THINKING AHEAD. BEING PREPARED.

Cyber Security Resilience of New Zealand's Nationally Significant Organisations 2017-2018

NATIONAL CYBER SECURITY CENTRE
A PART OF THE GCSB

New Zealand Government

Contents

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

In order for New Zealand to stay competitive we need to keep pace with the rapid changes in technology. Cyber security concerns are affecting our confidence in keeping on top of this. With a mindset shift, organisations can benefit from having a robust plan. It's all about maintaining good oversight, good resources, getting the right expertise on board, and being in a state of constant readiness. It's simple when it comes down to it; thinking ahead and being better prepared.

FOREWORD

The cyber security risks facing New Zealand's nationally significant organisations (NSOs) are increasing at the same rate as society's dependency on information technology.

Cyber security is a complex issue affecting a broad spectrum of New Zealand organisations, and New Zealand society as whole. From NSOs to individuals; from the executive board room to technical specialists on the front line, a joined up approach is key to improving New Zealand's cyber security posture.

New Zealand's National Cyber Security Centre (NCSC) – a part of the Government Communications Security Bureau – has developed a nationwide understanding of the cyber security resilience of New Zealand's NSOs. This report shares insight gathered from the first comprehensive cyber security survey of New Zealand's NSOs.

It identifies four key focus areas in which New Zealand organisations could improve, and provides practical steps that organisations can take to strengthen their cyber security posture and resilience.

The NCSC would like to acknowledge the vital contribution made by NSOs in taking the time to talk with us over the past year. This report would not have been possible without the input and cooperation of NSOs up and down the country.

Each contributing organisation has received an individual response that outlines areas for their own improvement. At the same time, the NCSC is publishing this summary assessment to highlight wider trends and to inform decision making more generally.

New Zealand's NSOs should be optimistic about their ability to improve their own cyber security posture. There is a risk that organisations feel powerless to improve cyber security when the most commonly noted trend is that threats and incidents continue to increase. However, international data shows us that improvements in cyber security are possible when pursued systematically and strategically.

Continual improvement of cyber security across New Zealand's NSOs demands a joint effort. The NCSC will continue to provide support and guidance as part of our core business. But at the same time, organisations themselves, security suppliers and IT vendors play an integral role in lifting the cyber security resilience of our most important information infrastructures and in turn protecting the national security of New Zealand.

Andrew Hampton
Director General
Government Communications Security Bureau

WHAT WE DO

The NCSC is a part of the Government Communications Security Bureau (GCSB). We deal with advanced cyber threats that have the potential to affect New Zealand's national security and the economy.

Our mandated focus is on New Zealand's nationally significant organisations. These include the most critical government departments, key economic generators, niche exporters, research institutions and operators of critical national infrastructure.

We are aware of a range of international cyber threat actors that target New Zealand computer systems and information infrastructure for financial gain or as a means of advancing their own position.

New Zealand's cyber threat environment is increasingly complex and far from benign. The sources of hostile cyber activities and cyber crime include both state-sponsored and non-state actors.

The NCSC works with New Zealand's NSOs to counter these threats:

- We supply advanced cyber threat detection and disruption services (CORTEX) to organisations of national significance.
- We respond to cyber incidents that pose a potential threat to New Zealand's national security and economic well-being.
- We provide analysis and assessment of cyber threats to our customers and partners.
- We foster a mature security culture based on standards set out in the Government's Protective Security Requirements and the New Zealand Information Security Manual.

The NCSC also works closely with CERT NZ (Computer Emergency Response Team) to provide guidance and help on cyber threats. CERT NZ helps business, organisations and individuals wanting prevention and mitigation advice about online security issues.

"New Zealand's cyber threat environment is increasingly complex and far from benign."

EXECUTIVE SUMMARY

As New Zealand organisations adopt digital products and services at pace, they need to ensure they adjust their business risk settings, particularly the implementation of good cyber security policies and practices.

Digital transformation is underway in organisations across the public and private sectors and cyber security is crucial to ensure this transformation is sustainable and achievable. Without effective cyber security, organisations will struggle to consistently deliver digital products and services in a way that retains the trust and confidence of their customers or stakeholders.

The NCSC's analysis of data gathered from 250 New Zealand NSOs has identified four areas of good practice where organisations can focus their efforts for the greatest effect. These areas are:

- **Governance** – Promoting cyber security at a senior leadership level to protect an organisation's most important digital assets.
- **Investment** – Investing in cyber security to minimise risk and maximise returns.
- **Readiness** – Preparing the organisation to detect, respond, and recover from a cyber security incident.
- **Supply Chain** – Maintaining oversight and awareness of the cyber security risks in an organisation's supply chain.

The diversity and size of New Zealand organisations means they are not conducive to a 'one-size-fits-all' approach. Often, small organisations have insufficient resources to protect all assets equally or a growing organisation may have a higher risk appetite. However, the focus areas identified in this report overlap and are mutually reinforcing; even small improvements in any of these categories will help raise cyber resilience overall.

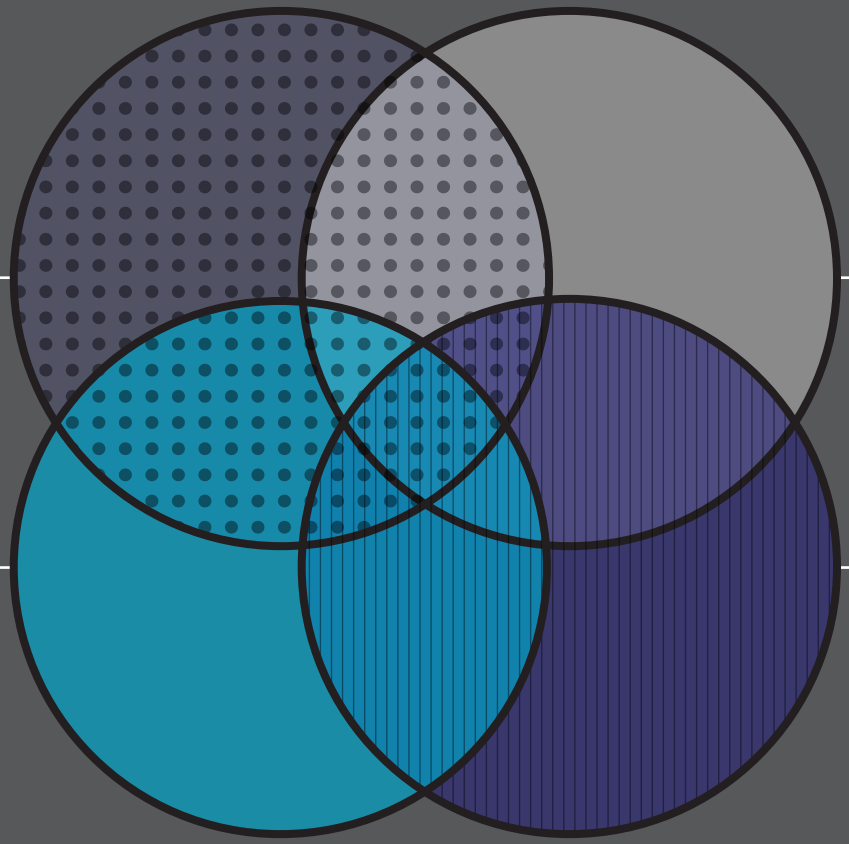
To assist organisations to improve their cyber security and resilience, the report outlines practical steps that can be taken in the four areas mentioned and provides links to useful resources.

GOVERNANCE

Promoting cyber security at a senior leadership level to protect an organisation's most important digital assets.

INVESTMENT

Investing in cyber security to minimise risk and maximise returns.



READINESS

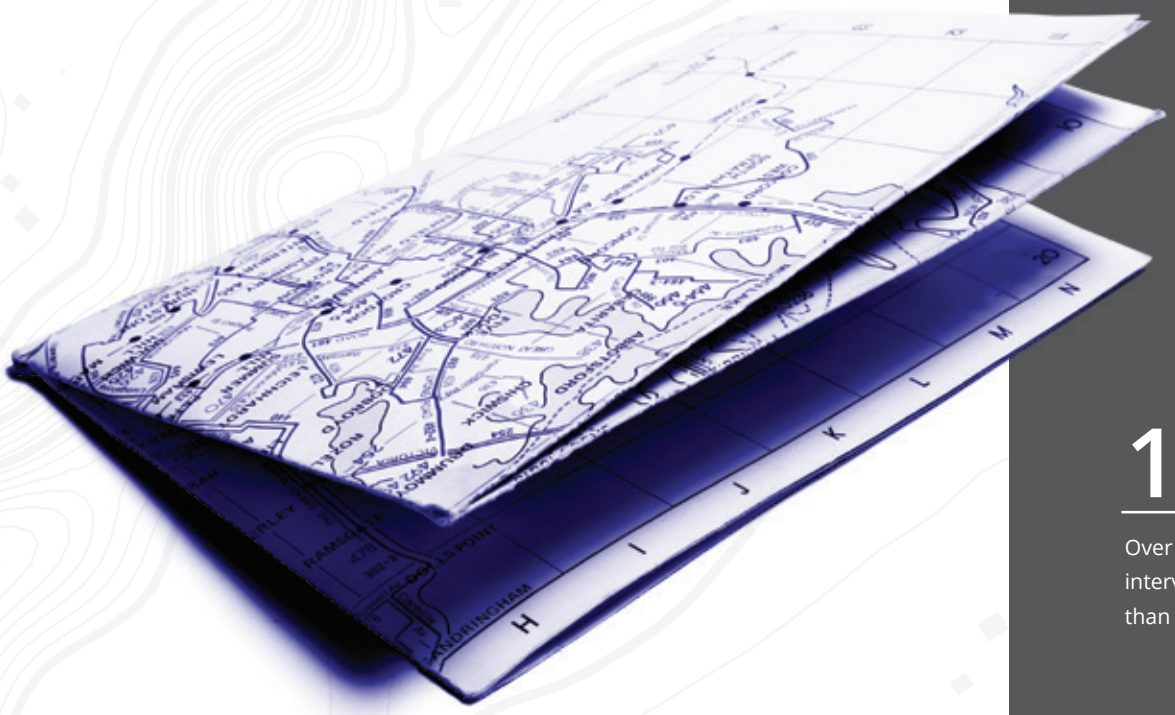
Preparing the organisation to detect, respond, and recover from a cyber security incident.

SUPPLY CHAIN

Maintaining oversight and awareness of the cyber security risks in an organisation's supply chain.

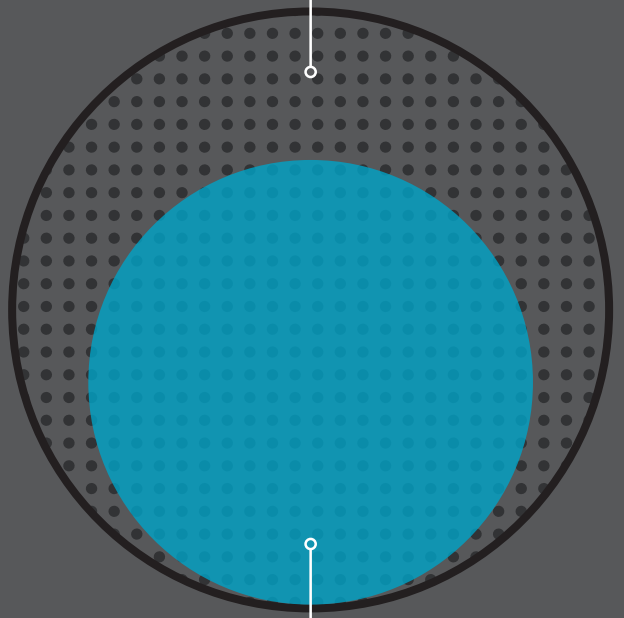
INTRODUCTION

This report summarises key findings from cyber security assessments undertaken with New Zealand's NSOs.



250

250 organisations of national significance responded to a survey developed by the NCSC.



135

Over half of the organisations interviewed have fewer than 500 employees.

The report provides organisations and cyber security professionals with a New Zealand-centric snapshot of where the greatest improvements in cyber security can be achieved. The NCSC is using the information gathered in our survey to focus and inform decisions about our cyber security products, services and the support we provide to NSOs. The data will also assist us to measure New Zealand's progress towards improved levels of cyber security over time.

Methodology of survey

This report is based on the responses of 250 organisations of national significance to a survey developed by the NCSC. All respondents are nationally significant organisations. The survey was composed of 50 questions based on industry standards and principles contained in the New Zealand Information Security Manual and Protective Security Requirements.

The survey was delivered by the NCSC's Outreach and Engagement team, which conducts over 2000 engagements annually with NSOs. Each organisation's response to these questions was based on their own perception and not the NCSC's assessment of their capabilities. The information provided by individual organisations has been anonymised to protect their identity.

NCSC's focus on NSOs

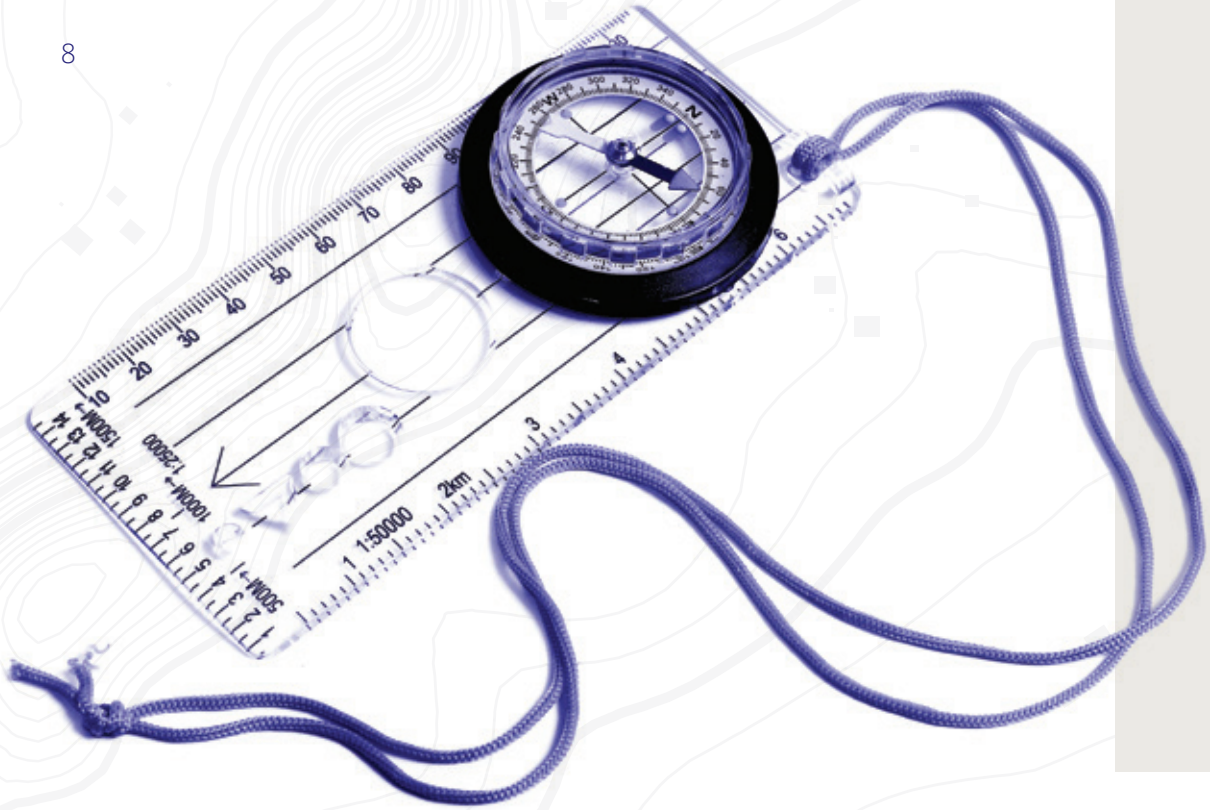
The NCSC's mandated focus, and the focus of this report, is on New Zealand's NSOs. These include the most critical government departments, key economic generators, niche exporters, research institutions and operators of critical national infrastructure. Although modest in size by international standards – over half of the organisations interviewed have fewer than 500 employees – they all provide an important contribution to New Zealand's economic security and wellbeing.

The assessment data identifies how these NSOs would benefit from the NCSC's support. It allows the NCSC to use an evidence-based approach to focus its attention and target resources to achieve the best value for government investment in cyber security. The baselining of cyber security of New Zealand's organisations of national significance is an important step in a journey to support our most important organisations to raise their cyber security resilience.

> "The assessment data identifies how these NSOs would benefit from the NCSC's support."

CHARTING YOUR COURSE.

Promoting cyber security at a senior leadership level to protect an organisation's most important digital assets.



What is cyber security governance and why is it important?

Governance refers to the oversight of cyber security at a board or executive level. Boards and executives are ultimately responsible for the outcomes of any cyber incident, including the impact on stakeholder and customer confidence. Executives and board members play a critical role in driving cyber security as a priority within the organisation, and equally important, ensuring it aligns with organisational objectives.

The creation or elevation of the Chief Information Security Officer (CISO) role within an organisation recognises the need for cyber security to be represented at a senior level. The effectiveness of the CISO function influences the alignment between cyber security investment and the organisation's business objectives. The CISO should be able to articulate to other board members the impact of poor security on the organisation's business operations, new projects and legal risks; as well as monitoring the return on investment in security.

The New Zealand cyber security governance gap

Only 19% of organisations surveyed have a dedicated Chief Information Security Officer (CISO). The remaining 81% either do not have a CISO at all, or have a senior manager that performs the CISO function as part of a broader role. When a CISO has two roles there is inevitable tension between delivering technology projects and advocating for security. Having separate roles ensures both outcomes are effectively represented.

The absence of a dedicated CISO often reflects the smaller size of New Zealand organisations, where specialisation to this extent is not always financially viable. However, it also shows cyber security can lack a strong advocate at executive or board level discussions.

The absence of high level representation within organisations is compounded by a lack of regular reporting of cyber security information to senior management – 39% of organisations do not provide cyber security reporting to senior management or only do so on an ad hoc basis. Even without a CISO, an organisation can still make cyber security issues visible to management through regular reporting of incidents or issues.

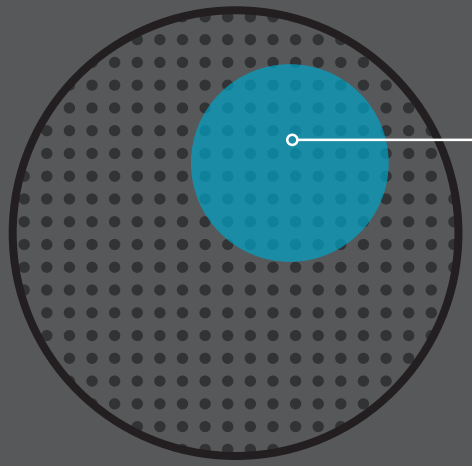
Suggested steps to increase maturity

- Identify the person, or people, who are accountable for cyber security in your organisation.
- Ensure your organisation's leadership receives regular reporting on security issues from your IT team or service provider.
- Make cyber security reporting easier to consume. For example, report cyber security 'near misses' in the same way as you might report Health and Safety issues.

Useful resources

- **https://www.iod.org.nz/Governance-Resources/Publications/Practice-guides/Cyber-Risk-Practice-Guide**
- **https://www.ncsc.govt.nz/assets/NCSC-Documents/cyber-security-risk-management-board.pdf**

The organisations surveyed:

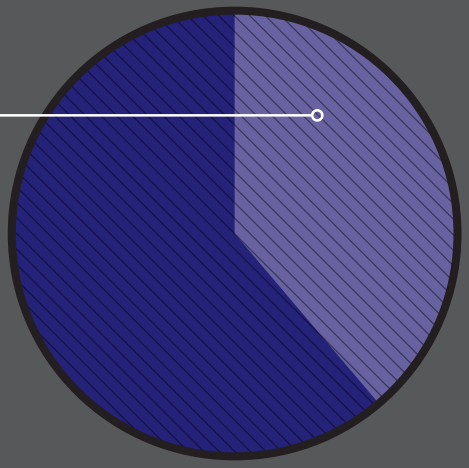


19%

of organisations surveyed have a dedicated Chief Information Security Officer (CISO).

39%

of organisations do not provide cyber security reporting to senior management.



PUTTING THE RIGHT THINGS IN PLACE.

Investing in cyber security to minimise risk and maximise returns.

Cyber security investment in New Zealand

73%

The majority of organisations surveyed (73%) increased their spending on cyber security in the past year. However, the NCSC's survey suggests that this investment had not translated into an increased confidence in their cyber security resilience.

33%

A likely contributing factor is that only 33% of organisations had fully identified their critical information assets. If an organisation is unclear about what its most critical assets are, it is difficult to be confident they are protected. It also becomes very difficult to make risk-based decisions to prioritise spending in the most important areas.

52%

Spending has increased across all areas of cyber security, but most organisations are spending on new tools and vulnerability assessments. This focus on investment in technology has come at the cost of investment in people. As a result, 52% of organisations reported they had insufficient numbers of skilled staff to satisfy their perceived security requirements.

38%

Only 38% of organisations surveyed had some separation between their cyber security budget and regular IT budget. This lack of separation can result in cyber security budgets being used for non-security related IT purposes, and limits the ability to track return on cyber security investments.

Why is well-directed investment critical for cyber security?

Investment is necessary for any organisation to improve their cyber security. An organisation that decides not to invest in cyber security is more likely to become a victim and experience higher costs in the event of a cyber incident. However, not all investment returns the same value to an organisation. Agreement at a governance level on the organisation's risk appetite and identification of key assets are critical first steps to ensure investment is directed and balanced appropriately.

Area of spending	Percentage of organisations that increased spending in this area in the past 12 months
IT STAFF TRAINING	54%
MORE IT SECURITY STAFF	45%
VULNERABILITY ASSESSMENTS	61%
NEW TOOLS	70%
AUDITS	55%

Suggested steps to increase maturity

- Balance strategic, longer term investments in the development of assets and staff over "one off' costs for vulnerability assessment snapshots.
- Identify the information assets that are most critical to your business and assess the risks posed to these assets.
- Create a separate budget line to effectively manage and track IT security spending.

Useful resources

- **https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697**
- **https://www.ict.govt.nz/assets/ICT-System-Assurance/Risk-Assessment-Process-Information-Security.pdf**

> "The focus on investment in technology has come at the cost of investment in people."

KEEPING WATCH.

Preparing the organisation to detect and recover from a cyber security incident.

Why focus on readiness for a cyber security incident?

It is a matter of 'when' not 'if' an organisation will experience a cyber security incident. Readiness for an incident enables organisations to reduce the overall cyber security risk through prompt and effective recovery. The longer a breach or incident goes undetected, the greater the impact it will likely have. A 2018 report commissioned by IBM and undertaken by the Ponemon Institute found the average time taken by organisations to identify an intrusion was 197 days. The ability to detect an intrusion and to respond promptly is the difference between a minor and a major compromise.

The level of cyber security readiness in New Zealand

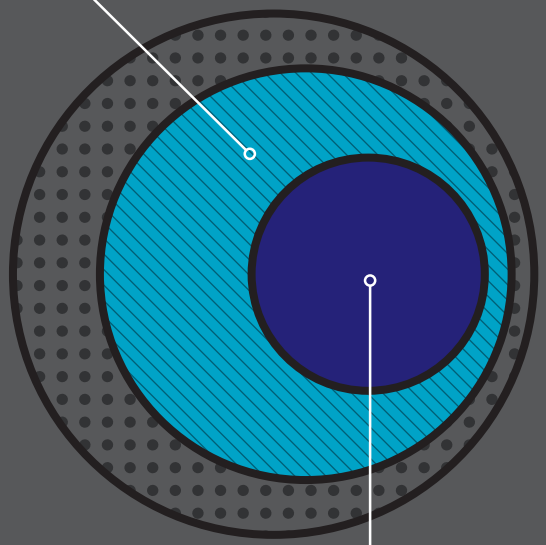
The first step in responding to any cyber incident is knowing it has occurred. In New Zealand, 41% of organisations are either mildly confident or not confident in their ability to detect an intrusion.

Without the ability to detect cyber threats, intrusions can go unnoticed for long periods and have a greater impact. The ability to detect cyber threats requires the right tools and the right people. Trained staff with a focus on security can help organisations evaluate risk, make informed decisions and plan ahead. When things go wrong, trained staff will help an organisation detect and recover from an incident. Only 38% of organisations reported having full time IT security staff, while 67% also include IT security functions as an add-on to an existing IT role.

The organisations surveyed:

63%

of organisations have an incident response plan.



33%

have not tested their plan in the last year.

When an organisation becomes aware of an incident, being ready to respond can reduce the impact of a compromise. A key readiness factor is having a plan to allow an organisation to react quickly and decisively when an incident occurs – just 63% of organisations have an incident response plan. However, 33% have not tested their plan in the last year. An up-to-date incident response plan takes the guesswork out of determining appropriate actions, roles and responsibilities in the midst of a crisis. It also serves as a framework to preserve evidence in the event legal action is sought following an incident.

Suggested steps to increase maturity

- Acquire the tools or services that enable detection of incidents.
- Prepare a cyber security incident response plan and test it on a regular basis.

Useful resources

- **https://acsc.gov.au/publications/protect/essential-eight-explained.htm**
- **https://www.ncsc.govt.nz/assets/NCSC-Documents/New-Zealand-Security-Incident-Management-Guide-for-Computer-Security-Incident-Response-Teams-CSIRTs.pdf**
- **https://www.cert.govt.nz/it-specialists/critical-controls**

IN SAFE HANDS.

Maintaining oversight and awareness of the cyber security risks in your supply chain.

Why is supply chain security increasing in importance?

Outsourcing cyber security requirements to third-parties or managed services providers can be an effective way for a small organisation to overcome the challenges of IT investment. However, this does not transfer risk. Even if an organisation outsources IT or security functions, the board and executives must remain accountable for the performance of those functions.

Outsourcing IT, cyber security or other business functions can enhance security but it also reduces visibility of potential risks. Organisations need to be aware of the strength of each link in their IT or security supply chain. Organisations are also responsible for ensuring third party providers are delivering improvements to security at the outset and for the duration of a contract.

To understand cyber security risk, good information is critical. For those organisations reliant on their service provider for cyber security reporting, it is important that regular and clear reporting is part of the contract.

Supply chain security in New Zealand

For many organisations, the primary opportunity to influence the security levels of IT services provided by third parties is during contract negotiation. Out of those organisations that contract with managed service providers, 64% considered IT security as part of the vendor contracting process.

However, after the contract was signed, many organisations were unsure whether these clauses were adhered to by their providers. While 72% of organisations use some type of managed service provider, 36% of those have no mechanisms in place to confirm whether their vendor is delivering on the agreed level of IT security. As a result, 41% of organisations remain less than confident of their ability to detect an intrusion.

Suggested steps to increase maturity

- Include cyber security as a consideration when assessing new vendors.
- Include regular security reporting as part of the contract and, where possible, build specific security clauses into Service Level Agreements.
- Ensure you have the right to audit your vendor's performance periodically to validate the agreed level of security is being provided.

Useful resources

- **https://www.us-cert.gov/APTs-Targeting-IT-Service-Provider-Customers**
- **https://acsc.gov.au/publications/protect/questions-for-service-providers.htm**
- **https://www.baesystems.com/en/cybersecurity/blog/how-to-manage-your-supply-chain-cyber-risk**

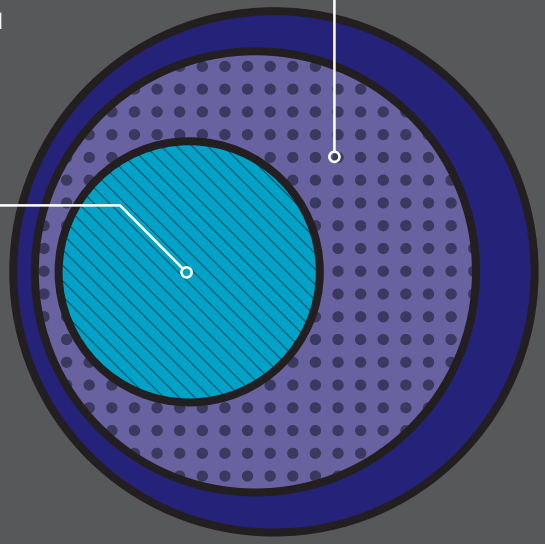
The organisations surveyed:

72%

of organisations use some type of managed service provider.

36%

of those have no mechanisms in place to confirm whether their vendor is delivering on the agreed level of IT security.



41% of organisations remain less than confident of their ability to detect an intrusion.

NEXT STEPS

The survey results have given the NCSC a unique insight on the cyber resilience of New Zealand's NSOs. We are committed to supporting them to improve their cyber security resilience.

Using the evidence gathered, the NCSC will:

- Provide individual and aggregated reporting to all the organisations that were surveyed.
- Use information provided to refine and tailor future NCSC products and services to better meet customer needs.
- Work with different industries and sectors to address key sector specific resilience issues.
- Develop information campaigns, based on the focus areas of this report, to continue to drive improvements in New Zealand's NSOs security practices.
- Conduct future surveys to observe and measure changes to the cyber resilience of NSOs.

If you wish to discuss the findings of this report please email the NCSC at info@ncsc.govt.nz

REFERENCE LIST

Focus area	Suggested steps to increase maturity	Useful Resources[1]
GOVERNANCE	• Identify the person, or people, who are accountable for cyber security in your organisation. • Ensure your organisation's leadership receives regular reporting on security issues from your IT team or service provider. • Make cyber security reporting easier to consume. For example, report cyber security 'near misses' in the same way as you might report Health and Safety issues.	• https://www.iod.org.nz/Governance-Resources/Publications/Practice-guides/Cyber-Risk-Practice-Guide • https://www.ncsc.govt.nz/assets/NCSC-Documents/cyber-security-risk-management-board.pdf
INVESTMENT	• Balance strategic, longer term investments in the development of assets and staff over 'one off' costs for vulnerability assessment snapshots. • Identify the information assets that are most critical to your business and assess the risks posed to these assets. • Create a separate budget line to effectively manage and track IT security spending.	• https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697 • https://www.ict.govt.nz/assets/ICT-System-Assurance/Risk-Assessment-Process-Information-Security.pdf
READINESS	• Acquire the tools or services that enable detection of incidents. • Prepare a cyber security incident response plan and test it on a regular basis.	• https://acsc.gov.au/publications/protect/essential-eight-explained.htm • https://www.ncsc.govt.nz/assets/NCSC-Documents/New-Zealand-Security-Incident-Management-Guide-for-Computer-Security-Incident-Response-Teams-CSIRTs.pdf • https://www.cert.govt.nz/it-specialists/critical-controls/
SUPPLY CHAIN	• Include cyber security as a consideration when assessing new vendors. • Include regular security reporting as part of the contract and, where possible, build specific security clauses into Service Level Agreements. • Ensure you have the right to audit your vendor's performance periodically to validate the agreed level of security is being provided.	• https://www.us-cert.gov/APTs-Targeting-IT-Service-Provider-Customers • https://acsc.gov.au/publications/protect/questions-for-service-providers.htm • https://www.baesystems.com/en/cybersecurity/blog/how-to-manage-your-supply-chain-cyber-risk

[1] The links provided are merely an example of the information available. The inclusion of these links is not an endorsement of one vendor over another.

For futher information visit: **www.ncsc.govt.nz**
or email: **info@ncsc.govt.**nz