governance Leadership centre

PRACTICE GUIDE

# Cyber-Risk Practice Guide

Put cybersecurity on the agenda before it becomes the agenda

Institute of Directors

At the Institute of Directors we're raising the standard of governance in all areas of New Zealand business and society.
iod.org.nz

***This guide provides boards with five useful principles to help them understand and monitor cyber-risk, develop strategies for seeking assurance, and oversee management. It also poses critical questions directors have a duty to ask.***

Virtually all levels of business activity have technology implications. The potential for significant financial, competitive and reputational damage is not only high, but also difficult to predict, recognise and treat.

Directors must understand cyber risk as part of *enterprise risk*. Resiliency will be a key hallmark of a modern business.

Cybersecurity may be a relatively new feature of boardroom agendas, but its the director's responsibility to identify and manage risks is not unfamiliar territory. The principles behind cyber-risks are no different to other areas of risk. Directors must grasp the specific risks, determine risk appetite and take actions to deal with cyber-risk.

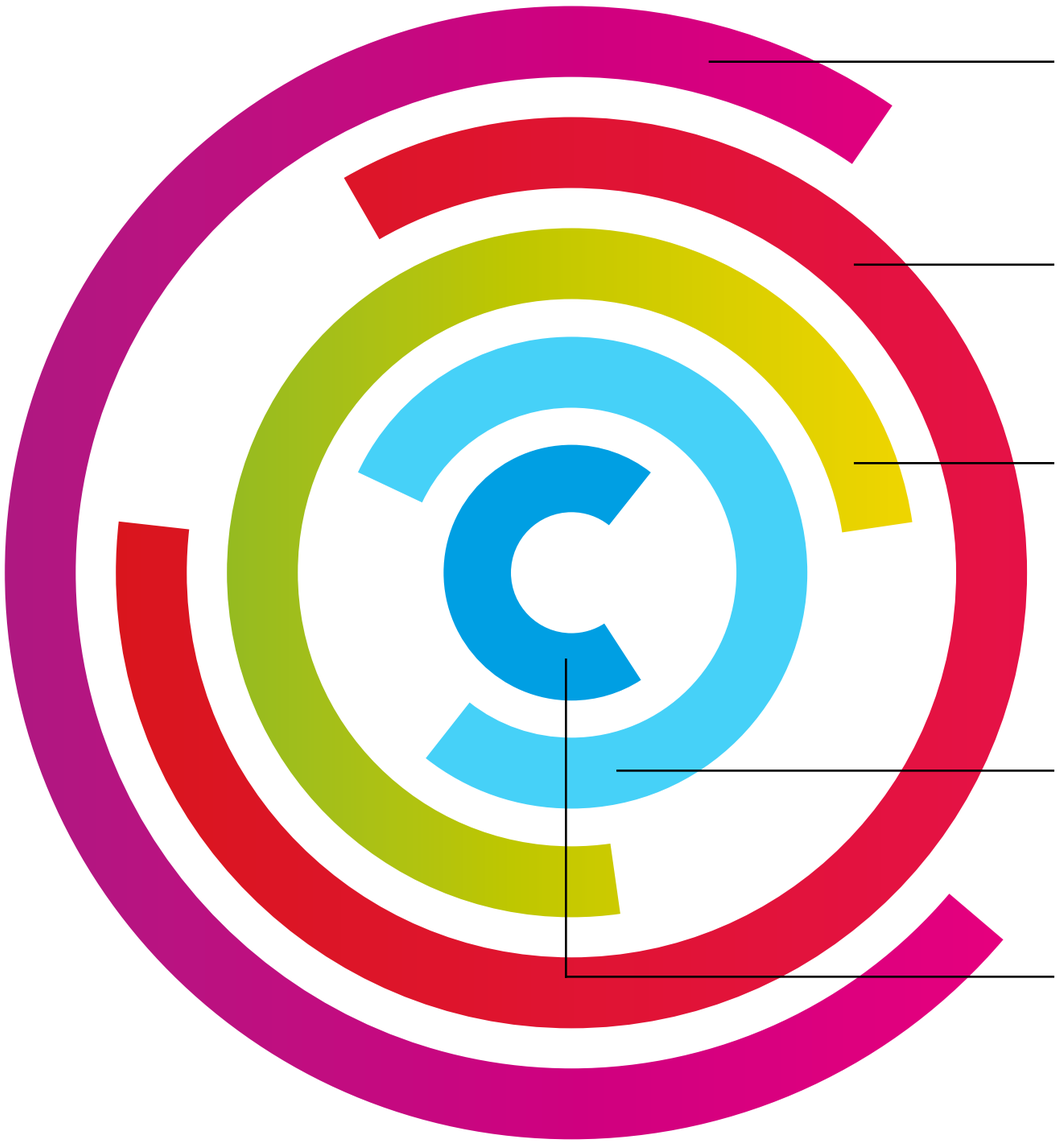
The Institute of Directors (IoD) is a proud partner of the New Zealand Government's Connect Smart initiative which is a public private partnership to improve individual and business online security. This collaborative approach aims to put cybersecurity on the boardroom agenda before it becomes the agenda.

*The IoD remains committed to ensuring members receive up to date guidance and resources on contemporary issues in the boardroom. This guide is underpinned by international best practice and based on the National Association of Corporate Directors' (USA) Cyber-Risk Oversight Directors' Handbook. We are grateful for the assistance from the National Association of Corporate Directors (NACD), and acknowledge the support they received from AIG Insurance Ltd and the Internet Security Alliance in the United States.*

**Disclaimer:** This practice guide has been prepared as a resource for boards and should not be used or relied upon as a substitute for proper professional advice.

# Five core principles

**There are five core principles for boards in their oversight of cyber risks.**



## 1 Take a holistic approach

Directors should approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

## 2 Understand the legislative environment

Directors should understand the legal implications of cyber risk as they apply to the company's specific circumstances.

## 3 Access expertise and put cybersecurity on the board agenda

Boards should have adequate access to cybersecurity expertise. Discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.

## 4 Establish a framework

Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework.

## 5 Categorise 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 holistic approach

*Directors should approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.*

Historically, cybersecurity has been treated as an operational or technical matter. It was often overseen by a highly specialised business unit. Siloed business departments tend to have assumed that responsibility lies in the IT office. This has prevented critical analysis and co-ordinated communication about security issues on an enterprise-wide basis.

The approach to cyber risk must change in 2015. Cybersecurity has to be seen as an enterprise-wide risk management issue. We live in a digital world and all business needs to be responsive to this.

The key question for any board is a simple one: *What is the critical IT infrastructure we need to protect?*

This question calls for pragmatism. The cost of protecting all IT is prohibitive, and the ability to do so may be impossible. Identifying critical IT infrastructure requires discussion and consultation with management. What data assets would be mission critical if your company was to lose them?

Cybersecurity needs to be addressed from a strategic, cross-departmental, and economic perspective[1]. This can also involve looking outside of the organisation. Companies often store data on external networks or in the cloud which they don't own or operate, and boards need to understand the associated security implications.

## Why would they attack us?

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 cyber-attack. In fact, cyber criminals target companies of all sizes and from every industry, seeking anything that might be of value, including:

- business plans, including merger or acquisition strategies, bids, etc
- trading algorithms
- contracts with customers, suppliers, distributors, joint venture partners, etc
- employee log-in credentials
- information about company facilities, including plant and equipment designs, maps, and future plans
- product designs
- information about key business processes
- source code
- lists of employees.

Rather than stealing information some cyber criminals will lock-up a company's website rendering it unusable until a ransom is paid.

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

# Principle 1: Take a holistic approach

**CASE STUDY**

Last year when hackers were unable to breach a major oil company's computer network they inserted malware into the online menu of a local Chinese restaurant. When employees of the company browsed the menu, they downloaded code which enabled an attack on their core business.

*Nicole Perlroth, "Hackers Lurking in Vents and Soda Machines," The New York Times, April 7, 2014*

## 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. In some cases these vulnerabilities have the potential to transfer risk from corporations to public or national security. In the same way, long international supply chains can augment cyber risks.

Directors need to recognise the wider eco-system within which their organisation operates, and assess cyber risks and threats in that context.

For example:

- Do internal departments understand their responsibility for data and IT protection?
- Do we understand what data assets might walk out the door each evening with the staff?
- Do we have a policy about using Wi-Fi or open access internet supply?
- Are all work devices password protected by default?

A practical example relates to law, accounting and other firms that act as service providers. Many directors may not realise that a law firm is a highly attractive target 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?

Questions for directors to ask:

- What are our company's most mission-critical data assets (the crown jewels), where do they reside and who can access them?
- Do departmental silos prevent dispersed responsibility and accountability for data-security?
- Do we have a strategy for dealing with cloud computing, mobile workforce and supply-chain threats?
- Do third parties we engage with (eg outsourced providers and contractors) have cyber controls, policies and processes in place and monitored? Do they align with the organisation's expectations?
- Is there meaningful engagement between the IT department and the board? Do we understand each other?

# Principle 2: Understand the legislative environment

*Directors should understand the legal implications of cyber-risk as they apply to the company's specific circumstances.*

Liability for cybersecurity is not always clear cut. Director obligations span from fundamental fiduciary duties, to responsibility for ensuring privacy law is complied with. As a baseline, clear and reflective board minutes should be kept as a record of the board's engagement in cybersecurity risk management.

It is important that both management and the board understand liability implications of cyber risk. Regulators and insurers may require notification and/or investigation of cyber incidents. Privacy breaches may relate to individual privacy and data. Human resource policies and processes should be capable of dealing with and responding to cyber issues at employee level.

## Breach notification

There are no mandatory reporting requirements for cyber incidents in New Zealand. The focus is generally on significant breaches in the following two areas:

- **Cyber incidents relating to critical national infrastructure** are currently reported to the New Zealand National Cyber Security Centre (NCSC) on a voluntary basis. The NCSC can also provide assistance to companies in some instances.
- **Personal data breaches** (eg bank information/ credit card details) which carry a focus on if/ how individuals should be notified.

The Privacy Act 1993 does not currently require breach notification. The Privacy Commission, however, has published privacy breach guidelines on their website.

The Law Commission's review of privacy law discussed mandatory and voluntary notification and in 2011 recommended, "that notification should be mandatory but only in a clearly confined set of situations."[2] Mandatory reporting is one of the key proposals in updating the Privacy Act.

In the United States, the risk has been posed of shareholder derivative suits in cases where an incident occurs and the company share price drops. The directors might be liable to accusations of inadequate disclosure and a failure to execute their fiduciary duty to confirm adequacy of protections of consumer data and consequences.

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 should seek external advice regarding disclosure considerations as this will inform response plans.

2 New Zealand Law Commission, Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4, (2011) page 210.

# Principle 3: Access expertise and put cybersecurity on the board agenda

*Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.*

Despite the increasing risk of exposure to cyber threats, executing a comprehensive strategic response continues to be a challenge for directors.

***"59% of companies do not have adequate intelligence or are unsure about attempted attacks and their impact[3]."***

IT expertise is not common among boards and many directors do not have confidence in the reporting they receive. The 2014 IoD/NZIER Director Sentiment Survey found that less than half (47%) of boards said they received good quality reports and information from management on technology-related matters and engaged in robust discussion on this topic.

Directors may also experience difficulty extracting cyber information from management. It is not uncommon for managers to downplay the nature of the risk environment. In fact, one recent Ponemon Institute study[4] found that 60 per cent of IT staff do not report cyber-risks until they are urgent (and more difficult to mitigate) and acknowledge that they try to filter out negative results.

Directors need to think about their strategic context and any implications for future board composition and board upskilling. Skilled and capable people are essential for cyber-risk mitigation.

## Access to external information

There are a range of ways to supplement board access to cyber expertise. The board should be prepared to consult external expertise in the same way that it would on other key risk issues, for example:

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

It is critical that boards include time on their agenda to discuss their approach to cybersecurity.

3 Ponemon Institute LLC, Exposing the Cybersecurity Cracks - A Global Perspective Part 1: Deficient, Disconnected & in the Dark (2014)
4 Sean Martin, "Cyber Security: 60% of Techies Don't Tell Bosses About Breaches Unless It's 'Serious'," International Business Times, April 16, 2014.

# Principle 3: Access expertise and put cybersecurity on the board agenda

Beyond this, there are benefits in participating in high-quality cybersecurity information exchanges on the dynamic nature of sophisticated cyber threats[5]. This is especially important in an environment where information can be scarce beyond what is released in public reports and media.

An emerging international trend is the use of independent information sharing entities and groups. These are particularly strong in the United States.

The bottom line is simple, if a board doesn't receive regular information regarding the company's context and position with regard to cyber risks, it is impossible to provide authentic oversight or to effectively approve management's plans and initiatives.

## Useful questions to ask management

1. Have we been told about cyber attacks that have occurred in the past and how severe they were?
2. What are the organisation's cybersecurity risks (internal and external) and how are we managing them?
3. What is managements response plan regarding cyber-attacks? What disclosure obligations exist for our organisation? Are these plans and obligations regularly tested and checked for effectiveness?
4. Have we conducted a penetration test, external assessment or cybersecurity audit? What were the results and what have we changed/ improved since then? Where are the priorities?
5. Do we have a systemic framework in place (US National Institute of Standards and Technology or equivalent) to address cybersecurity to assure adequate cyber-hygiene?
6. Do we have access to cyber expertise?
7. Is management reporting regularly with quality information and engaging in robust discussions about cybersecurity?
8. Is management aware of the threats and who may see our organisation as a target, as well as their methods and motivations?

There is an underlying theme in these questions of putting the company in the shoes of an attacker. Where are the vulnerabilities in our systems? Where could cyber criminals cause our company the most damage and how?

The 2014 the US National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity, describes how organisations can apply a risk-based approach to improve security. It pulls together existing standards and practices to help organisations understand and manage cyber risks.

5 AFCEA Cyber Committee, The Economics of Cybersecurity Part II: Extending the Cybersecurity Framework, April 2014.

# Principle 4: Establish a framework

*Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework.*

Boards of directors 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.

## At the board level

As with many risk-related governance functions, there is some debate as to whether cyber risk should be an allocated responsibility. Some boards regard this as a whole board responsibility, and others appoint audit and risk committees to oversee the issues. Other boards may establish purpose-formed cyber-risk committees. The answer requires board discussion and will differ with needs across different organisations. The more digitally/IT dependent your company is, the higher the priority must be for engaging on the issues.

Since cyber risks and threats operate on a highly dynamic and variable landscape, dedicated committees should receive briefings at least on a quarterly basis and the full board should be briefed at least semi-annually or as warranted. Some companies may require more frequent briefings.

## At the operational level – an integrated approach

The Internet Security Alliance[6] proposes a framework whereby a senior manager with cross-departmental authority (outside of the CIO) is appointed to lead an enterprise-wide cyber-risk team. This team contains representation from across the organisation and works to identify, analyse and contextualise risks.

The cyber-risk team leads development of a cyber-risk management plan, involving all departments and receives an adequate resource allocation (which shouldn't be tied to one department).

The team regularly reviews this 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 on a quarterly basis.

6 Internet Security Alliance, Sophisticated Management of Cyber Risk, 2013,

# Principle 5: Categorise the risks

*Board 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 share price 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.

## Avoid

As discussed under Principle 1, organisations must identify the most mission critical assets (the crown jewels) and determine what other data assets are important to the running of the organisation. An awareness of valuable data in the company enables the board to determine risk appetite.

The key principle is to allocate resources where they will have the greatest impact.

In 2012 the Australian Department of Defence issued guidance regarding a set of 35 controls[7] that avoid, counteract, or minimise security risks. Research conducted in 2013[8] revealed that the first four of these controls are effective in protecting against 85 per cent of the targeted cyber intrusions addressed by the Defence Signals Directorate, in addition to improving both operational effectiveness and cost efficiency even before taking into account reduced cyber-breaches.

The four controls are:

1. Restricting user installation of applications (called white-listing).
2. Ensuring the operating system is patched with current updates (especially security updates).
3. Ensuring software applications have current updates.
4. Restricting administrative privileges.

7 Strategies to Mitigate Targeted Cyber Intrusions, Australian Government, Department of Defence Intelligence and Security, October 2012.

8 Top 4 Strategies to Mitigate Targeted Cyber Intrusions, Australian Government, Department of Defence Intelligence and Security, April 2013

# Principle 5: Categorise the risks

After establishing a comprehensive and secure baseline of controls, the Armed Forces Communications and Electronics Association (AFCEA) recommends focusing security investment to counter more sophisticated attacks against the functions and data that are most critical to the organisation[9]. The AFCEA also note that the best return on investment (ROI) tends to come from employing countermeasures beyond the baseline controls in response to recognised specific attack patterns.

Sophisticated cyber resilience comes from tailoring responses/controls for dynamic threats, which require an organisation to have a clear understanding of context, and hire employees who are adequately trained in cybersecurity to suit their needs.

## Accept

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[10].

## Mitigate or transfer

Insurance coverage for financial loss, employee training and access to expert response services 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.

If a board decides to acquire insurance, it is important to choose a provider with a breadth of global capabilities, expertise, market experience and capacity for innovation that best fits the organisation's needs.

9 AFCEA Cyber Committee, The Economics of Cybersecurity Part II: Extending the Cybersecurity Framework, April 2014.
10 AFCEA Cyber Committee, The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment, October 2013.

# In summary

*Cybersecurity is more than an IT issue. Directors need to be constantly assessing and reassessing their capacity to address cybersecurity threats. Approaches taken by different boards and their respective organisations will vary according to their circumstances and needs, but all boards should find the principles-based approach outlined in this guide useful.*

Total insulation from risk is neither realistic nor advisable, as increased vulnerability often stems from the very technological business innovations we seek, to bring our companies forward in efficiency and market reach.

Lastly, a word of assurance. Cyber risk is a new area for many boards but directors should know that upskilling and understanding the subject is not an impossible challenge. This guide supports directors by providing the most contemporary information available in a landscape that is evolving.

governance Leadership centre

**For more information see the Governance resources section of our website www.iod.org.nz**

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

***Telephone:*** 04 499 0076
***Facsimile:*** 04 499 9488
***Email:*** mail@iod.org.nz
**iod.org.nz**

Institute of Directors