Reporting cybersecurity to boards

Institute of DIRECTORS NEW ZEALAND

aura INFORMATION SECURITY | POWERED BY KORDIA

Reporting cybersecurity to boards

Cyberattacks rank as a top risk to organisations, both in terms of likelihood and overall impact, in the 2018 Global Risks Report by the World Economic Forum. In the modern world, virtually all levels of organisational activity have technology implications, and the potential damage from a cyberattack or data breach can be significant. It is important that boards receive comprehensive reporting from management about cyber risks and incidents, and actions taken to address them. However, many New Zealand directors say they are not getting sufficient information.*

Improving cybersecurity reporting

To help improve cybersecurity, we have set out:

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

This resource should be read in conjunction with the IoD's ***Cyber-Risk Practice Guide***.

Data breaches and privacy

The growth of the internet and the digital economy, as well as the emergence of new technologies, have changed the way organisations operate and how personal information is used.

Data breaches are on the rise and increasingly making headlines especially where private information of customers or stakeholders is exposed. Global trends show that many jurisdictions including the United States, the European Union, Canada, Australia, and New Zealand have enacted (or are about to) some form of mandatory privacy breach notification law.

Oversight and monitoring of cybersecurity

Cybersecurity is all about security in the cyber realm including of information and IT systems. Cyber risk is like any other business risk, and requires board level attention and responsibility. Given this, it is critical that boards include time on the agenda to discuss their approach to cybersecurity, and constantly assess and reassess their capacity to address cybersecurity threats. As part of the board's oversight and monitoring role, it is responsible for holding management to account in establishing a fully integrated organisational approach to cybersecurity (e.g. having appropriate policies, processes and procedures in place). To provide effective oversight, boards need to see high-level, holistic reporting on cyber risks and the state of their organisation's cybersecurity programme.

> "Cyber risk is like any other business risk, and requires board level attention and responsibility."

*Only 47% of directors in the IoD's 2018 Director Sentiment Survey said they received comprehensive cybersecurity reports.

Reporting to the board

It is important that reporting is tailored to the organisation and the needs of the board. There is no one-size-fits-all approach. Cybersecurity reporting should start with the greatest business risk due to cyber risk.

Some organisations will have relevant reporting and others will only just be starting their journey to developing comprehensive cybersecurity reports.

Boards and management need to consider the format and frequency of reporting, and consider what information and detail is most valuable in maximising the effectiveness of board oversight in this area. Organisations may find it useful to start by reporting on a small number of the most significant and relevant cybersecurity metrics (often the highest rated cybersecurity risks and associated controls) and increasing these over time. Reporting to the board on cybersecurity has similar principles to reporting on other areas of an organisation such as health and safety and financial reporting.

Guiding principles for board reports

Relevant: Relevant to the audience (full board; key committee)

Reader-friendly: Use summaries, callouts, graphics, and other visuals, avoid technical jargon

Meaningful: Communicate insights, not just information. Highlight changes, trends, patterns over time

Concise: Avoid information overload

Discussion: Reports should also enable dialogue and debate

Continuous improvement: Review the format and content regularly.

Key questions to help identify and develop cybersecurity metrics

What metrics do we have that indicate risk to the organisation?

Boards need to know that the organisation's critical assets are being protected.

What cybersecurity investments are necessary?

Organisations need to understand their current and future cybersecurity needs before they decide what investments will drive down risk. Useful questions include:

- What initiatives were not funded in this year's budget and why?
- What trade-offs were made?
- Do we have the right resources, including staff and systems, and are they being deployed effectively?

How do we measure the effectiveness of our organisation's cybersecurity programme and how does it compare to those of other organisations?

Board-level metrics should highlight changes, trends and patterns over time, show relative performance, and indicate impact. External cybersecurity specialists may be able to provide useful comparisons within industry sectors.

How many data incidents (e.g. exposed sensitive data) has the organisation experienced in the last reporting period?

This metric will inform conversations about trends, patterns and root causes.

How do we assess the cyber-risk position of our suppliers, vendors, JV partners and customers?

Supply chain relationships typically pose increased risk for organisations given the degree of system interconnectivity and data-sharing that is now part of everyday business operations. Useful questions include:

- How do we conduct ongoing monitoring of third party risks?
- How many external vendors connect to our network or receive sensitive data from us?

What metrics do we use to evaluate cybersecurity awareness across the organisation?

People are often the biggest cybersecurity threat for many organisations. Data about policy compliance, and the implementation and completion of training programmes will help inform conversations about insider risks.

The following two examples of cybersecurity dashboards are for fictitious organisations and are not intended to be used as templates. They include common cybersecurity issues and topics, and are intended to inform and inspire to improve reporting to boards.

Example 1 – Cybersecurity dashboard

Example 1 is a large New Zealand organisation (over 300 staff) providing professional services. In order to understand their cybersecurity risks, the organisation undertook a cybersecurity risk assessment. The following major findings were made:

- The organisation has no security policy. This needs to be put in place so that the organisation can ensure that staff are clear on expectations around data handling and protection, as well as a range of other security requirements.
- There is no security-related training in place for staff. As staff accessing malicious or phishing emails is the main type of attack in New Zealand, awareness education must be put in place.
- There is no regular security assessment of the business assets, meaning that these may be vulnerable to attack. A regular programme needs to be put in place.
- The organisation's main client database has been attacked in the past, and client information downloaded. This is a key risk, and needs attention to ensure that a breach like this is far less likely to happen in the future.

All risks related (these and others) to cybersecurity have been added to the organisation's risk register, where they can be reviewed in full. This dashboard pulls out some of the main risks for this organisation.

Current cybersecurity risk status

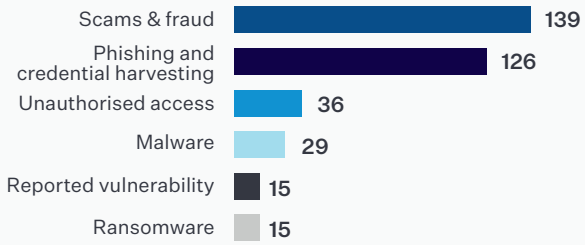
	Key risk	Risk level	Trend
Business continuity planning	Current business continuity planning does not include recovery from any form of cyberattack (including phishing, ransomware, etc.)	M	▲
Access management	Most organisational data has recently been placed with a cloud-based service. Access to this data needs to be further catagorised and restricted to prevent the risk of accidental transmission	L	■
Policy	The current lack of a security policy leaves the business open to a wide range of attacks as there is no single approach to inform procedures and staff training	H	■
Information protection	The client database is still at risk until a number of security fixes have been implemented	H	▲
IT risk management	Lack of a regular security review programme will lead to unknown risks being exploited	M	▼
Physical security management	Physical access via two improperly secured building entrances could allow for access to the rest of the head office, exposing the server room to risk	L	■
Security awareness	Staff need to be adequately trained in security awareness to help prevent attacks such as phishing	H	▲
Third party security management	Three of the existing third party contracts have omissions that expose the business to unnecessary risk. These are currently being amended.	L	▼

▲ Trend increasing ■ No change ▼ Trend decreasing

Emerging risks, threats or vulnerabilities

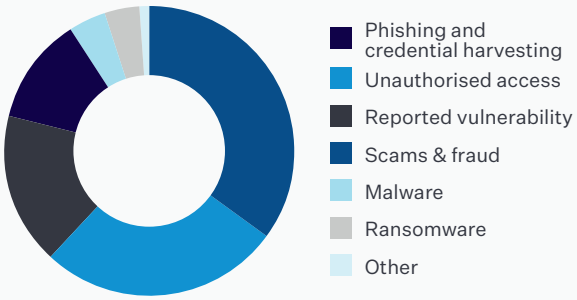
The following information is supplied by CERT NZ*, and notes particular cybersecurity trends in the professional services sector. This information, along with information shared between our organisation and other organisations in our sector informs the commentary given below.

Incidents reported by type



Reporting for specific sectors

The professional, scientific, technical, administrative and support services sectors.



Impacts for our organisation

The latest CERT NZ quarterly report points to the increase in both scams and fraud, as well as phishing and credential harvesting. In discussions with others in the sector, there has been a significant increase in fraud, with several other entities, as well as our own, having made authorised payments to clients, that have turned out to be fraudulent requests. This could ultimately have an impact on insurance premiums for the sector, and decrease levels of client trust for the execution of these types of requests.

Reports continue to focus on unauthorised access to both internal and client information. Several internal incidents have been due to incorrect staff access rights being applied, and there have been some external, malicious attacks attempting to access data. In conversations with other similar organisations, this risk is highlighted and a number of organisations are working to refine and implement proper access control to files.

*CERT NZ receives cybersecurity reports from government, businesses and individuals. They also provide quarterly updates on what they have seen in the threat landscape of New Zealand. To find out more, visit **www.cert.govt.nz.**

Incidents

In the past month, there has only been one significant security incident.

Type of incident	Status
Unauthorised information disclosure	Resolved

Description
A staff member working with information on four clients accidentally sent one of the clients the information for all four.

Discovery
The client emailed the staff member to let them know they had received the incorrect information.

Resolution
The client has confirmed and provided evidence that the three files containing other client data have been deleted. All affected clients have been informed and apologies issued. One client has decided to not continue to work with our organisation.

Time to discover	Time to resolve	Quantifiable Cost	Unquantifiable Cost
3 days	5 hours	$5,000	Potential brand damage etc. unknown

Summary of learning opportunities from our successes and failures

A review is currently underway to determine how information is communicated to clients, and to ensure that the system will alert staff if they are sending out more than one client file at a time, or a spreadsheet with multiple sheets of data.

Compliance

Over the past year we have decided to become ISO27001 compliant to meet international client requirements.

Areas still to be completed for ISO27001 compliance to be met

- Development of security policy
- Completion of BCP to include cybersecurity incidents
- Compliant access management plan
- Annual staff training

New privacy legislation

Update on the Privacy Bill. This was tabled in Parliament in Q2 2018 and includes a proposal for mandatory data breach notification to the Privacy Commissioner and affected individuals for certain breaches. We are reviewing our processes and procedures to ensure we are compliant.

Summary of key insights

- Information protection and security awareness weaknesses could have a significant impact on our organisation's security, and these issues need to be resolved as soon as possible.
- Fraudulent activities are a key security threat in our sector.
- An unauthorised information disclosure incident has cost the organisation $5,000.
- There are four key tasks left to complete to meet our ISO27001.

Example 2 – Cybersecurity dashboard

This is a large organisation in the medical sector (about 500 staff). The organisation underwent a risk assessment two years ago, and has been implementing the recommended changes since then. The main purpose of this report to the board is to show the maintenance of the current status, the completion of the remaining projects to get the organisation to their desired level of security, and preparation for any potential attacks.

Top 5 security risks

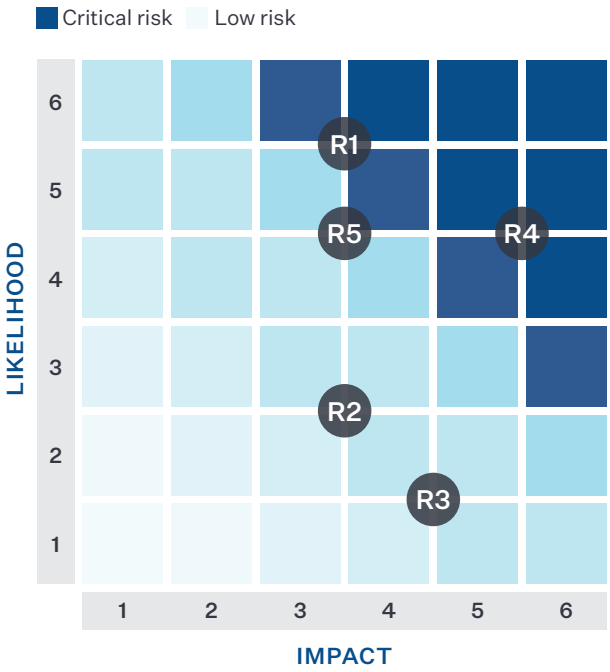
R1. Risk of attack through email (phishing or fraud) leading to leak of customer data or incorrect payment of funds.

R2. Risk of physical access to sensitive information as staff computers and physical files are accessible in all branches, linking back to the central customer database.

R3. A lack of agreed standard operating procedures for staff (including implementation of the security policy) means there is an increased risk of staff operating in an insecure manner.

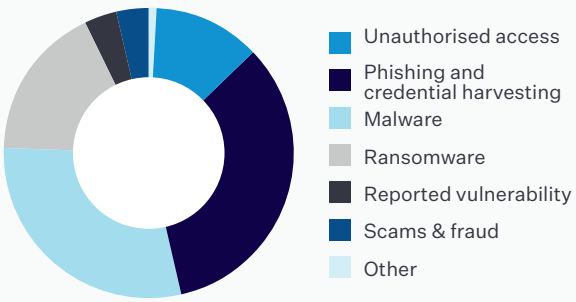
R4. There is a risk that the business is exposed to a security risk from third party suppliers, as the security requirements of suppliers have not been adequately covered in a number of contracts.

R5. As there is no agreed plan in place for dealing with a security breach or malicious attack, there is a risk that damage to the business could be more extensive than necessary.



Emerging risks, threats or vulnerabilities

Reporting for specific sectors
Healthcare and social services



Impacts for our organisation

There has been increased interest by attackers on the medical service in New Zealand. Some major and sustained attacks on DHBs have been recently reported, and we see a similar pattern in other, smaller medical facilities. Hackers are known to prize medical data for resale on the dark web, and this, along with the increased activity, puts most organisations holding medical data, at risk. There is a need to review traffic logs, and look for the types of attacks affecting the organisation, as these may be an indicator if this organisation is being targeted.

Key projects

The organisation is addressing the 20 most urgent IT issues from its security assessment. Most of the items are now in the testing phase and it is anticipated that work will be complete by the end of Q3 2019.

Risk level	Number of issues	Issues complete	Issues WIP	Issues not being addressed this year
High	2	2	0	0
Medium	8	2	5	1
Low	18	0	11	7
Total	28	4	16	8

Implementation of projects

A number of projects were set up after our initial security assessment two years ago. Annual assessments have determined which projects have been successfully implemented, which projects still needed to be completed, and identified new risks that needed to be addressed. These are the top 5 security-related projects currently underway.

Project	Completion due	On track	Notes
Roll out of 2-factor authentication across the business	Q3, 2018	Running to schedule	No issues
Reconfiguration of building access and layout to ensure physical security	Q1, 2019	Design work underway – to be approved before building started	May need additional permissions from landlord for some of the changes
Upgrade of staff computer operating system	Q3, 2019	New OS selected, costings underway	No issues
Re-signing of all third-party suppler contracts to include security responsibilities	Q3, 2018	Two re-signed, one underway	May need to change supplier if unable to re-sign
Appointment of a Security Officer to the Risk and Assurance team	Q2, 2019	Role has been approved and budgeted for. Advertising underway	No issues

Ongoing maintenance activities

	Activity	Status
People	Awareness training	% of staff completed training: 78%
Technology	Upgrade of organisation wide operating system	Date for cutover to Windows 365: 28/10/2018

Cyber-insurance

We are reviewing our cyber insurance arrangements including to ensure that we have clarity about what it will and will not cover (and in what circumstances). Some areas that we are considering include:

- Payment of ransom for ransomware attacks
- Loss and restoration of customer data
- Recovery to restore system, cover legal costs and cover media costs in the event of a breach.

The Institute of Directors in New Zealand connects, equips and inspires its more than 9000 members, to add value across New Zealand business and society, through thought leadership, our extensive network, professional governance courses, events and resources. **www.iod.org.nz**

Aura Information Security is a leading provider of information security consulting services to corporates and governments in Australia and New Zealand. Our focus is to provide the very best independent security advice and support to businesses, so that their digital world is more secure, reliable and resilient. **www.aurainfosec.com**

Acknowledgement: We want to acknowledge the National Association of Corporate Directors (USA) and Internet Security Alliance (USA) for their 2017 Cyber-Risk Oversight publication which was invaluable in preparing this resource.

ISBN: 978-0-473-45846-1