Photo credit: Chris Tse

Mind the gap: Governing cyber security risks

April 2025

Robust cyber security allows public organisations to provide services safely and reliably. It helps maintain trust in how the government handles and protects information.

Governors play an important part in making sure that public organisations are vigilant about cyber security. They need to spend enough time and engage the right expertise to properly understand cyber security risks and make sure their organisation is prepared to respond.

We recently looked at selected public organisations to see how well they were governing their cyber security risks. We found that although governors are taking cyber security seriously, they have more work to do to support their organisations to reduce the gap between the amount of cyber security risk they are comfortable with and the amount of risk they currently face.

At the end of this article is a list of further resources and a checklist for governors to inform their cyber security work.

More digital services, more cyber threats

The public sector is increasingly providing services digitally. In 2024, KPMG reported that annual public sector spending on information technology was approaching $1 billion.

Meanwhile, cyber threats are evolving, both in volume and sophistication. Effective cyber security is critical to the public sector's ability to maintain public trust and carry out its work.

Public organisations hold a considerable amount of sensitive personal and commercial information. Some also hold information on matters of national security, defence, and international relations.

Misuse of any of this information could be damaging to the people who provided the information, the people the information is about, and to the reputation of the organisations holding the information. Ultimately it could be damaging to New Zealand's global interests.

A cyber attack on public services can have widespread and ongoing effects, including significant costs and social disruption. Even small incidents can undermine public trust and confidence.

This article is based on our observations from a performance audit that looked at how a selection of public organisations govern cyber security risks.[1]

Types of cyber threats

Cyber threats take many forms and come from a wide range of sources. The Ministry of Foreign Affairs and Trade has identified that these threats include:

- *cyber espionage* for political, economic, and commercial gain, such as intellectual property theft;
- *cyber terrorism*, such as disrupted services or damage to critical infrastructure systems;
- *cyber crime*, such as scams involving online trading, dating sites, fake investments, or the theft of financial or identity data; and
- *cyber vandalism or "hacktivism"*, such as websites being defaced or their services interrupted for political purposes.[2]

Public organisations need to be aware of the cyber threats they face, and the risks these present, in the context of their organisation's vulnerabilities.

Who's involved

Although public organisations are responsible for their own cyber security arrangements, many other organisations support the public sector's cyber security system. These include the National Cyber Security Centre and the offices of the Government Chief Information Security Officer and Government Chief Digital Officer.[3]

The Government has also established Protective Security Requirements – complying with these is mandatory for a core group of public service organisations, but not for others (such as councils, schools, or Crown entities).

Private organisations such as specialist providers also work with public organisations on cyber security matters.

Good cyber governance

Effective governance of cyber security risks is increasingly important and challenging.

Many public organisations' cyber security challenges involve:

- rapid technological changes;
- increasing cyber security threats;
- risks that are difficult to understand and govern because they can be highly technical and involve staff, contractors, and third-party providers;
- a limited pool of people with suitable skills and experience to draw on for staffing and governance needs; and
- use of cloud technologies, where third parties form part of an organisation's cyber defences.

1 We audited the governance of cyber security practices, not the practices themselves. We focused on how cyber security risks were identified and understood and how risk management was resourced, reviewed, and monitored at a governance level. We used the resources included at the end of this article to inform our expectations.

To protect the integrity of their cyber security practices, we haven't identified the public organisations we audited. We thank them for their co-operation and assistance, and we also thank the government cyber security leads and organisations for their insight, co-operation, and assistance.

2 See "Cyber security" at mfat.govt.nz.

3 The National Cyber Security Centre (NCSC) is part of the Government Communications Security Bureau (GCSB). The NCSC provides cyber security services to all New Zealanders, from individuals to nationally significant organisations. The NCSC helps detect and respond to cyber incidents and disrupt cyber security attacks.

The Director-General of the GCSB is also the Government Chief Information Security Officer (GCISO). Among other responsibilities, the GCISO's role includes setting information security standards in the New Zealand Information Security Manual, providing guidance and advice, and providing services to enable the public service to improve its cyber resilience.

The Government Chief Digital Officer is a system lead role held by the Chief Executive of the Department of Internal Affairs. Their responsibilities include setting digital policy and standards, establishing and managing services, and developing capability.

Governors can help by supporting their organisation to understand cyber threats, set a clear risk appetite, and implement mitigations. This includes ensuring that "the right security investment is made at the right time and in the right place".[4]

Remember the basics

No matter how well-developed, large, or sophisticated a public organisation is, getting the basics right is a fundamental cyber security priority. The basics are often described as:

- installing software updates;
- using two-factor or multi-factor authentication; and
- regularly backing up data.

Governors need to be assured that appropriate attention is being paid to these fundamental protections. Regular testing of cyber security awareness among staff is also important.

Some of the organisations we looked at were reporting to governors about operational activities, such as software patching, the outcomes of testing staff with fake phishing attempts, and cyber security awareness training.

The National Cyber Security Centre told us it is preparing a set of baseline cyber security standards for public service organisations.

Security by design

Public organisations need to ensure that cyber security is embedded in the design of systems from the outset. The term "security by design" is often used to describe this approach.

Public organisations that are mandated to comply with the Protective Security Requirements must use certification and accreditation processes to manage the cyber security of a system before it is fully implemented. Some of the other organisations we looked at were also using, or intending to use, these processes.

Some organisations' policies pointed to the need for consideration of information security early in the planning and implementing of new systems.

That's important, but this type of work should not be limited to the implementation of new systems – there needs to be an ongoing process for ensuring that system certification is kept current as new threats emerge.

Governors should seek assurance about these types of protections when considering changes to information technology systems and platforms.

Roles and responsibilities

Governors and managers need to work together in clearly defined roles to effectively govern and manage cyber security. Public organisations also need to ensure that cyber security gets enough governance focus.

The separation of governance and management is not always clear in public organisations – senior managers and technical leaders may also have governance responsibilities, including for cyber security matters. Roles and responsibilities should be clearly defined for each party, including governors, managers, staff, and third-party suppliers. This ensures that expectations are understood and fosters effective and efficient decision-making.

Governors are often pulled in many different directions, and cyber security matters can sometimes be only a small part of broader information technology or risk discussions. In our view, governors need to spend enough time to properly understand cyber risks, assess them, and ask the right questions of the managers responsible for cyber security.

Governors also need to make sure that they are maintaining the necessary skills and knowledge to carry out their responsibilities effectively. This might require specialist assistance and ongoing education and development.

Some of the resources listed at the end of this article contain questions that governors might find useful.

4 National Cyber Security Centre (2022), *Charting Your Course: Cyber Security Governance*, page 3, at ncsc.govt.nz.

Understanding risk

To manage cyber security effectively, governors of public organisations need to set and understand their "risk appetite". This means clearly knowing the overall level of cyber security risk that they are prepared to take on.

Governors need to support their organisations to identify and mitigate cyber security risks to match their risk appetite. Governors also need to fully understand the costs of achieving this, so they can prioritise and plan accordingly.

Common risks

In our view, public organisations should pay more attention to these four risks:

- *Third-party risks*, where third parties either supply services or information or use an organisation's services or information. This is not limited to technology and cyber security providers, but can involve any parties who connect to an organisation's systems. Mitigating this risk requires a clear understanding of the connections between an organisation and its contractors, service providers, and customers.
- *Artificial intelligence (AI)*, which is rapidly evolving and provides new ways for penetrating cyber defences. Although a risk, some forms of AI might be able to be used to support an organisation's cyber security.
- *Operational technology risks*, where cyber attacks target information technology that is embedded in equipment and facilities. This risk is increasing as more items become connected to and controlled over the internet, such as lighting, cameras, and security systems.
- *Spear phishing*, where system users with delegated financial authority are targeted to get a payment out of their organisation. Successful spear phishing attacks can result in a direct financial loss.

Setting an organisation's risk appetite requires a good understanding of what that level of risk would mean for the organisation in the event of a cyber attack. Risks need to be understood in relation to the organisation's size and role, the information it holds, its work and services, and its ability to put good mitigation steps in place.

This can be complex for many public organisations, who face competing priorities and constrained resources. Generally, the public organisations we looked at thought that a low level of residual risk (the level of risk left after mitigation) was appropriate for their circumstances.

We were encouraged to see that these organisations are using well-established cyber security frameworks to inform their risk management.[5] Given the evolving nature of risks and technology, it is important to keep up to date with how these frameworks are changing.

Understand the possible consequences

Most of the public organisations we looked at had higher levels of residual cyber security risk than they had an appetite for. Although they were all working to keep systems and information safe through a range of protections and plans, it was uncertain whether they could reduce the gap between their residual risk and their risk appetite or target risk.

Rapid technological change and increasing cyber threats also mean that simply maintaining existing controls and capability might lead to a higher level of residual risk over time.

Governors need to understand the consequences of not reducing the gap, and carefully weigh this against other organisational risks and investment priorities. In our view, there is scope for more use of a "mission-critical" approach to risk mitigation.

5 These include frameworks by the Centre for Internet Security, the New Zealand Protective Security Requirements, the New Zealand Information Security Manual, and the National Institute of Standards and Technology.

Take a mission-critical approach

A mission-critical approach involves identifying what data and systems are most critical for an organisation to achieve its objectives and function effectively.

Governors need to have a sound understanding and regular visibility of specific risks, their potential impacts, and what is being done to mitigate them. Both the cost of risk mitigation and the potential scale of costs of not mitigating a risk need to be considered.

Constrained resourcing means that careful planning and prioritisation are essential when deciding which mitigation steps to take, particularly for public organisations that use outdated "legacy" systems and have underinvested in cyber security.

Information needs to be frequent and specific

In the public organisations we looked at, we saw that cyber security featured among the highest organisational risks reported to senior management teams and governing bodies. The reports identified a wide range of current and emerging cyber security risks, including risks of human error or carelessness, operating legacy systems, and denial-of-service attacks (where websites are made inaccessible).

However, the frequency and level of detail covered in the reporting varied. Risk reporting needs to be frequent enough to reflect the dynamic nature of cyber threats, and should lead to specific mitigation steps that governors can see the impacts of.

Independent assessments can assist

The governors of public organisations need to ensure that their organisation periodically assesses their cyber security maturity – that is, their overall capability and ability to manage risks and respond to incidents. Independent assessments can provide governors with confidence that they are focusing on the right areas.

The organisations we looked at that must comply with Protective Security Requirements tested their maturity through regular self-assessments, and shared the results with governors. The other organisations we looked at also carried out assessments of their maturity, sometimes through specialist external organisations.

The scale and frequency of these overall assessments should be considered as part of risk assessment and planning. In our view, material in the Protective Security Requirements could also be useful to public organisations that are not required to comply with them. The National Cyber Security Centre has published a cyber security framework that all public organisations can use to inform their cyber security programme.

Test and practice

Having the capability to protect against, detect, and respond to cyber attacks requires regular testing and practice.

The degree of involvement of governors will depend on the significance of a cyber security incident. In our opinion, the role of governors should be explicitly built into response and recovery activities, as well as set out in policies and processes. We saw variability in the extent to which this role was set out in organisations' documents.

When scheduling practices, public organisations need to consider the likelihood and consequences of the risks they are preparing for. Because responses are needed at short notice, the people involved need to be able to draw on "muscle memory" – they should be familiar with what they need to do, rather than doing it for the first time when there is a cyber attack. The results of real and practice responses should be systematically reviewed so improvements can be made.

In our view, many of the public organisations we looked at had insufficient testing and practising. Although they had plans for responding to cyber security incidents, some of these were not detailed enough.

We saw variable use of testing for phishing and other attacks, which is important, but governors also need to ensure that management teams have practised responding to incidents that might have greater consequences, such as a denial-of-service attack.

Cyber security starts at the top

The right capability

Governors need to have, or have access to, sufficient cyber security skills and experience to appropriately question and be assured about their organisation's cyber security risks and maturity. This includes engaging independent expertise when appropriate.

There was a wide range of cyber security skills and experience in the organisations that we looked at, including at the governance level. However, there is scope for greater consideration of cyber security knowledge, skills, and experience when recruiting and appointing governors. This is especially important when those governors have specific oversight of technology.

Governors need to ensure that their organisations periodically review their cyber security capability at all levels, including governance, and have plans to address any capability gaps.

The tone from the top

It is important that governors and managers fully comply with an organisation's cyber security requirements and practices. How governors and managers behave sets the "tone from the top" and needs to align with the expectations an organisation has of all staff.

Another aspect of governors setting the right tone is how they build their organisation's cyber security culture. We encourage governors to think about how they can play a more visible role in supporting management teams to promote cyber security awareness.

Working with others

Using wider public sector networks to source knowledge, skills, and experience can be useful, particularly when funding is limited. One organisation told us that effective cyber security is a team effort, and sharing learning goes a long way.

We saw public organisations connecting with each other, with government cyber security organisations, and with sector and professional organisations to support their cyber security activities. This wide range of networking is a strength of the public cyber security system.

The National Cyber Security Centre facilitates security information exchanges for industry sectors, in which participants can discuss cyber security challenges in a confidential and trusted environment.

In the event of a cyber attack, public organisations can access support from others in the cyber security system regardless of whether they are mandated by the Protective Security Requirements. For example, the National Cyber Security Centre has dedicated incident response resources.

We encourage all public organisations to report cyber incidents to the National Cyber Security Centre and understand and access the full range of available support.

Cyber security is never finished

With cyber threats increasing, effective cyber security is essential for public organisations to provide services safely and reliably.

Although we saw public organisations increase their cyber security focus and resourcing after significant cyber attacks, organisations need to be careful not to become complacent once the response is over.

Maturity assessments and other reviews should be carried out regularly, particularly after mitigation steps have been put in place, to identify where further improvements are needed. Public organisations should use the findings from assessments to improve their cyber security protections and risk mitigation. It is important that governors monitor this progress.

In some of the organisations we looked at, assessment findings were used to inform plans for improving their cyber security. This is positive – but given the rapidly changing nature of cyber threats, cyber security is never finished.

We encourage governors to continue to "mind the gap" between their organisation's risk appetite or target risk and the cyber security risks they face.

Cyber security checklist for governors

Set clear expectations for cyber security risk management	• Set and understand your organisation's risk appetite (the level of risk it is prepared to accept). • Set risk management expectations and direction for management.
Ensure appropriate cyber security risk mitigation and incident response controls are in place	Ensure that your organisation: • applies basic cyber security risk protections (such as software updates and regular data backup), uses relevant cyber security frameworks to guide risk identification and maturity improvements, and considers cyber security from the outset when designing new systems; • prioritises and plans cyber security risk mitigations based on careful consideration of: - the data and systems most critical to its business if a cyber security incident occurs ("mission-critical" approach); - the consequences of not being able to mitigate all the organisation's cyber security risks, leaving a gap between residual risk and risk appetite or target risk; - the costs of reducing this gap (and of not reducing it) and the organisation's ability to fund this; and - other organisational risks and investment priorities; • performs periodic internal and independent assessments of its cyber security capability and monitors its progress in responding to these assessments; • rehearses and practises incident response and recovery activities (including for high-impact incidents such as a denial-of-service attack) and prioritises and acts on recommendations from those exercises; and • is clear about the roles and responsibilities of governors in a significant response.
Have the necessary and current capability to govern cyber security	• Have, or have access to, the right technical skills and experience to appropriately question and be assured about cyber security reporting. • Maintain the necessary skills and knowledge to carry out cyber security responsibilities in an evolving threat and protection environment.
Invest the time to support cyber security	• Invest sufficient time in properly understanding cyber security risks and their potential impacts to make informed assessments and decisions. • Demonstrate "tone from the top" by fully complying with organisational cyber security requirements and by supporting wider cyber security awareness and practices.

Resources and further reading

Australian National Audit Office (2023), "Cybersecurity: Audit insights", at anao.gov.au.

Australian Securities and Investment Commission (2024), *"Cyber resilience good practices"*, at asic.gov.au.

Australian Signals Directorate (2024), *Essential Eight Maturity Model and ISM Mapping*, at cyber.gov.au.

Australian Signals Directorate (2023), "Learn the basics", at cyber.gov.au.

Australian Signals Directorate (2022), *Questions for Boards to Ask About Cybersecurity*, at cyber.gov.au.

Centre for Internet Security, "Creating Confidence in the Connected World", at cisecurity.org.

Controller and Auditor-General (2018), "Data security", at oag.parliament.nz.

Cybersecurity and Infrastructure Security Agency, "Cybersecurity Best Practices", at cisa.gov.

Federation of European Risk Management Associations and European Confederation of Institutes of Internal Auditing (2024), *At the junction of corporate governance & cybersecurity*, at eciia.eu.

Government Communications Security Bureau and New Zealand Security Intelligence Service (2017), *Briefing to the Incoming Minister*, at beehive.govt.nz.

Harvard Law School Forum on Corporate Governance (2020), "Cybersecurity: An Evolving Governance Challenge", at corpgov.law.harvard.edu.

Institute of Directors New Zealand (2023), *Cyber risk: A practical guide*, at iod.org.nz.

Institute of Internal Auditors Australia (2022), *The 20 Critical Questions Series: What Directors should ask about Information and Cybersecurity*, at iia.org.au.

International Organisation for Standardization (2020), *Information security, cybersecurity and privacy protection – Governance of information security*, at iso.org.

National Audit Office (2021), *Good practice guide: Cyber and information security*, at nao.org.uk.

National Cyber Security Centre NZ (2024), *Charting your course: Cyber Security Governance*, at ncsc.govt.nz.

National Cyber Security Centre NZ (2024), *Cyber Threat Report 2023/2024*, at ncsc.govt.nz.

National Cyber Security Centre NZ (2023), *Cyber Threat Report 2022/2023*, at ncsc.govt.nz.

National Cyber Security Centre NZ (2023), *NCSC Cyber Security Framework*, at ncsc.govt.nz.

National Cyber Security Centre NZ, "Top online security tips for your business", at ownyouronline.govt.nz.

National Cyber Security Centre UK (2023), *Cyber Security Toolkit for Boards*, at ncsc.gov.uk.

National Cyber Security Centre UK (2020), *Questions for boards to ask about cyber security*, at ncsc.gov.uk.

National Cyber Security Centre UK (2021), "Top tips for staying secure online", at ncsc.gov.uk.

National Institute of Standards and Technology, "Cybersecurity Framework", at nist.gov.

New Zealand Government, "Self-assessment and reporting: Information and tools to help your organisation assess and report on your protective security capability maturity", at protectivesecurity.govt.nz.

New Zealand Government (2025), *Responsible AI Guidance for the Public Service: GenAI*, at digital.govt.nz.

Queensland Audit Office (2021), "The role of governance committees in managing cyber security risks", at qao.qld.gov.au.

Reserve Bank of New Zealand (2021), Guidance on Cyber Resilience, at rbnz.govt.nz.

Office of the Auditor General Western Australia (2021), *Cyber Security in Local Government*, at audit.wa.gov.au.

World Economic Forum (2021), *Principles for Board Governance of Cyber Risk*, at weforum.org.