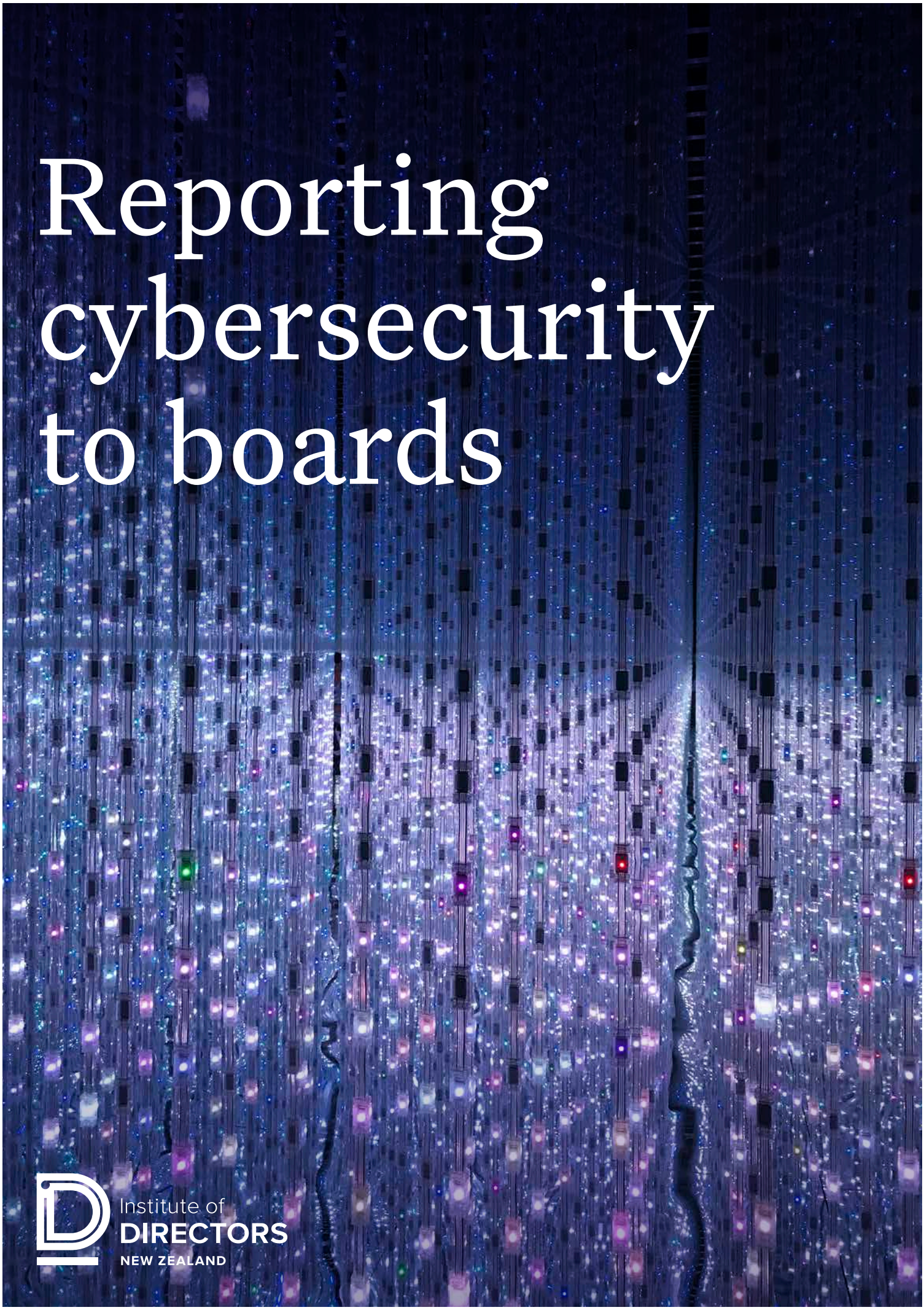


Reporting cybersecurity to boards

Institute of DIRECTORS NEW ZEALAND

Reporting cybersecurity to boards

Cyberattacks rank as a top risk to organisations, both in terms of likelihood and overall impact, according to the 2024 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 receiving sufficient information.*

Improving cybersecurity reporting

To help improve cybersecurity, this resource sets out:

- Guiding principles for reporting to boards
- Questions to ask when developing meaningful metrics
- Sample dashboard formats

This resource should be read in conjunction with the IoD's Cyber Risk: a practical guide.

Data breaches and privacy

The growth of the internet and the digital economy – along with the emergence of new technologies, particularly AI – have changed the way organisations operate and how personal information is collected, used and stored.

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

Oversight and monitoring of cybersecurity

Cybersecurity refers to the protection of information and IT systems in the cyber realm. Like any other business risk, cyber risk requires board-level attention and responsibility. Given this, it is critical that boards allocate time on the agenda to discuss their approach to cybersecurity, and regularly assess their capacity to address evolving threats.

As part of the board's oversight and monitoring role, it is responsible for holding management to account for establishing a fully integrated organisational approach to cybersecurity. This includes having appropriate risk management, policies, processes and procedures in place. To provide effective oversight, boards need access to high-level, holistic reporting on cyber risks and the overall maturity of their organisation's cybersecurity programme.

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

* Only 55% of directors in the IoD's 2025 Director Sentiment Survey said they receive reporting on cyber and data breach risks, meaning a large share are not confident they're getting regular or structured information.

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 from cyber threats. This requires adopting a risk management framework and conducting regular risk assessments.

Some organisations will already have well-developed reporting, while others may be starting their journey to develop comprehensive cybersecurity oversight.

Boards and management need to consider the format and frequency of reporting, and determine what information is most valuable in maximising effective board oversight. It can be useful to start with a small number of the most significant cybersecurity metrics – such as the highest-rated risks and associated controls, particularly those tied to key business goals and strategic initiatives – and expand reporting over time. Reporting to the board on cybersecurity should follow similar principles to reporting in other key areas, such as health and safety or 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 should be front and centre?

Many boards become sidetracked by focusing on controls rather than the risks they are designed to mitigate. Boards need to first agree on the organisation's top 10 cyber risks.

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

Boards need to know the organisation's critical assets are identified and protected. A first step is confirming whether those assets have been correctly defined and understanding their current state. Many organisations struggle to articulate what their critical assets are, and this gap should be one of the first issues reported to the board.

What cybersecurity investments are necessary?

Organisations need to understand their risks before deciding which investments will deliver the biggest return in reducing those risks. Useful questions include:

- What are the highest risks to our key assets?
- What controls can mitigate the largest amount of risk?
- Do we have any legal or compliance requirements that must be met?

How do we measure the effectiveness of our organisation's cybersecurity programme – and how do we compare to others?

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 effective has our risk mitigation strategy been in the last reporting period?

This metric will inform conversations about addressed risks and whether the situation has improved or worsened over time.

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

Supply chain relationships often pose increased risk because of system interconnectivity and data-sharing. Useful questions include:

- How does our organisation monitor third-party risks?
- How many external vendors access 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 risk. Data on policy compliance, training implementation and completion rates can help boards monitor and assess insider risk.

The following two examples of cybersecurity dashboards are based on fictitious organisations. They are not intended to be used as templates, but to inform and inspire better reporting to boards. The main differentiator is whether they are using a risk-based approach to assessing their cybersecurity posture or a maturity gap approach.

Example 1 – Cybersecurity dashboard

Example 1 is based on a large New Zealand organisation. To better understand their cybersecurity risks, the organisation undertook a comprehensive cybersecurity risk assessment.

All identified cyber risks – including those shown here – have been added to the organisation's overall risk register, where they can be reviewed in full.

This dashboard presents a selection of the key cyber risks facing the organisation. A critical element for board consideration is the financial exposure associated with each risk – both before and after mitigation – to support robust return on investment (RoI) decision-making.

Current Cybersecurity Risk Status

Critical Asset	Key Risk	Financial Risk Now	Financial Risk After Mitigation	Mitigation Progress Trend
CRM	The CRM runs on outdated and end-of-support software that has known vulnerabilities that could be exploited, exposing sensitive data.	$250,000	$20,000	↓
Billing database	The billing database is hosted by a third-party that has repeatedly failed a third-party security assessment. This could lead to a breach.	$75,000	$35,000	↑
HR system	The HR system holds sensitive data on staff who no longer work in the organisation. This could be a privacy issue.	$100,000	$15,000	▢
Web portal	The web portal has only an 8-character password and no multi-factor authentication functionality, making it easy to brute force access.	$500,000	$150,000	↓
Web portal	The web portal is not backed up, so any issue could lead to an inability to restore service.	$350,000	$40,000	↓

↑ Improvement ↓ Stalled ▢ Getting Worse

Training

Staff require ongoing training on threats such as phishing, smishing, vishing and other emerging cyber risks. Results from these activities should be reported to the board to provide visibility into the organisation's overall level of awareness. It is also important to include the board in cybersecurity training and simulated phishing exercises. As high-profile targets, directors may not otherwise receive targeted education.

	Click Rate	Monthly Trend
Phishing click rate	8%	↑
Smishing click rate	13%	↓
Vishing click rate	5%	↑

Training Completion Rate	Monthly Trend
85%	↓

Testing

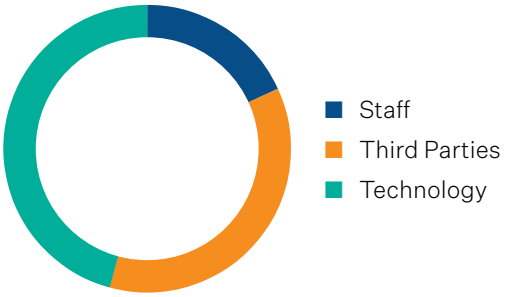
Where audits, penetration tests or red team exercises have been conducted, a high-level summary of the findings should be provided to the board to give visibility into the organisation's control effectiveness.

Web Portal Pen Test Results		
Issue	**Priority**	**Status**
Susceptible to cross-site scripting	Critical	Open
Running out-of-date software	High	Open

Incidents

Incidents should be reported, with high-level trend data to help the board identify where issues are emerging or recurring.

Cause of incidents in the last month

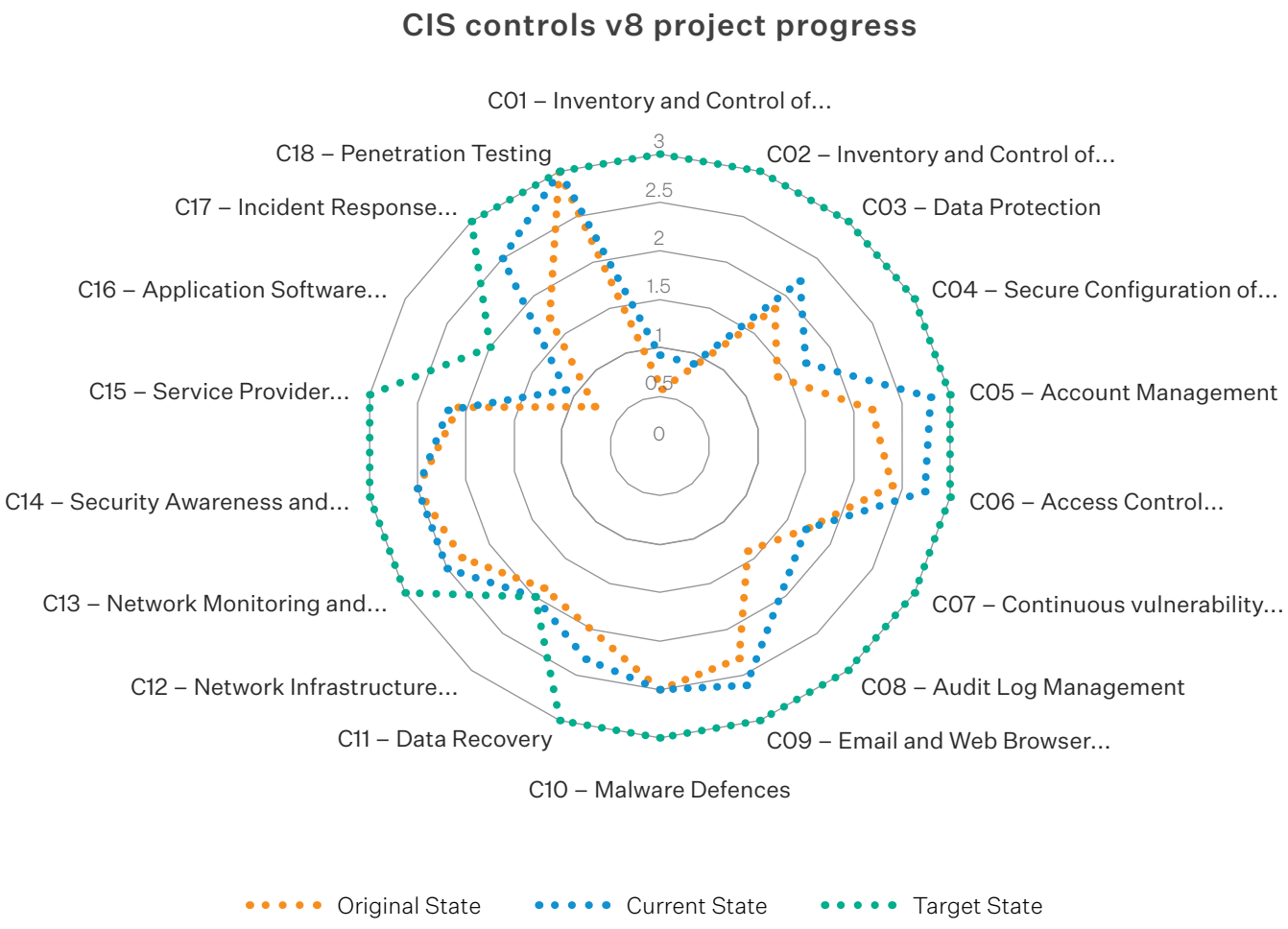


Example 2 – Cybersecurity dashboard

This example represents a less mature organisation that has not yet undertaken a formal cyber risk assessment. Instead, it has completed a maturity gap assessment, using the CIS Controls v8 framework. The main purpose of this dashboard report is to show progress towards improving current maturity scores relative to the organisation's target scores.

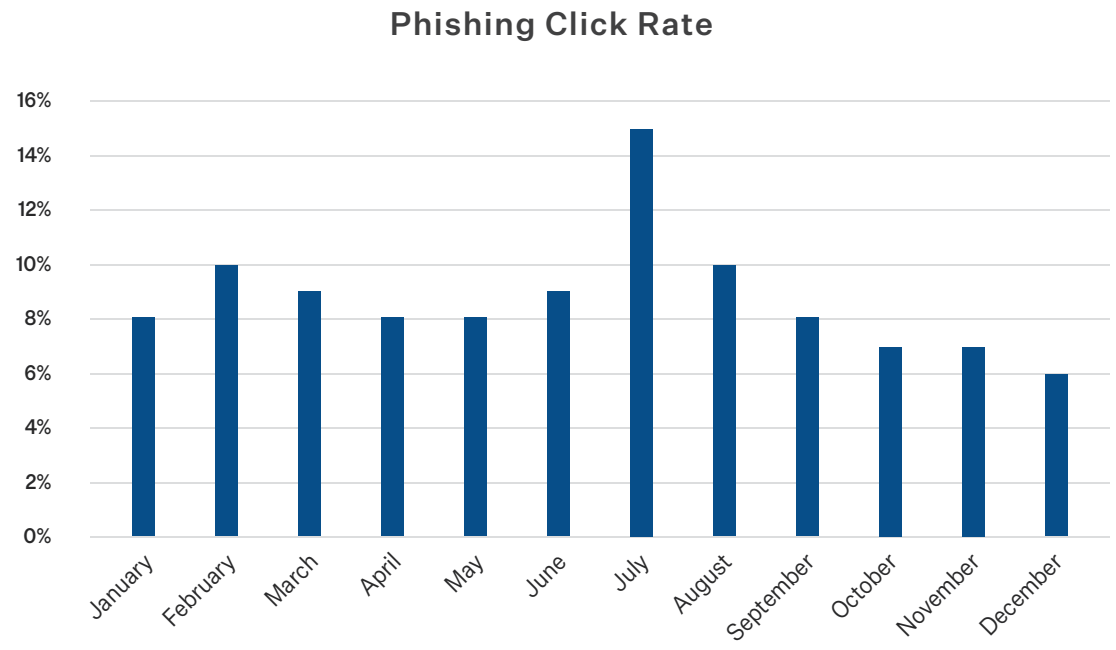
A key limitation of not having a risk assessment is that it becomes difficult to link the criticality of specific controls to the risks faced by key business assets. As a result, return on investment (RoI) decisions are often based on intuition rather than evidence.

CIS controls v8 project progress



Training

Another way to present the security awareness training.



Business Continuity and Disaster Response

It is essential the organisation has robust plans and processes in place to respond to business interruptions – whether from a pandemic, natural disaster or cyberattack.

Key Asset	Existing BCP and DRP
CRM	In place
Billing Database	Out of date
HR system	Non-existent
Web Portal	In place

Also, the result of testing should be reported as a plan needs to be tested to prove its worth.

Test	Result
Tabletop simulation of CRM failure for 2 days	Plan was successsfully followed, with only minor updates required.
Failover test of billing database	Billing database was unable to fail over. A new solution is needed.
Restore of HR system data from backup	Data was restored in 5 hours, but some corruption occured. A new data backup and restore system is required.

The Institute of Directors in New Zealand connects, equips and inspires its more than 10,500 members, to add value across New Zealand business and society, through thought leadership, our extensive network, professional governance courses, events and resources.

iod.org.nz

About Kordia

Kordia is a leading provider of innovative technology solutions. For more than 65 years, we've been keeping New Zealanders and their businesses stay safe, connected, and prepared for the future. We work across New Zealand, Australia, and the Pacific, delivering mission-critical technology in cloud, cyber security, broadcasting, maritime communications, critical communications infrastructure, and more. Backed by a team of 480+ experts, we're trusted by some of New Zealand's biggest organisations to keep them and their customers protected. We're proudly Kiwi-owned and here to help NZ Inc create, innovate, and grow.

Learn more at **www.kordia.co.nz**

ISBN: 978-0-473-45846-1