The cyber security playbook for SMEs

A roadmap to improve your cyber resilience – powered by CA Catalyst

CHARTERED ACCOUNTANTS™
AUSTRALIA + NEW ZEALAND

DIFFERENCE MAKERS™

Snapshot

‘SMEs can be considered the new big target for cyberattacks, being among the least mature and most vulnerable in terms of their cyber security risk and resilience.’[1]

Cyber threats are increasing, and pose serious and continuous risks to organisations and individuals everywhere.

Everyone must take responsibility for the data, software and devices we use. One person can bring down a network with a careless error.

Strengthening your cyber security posture and maturity is a continual iterative process.

Invest in best-practice security. Cyber threats are a major risk whatever the size of your business or organisation.

Too few organisations plan both to prevent cyber incidents as well as respond to and recover from them. It’s when, not if, they occur.

Focus on people and process, not just technology. You need people to be aware of threats and with knowledge and skills to respond effectively.

1 Boletsis, Costas, et al. Cyber security for SMEs: Introducing the Human Element into Socio-technical Cyber security Risk Assessment. VISIGRAPP (3: IVAPP). 2021.

CA Catalyst

Chartered Accountants Australia and New Zealand’s (CA ANZ) strategic programme, CA Catalyst, creates pathways for members in small and medium-scale practices (SMPs) to embrace the future of accounting in a data-driven, technology-empowered world and master new ways to create value in the profession. The CA Catalyst initiative focuses on three areas:

- supporting SMP growth and strategy by empowering accounting firms to move up the value chain, by offering new services that have a larger impact on their clients’ growth
- improving the efficiency and effectiveness of businesses’ infrastructure, by actively supporting productivity and tech adoption
- increasing confidence and demand for CAs, by promoting CAs as trusted advisors.

LEARN MORE

About this playbook

We've published this playbook for small businesses because most don't have the in-house expertise in this area. We want to help our SME members take practical steps to build their cyber security strategy and also be better positioned to discuss this issue with clients and stakeholders.

Part 1 includes **recent and relevant statistics** that indicate the scale and impact of cyber security issues around the world and explains why the **risks to organisations are rising.**

Part 2 describes **a model to plan your cyber security enhancement** by assessing risks, creating a defensive plan, sharing your strategy and building resilience. It includes a summary with interactive links to the following:

- **Self-assessment tool** compiled by Continuum Cyber for CA ANZ. This is a checklist SMEs can use to assess the state of their cyber security in about 20-30 minutes.
- **Checklist of baseline risk mitigation measures** relevant to any SME with a few or a hundred employees, combining advice from Australia, New Zealand and the UK.
- **The Essential Eight**, a mitigation strategy developed by the Australian cyber security agency.

Part 3 focuses on the detection of threats, incident response and recovery, and includes:

- a summary of **a blueprint for incident response**
- guidance on **when and how to report a data breach** in Australia and New Zealand
- tips on **finding and working with cyber professionals.**

Part 4 defines cyber security terms in a **glossary** and lists **further resources** with links to organisations that make our digital lives safer.

Resources Hub

This playbook forms part of a cyber security hub on our website. It includes tools, checklists, and case studies – and covers governance, processes and technology. It aims to help you:

- talk to clients, suppliers, peers and others about cyber security
- identify, evaluate and mitigate risks and develop a culture of cyber resilience.

CA ANZ has regularly advised members to pay attention to the rising risks of cyber threats and crime. In 2014, we produced a thought leadership paper on cyber security Protect our cyber future; then Cyber security for SMEs and practitioners in 2018, followed by a 2019 paper with ACCA Why CFOs should take the lead on cyber security.

Statistics at a glance

Globally

40+ billion records

exposed by cyber incidents in 2021
78% up on 2020.

$945 billion

Losses to businesses in 2020 from cybercrime.[3]

150% increase

in data breaches from a year earlier.

$145 billion

spent on cyber security by businesses in 2020, more than double 2018.[4]

21,957

common vulnerabilities and exposures[2]

38%

of data breaches reported are ransomware attacks[5]

43%

of cyber attacks target small business.[6]

Australia[7]

$33 billion

Losses to cybercrime by Australian businesses in the 2020-21 financial year.

67,500 cybercrime reports

An increase of nearly 13% from the previous financial year.

25% of cyber security incidents

responded to by the Australian Signals Directorate last year were against critical infrastructure, such as energy, water, telcos and health.[8]

22,000 calls received

by the Cyber Security Hotline, an average of 60 per day and an increase of more than 310% from the previous financial year.

New Zealand

28%

The number of cyber incidents in New Zealand linked to foreign state-sponsored computer network exploitation groups.[9]

404 cyber incidents

Nationally significant organisations impacted in the 2020-21 financial year, a 15% increase from a year earlier

8,831 incidents reported

The number of incidents reported to CERT NZ in 2021, a 13% increase on 2020[10]

2 Tenable website. These figures are for the year to October 2021 and are based on an analysis of publicly disclosed information

3 McAfee Hidden costs of cyber crime

4 McAfee

5 2020-2021 NCSC NZ Cyber Threat Report By the Numbers

6 PurpleSec 2021 Cyber Security Statistics The Ultimate List of Stats Data & Trends

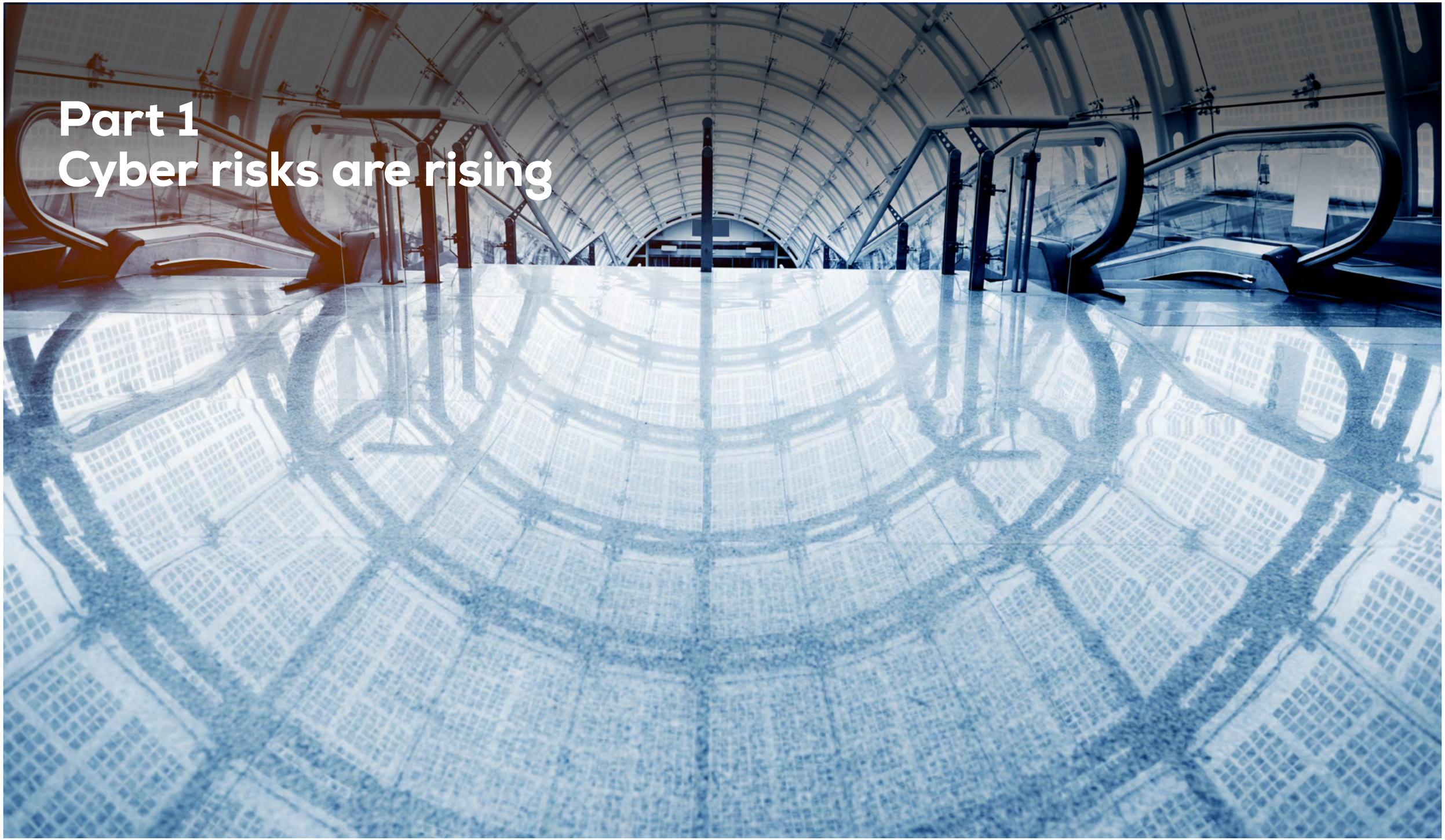
7 ACSC Annual Cyber Threat Report 2020-21

8 Australian Signals Directorate website

9 NCSC

10 CERT NZ's Quarter Four (Q4) Report

Part 1
Cyber risks are rising



Part 1

Cyber risks are rising

Organisations everywhere are impacted by rising cyber security threats as the world undergoes rapid digital transformation

Cyber security is one of the major risks facing organisations worldwide. Top executives put cyber attacks and data breaches among the top two risks businesses face.[11]

Everyone in an organisation of any size needs to understand the potential costs of a cyber security incident. Costs include:

- financial and other penalties due to compliance failures
- reputational damage from breaches of privacy
- disruption to operations and loss of revenue
- investment in recovery measures
- business failure.[12] [13]

Many SMEs face an existential threat from a critical cyber security incident or data breach. Cyber criminals know that they have business relationships with larger businesses and that they are the 'gateway' into these organisations because usually their cyber security protection is weaker than their larger colleagues.[14]

Cyber risks topped the list of concerns for CEOs surveyed by PwC over the past two years. Australian CEOs were particularly anxious, with 71% reporting they were very or extremely concerned,[15] while half of CEOs in New Zealand surveyed shared this sentiment.[16]

Ransomware threats increasing

In their first ever joint advisory, cyber security agencies in the US, UK and Australia warned that ransomware threats were more professional, sophisticated and high-impact. Ransomware encrypts data so that you can no longer access it. Criminals then offer to provide a key for payment.

It's critical that individuals, businesses and industry follow advice and mitigation strategies, the Australian Cyber Security Centre (ACSC) says.[17]

In the last year, ACSC reported ransomware attacks against Australian organisations increased 60%.[18] Victims are advised not to pay ransom, although 30% of organisations who do pay, receive all their money back.[19]

Threats including viruses, spyware and trojans, and vulnerabilities in the burgeoning market for apps are growing exponentially and evolving rapidly. Growth in the Internet of Things (IoT) and inter-connectivity with smartphones, cloud services and social media has motivated cyber criminals to innovate and increase cyberattacks.

Malware enables criminals to steal information, such as bank or credit card details or intellectual property, destroy data, disrupt whole organisations and even shut down critical infrastructure.

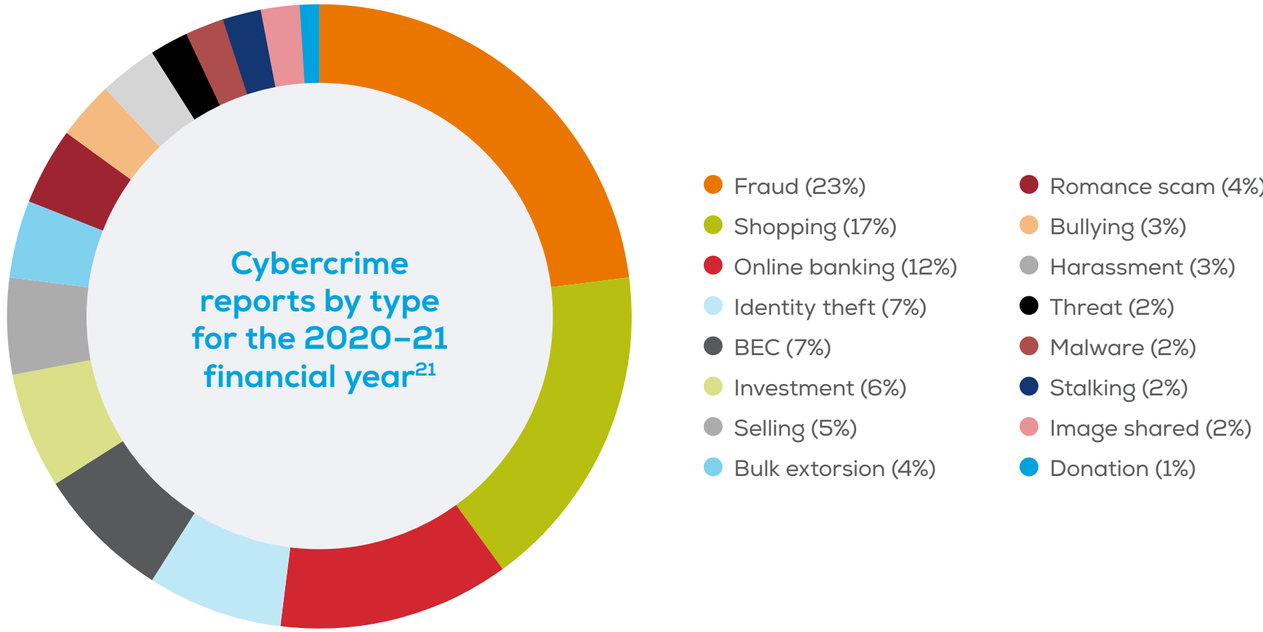
Phishing, the use of emails, messages or phone calls to trick people into transferring money or data, or installing malware on their computers or phones, is one of the top **cyber security threats** accounting for more than a third of attacks reported globally.[20]

Attackers pretend to be trusted individuals or organisations such as police, banks and government authorities, as well as companies with instantly recognisable brands, such as Amazon, PayPal, Google, Apple or Facebook.

11 2021 Global Risk Management Survey – Results | Aon
12 In Lee, Cyber security: Risk management framework and investment cost analysis, Business Horizons, 2021
13 IBM Cost of a Data Breach
14 US Securities and Exchange Commission The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses 2015
15 PwC's 25th Annual Global CEO Survey: Optimism in the face of challenge
16 PWC Remaining resilient through uncertainty
17 NCSC media release, 9 Feb 2022
18 Australian organisations are quietly paying hackers millions in a 'tsunami of cyber crime' - ABC News
19 PurpleSec 2021 Cyber Security Statistics The Ultimate List of Stats Data & Trends
20 2021 Data Breach Investigations Report | Verizon

Part 1

Cyber risks are rising (continued)



Global threat to business and national security

Sophisticated cyber attacks are often carried out by organised criminal gangs internationally, some of which are state-sponsored.

Russia's invasion of Ukraine raised threat levels because both countries use cyber warfare capabilities. Russia may step up cyber attacks against targets in countries that support Ukraine militarily and this could also spill over into the civil domain.

This invasion prompted the ACSC and National Cyber Security Centre (NCSC) in the UK to warn organisations of the need to adopt an enhanced cyber security posture because of "a historical pattern of cyber attacks against Ukraine that have had international consequences."

A suspected Russian cyber attack in 2017 used Malware called 'NotPetya' to disrupt Ukrainian airports, railways and banks. The attack spread globally affecting multinational companies including global shipping company Maersk, pharmaceutical giant Merck, TNT Express and others.[22]

21 ACSC Annual Cyber Threat Report 2020/21

22 Harvard Business Review What Russia's Ongoing Cyberattacks in Ukraine Suggest About the Future of Cyber Warfare

Part 1

Cyber risks are rising (continued)

SMEs face a disproportionately higher risk

Medium-sized businesses take the brunt of cyber attacks. In the 2020-21 financial year, the ACSC found based on the average cost of each threat, these businesses fared worse than larger organisations.

In New Zealand, a study of 1,000 SMEs revealed that 24% had experienced a cyber attack in the last year. Of those, half had been phishing attacks and a quarter were ransomware, while a further 30% said their customer data had been leaked to the dark web.[23]

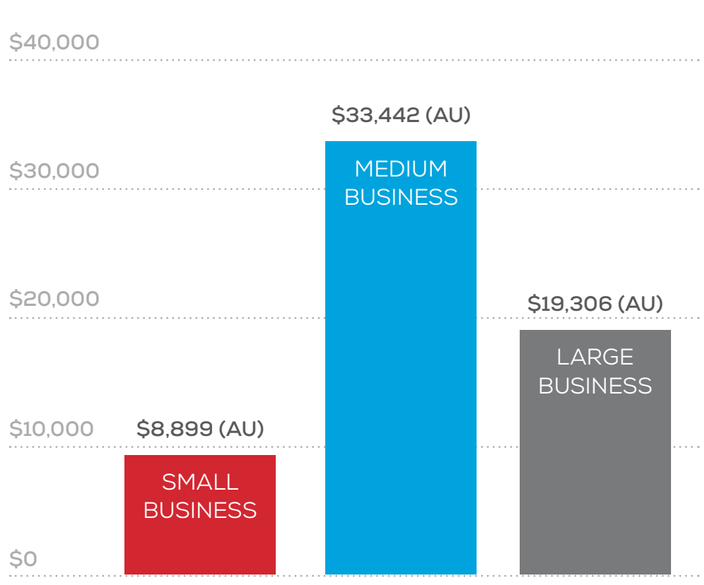
A study of 5,000 SMEs in Germany concluded: "Security awareness has arrived in all SMEs, but this awareness is not yet spread to all staff, mostly left to management and tech departments, which opens SMEs up to phishing, insider attacks and advanced persistent threats."[24]

In Australia, governments are the biggest target, followed by professional, scientific and technical services (which includes accounting).[25] Globally, top sectors targeted by malware in 2020 were professional services, followed by manufacturing, public administration, health and IT.[26]

A study by the Cyber Security Co-operative Research Centre found that the SMEs studied regarded cyber security as an 'add-on' and not a core part of operations. Half of the SMEs interviewed said that they were poorly prepared for a cyber attack, and they either had no processes in place or limited undocumented processes. This was due to a lack of financial resources. Many employees also brought their own devices to work and these were inadequately protected against an attack.[27]

Who is the biggest cyber security target?

Source: Australian Cyber Security Centre



SMEs' preparedness in the US

70% are not prepared to respond to a cyber attack.[28]

3/4 say they don't have sufficient staff to address IT security.

14% rate their ability to mitigate cyber risks, vulnerabilities and attacks as highly effective.

16% are very confident in their cyber security readiness.

4/5 report malware has evaded antivirus software

23 MYOB Nearly a quarter of SMEs in New Zealand victims of cyber-attacks
24 30th USENIX Security Symposium. Aug 2021, A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises
25 ACSC Annual Cyber Threat Report 2020-21 | Cyber.gov.au.
26 Industries most targeted by malware 2020 | Statista
27 Cyber Security CRC Smaller but stronger: Lifting SME cyber security in South Australia
28 Purplesec, 2021 Cyber Security Statistics

SPOTLIGHT

MARTIN BOYD
VERTEX CYBER
SECURITY

‘I didn’t take your advice and now we’ve been hacked’

Offering tailor-made solutions for small and medium-sized businesses is how Vertex Cyber Security keeps them safe from cyber attack or helps them recover.

During nine years in cyber security at the Commonwealth Bank of Australia, Martin Boyd saw a gap in cyber protection. “Governments and cyber companies couldn’t help small and medium-sized businesses - they had to turn them away and this meant they literally had to fend for themselves.”

In 2016, he set up his own consultancy, Vertex Cyber Security, to help any business, from micro to large, that needs cyber security help such as with their online cyber security training, policies, penetration testing, ISO27001, log monitoring and protection. “We help companies that have been hacked and we protect and train others to have a good level of protection to avoid getting hacked,” says Boyd.

Every business Vertex engages with is at a different stage of maturity or growth and therefore faces particular risks. “Wherever they’re at, we give businesses options and tools to make decisions and take action to be as safe as they can be,” says Boyd.

Too much hesitation

He describes how one financial advisory business with ten employees hesitated to invest in cyber security. Nine months later, the business owner called Boyd in a panic. “He said ‘I didn’t want to be that guy who didn’t take your advice and paid the price, well, I didn’t take your advice and now we’ve been hacked!”

A cyber criminal had taken control of the business’ email and phone number. Vertex was able to stem the damage in a couple of hours and ultimately regain control. “It’s not a small fix, and the business owner later informed me that this was the worst time of his life” says Boyd. “It takes forensic work to determine which systems have been hacked. We traced it to an international hacker who probably intended to charge ransom.”

In this case, the response was quick so the attacker wasn’t able to steal any client data and so clients didn’t need to be informed, avoiding potentially irreparable reputational damage which could have led to the closure of the business.

The business set up a new password management system and signed up to improve their cyber security protection, from Browser Phishing protection to Vertex training so that all employees were better equipped to avert future incidents.

See Finding and working with experts

Part 2
Planning for cyber security

Part 2

Planning for cyber security

Involve your whole organisation and its employees to adopt a structured approach to defend against cyber threats

‘Look at any cyber security incident and you’ll find a failure of decision making, not a failure of technology.’

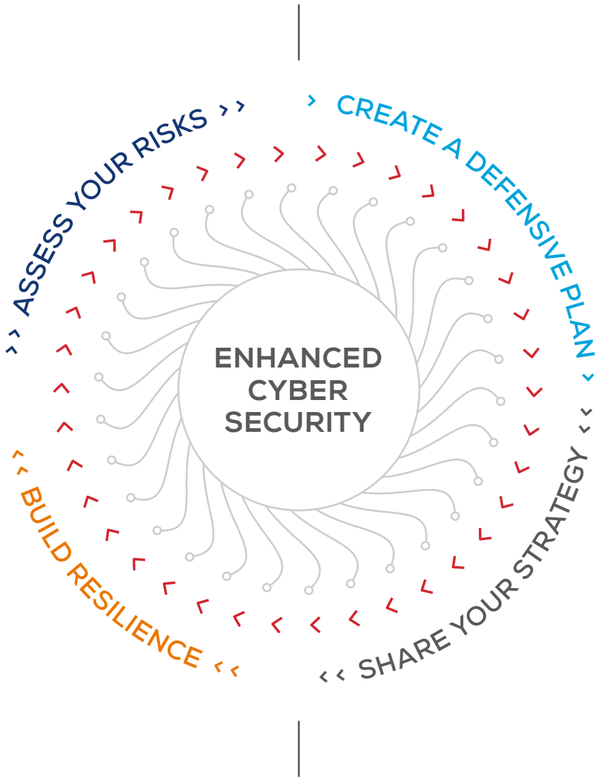
- Paul Proctor, cyber security expert at Gartner[29]

ASSESS YOUR RISKS

Identify, measure and evaluate your risks. This includes sensitive data or intellectual property, your technology systems and processes, as well as employees, contractors and even customers.

BUILD RESILIENCE

Detect and manage threats, plan your incident response, test your systems, and enhance your cyber resilience.



CREATE A DEFENSIVE PLAN

Adopt a plan to strengthen cyber security with practices, behaviours and technical solutions suited to your organisation’s risk appetite. Regularly review and update this plan.

SHARE YOUR STRATEGY

Create awareness among employees, clients, suppliers and others to create a culture of cyber security. Adopt or develop a program of training and coaching that ensures employees’ knowledge is current.

29 Gartner, March 2022, ‘Cyber security as a Business Decision: A Manifesto’

Part 2

Assess your cyber risk

Before setting up a cyber security risk management system, the business must determine what assets it needs to protect and prioritise

Understand your business' cyber security exposure by assessing all your assets as well as operational processes. Examine the confidentiality, integrity and availability of data and how you keep it safe, including how you collect, store and destroy data when you need to.

You will need to update this information frequently and assign people to maintain each asset, as well as discover gaps that may require additional training.[30] Whoever is handling the development of your cyber security will need to:

- interview managers, employees and other stakeholders.
- review documentation from a variety of sources.
- analyse your systems and infrastructure.

Data: your most critical asset

Accountants deal with high-value commercial data and sensitive financial information daily. Additionally, one of the key roles of an accountant is to highlight business risk in their clients.

The sensitivity of this data is what makes accountants of all sizes prime targets for cyber criminals. Accounting firms are 30% more likely to be targeted than other companies[31] and with more and more data stored across varying electronic formats and methods, risk has increased proportionally alongside the attack surface of each firm's software environment.

Software can find and assess how data is collected, stored and destroyed across your business and ensure no sensitive data is stored in exposed places.

Review cloud services

As cloud services become more widespread, it is critical to understand the threats and vulnerabilities of any cloud-based apps available to your business, along with any data they may contain. Document what services you are using and how the data is stored and updated by employees of your organisation, and assess the potential vulnerabilities of any of the services you are using.

Audit all devices

List all the devices employees use for work and understand the threats and vulnerabilities of each device. Do they work only on authorised office computers or are they signing into the company intranet through their home computers, laptops, phones and other devices?

A risk assessment should cover many possible scenarios, from a lost smartphone on the back seat of a taxi, through to home networks and how employees work in different scenarios, for example, visiting clients' offices and connecting to their networks.

Cyber risk, threat, and vulnerability

Risk is the potential for loss or damage, including financial, caused by a cyber threat.

Threat is a process that exploits a vulnerability.

Vulnerability is a weakness in your system that exposes you to threats.

30 NCSC UK Asset management

31 Cyber security challenge | ACCA Global

Part 2

Assess your cyber risk (continued)

Your peoples' capabilities

The majority of cyber breaches arise because of human error - often a person's unintentional action or decision. Negligence by employees or contractors leads to about two-thirds (63%) of cyber attacks, research by IBM found.[32]

Cyber criminals use 'social engineering' to exploit the basic human characteristics of curiosity, reciprocity, greed and trust.[33] This requires understanding and training to create a culture of security.

Assess the levels of cyber awareness of everyone who interacts with your business.

Adopt or develop an appropriate training or coaching program for your employees and other groups of people (e.g. suppliers, customers) to improve their capabilities.

Insider vulnerability

No one wants an atmosphere of distrust in the workplace. Yet an IBM survey[34] found that almost two out of five cyber attacks were caused by malicious or criminal insiders within organisations. This is an uncomfortable reality. As part of your risk analysis, reassess your processes of hiring and onboarding new employees. You should determine the levels of access they have to systems and data, and how that access will be tracked or monitored.

You should also consider the adequacy of thorough pre-employment screening, including questions surrounding device and network use/misuse, as a preventive measure.

External vulnerabilities

Assess how your clients and suppliers - and other external parties - interact with your business, from the client who might give a staff member an external thumb drive with a file of spreadsheet data (and who knows what else) on it, to your managed services provider who has extensive access to your network in order to carry out their work. What processes do you need to make more rigorous?

Businesses can use their findings to determine a baseline for their current risk posture and what the enterprise needs to do to move from its current state to the desired state of risk exposure. So long as proactive steps are taken to understand potential risks, there will be less likelihood of risk exposure and falling victim to a cyber security incident.

Risk-reward calculation

Experts recommend performing a risk-reward calculation and prioritising network security enhancements that will provide the most significant improvements at the lowest cost.

Example risk assessment for a small business

- Determine what cyber threats are relevant to your organisation.
- Identify your organisation's vulnerabilities and how likely they are to be exploited.
- Estimate potential financial loss as a result of a cyber incident.
- Score the risks you identify from 1-5 (very low, low, moderate, high, very high).
- Consider actions or controls for each moderate-very high risk with a cost estimate.

THREAT	VULNERABILITY	ASSET	RISK	SOLUTION/ACTION
Distributed denial of service (DDos attack)	Firewall configuration	Website unavailable	Low	Check firewall configuration and monitor
Phishing	Employee awareness, error	Entire network	High	Employee training. Set up SPF, DKIM, DMARC authentication

32 IBM Cost of Insider Threats
33 ACCA and CA ANZ Cyber and the CFO
34 IBM Cost of Insider Threats

Part 2

Assess your cyber risk (continued)

CA ANZ has partnered with Continuum Cyber to develop a cyber security assessment tool to help you assess the safety of your organisation.

ASSESS YOUR BUSINESS

Assessment method: Applying the Capability Maturity Model

	1. ● ○ ○ ○ ○ Initial	2. ● ● ○ ○ ○ Developing	3. ● ● ● ○ ○ Defined	4. ● ● ● ● ○ Managed	5. ● ● ● ● ● Optimised
PEOPLE	Activities unstaffed and uncoordinated	Infosec leadership established, informal communication	Some roles and responsibilities established	Increased resources and awareness, clearly defined roles and responsibilities	Culture supports continuous improvement to security skills, process, technology
PROCESS	No formal security program in place	Basic governance and risk management process, policies	Organisation-wide processes and policies in place but minimal verification	Formal infosec committees, verification and measurement process	Processes more comprehensively implemented,risk-based and quantatively understood
TECHNOLOGY	Despite security issues, no controls exist	Some controls in development with limited documentation	More controls documented and developed, but over-reliant on individual efforts	Controls monitored, measured for compliance, but uneven levels of automation	Controls more comprehensively implemented, automated and subject to continuous improvement

Part 2

Create a defensive plan

Develop a tailored, targeted plan to proactively mitigate risks and enhance your organisation's cyber security

To protect against threats, you will need to either eliminate or reduce the vulnerabilities revealed in your risk assessment. Taking these steps will strengthen your business on several fronts. Prioritise your plan so you address your most significant risks first.[35]

Whilst SMEs may not need to adopt a formal framework – nor face the same compliance obligations as large organisations – given the rapidly changing digital environment, even a small business should regularly review its cyber security arrangements with a view to upgrading and enhancing protection.

Frameworks to protect your organisation

There are many ways to approach cyber security including compliance frameworks, maturity models and standards.

The ISO 27001 is an internationally recognised Information Security Management System (ISMS) standard. These standards enable a business of any size to manage the security of their financial information, intellectual property, employee details or information entrusted by third parties

The National Institute of Standards and Technology (NIST) Cyber Security Framework organises cyber security activities in five categories: Identify, Protect, Detect, Respond and Recover.

35 ACSC Strategies to Mitigate Cyber Security Incidents

Australian Taxation Office information on cyber security for business

Proactive:

PROTECT YOUR BUSINESS

TOP CYBER SECURITY TIPS

ONLINE SECURITY

Reactive:

HELP FOR IDENTITY THEFT

DATA BREACH GUIDANCE FOR TAX PROFESSIONALS

If you encounter a data breach involving tax related information (e.g. payroll data) you should contact the ATO's Client Identity Support Centre on:

It can apply measures to protect your business, staff and clients where necessary.

1800 467 033

Monday to Friday, 8.00am–6.00pm AEST.

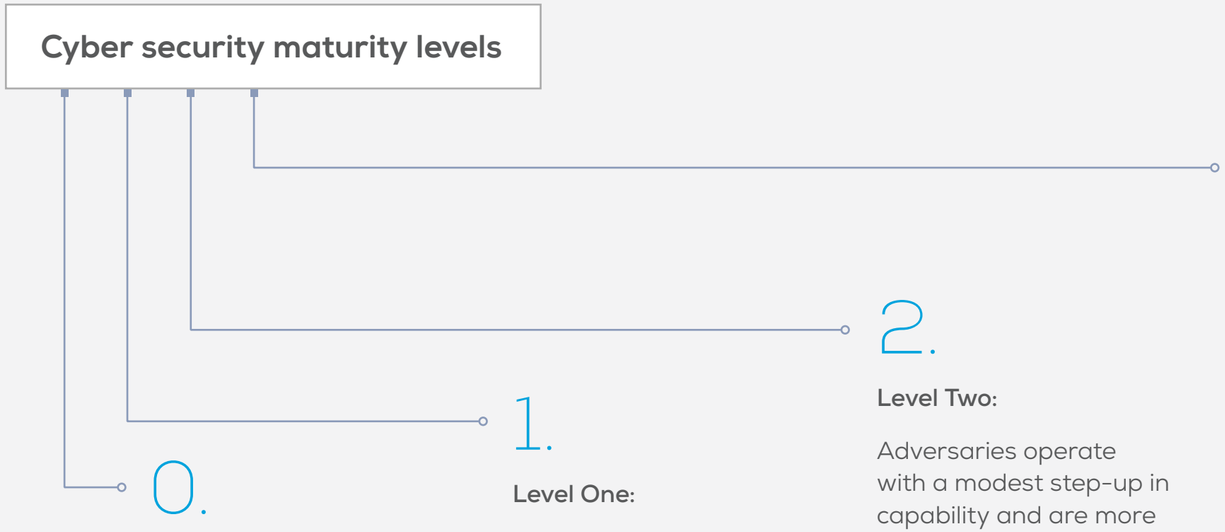
Part 2

Risk mitigation steps

While no set of mitigation strategies are guaranteed to protect against all cyber threats, the Strategies to Mitigate Cyber Security Incidents by the ACSC includes a list of measures that organisations are advised to adopt as a baseline level of security known as The Essential Eight. (see page 17)

This baseline makes it much harder for adversaries to compromise systems. If implemented proactively, this is more cost-effective than having to respond to a large-scale cyber security incident, the ACSC says.

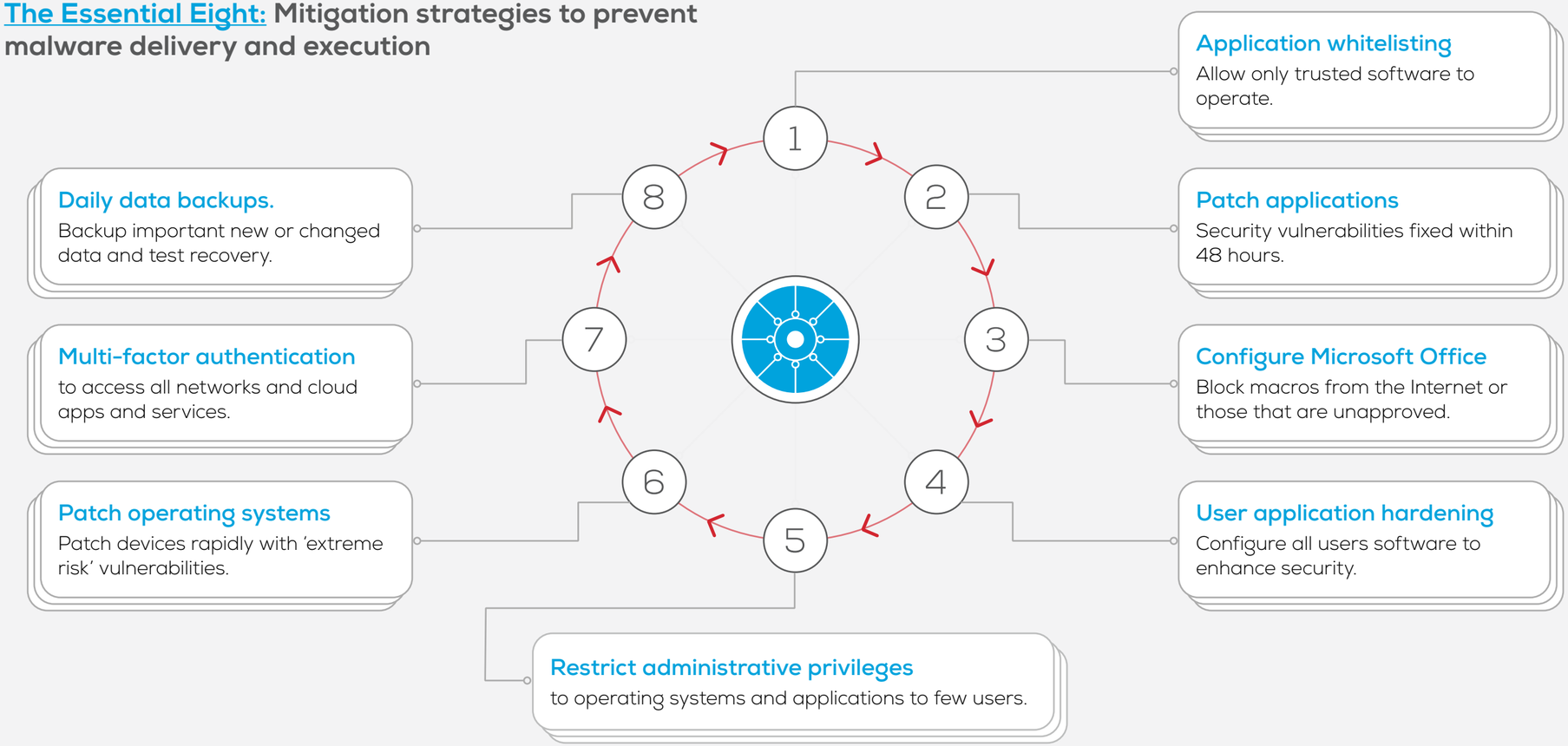
For each of these areas, advice is pitched at four different levels of threat or 'maturity levels', based on the behaviours, practices and processes of adversaries that might lead to a security breach.



Part 2

Risk mitigation steps (continued)

The Essential Eight: Mitigation strategies to prevent malware delivery and execution



Application whitelisting
Allow only trusted software to operate.

Daily data backups.
Backup important new or changed data and test recovery.

Patch applications
Security vulnerabilities fixed within 48 hours.

Multi-factor authentication
to access all networks and cloud apps and services.

Configure Microsoft Office
Block macros from the Internet or those that are unapproved.

Patch operating systems
Patch devices rapidly with 'extreme risk' vulnerabilities.

User application hardening
Configure all users software to enhance security.

Restrict administrative privileges
to operating systems and applications to few users.

Each of these eight areas of focus cover a number of specific operations or tasks, the number and scope of which increase as an organisation raises its cyber security posture to a new level of maturity.

Part 2

Risk mitigation steps (continued)

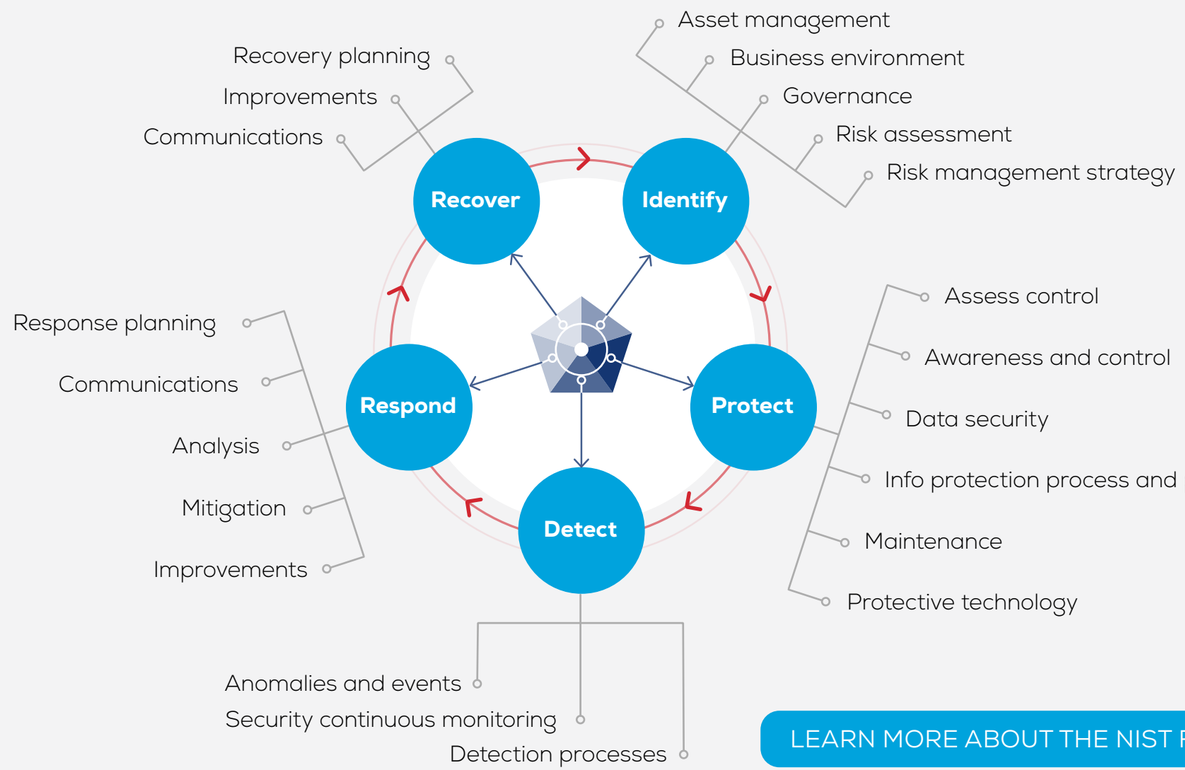
The US National Institute of Standards and Technology (NIST) developed its first risk-based Cyber Security Framework in 2014. It was updated in 2018.

The framework provides voluntary guidance to better manage and reduce cyber security risks, and is:

- based on existing standards, guidelines and practices
- intended primarily for critical infrastructure organisations
- designed to encourage communications among internal and external organisational stakeholders on cyber security risk and management.

Also, increasingly sophisticated solutions are becoming more accessible for small to medium-sized businesses as technology develops and as the cyber security industry matures. SMEs should pay attention to developments in these areas.

The NIST Cyber Security Framework



LEARN MORE ABOUT THE NIST FRAMEWORK

(Source: Achieving NIST CSF Maturity with Verve Security Centre)

Part 2

Risk mitigation steps (continued)

Roles and responsibilities: who does what?

Set the cyber security roles and responsibilities in your organisation, and determine who is best suited to perform them.

Involve all stakeholders, if possible, to gather perspectives from everyone involved in the practice or business.

Responsibility for planning and building a cyber-resilient organisation ultimately rests with the business owner, managing partner or CEO (and the board if you have one). However, the detailed work should be undertaken by a team or committee within the organisation.

Involve and train all employees so that they understand how cyber security works and how they should follow security protocols.

DOWNLOAD BASELINE CYBER SECURITY CHECKLIST HERE

RASCI: a model for assigning roles

One method for defining roles and responsibilities is to use the RASCI model.[36] It lists activities in a table and assigns a role to each individual (or team in large organisations).

RESPONSIBLE	Role or team assigned to undertake a task. At least one role has primary responsibility, others can provide support.
ACCOUNTABLE	Role that ultimately approves the activity and ensures that it is carried out. There must be one role that is accountable for each specified task or function.
SUPPORTING	Roles and teams that support the responsible and accountable individuals in completing the activity.
CONSULTED	Stakeholders who need to be formally consulted regarding the activity, and who may provide input and feedback.
INFORMED	Stakeholders to be kept informed about the progress of the activity.

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	SUPPORTING	CONSULTED	INFORMED
Risk assessment	Raj	Mary	Wei	Jane	Jane
Employee training	Jane	Juan	Raj	Jed	Tom

36 A Guide to the Project Management Body of Knowledge (PMBOK Guide) (5th ed.). Project Management Institute. New Zealand's cyber security agencies suggest this approach.

SPOTLIGHT

DAVID WAINE CA
MATLEY FINANCIAL
SERVICES

Recovering from a trojan attack

Experiencing a trojan attack first-hand was an unsettling experience for David Waine CA – one he would never like to repeat. A virus got into his business network and started destroying data

The incident happened at a highly inconvenient time: in October, right at the half-yearly reporting schedule for all of his clients. "We'd enter data into the computer one day and the next day it would be literally wiped clean," he says.

Waine's outsourced IT consultant came to his rescue and managed to get rid of the malicious code, but he realised that having all of his clients' data on an in-house desktop server was no longer safe. "We decided to move everything into the cloud," he says.

His business is now conducted using Xero, as well as other apps such as Spotlight that integrate with this platform. Clients upload files themselves directly to Xero. Waine is confident that Xero itself has extremely robust cyber security measures.

Choosing the right IT expert is important, Waine says. An SME doesn't need a high-level consultant but someone with adequate capabilities. "We're in regular contact with our IT consultant but not every day," he says. "We know they're doing their job well and you only want to be in touch with them when it's necessary," he says.

Waine's business has now grown to 23 staff in four locations (Hamilton, Tauranga, Tokoroa and Christchurch). He's only too well aware of the risks of human error, so the business has adopted a security policy that all staff must follow.

The policy advises, for example, that no one opens emails that have suspicious addresses or ask for payments without verification. "When we get them we send them to our IT people," he says. "The best way to test how tough something is to try and break it – and so far our cyber security is holding up."

Part 2

Share your strategy

Everyone involved with your organisation must know their role in supporting its cyber safety

People must understand the gravity of the threat to the organisation's reputation, profit and continued viability, that could eventuate from individual negligence.

One of the best ways to convince everyone of the importance of cyber security is to involve them in a cyber security assessment so that they can see the risks for themselves.

Involve employees, leadership, board members and senior management in the creation of the plan so that they have ownership of it. Discuss it with relevant suppliers and contractors too.

In a survey by CA ANZ and ACCA, 20% of CFOs said they were not involved in creating their organisation's cyber security plan and 10% had no idea who dealt with day-to-day cyber security.[48] Yet 57% of them said cyber security was among the top five most important risks their organisations faced.

Involving stakeholders in decision making means they're more likely to enact the measures that follow. This prevents your organisation from having a siloed approach to security.

Suppliers and clients

Every small business will have suppliers. Whichever employee is responsible for procurement will need to discuss cyber security with existing and potential suppliers.

Include training about cyber security as part of the onboarding process for new customers and suppliers. Also provide an opportunity to existing clients and suppliers to take part in this process too to mitigate your risks, and theirs. It's important to discover:

- Has the supplier already had a security breach that they need to declare to you?
- Are you satisfied with your supplier's existing cyber security defence plan?
- Are you satisfied with how this plan will protect your data?
- Does the supplier have a business continuity/disaster recovery plan in place to provide minimum service levels if they're attacked?
- Does your contract with the supplier state requirements about how they will manage and report incidents, including reporting timescales and who to report to?[50]

Training

Cyber security is only partly a technical challenge. Its success is heavily affected by non-expert users who connect to the internet for both their work and personal lives. Technical measures alone are not enough.

If you don't have an in-house training department, consider using an online learning platform or hiring a consultant to do this. Also a variety of multimedia educational tools for non-expert end-users are available to increase awareness of cyber security.[49]

Keep your staff up-to-date with new cyber security developments and best practices so they feel confident that your business is doing its bit. Human resources managers will need to include cyber security training in the on-boarding process for new hires.

48 Cyber and the CFO

49 Leah Zhang-Kennedy and Sonia Chiasson, Jan 2022. A Systematic Review of Multimedia Tools for Cyber security Awareness and Education. ACM Comput. Surv. 54.

50 NCSC UK Supply chain security

Part 2

Build cyber resilience

Continually develop your organisation's capabilities to bounce back after a cyber incident.

Cyber resilience reflects an organisation's ability to continue to carry out its core functions even as a cyber event or incident threatens to disrupt it, as well as being able to recover those functions quickly if a cyber attack succeeds.

The process of enhancing your organisation's resilience means going through a series of iterations in planning, implementation, review and evaluation based on what you learn and experience.

Be open to reassessing your approach and look for strategies and models that can assist you to upgrade your security posture and continuously improve your controls.

Here are a few approaches your organisation might consider to enhance your resilience:

New Zealand's approach to cyber resilience

Charting Your Course is a series of documents created by New Zealand's National Cyber Security Centre containing practical advice on enhancing cyber security. They include an introduction to governance followed by six steps to building resilience:

Step One:
Building a culture of cyber resilience

Everyone in the organisation should feel supported to make decisions that protect assets.

Step Two:
Establishing roles and responsibilities

Clearly define who is best to perform what roles and responsibilities.

Step Three:
Holistic risk management

Effective risk management is embedded within an organisation's overall risk framework.

Step Four:
Cyber security collaboration

Communicating strategy via a group of stakeholders to gain organisation-wide support.

Step Five:
Create a cyber security programme

Ensure your investment provides the best possible improvement in cyber resilience.

Step Six:
Measuring resilience

Measurement and reporting provide the basis for continuous improvement.

Part 3
Incident detection, response and recovery

Part 3

Incident detection, response and recovery

Developing a strategy to defend your assets against threats must also include how you respond to and recover from a cyber incident or breach in supporting its cyber safety

Surveys show many business leaders doubt their ability to identify the root cause of a cyber attack, and consider their organisation's incident response plans inadequate.[51]

In CA ANZ's Cyber and the CFO survey, only a third (32%) of respondents said they had a remediation plan that they update and test frequently, while 38% either did not have a plan or were unsure.

Having a cyber incident detection and response plan in place and practising its procedures regularly will increase confidence and ensure your business survives.

51 VMWare, Kroll 2021 State of Incident Response Report

Cyber incident detection and response plan

Source: NIST

Part 3

Incident response

DOWNLOAD BLUEPRINT INCIDENT RESPONSE CHECKLIST HERE

When, how and who to notify about a cyber incident

Report cyber incidents as soon as possible when they come to your attention. Even if there is no obligation to report them, doing so may provide agencies with worthwhile threat intelligence. Cyber incidents you should report include:

- suspicious system and network activities
- compromise of sensitive or classified data
- unauthorised access or attempts to access your system
- emails with suspicious attachments or links
- denial-of-service attacks
- ransomware attacks
- suspected tampering of electronic devices.

In New Zealand, if you think you've received a phishing email you can find out more about what to do here or forward it to the Computer Emergency Response Team (CERT NZ) here.

If your organisation deals with nationally significant information, contact the government's National Cyber Security Centre, phone (04) 498-7654, complete the Cyber Security Incident Request for Assistance Form [DOCX, 61.36 KB], or email incidents@ncsc.govt.nz.

In Australia, contact the Australian Cyber Security Centre on 1300 CYBER1 (1300 292 371) or go to Report Cyber. Your report will also be referred to the appropriate police jurisdiction for assessment.

A government organisation or private business in Australia with turnover of over AU$3 million that holds data on the medical records, bank account, credit card or identification details of clients or customers, must report a cyber breach to the Office of the Australian Information Commissioner (OAIC) when they have reasonable grounds to believe an eligible data breach has occurred.

Main reasons for a strong cyber incident response plan

1. Prepares you for emergency–security incidents happen without warning
2. Repeatable process–without an incident response plan, teams cannot respond in a repeatable manner or prioritise their time
3. Coordination– gives employees defined roles and keeps everyone in the loop during a crisis
4. Exposes gaps– organisations with limited employees or limited technical maturity have time to get more training or expert help
5. Preserves critical knowledge–ensures best practices for dealing with a crisis are honed and lessons learned added
6. Practice makes perfect–a clear, repeatable process followed in every incident, improves coordination and effectiveness of response over time
7. Documentation and accountability– reduces an organisation's liability and allows you to demonstrate to auditors or compliance authorities the actions taken to prevent the breach.[59]

59 NIST SP 800-61

Incident response (continued)

Scale of attack severity

CRITICAL

Over 80% of staff (or several critical staff/teams) unable to work

Critical systems offline with no known resolution

High risk to ordefinite breach of sensitive client or personal data

Financial impact of <$ amount>

Severe reputational damage likely to impact business long term

HIGH

50% of staff unable to work

Risk of breach of personal or sensitive data

Non-critical systems affected, or critical systems affected with known (quick) resolution

Financial impact of <$ amount>

Potential serious reputational damage

MEDIUM

20% of staff unable to work

Possible breach of small amounts of non-sensitive data

Low risk to reputation

Small number of non-critical systems affected with known resolutions

LOW

Minimal, if any, impact

One or two non-sensitive / non-critical machines affected

<10% of non-critical staff affected temporarily (short term)

Source: NCSC UK

Part 3

Incident response (continued)

What is a data breach?

An eligible data breach occurs when the following criteria are met:

- There is unauthorised access to or disclosure of personal information held by an organisation or agency (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).[60]
- This is likely to result in serious harm to any of the individuals to whom the information relates.
- The organisation or agency has been unable to prevent the likely risk of serious harm with remedial action.

Obligation to notify

Keeping your clients' data safe is your primary responsibility and you have legal obligations about what you can do with any of their personal information. These are outlined in the Australian Privacy Principles listed in the Privacy Act 1988.

These principles apply to most government agencies, private sector and not-for- profit organisations with more than AU$3 million annual turnover. These organisations must "take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances."

The Australian government also introduced the Notifiable Data Breach (NDB) Scheme in 2018, to better protect the public from data breaches. This scheme applies to all organisations that handle medical records, credit card or bank account details or identification documents.

The NDB scheme requires organisations to report a data breach to the Office of the Australian Information Commissioner (OAIC) and also directly inform the customers or clients whose data they hold.

New Zealand Privacy Act

In New Zealand, the Privacy Act 2020 replaced the Privacy Act 1993. Principle 5 of the act says that organisations must have reasonable safeguards to prevent loss, misuse or disclosure of personal information. Within 72 hours of a serious privacy breach, the organisation must notify the people affected and the Office of the Privacy Commissioner at:

notifyus@privacy.org.au

or phone 0800 803 909

60 This section drawn from Office of the Australian Information Commissioner About the Notifiable Data Breaches scheme

Part 3

Finding and working with experts

Most SMEs will need external help to implement robust cyber security measures

Cyber security is not a 'set and forget' strategy. It requires constant vigilance and a deep understanding of the methods used by attackers and defenders alike.
This is known as 'tradecraft', and there's growing demand for cyber professionals with such skills.

Contract external service providers with the specialist knowledge and skills to mitigate risks, detect threats, and assist your response to incidents and recovery. Most SMEs will need external help to implement robust cyber security measures.

Tips to find a cyber security expert:

Determine what you are prioritising and the services you are seeking to purchase first. Most businesses start with one of the following:

- Cyber Security Training (Good starting point with a small budget ~$5pp/month)
- Cyber Security Audit (Provides a report of Cyber risks specific to your business)
- Penetration Testing (Good for testing the security of your website or office network to identify vulnerabilities before a hacker identifies them)
- Cyber Security Services (Good for getting Cyber protection implemented can be broken into bite size monthly amounts.)
- Check Google reviews of cyber security consultancies or use Aucyberscape.com.au to locate listed providers in an area most relevant to you.
- Assess their training - programs customised to your specific situation are likely to be better than off-the-shelf international courses.
- Check their physical location (a simple online search of their stated physical offices will assist), and the country in which they are headquartered, if applicable. For example: are they a reputable provider, with a presence or major base in Australia or New Zealand?
- Determine if the consultancy has tailored pricing for different-sized businesses.
- Ask for a demonstration of any software they recommend for your business and whether you can establish a free trial or set up a dummy account to experiment.

Directory of cyber expertise

Aucyberscape is a national directory of more than 300 cyber security businesses. Founded in 2021, it connects these businesses with those who need services, products and software, as well as investors.[61] The directory is a valuable resource for SMEs that need support to:

- strengthen the defence of computer hardware
- protect software and platform security including mobile, cloud and web applications
- improve operational, network and systems security
- be proactive in defending against a cyber attack
- find tools to prevent user mistakes and support business' cyber governance and regulatory compliance.

The site also offers educational resources so people can become more cyber security savvy by deepening their knowledge and expanding their skills. It also links them with further cyber security courses at universities and TAFE.

The ACSC provides advice on working with Managed Service Providers.

In New Zealand, report cyber security incidents in the first instance to CERT NZ - a Computer Emergency Response Team that was established by the government in 2016. It supports organisations and individuals with a range of information and services, including:

- threat and vulnerability identification by analysis of local and international data
- incident reporting to assist organisations and individuals online and by phone
- response coordination where an organisation has to work with others
- readiness support by raising awareness of cyber security best practice

61 Interview with Dr Jed Horner, Head of Government Relations & Advocacy at Stone & Chalk. AustCyber, part of the Stone & Chalk Group was instrumental in creating the directory in 2021.

SPOTLIGHT

BEN JONES
CONTINUUM
CYBER

Creating cyber equity for SMEs

To ensure small businesses protect their crown jewels, Continuum Cyber gives them access to resources and industry-specific threat intelligence.

During years spent working in cyber security for large corporations, Ben Jones saw a gap in the market to provide SMEs a similar level of service.

"There's real cyber inequity for these smaller players," he says. "They might have one IT guy or a small team if they're lucky, but many feel the cost is prohibitive to address this issue adequately and access the experts."

This prompted Jones to establish Continuum Cyber, a security platform providing cyber security software and support to SMEs.

When businesses partner with Continuum, its consultants first carry out a risk assessment – a "deep dive" into technology, processes and employees. Once they have insights into any vulnerabilities, consultants will create a plan to remediate weaknesses and make the business more cyber safe.

The software provides employees with a dashboard delivering real-time updates on a business' security using best practices and cyber security global standards.

"Human error causes 95% of security breaches so we spend a lot of time focusing on training your employees, developing a tailored, overarching technology plan and processes, and helping you to implement it," says Jones. "This is how you start creating a security-aware culture."

The company provides continuous access to resources and industry-specific threat intelligence. It will also run a variety of simulated cyber-intrusion tests to check the strength of a client's cloud services and software, as well as employee awareness.

"From your client's and customer's perspective, we also ensure that their data and privacy is protected and legally compliant. These are the crown jewels and what your business' reputation rests on," he says, adding that businesses should ask questions about their suppliers' cyber security before partnering with them.

SPOTLIGHT

JON MELLOY
PRACTICE
PROTECT

One-stop security for accounting firms

Practice Protect provides ongoing employee training as well as updates on international and national cyber security breaches so employees are alert and aware.

Practice Protect enables busy firms to expand their practice, hire with confidence, operate remotely and support their teams wherever they are with upgraded login security, email protection, cyber threat training and compliance documentation.

Jon Melloy, Head of Growth for Practice Protect, emphasises the importance of firms taking a proactive approach to cyber security, citing an example from the company's experience of its own approach to security during the pandemic.

Melloy describes how one of the company's employees asked to use her home computer to log on to the office. "Her teenage brothers had been using her computer to download games and free movies. We discovered over 150 viruses on it! It was good we checked and it took us over two hours to get rid of them," he says.

Cyber security must become part of your company culture, says Melloy. "You can't just give employees annual security training and tick that box. Keep reminding them. If anyone gets a scam email, screenshot it and pass it around the office. Inform them about international and national cyber security breaches so it's always front of mind."

Phishing scam

Melloy describes the experience of an accounting firm of ten employees in Victoria which faced a damaging cyber security breach. One of their junior accountants inadvertently clicked on a Phishing scam email attachment.

The scammer was then able to hack into the employee's Microsoft Office 365 email inbox even though they had two factor authentication switched on. "It was pretty nasty because then they sent Ransomware emails from her address to every address in her contact list," says Melloy.

Once the clients informed them about what had happened, the firm reported the incident to the Australian Cyber Security Centre and then had to alert their entire client base.

"The incident took an emotional, reputational and financial toll on the firm," says Melloy. "For some clients, this cyber incident was the tipping point and they left the firm."

In total, the time it took to contact their client base and remediate the damage cost them more than $62,000 in lost billable hours and revenue. The firm didn't have adequate cyber insurance and they couldn't claim the money back.

62 Cyber Security CRC Smaller but stronger: Lifting SME cyber security in South Australia

Part 4
Further resources

Part 4

Glossary of terms

Malware – a malicious software attack with the intention to cause harm, to a computer or a network, steal data or an identity.

Ransomware – malicious software controlled by a cyber criminal that locks or encrypts your computer documents, financial information, photos or other critical data. The criminal holds your data hostage and tries to extort a ransom (often in a crypto currency such as bitcoin) to unlock it.[63]

Distributed Denial of service (DDos) and Denial of service (DoS) attack – DDos attack is when multiple connected online devices collectively overwhelm a target website, server or intranet with fake traffic. Normal web traffic is blocked. A DoS attack comes from a single source or location and is easier to block than DDos.[64]

Virus – code inserted in an application program or system that lies dormant until it's unintentionally deployed by the victim when they click on an email attachment or direct message. It can then send infected files to contact lists, steal data, launch ransomware and DDoS attacks.

Worm – unlike a virus, a worm doesn't need humans to deploy it. Worms can delete or modify files, steal data, launch DDoS or ransomware attacks and infect many computers at once

63 What is ransomware? Ransomware explained and how it works | Norton

64 What is a distributed denial-of-service (DDoS) attack? | Cloudflare

Trojan – deceives victims by masquerading as a genuine app or software. When the victim unknowingly clicks on it, it takes control of their device, deleting, modifying or stealing data, spying on users or accessing networks.[65]

Adware Malware – happens when advertising-supported software tracks your buying patterns and shows you ads, but with malicious intent to steal your data to sell it to third parties, for credit card fraud or identity theft.

Phishing or Business Email Compromise – a cyber criminal sends emails that appear to come from a reputable source but with the goal of stealing data such as credit card or login details or installing malware. This includes spear phishing - targeting individuals as a first step to penetrate an organisation and then whale phishing - when they target the CEO or executives who usually have a higher level of access to classified information.[66]

Botnets – access computers or devices through a piece of malicious coding, enabling cyber criminals to take remote control of a device to launch DDoS attacks, observe your activity and take screenshots of your use of the keyboard or webcam. They can also send phishing emails.

Dwell time – the period of time an attacker has access to a network or system before they are discovered and removed.

65 Understanding Trojan Viruses and How to Get Rid of Them | McAfee Blog

66 What Is a Phishing Attack? Definition and Types - Cisco ,Protecting Against Business Email Compromise | Cyber.gov.au

Part 4

Further resources

CA ANZ

- Why CFOs should take the lead on cyber security
- Cyber and the CFO
- Protect our cyber future
- Cyber security for SMEs and practitioners

Standards

- ISO 27001 is an internationally recognised Information Security Management System (ISMS) standard.
- National Institute of Standards and Technology (NIST) Cyber Security Framework

Australia

Australian Cyber Security Centre

- Small & medium businesses Cyber.gov.au
- Essential Eight

Australian Tax Office resources

- Top cyber security tips for businesses | Australian Taxation Office
- How to prepare for a cyber security incident | Australian Taxation Office

Australian Government Department of Business

- Create a cyber security policy

Office of the Australian Information Commissioner

- About the Notifiable Data Breaches scheme

Australian Securities and Investments Commission

- Cyber resilience good practices | ASIC - Australian Securities and Investments Commission

New Zealand

New Zealand Cyber Security Centre

- Guides | CERT NZ
- Charting Your Course

New Zealand RASCI approach to cyber security

- A Guide to the Project Management Body of Knowledge (PMBOK Guide) (5th ed.). Project Management Institute.

United States

US's National Institute of Standards and Technology

- Framework for Improving Critical Infrastructure Cyber Security, 2018

Assessment Tool

- Self-assessment tool compiled by Continuum Cyber for CA ANZ

United Kingdom

UK's National Cyber Security Centre (NCSC)

- 10 Steps to Cyber Security 2021
- Small_Business_Guide 2020

Singapore

The Singapore Government's Cyber Security Awareness Alliance Go Safe Online website SMEs

Reporting Obligations

Office of the Australian Information Commissioner

- About the Notifiable Data Breaches scheme
- Australian Privacy Principles listed in the Privacy Act of 1988

New Zealand, the Privacy Act 2020

- Principle 5

Acknowledgements

CA ANZ wishes to acknowledge the contributions to this report of David Waine CA (Matley Financial Services), Ben Jones (Continuum Cyber), Martin Boyd (Vertex Cyber Security), Jed Horner (AustCyber), Jon Melloy (Practice Protect), Dushern Pather (TechSpecialist), Sunny Sirabas (CA ANZ), Lauren Geraghty (CA ANZ), Priya Kumar (CA ANZ), Debbie Kandauw CA (CA ANZ), Karen McWilliams FCA (CA ANZ).

Disclaimer

This Playbook has been prepared for use by members of Chartered Accountants Australia and New Zealand (CA ANZ). It is not intended for use by any person who is not a CA ANZ member. Before using this Playbook, you should read it in full, consider its effect and determine whether it is appropriate for your needs. This Playbook is intended to provide general information only and is not intended to provide or substitute legal or professional advice on a specific matter. This Playbook was created in April 2022. Laws, practices, statistics, information and regulations may have changed since that time. You should make your own enquiries as to the currency of relevant laws, practices, statistics, information and regulations and you should contact IT security professionals to ensure your approach to cyber risk mitigation is appropriate. No warranty is given as to the correctness of the information contained in this Playbook, or of its suitability for use by you. To the fullest extent permitted by law, CA ANZ is not liable for any statement or opinion, or for any error or omission contained in this Playbook and disclaims all warranties with regard to the information contained in it, including, without limitation, all implied warranties of merchantability and fitness for a particular purpose. CA ANZ is not liable for any direct, indirect, special or consequential losses or damages of any kind, or loss of profit, loss or corruption of data, business interruption or indirect costs, arising out of or in connection with the use of this publication or the information contained in it, whether such loss or damage arises in contract, negligence, tort, under statute, or otherwise.