications advice and guidance
- Coordinating with New Zealand's National Security System.

Principle 5. Categorise and address the risks

Board and management discussion of cyber risks should include identification of which risks to *avoid*, which to *accept*, and which to *mitigate or transfer* through insurance, as well as specific plans associated with each approach.

Conducting a comprehensive and accurate assessment of the potential impacts of cyber risks and breaches can be difficult as there are many variable factors at play. For example, an organisation does not just face financial losses, but loss of intellectual property, reputational damage, and flow-on damage to organisational value and consumer confidence which can add further complications to the breach itself.

Publicity about data breaches carries its own complexities. Stakeholders may see little or no difference between a comparatively small breach and a large and dangerous one. This means the extent of financial damage may vastly outstrip the magnitude and seriousness of the breach itself. The board should seek assurance that management has thought such matters through carefully.

As with any risk management strategy, the goal is not to insulate the organisation from risk entirely. Business requires risk and the establishment of a digital strategy necessitates a certain degree of risk alongside opportunity. The board needs to develop its cyber risk appetite in alignment with organisational strategy and resource allocation.

The key principle is to allocate resources where they will have the greatest impact including to ensure the organisation establishes a comprehensive and secure baseline of critical cybersecurity controls.

Cert NZ guidance

CERT NZ recommends 11 top tips for cybersecurity. While these will not cover every potential attack, they give organisations a realistic start to improving their overall cybersecurity position. The first four of these tips can be easily implemented, both in work and personal life, to ensure better levels of security. These are:

1. Back up your data
2. Keep your devices and apps up to date
3. Choose unique passwords
4. Turn on two factor authentication.

Organisations may also need to invest in measures beyond baseline controls – depending on their context and risks.

An organisation may accept the security risk of not protecting functions and data that are of lower impact to the organisation's mission and where cost exceeds benefits.[5]

Insurance coverage for financial loss resulting from a cyber-incident, access to expert response services, and resulting third party liability can add another layer of protection and expertise to the framework. It is important to assess and implement solutions that can assist in mitigating and transferring some portion of cyber risk.

The human dimension – setting the right culture

People are central to organisational success but they can also pose risks. A high percentage of data breaches are often attributed to human error (eg due to carelessness or lack of training). Breaches by staff may also be deliberate, for example where a disgruntled employee sabotages a system or network.

A strong cybersecurity culture can help limit staff breaches and provide an extra defence to cyberattacks. It is essential that staff are adequately trained and that there are appropriate cybersecurity and privacy policies and procedures in place.

Asset Governance

A key question for a board is *what are the critical assets the organisation needs to protect?* This question calls for pragmatism. The cost of protecting all assets is prohibitive and not practicable. Identifying critical infrastructure requires discussion and consultation with management. Another important question is *what data assets would be mission critical if the organisation was to lose them?*

Cybersecurity needs to be addressed from a strategic, cross departmental, and economic perspective.[6] This must also involve looking outside of the organisation. Data is often stored on external networks or in the cloud and boards need to understand the associated security implications and risks. Third parties can also present significant risks (eg in supply chains).

Third party risks

Major opportunities for business growth may exist through improved digital infrastructure and interconnectivity. Conversely, vulnerability grows as businesses extend access to vendors, suppliers, partners, customers and a range of connected entities.

Complex networks and connections create interrelated points of vulnerability. For example, small organisations are often targeted as a pathway into larger organisations. In some cases these vulnerabilities have the potential to

transfer risk from organisations to public or national security. In the same way, international supply chains can augment cyber risks.

It is critical that the board recognises the wider eco-system within which the organisation operates, and that cyber risks and threats are assessed in that context.

A practical example relates to law, accounting and other firms that act as service providers. Law firms can be highly attractive targets for hackers and industrial spies. Firms hold a concentrated and extensive range of information on a number of clients and can be targeted because they may not have the same level of security as their clients. *Does management understand the level of security on the IT systems of third party providers such as law firms?*

Planning for an incident

Organisations who haven't planned for an incident tend to perform badly: for most organisations this is their first experience of an event of this type, and they tend to panic and waste time and energy working out their approach, while the attacker continues to disrupt services or accessed data.

A clear plan must be put in place that outlines the organisation's response, where everyone understands their role (based on the severity of the incident) and knows when to notify other people, including communications to staff and customers. This process will often include members of the board, and so the board should be involved in the planning process and understand the decisions they may have to make during an attack.

Lastly, once the plan is in place, a number of scenarios should be practiced on a regular basis. Just like a fire drill, all members of staff should know how a scenario is likely to play out and what their role is to minimise risk to the organisation and their customers.

Example

Latitude Financial suffered an attack in March 2023 that was the largest event in the region, with over 14 million sets of customer data exposed. It appears that this attack was through a third party IT supplier. Even though a third party was involved, it was Latitude's name that made the headlines for the breach.

In a statement in response to the Latitude incident, the Office of the Privacy Commissioner has emphasised the importance of considering data retention as a key issue.

Questions for directors to ask:

- *What are the organisation's most mission-critical data assets (the crown jewels), where do they reside and who can access them?*
  - *What data sets need to remain confidential – that is, not accessed or shared inappropriately?*
  - *What systems, applications or data do you not want to lose integrity of – that is, they are accessed or manipulated in a way that you can no longer trust?*
  - *What are the systems or applications to which you require constant availability – that is, if they were to be taken off-line, would result in business continuity impacts?*
- *Do departmental silos prevent dispersed responsibility and accountability for data security?*
- *Is there a strategy for dealing with cloud computing, mobile workforce and supply-chain threats?*
- *Do third parties (eg outsourced providers and contractors) have cyber controls, policies and processes in place (and are they monitored)? Do they align with the organisation's expectations?*
  - *Do you have contractual protections in place with the providers of your most critical systems, to ensure timely restoration of services or regular backups of data?*

Cybersecurity tips for directors

Directors should ensure that their own personal security networks and devices (eg phones, tablets, and computers) are secure. Directors often work in multiple locations including home offices and have access to confidential and sensitive information. CERT NZ has practical guidance for individuals on how to keep information safe and secure online.

Cyber insurance

It is important to choose an insurance provider with a breadth of global capabilities, expertise, market experience and capacity for innovation that best fits the organisation's needs. Different insurance policies can deal with different types of losses that occur from a cyber event. Some types of loss, such as property damage stemming from a cyber event, may not automatically be covered and some events can be expressly excluded from policies. Boards will need to consider and understand, in conjunction with expert advice, what level and type of cover is most appropriate and where any gaps in cover may be.

Develop and test incident response plans

The best form of crisis management is preparation before a crisis occurs. Boards are responsible for ensuring management has developed and implemented appropriate crisis management plans and monitoring such plans over time. The board's role in a crisis, published by Resilient Organisations in partnership with the IoD and QuakeCoRE, includes guidance and insights from interviews with chairs, board members and CEOs who have experienced major crises.

Dealing with cyberhate and misinformation

*Note: Cyberhate and mis/dis-information are not technical cyber security issues, however, they are often used by attackers to create an environment for attacks.

Cyberhate describes various forms of online abuse and harassment including cyberbullying and trolling. Cyberhate is a product of the digital world and board members and their employees are not immune from attack. Cyberhate can have real-life consequences for its victims including mental and emotional stress, feeling physically unsafe, and damage to a victim's reputation. For tips on responding to cyberhate and ensuring workers are protected, see the article Haters gonna hate – dealing with cyberhate for directors, on the IoD website. In addition to directors looking after their own wellbeing, directors have responsibilities for ensuring their workers are also safe online at work, highlighting the importance of both cyber risk and health and safety risk assessments being carried out together.

Mis- or dis-information is where people knowingly create false information, often using technical tools (eg deepfakes) or digital data (eg fake news sites) to spread false or incorrect information, often for a political or social gain. However, these tools can also be used by attackers as a vehicle to deliver their attacks, eg a particularly alarming article could have links enticing users to click on the link and download malicious software.

In summary

It is clear that cybersecurity needs to be a focus for all industries and sectors and ultimate responsibility lies at the feet of the board. It is essential for boards to build their cyber competency and ensure that risks are taken seriously. It is also vital that boards take a holistic view, approaching cybersecurity as an enterprise-wide risk management issue and also as a strategic business enabler.

Since the 2021 edition of this guide, boards have stepped up their focus. It is no longer sufficient that cybersecurity is on the agenda; it also needs to be given regular and adequate attention.

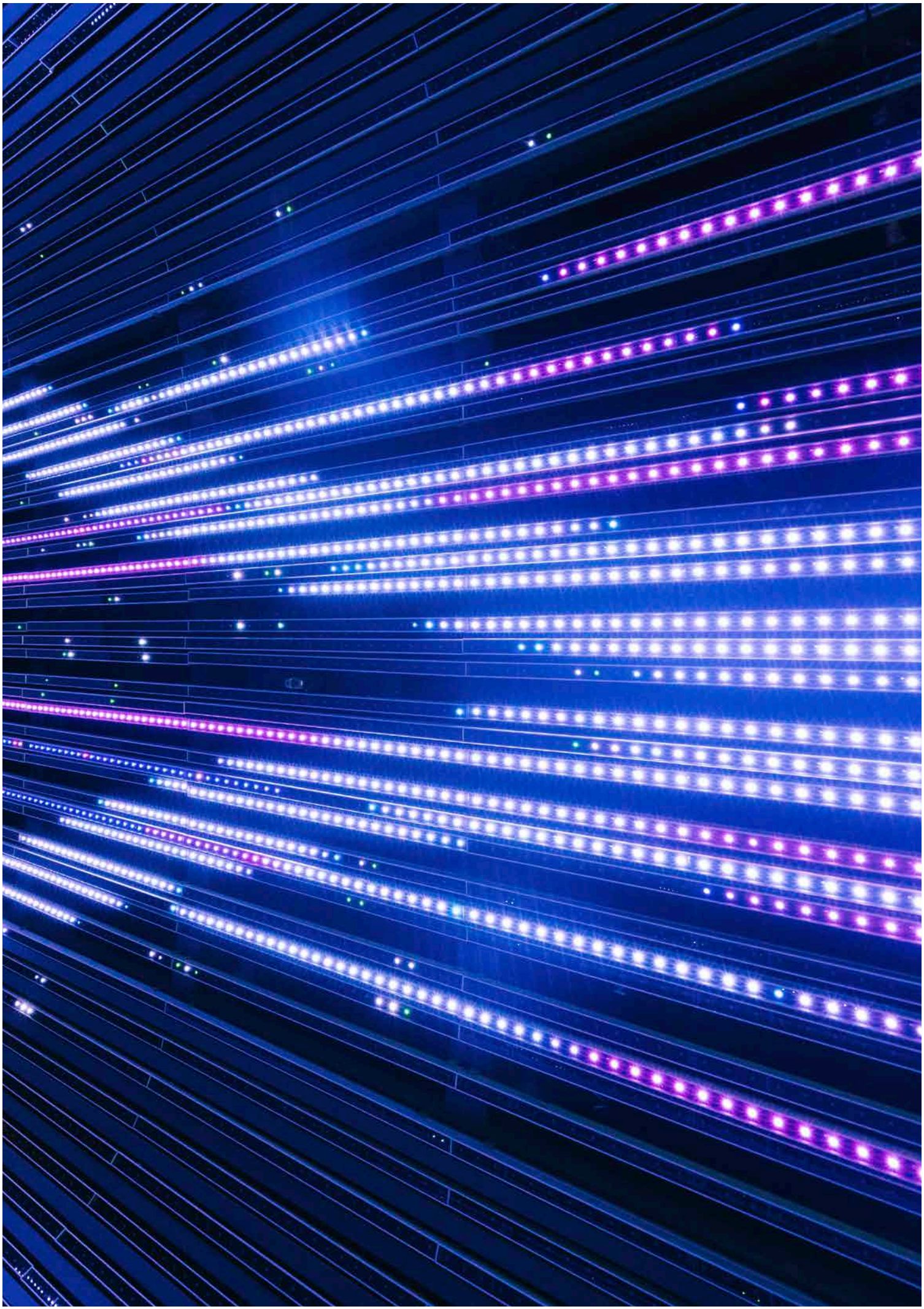
Cybercrime has broad-reaching consequences for organisations with the potential to negatively affect and compromise many areas including staff, customers, intellectual property and reputation. There is a lot at stake but boards that focus on cyber resilience, build their expertise and stay interested in global trends and threats will be better equipped to lead organisations into the future.

Key resources:

- Reporting cybersecurity to boards (IoD/Kordia 2018)
- Cyber-resilience in FMA-regulated financial services (Financial Markets Authority 2019)
- Improving cyber resilience for regulated entities (Reserve Bank)
- Charting your course: Cyber Security Governance (National Cyber Security Centre 2019)
- ISO/IEC 27000 series of information standards (International Organization for Standardization and the International Electrotechnical Commission)
- Principles for board governance of cyber risk (World Economic Forum 2021)
- The National Institute of Standards and Technology framework
- The Payment Card Industry (PCI) Data Security Standards

End notes:

1. Cybersecurity Ventures, *2021 report: cybersecurity in the c-suite* (2021).
2. World Economic Forum, *Principles for board governance of cyber risk (2021).*
3. World Economic Forum, *Principles for board governance of cyber risk (2021).*
4. NCSC and CERT NZ will merge into a single agency in late 2023. Their functions are expected to remain largely unchanged.
5. Armed Forces Communications and Electronics Association, Cyber Committee, *The economics of cybersecurity: a practical framework for cybersecurity investment (2013).*
6. Internet Security Alliance and American National Standards Institute, *The financial management of cyber risk: an implementation framework for CFOs (2010).*



Institute of
DIRECTORS
NEW ZEALAND

iod.org.nz

Institute of Directors in New Zealand (Inc)
Mezzanine Floor, 50 Customhouse Quay
PO Box 25253, Wellington, 6146
New Zealand

Telephone +64 4 499 0076
Email mail@iod.org.nz