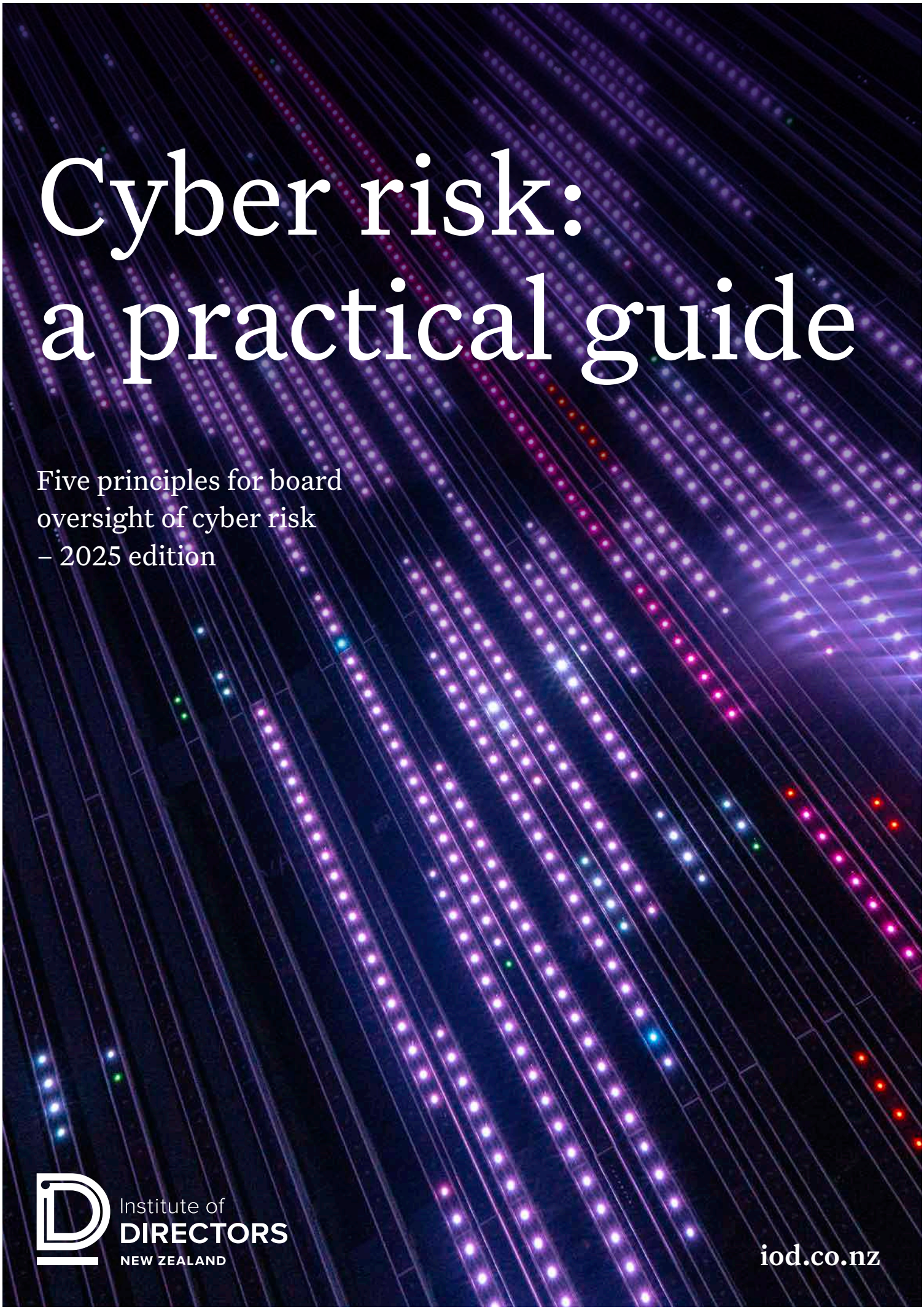

Cyber risk: a practical guide

Five principles for board oversight of cyber risk – 2025 edition

Institute of DIRECTORS NEW ZEALAND

iod.co.nz

Five principles for board oversight of cyber risk – 2025 edition

About the Institute of Directors in New Zealand

The Institute of Directors in New Zealand (IoD) is the leading professional organisation for directors and boards, and promotes high standards of governance. We offer a range of resources to the governance community, including training programmes, networking events and practical tools to improve governance practices. IoD membership demonstrates a commitment to professional development and ethical conduct, aiding directors in their roles. The IoD facilitates knowledge exchange and collaboration among directors, to help contribute to organisational success. More information is available at www.iod.org.nz

Acknowledgement:
This guide was authored by the Governance Leadership Centre at the IoD.

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

ISBN 9789514596957

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. This connectivity, while essential, has made us profoundly dependent – and increasingly vulnerable. For many organisations it is no longer a question of 'if' a cyberattack will occur, but 'when'.

Cyber risk is now a standing governance issue, requiring board-level attention and response. The scale of cybercrime continues to grow at an alarming rate, with global losses expected to reach $10.5 trillion annually by 2025 and could reach $15.63 trillion by 2029. In New Zealand, CERT NZ has reported financial losses in the tens of millions, but the true cost – including reputational harm and operational disruption – is far greater.

Boards must ensure they are cyber literate and equipped to effectively oversee risk as technology risks and opportunities evolve. Regulatory expectations are increasing, with stronger privacy laws, mandatory breach reporting and rising penalties for inadequate governance. Cybersecurity cannot be treated as a technical issue alone – it must be understood as a fundamental business risk that affects strategy, operations and resilience.

This guide sets out five core principles to help boards navigate cybersecurity governance and risk oversight. These principles are designed to provide a clear, practical framework to support informed decision-making, ensuring organisations can effectively manage cyber risk while maintaining business continuity and stakeholder confidence.

The evolving threat landscape

New cyber threats are emerging rapidly, requiring boards to stay informed and ensure their organisations have adaptive risk mitigation strategies in place. Key developments include:

- **AI-driven phishing attacks:** Cybercriminals are leveraging AI to create highly sophisticated personalised phishing attempts that are difficult to detect.
- **Deepfake impersonation scams:** Attackers are using deepfake technology to convincingly mimic executives or key personnel, facilitating fraudulent transactions or disinformation campaigns.

- **Misinformation and disinformation threats:** Malicious actors create false narratives, often leveraging fake news sites or deepfake content, to manipulate public perception or deceive employees. These attacks can be a vector for malware distribution as individuals are lured into clicking on malicious links.
- **Quantum computing vulnerabilities:** While still in its early stages, quantum computing has the potential to break traditional encryption methods, making current cybersecurity measures obsolete.

No organisation is immune

It's a mistake to assume cybersecurity threats only impact large corporations or data-heavy industries. Many organisations believe that because they are smaller or do not store highly sensitive consumer data – such as credit card numbers or medical records – they are unlikely targets. The reality is that any organisation connected to the internet is at risk.

Cyber criminals exploit vulnerabilities in businesses of all sizes, seeking anything of value, including:

- Employee log-in credentials (often used in credential-stuffing attacks)
- Staff and customer data (Personally Identifiable Information – PII, medical and financial data)
- Payment and banking 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
- Confidential operational processes and trade secrets
- Source code and proprietary software
- Lists of employees and stakeholders

In addition to data theft, some cybercriminals deploy ransomware, encrypting an organisation's files or locking down networks until a ransom is paid. These attacks can bring operations to a standstill, inflicting severe financial and reputational damage.

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.

Back to contents

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 a technical or operational matter managed by IT teams or specialised staff. However, this limited perspective no longer reflects today's reality.

Cybersecurity is now viewed as an enterprise-wide risk management issue – one that directly affects strategy, stakeholder trust and long-term organisational resilience. Beyond risk mitigation, a strong cybersecurity posture also enables innovation, enhances competitive positioning and protects the organisation's ability to create and sustain value in an increasingly digital world.

Cybersecurity is a board-level responsibility

Boards must view cybersecurity as a strategic priority that intersects with all aspects of governance. The financial, legal and reputational consequences of a cyber incident can be severe, making oversight and proactive risk management essential. Directors should ensure cybersecurity is integrated into risk frameworks, strategic discussions and business continuity planning, rather than being siloed as a technical concern.

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

Boards must ensure cybersecurity is embedded within the organisation's strategic planning and risk management processes. This requires establishing a comprehensive, enterprise-wide cyber risk management framework that integrates governance, risk oversight and operational resilience.

A well-defined cybersecurity framework not only protects critical assets and data but also enhances business continuity, regulatory compliance and long-term competitiveness. With cyber threats growing in frequency, sophistication and financial impact – including AI-driven attacks, deepfake fraud, supply chain vulnerabilities and the future risks posed by quantum computing – organisations must adopt adaptive, proactive security measures that evolve with the threat landscape.

Board accountability in cyber risk governance

Boards must hold management accountable for implementing a fully integrated and future-proof cybersecurity strategy. This means:

- **Aligning cybersecurity with business objectives** – Cybersecurity should be embedded into strategic goals, financial planning and risk mitigation frameworks
- **Championing a "cyber resilience by design" approach** – Cybersecurity should be built into processes from the outset, not treated as an afterthought
- **Requiring regular risk assessments and scenario planning** – Organisations should test and model their cyber risk frameworks against emerging threats
- **Overseeing the transition to quantum-resistant encryption** – Quantum computing, once viable, will render current encryption methods obsolete. Boards must ensure management is proactively assessing and implementing quantum-safe cryptographic solutions.
- **Embedding cybersecurity into third-party risk management** – Supply chain vulnerabilities remain a top attack vector. Boards must require formalised due diligence, audits and contractual compliance clauses for vendors.
- **Tracking AI-driven cybersecurity risks** – AI is being used both as a security tool and as a weapon by attackers. Boards should ensure

Back to contents

management leverages AI for threat detection while developing safeguards against AI-powered attacks. Also the board should ensure that any AI tool used has the right level of data governance around it.

- **Ensuring investment in talent and security capabilities** – cyber resilience is as much about people as it is about technology. Boards must monitor whether organisations are allocating sufficient resources to cybersecurity staffing, skills development and leadership expertise.

Key governance considerations for boards include:

- Embedding cybersecurity into leadership structures – Cyber risk must be represented at the highest levels, ensuring board engagement with Chief Information Security Officer (CISOs) and cybersecurity leadership.
- Clarifying accountability and reporting lines – Establish clear roles, responsibilities, and escalation procedures for cybersecurity risk management.
- Ensuring cybersecurity funding aligns with risk exposure – Cybersecurity budgets should be reviewed and challenged to ensure they match the organisation's risk landscape.
- Fostering systemic resilience and collaboration – Boards should encourage cross-departmental collaboration on cyber risk and promote external partnerships with industry, regulators and cybersecurity alliances.
- Developing robust data governance and privacy controls – Organisations must have clear policies on data protection, encryption and regulatory compliance, particularly in response to evolving global privacy laws.
- Conducting external cybersecurity audits and stress testing – Boards should mandate regular third-party assessments, penetration testing and cyber-attack simulations to validate resilience strategies.
- Assessing whether Cybersecurity Mesh Architecture (CSMA) is appropriate – With remote workforces, cloud-based infrastructure and hybrid environments, boards should consider CSMA to provide scalable, decentralised security solutions

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.

Building a cyber-resilient future

The cyber threat landscape continues to evolve rapidly, driven by AI-powered automation, geopolitical tensions, shifting regulatory expectations and emerging technologies. These developments present both risks and opportunities for organisations. Boards that take a proactive approach – ensuring cybersecurity is embedded into governance structures, security investments align with business priorities and frameworks are regularly assessed against emerging threats – will be better positioned to safeguard resilience, meet regulatory obligations, and maintain stakeholder trust.

Principle 3.
Give cybersecurity regular attention on the agenda

Cybersecurity needs regular and structured time on the board's agenda. It is no longer an issue to be addressed only when a crisis arises. Boards should prioritise building their cyber competency and ensure they have access to external expertise.

In the 2024 IoD Director Sentiment Survey, 54.8 per cent of directors said their boards receive comprehensive reporting about data breach risks and incidents, an increase from previous years. However ,confidence in organisational preparedness remains too low, with only 62.2 per cent of directors stating they are confident that their organisation has the capacity to respond to a cyberattack or incident. This suggests that while cyber discussions are becoming more common at the board level, there remains a gap in the depth of engagement and the quality of reporting and oversight.

The percentage of directors who said their boards had overseen a cyberattack over the past 12 months increased significantly to 17.9 per cent in 2024.

Structuring board oversight of cybersecurity

Boards can be flexible in how they oversee cybersecurity. Some consider it a full board responsibility, while others delegate it to an audit, risk or technology committee. The right approach will depend on the organisation's size, risk profile and reliance on technology.

There is a growing trend towards formalising cyber risk governance, with more boards either expanding existing committee remits to include cybersecurity or establishing dedicated technology and digital risk committees. While there is no single optimal model, what matters is that cyber risk governance is structured, clear and given sufficient time and expertise.

Regardless of the structure, boards must ensure:

- Cybersecurity is a standing agenda item, receiving adequate time for discussion
- The CISO (or equivalent) has direct access to the board, ensuring cybersecurity insights are not filtered through other management layers, especially ones with conflicting goals and metrics
- Cyber risk is not siloed but integrated into broader strategic risk discussions, including resilience planning and business continuity strategies

Back to contents

Cybersecurity as an ongoing board focus

Despite the increasing risk of exposure to cyber threats, executing a comprehensive and strategic response remains a challenge for directors. Many organisations still lack board-level cyber expertise, and directors are continuing to build their competence in this area.

Cybersecurity should be embedded into board composition, succession planning and director education. To enhance board understanding, directors should:

- Engage in targeted development programmes focused on cyber governance
- Ensure cybersecurity expertise is factored into board recruitment and succession planning
- Allocate dedicated time for scenario-based cyber discussions, including ransomware attack simulations and cyber resilience exercises to strengthen incident response strategies

Boards should also consider engaging external expertise, whether through independent cyber advisors or industry bodies, to ensure they stay informed on emerging risks, regulatory changes and best-practice governance approaches.

Effective reporting from management

Cybersecurity oversight depends on high-quality, relevant and timely information from management.

To be effective, cyber reporting should provide:

- A clear picture of the organisation's current cyber risk exposure, including key assets, internal vulnerabilities and external threats
- Incident detection and response metrics, such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), which indicate how quickly threats are identified and mitigated
- Assessment of workforce resilience, including phishing test results and employee awareness training
- Status of vulnerability management, tracking how quickly security gaps are identified and patched
- Third-party and supply chain security risks, ensuring vendors comply with cybersecurity expectations

Guidance to Improve Reporting

The IoD and Kordia's Reporting Cybersecurity to Boards provides practical guidance for improving cybersecurity reporting and includes:

- Guiding principles for effective board-level cyber reporting
- Key questions for directors to ask when developing and evaluating cybersecurity metrics
- Sample dashboards that translate technical cybersecurity data into strategic, board-level insights

Boards should ensure they are receiving reporting that is clear, actionable and aligned with governance needs, rather than highly technical or reactive updates. If reporting lacks depth or strategic relevance, directors should challenge management to improve its quality and usefulness.

Tracking cyber risk performance: KPIs for the Board

To measure cyber resilience and oversight effectiveness, boards should track key performance indicators (KPIs) that provide real insight into the organisation's cyber health. The metrics should underpin the business goals rather than just be technical metrics.

If cyber reports lack depth, are too technical, or focus solely on compliance metrics, boards must challenge management to improve clarity, relevance and strategic value.

Directors should ask:

- Are we tracking cyber risk trends over time, rather than receiving one-off incident reports?
- Do we have independent validation of our cyber risk posture, such as external audits?
- Are our cybersecurity investments linked to actual risk reduction outcomes?

Leveraging external expertise

Boards regularly consult external expertise in financial, legal and regulatory matters – cybersecurity should be no different. Given the complexity and rapid evolution of cyber threats, engaging independent cybersecurity advisors can provide a critical external lens on governance strategy, risk posture and best-practice implementation.

Boards should consider:

- Regular briefings from cybersecurity firms, CERT NZ and NCSC, ensuring awareness of the latest threats
- External cyber risk audits, ensuring risk management practices are externally validated
- Industry networking and peer discussions, providing insight into how other organisations are structuring cyber governance

Back to contents

With cyber risks evolving faster than many internal capabilities, external expertise is an essential tool for governance, providing objectivity, challenge and strategic foresight.

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?*
- *How confident are we in our organisation's ability to respond to a cyber incident?*
- *Do our third-party suppliers meet our cybersecurity standards?*
- *Is all our key data backed up and have we tested our ability to restore it if something goes wrong?*
- *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? When did we last run an incident response simulation?*
- *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 cybercriminals cause the organisation the most damage and how?

Principle 4. Understand the legal environment

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

Director obligations span from fundamental fiduciary duties to ensuring privacy laws are met, including regulatory reporting and disclosure of cyber incidents. The board and management must have a clear understanding of their organisation's legal framework and the potential liability implications of cyber risk. Some organisations may have extensive obligations, particularly based on their size, industry and international reach.

Stakeholder expectations are also critical – regulators, insurers and investors increasingly expect timely notification, investigation and response to cyber incidents. The legal and regulatory landscape around cybersecurity continues to evolve, particularly regarding company disclosure obligations, data protection laws and the prosecution of cybercriminals.

Directors must be vigilant and may need to seek external legal or regulatory advice in certain circumstances. Clear and well-documented board minutes should be kept as a record of board engagement in cybersecurity risk management, helping demonstrate due diligence in the event of legal scrutiny.

Privacy breach notification

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

Recent developments

New Zealand is in the process of developing a refreshed National Cyber Security Strategy, with a targeted release in 2025. This updated strategy aims to address emerging cyber threats, modernise legislation and enhance national and regional cyber resilience, particularly in partnership with Pacific neighbors.

The Privacy Amendment Bill (2024), expected to come into force in 2025, proposes greater disclosure obligations and clarification on liability for third-party service providers.

The Privacy Commissioner continues to advocate for the introduction of a civil penalties regime, similar to Australia, to enhance compliance enforcement.

Back to contents

International protection laws

New Zealand directors should be aware of international data protection laws when trading overseas, handling foreign customer data or operating in multiple jurisdictions. These regulations can impose direct compliance obligations, affect contractual requirements with international partners and influence New Zealand's own privacy and cybersecurity policies.

European Union (EU) – The GDPR remains the global standard, imposing strict consent rules, individual data rights and high penalties (up to 4 per cent of global turnover or €20 million). Many jurisdictions, including Australia and parts of the US, have modelled laws on GDPR principles.

Australia – The new Cyber Security Act 2024 marks a clear policy shift towards stronger regulatory oversight. The Act introduces mandatory reporting of ransomware payments, government-enforced security standards for smart devices and an independent Cyber Incident Review Board to analyse major attacks and improve national resilience. It also expands critical infrastructure obligations, requiring businesses to manage both cyber and operational risks.

The Privacy Act reforms (2022-24) significantly increased penalties for serious breaches (up to AU$50 million), strengthened breach reporting rules and expanded regulatory powers.

United States – Lacking a federal privacy law, the US operates through state-based regulations (such as California's CCPA/CPRA). The US Securities and Exchange Commission now requires listed companies to disclose major cyber incidents within four business days.

China – The Personal Information Protection Law (PIPL) enforces strict data localisation and transfer restrictions. New Zealand businesses handling Chinese data must comply with stringent security and consent rules.

Worldwide, privacy laws worldwide are tightening enforcement, increasing penalties and expanding consumer rights. New Zealand's "adequacy" status with the EU remains intact, but organisations should anticipate further alignment with international best practices to maintain cross-border data flows.

CERT NZ and the National Cyber Security Centre

Since July 2024, CERT NZ has been integrated into the National Cyber Security Centre (NCSC) to create a single, centralised government cybersecurity agency. This restructuring enhances New Zealand's cyber resilience by consolidating resources and expertise under one agency.

Key Responsibilities of the NCSC:

- Cybersecurity threat monitoring and intelligence sharing
- Incident response and mitigation for nationally significant organisations
- Support for businesses and individuals impacted by cyber incidents
- Providing guidance on cyber hygiene and risk management
- Coordinating with international cyber agencies

The CERT NZ website remains operational as an access point for reporting cyber incidents and obtaining security best practices. However, directors should be aware that national cybersecurity support and response functions are now fully managed under the NCSC.

Boards should ensure their organisations understand the reporting channels available and have formalised incident response plans that align with NCSC and regulatory guidance.

Back to contents

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 because 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 ensuring the organisation establishes a comprehensive and secure baseline of critical cybersecurity controls. A risk assessment helps the organisation know where they don’t have to spend money.

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

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 (for example, 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 staff are adequately trained and 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 requires a pragmatic approach because the cost of protecting all assets is prohibitive and impracticable. Boards should ensure management identifies and maps these critical assets against the organisation's threat landscape, prioritising the most vital to achieving strategic objectives.

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?* Directors should oversee reassessments of critical assets, ensuring risks are continuously evaluated as new threats emerge.

Cybersecurity needs to be addressed from a strategic, cross departmental and economic perspective. This must also involve looking outside the organisation. Data is often stored on external networks or in the cloud and boards need to understand the associated security implications and risks. An understanding of the 'Shared Responsibility Model' with cloud providers is key to not leaving a gap between what the cloud will do and what the client thinks the cloud provider does. Third parties can also present significant risks (for example, in supply chains).

Back to contents

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 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 client information and can be targeted because they may not have the same level of security as their clients. Management should *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 many 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.

Once the plan is in place, various scenarios should be practiced regularly. Just like a fire drill, all 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. The board should also be involved in some of these drills.

The Latitude Financial breach highlights the importance of managing third-party vulnerabilities, demonstrating how inadequate oversight can lead to insignificant reputational and operational risks.

Example

Latitude Financial suffered an attack in March 2023 that was the largest event in the region, with more than 14 million sets of customer data exposed. It appears 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 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 (such as 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 (such as 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.

Back to contents

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 IoD article Haters gonna hate – dealing with cyberhate for directors. 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.

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 risks are taken seriously. It is also vital boards take a holistic view, approaching cybersecurity as an enterprise-wide risk-management issue and also as a strategic business enabler.

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.

Some key resources:

- Reporting cybersecurity to boards (IoD/Kordia 2025)
- Cyber resilience guidance (National Cyber Security Centre)
- The National Institute of Standards and Technology framework (NIST)

A more comprehensive list of cybersecurity resources along with topical articles for boards can be found on the IoD website.

Institute of
DIRECTORS
NEW ZEALAND

iod.org.nz

Institute of Directors in New Zealand (Inc)
Floor 6, Grant Thornton House
215 Lambton Quay
Wellington Central 6011
New Zealand

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