Cyber Security 25

Staying Ahead In A Fast-Changing Cyber World

#1 Cyber Security and/or Scams Education 2023–25 (=#1 in 2023).
In the Coalition Greenwich Voice of Client Australia Large Corporate & Institutional Transactional Banking Study, 2023-25 (=#1 in 2023). All ranking against four major domestic banks.

Executive Summary

Cyber security is now a core business risk. Generative AI, criminal groups, and new regulation are changing how attacks happen and how we must respond. The shift is from hoping to prevent everything to planning to operate through disruption.

This guide aims to support leaders with tips to turn cyber risk into clear actions: protect what matters most, practise incident response, and hold suppliers to the same standard as internal teams.

The goal is simple

Fewer incidents → Faster recovery → Better protection for our customers

Foreword: Dr. Maria Milosavljevic - ANZ Chief Information Security Officer

Cyber security in a rapidly changing world

Cyber security is a shared responsibility for every member of our organisation - every staff member, every partner, every supplier and every customer. This is no longer optional, as it is foundational for building trust in our highly connected, digital world.

But trust is also tested by how well we prepare for and bounce back from disruptions. Being resilient means having the right tools and processes, informed leadership, everyone working together to keep things running smoothly and understanding how to respond if challenges arise.

The need to evolve

As AI, cloud platforms, and digital ecosystems reshape how we operate, our approach to security must adapt. Reactive defence is no longer enough. We need proactive strategies that anticipate threats, respond in real time, and enable security to be built into every part of the business.

No organisation stands alone

We operate in complex networks of suppliers, partners, and platforms. This interconnectedness drives innovation - but it also introduces risk. Your resilience is only as strong as your weakest link. That's why cyber security must extend beyond internal systems and be embedded into third-party risk management.

The threat landscape is accelerating

AI is being exploited to craft hyper-personalised phishing emails, clone executive voices for deepfake scams, and deploy self-learning malware that adapts in real time.[1] Insider threats are rising too often amplified by behavioural manipulation and compromised credentials. State-sponsored actors continue to target critical infrastructure such as government services, energy grids, or defence systems.[2] Yet AI also helps to detect anomalies, automate responses, and secure digital assets quickly and precisely.

Technology sets the stage, but people determine the outcome

Human behaviour - whether through vigilance or vulnerability - is one of the most critical controls. The awareness, habits and instincts of our people shape our security posture. That's why we invest in human-centric security - simplifying authentication, increasing just-in-time education, and applying behavioural science to build secure habits.[3]

Resilience requires technology, processes and people

It's built through preparation, practice, and culture. Practicing through red team drills, tabletop exercises, and cross-sector simulations helps build rapid response and trust across teams. Because a well-trained and rehearsed team will work seamlessly to minimise the duration and potential impacts of a real incident.

The road ahead: adaptive, risk-based cyber security

To meet the demands of a volatile digital landscape, Australia's cyber security response must evolve from passive to predictive, and from reactive to adaptive.

To meet the speed and complexity of the threats we face, AI must power our defensive tools, enabling real-time defence. Equally, every organisation must risk assess their use of data and AI to ensure that we maximise its value while minimising any risks that can be introduced.

Reactive defence is no longer enough. We need proactive strategies that anticipate threats, respond in real time, and enable security to be built into every part of the business.

Organisations must move beyond compliance checklists and adopt risk-based frameworks that focus on resilience and continuity rather than betting everything on prevention alone.

Cyber security today is about readiness, agility and trust

Organisations that foster a culture of security will be best positioned to survive and thrive through digital evolution and malicious disruption.

This guide is designed to help support our customers in adopting a strategic, risk-based approach to cyber security.

Trust is earned through secure products and making sure only the right people and systems have access to the information and systems they need to perform their role.

Trust is sustained through collaboration, consistent standards, shared responsibility and contributing to the cyber security of the broader community.

Dr. Maria Milosavljevic

ANZ Chief Information Security Officer

Contents

Sections can be easily accessed throughout the document using the navigation menu on the left of each page.

The evolving cyber landscape

Pillars of cyber resilience

Trust

Technology

Collaboration

Adaptability

Cyber security is evolving, not just in response to rising threats, but through innovation, collaboration, and greater focus on risk management. As digital ecosystems grow more complex, resilience must go beyond recovery to readiness and adaptability.

Human behaviour is now a central factor in cyber risk. Threat actors increasingly target individuals using AI-powered deception and identity manipulation. Awareness and secure habits are as critical as technical controls.

Community and regulatory expectations are intensifying. This shift demands proactive, ethical security leadership.

Organisations operate within vast, interconnected networks. The security of your suppliers, partners, and customers directly impacts your resilience.

Human behaviour is now a central factor in cyber risk.

Leading organisations are adopting a risk-based approach to cyber security.

Cyber security must be embedded into third-party risk assessments and treated as a shared responsibility.

Resilience means having a clear, and practised, plan for crisis response which reflects critical dependencies between systems, third parties and services. Leading organisations are adopting a risk-based approach to cyber security –prioritising controls based on threat intelligence, business impact, and risk appetite – rather than relying solely on maturity models or compliance checklists.

In a digital economy where trust is the most valuable currency, cyber resilience is the foundation on which reputations are not only built, but protected, tested, and sustained.

The impact of rapidly advancing technology

Rapid adoption of emerging technologies has enabled greater flexibility, personal and business connectivity, as well as transformative insights and business opportunities from data analytics. New tech, more data, greater use of third parties, and complex systems are all factors that can help organisations perform better.

All of this has enabled people to be more connected virtually, at a time where they are becoming more distanced physically. With new innovations being developed to make life and work easier, it's important that leaders contemplate how these factors, if not well managed, could change their businesses' security and compliance position.

Key drivers behind the surge in cyber attacks

Increasingly adverse threat environment

Complexity of systems and technology

Phenomenal growth of data

Increased connectivity with third parties

Rapid adoption of transformative technology

Remote workforce and hybrid workplaces

Increasingly adverse threat environment

The global cyber security landscape is marked by an increasingly adverse threat environment, driven by several factors that challenge the resilience of organisations and institutions around the world. Geopolitics has moderately influenced organisations' cyber security strategy.

Cyber threats from state actors not only target critical infrastructure but also aim to destabilise political and economic systems.[4] The rapid adoption of emerging technologies, such as generative AI, has introduced new vulnerabilities. While these technologies offer significant benefits, they also create new attack vectors that cybercriminals can exploit.[5] The recent World Economic Forum's Global Risks Report highlights the profound impact of these technological advancements, noting that the potential for AI to be used in spreading misinformation and disinformation is a significant short-term threat.[6]

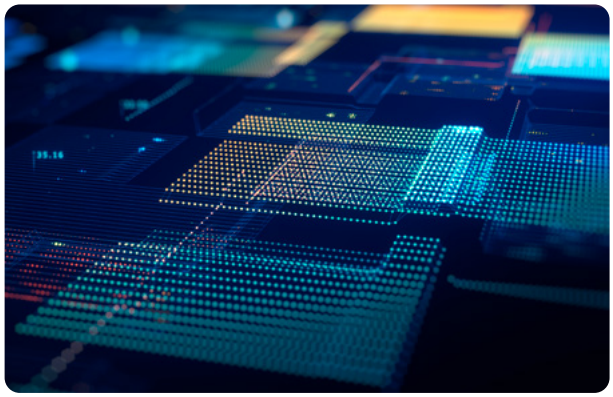
Ransomware remains a major concern, with Ransomware as a Service (RaaS) making it easier for attackers to deploy ransomware attacks. This model has lowered the barrier to entry for cybercriminals, leading to a proliferation of ransomware incidents. Business Email Compromise (BEC) scams are also becoming more sophisticated, resulting in significant financial losses for organisations worldwide.[7]

Environmental risks further complicate the cyber security landscape. The World Economic Forum's report underscores that extreme weather events and climate-related disruptions are expected to become more severe over the next decade.[8] These environmental challenges can strain resources and infrastructure, making it harder for organisations to maintain robust cyber security defences.

The rapid adoption of emerging technologies, such as generative AI, has introduced new vulnerabilities.

Additionally, the interconnected nature of global supply chains means that a cyberattack in one region can have cascading effects worldwide.

Governments are ramping up cyber security efforts through updated legislation and global partnerships. For instance, the U.S. CISA FY2025-26 International Strategic Plan focuses on securing global supply chains and enhancing international cyber deference.[9] The UK is revising its Telecommunications Security Code of Practice to address emerging threats.[10] Australia has expanded its regulatory powers under the Security of Critical Infrastructure Amendment Rules 2025.[11] The EU's Cyber Solidarity Act establishes cross-border mechanisms for threat detection and emergency response.[12]



As organisations and governments navigate this complex environment, the need for enhanced cyber resilience and proactive risk management has never been more critical.

Singapore's Cyber Security Strategy 2025 and Japan's industry revitalisation plan emphasise regional cooperation and innovation to counter evolving threats.[13,14]

Despite these efforts, the cyber security landscape remains highly dynamic and unpredictable. A recent report reveals a world "plagued by a duo of dangerous crises: climate and conflict". This pessimistic outlook is shared by many global experts, who anticipate a significant degree of instability and an elevated risk of global catastrophes over the next decade.[15] As organisations and governments navigate this complex environment, the need for enhanced cyber resilience and proactive risk management has never been more critical.

Complexity of systems and technology

Every day, new service options and applications add to an already large base of existing technology. Each addition can bring benefits, but also complexity to technology networks.

Technology teams face a delicate balancing act in maximising service uptime, while keeping systems up to date (patched) to guard against new vulnerabilities.

There's often a short time between vulnerabilities being identified and attackers determining how to exploit them. The number of security vulnerabilities distributed is increasing each year.[16]

There can be a price to pay when businesses fail to prioritise patching and vulnerability management, including data and financial loss leading to reputational, regulatory, and legal impacts.

Phenomenal growth of data

Governments worldwide are increasingly implementing regulations to manage the growth and use of data.

Governments worldwide are strengthening data protection laws to manage the growing complexity of digital data use. The European Union's General Data Protection Regulation (GDPR) continues to set the global benchmark, with recent amendments improving cross-border enforcement and extending adequacy decisions for data transfers.[17] In India, the government released the Digital Personal Data Protection Rules 2025 to operationalise its 2023 Act, focusing on consent management, breach notification, and child data protection.[18]

In the United States, the California Consumer Privacy Act (CCPA) was updated in 2025 to increase fines and thresholds, reflecting its growing role in shaping national privacy standards.[19] China launched a series of enforcement actions under its Personal Information Protection Law, targeting illegal data collection across apps, smart devices, and public spaces.[20] Australia's Privacy Act 1988 was amended in late 2024 to introduce new civil penalties, protections for children's data, and transparency around automated decisions.[21] New Zealand's Privacy Act 2020 remains aligned with GDPR principles and was updated in 2025 to improve clarity and enforcement.[22]

As data flows increasingly transcend borders, international cooperation and harmonization of standards are becoming essential. The World Economic Forum emphasizes that cross-border data regulations now require strategic, organization-wide compliance frameworks to maintain trust and operational resilience.[23]

Increased connectivity with third parties

Third- and fourth-party suppliers are becoming more valuable business partners that can support and uplift your business performance. Still, where they have access to your systems and information, it is important to check that they are adequately equipped to help protect your business and customer information.

Companies sharing data with third parties should check that both their own data and systems, and data held, or systems used to manage information on their behalf, are secure. This becomes even more important when third parties have their own subcontracting arrangements, meaning access to sensitive data extends to fourth parties and beyond.

Third parties make it easier for companies to do business, but when they hold sensitive information or operate services, businesses should implement active and ongoing monitoring, to help protect their information wherever it may be.

Many organisations use a Managed Service Provider (MSP) to support their systems and technology. MSP's are often vital to the running of businesses, and this makes them an attractive target to malicious cyber actors.[24] The fact that they service many companies is another reason why a malicious cyber actor may choose to target an MSP, and doing so may result in access to hundreds of organisations and their data.

Rapid adoption of transformative technology

Capitalising on the opportunities of emerging technology, including cloud, requires a commitment to embedding security from the beginning. Often the speed of change and desire to quickly adopt new technologies for their operational efficiencies can mean that security requirements get overlooked.

Cloud computing

The transition to the cloud is happening fast, with organisations embracing the benefits of the speed and efficiency that it delivers. Cloud computing also has the potential to solve many of the security challenges affecting organisations. For instance, managed cloud-based IT infrastructure can include automatic updates (patching) for security vulnerabilities to keep operating systems up to date.

Internet of things (IoT)

The importance of a security first approach to modern technology is illustrated by the rapid adoption of internet connected devices, such as smart TVs, digital assistants, and security monitoring, now collectively known as the Internet of Things (IoT). While these devices have quickly become invaluable tools, many companies and their employees fail to appreciate the risks they present.

IoT devices not only collect valuable user data, but they can also serve as a primary resource from which attackers can launch distributed denial-of-service (DDoS) attacks through botnets.[25]

With their focus on innovation and functionality, IoT developers can overlook security features that may increase manufacturing and maintenance expenses[26], potentially leaving businesses as well as their consumers exposed.

As we continue to digitally transform products and services, security should be at the forefront to maintain both resilience as well as confidence

Digital transformation of services

Increasingly, consumer services like virtual health are changing the way we live and work. Whilst the pandemic bought about mixed changes, this is a welcome shift.

And whilst consumers and clinicians are aware of the benefits that virtual care offers, the survey highlighted that there are concerns in relation to the confidentiality, integrity and availability of information.

As we continue to digitally transform products and services, security should be at the forefront to maintain both resilience in the service or offering that an organisation provides as well as confidence from their customers.

IoT developers can overlook security features that may increase manufacturing and maintenance expenses[26]

Artificial intelligence and machine learning

In today's rapidly evolving business landscape, innovation can be essential to success. Organisations that thrive are often those that foster creativity, embrace diversity, and encourage cross-disciplinary collaboration.

Artificial Intelligence (AI) and Machine Learning (ML) hold immense promise, but their successful integration can require a holistic approach. Organisations need to recognise how implementing AI may impact their workflows, roles, and culture.[27]

In the same breath, as AI advances, so can cyber threats. Deepfake technology can create convincing fake videos, posing risks to reputation and security.[28]

Automated phishing campaigns may exploit AI to craft personalised attacks.[28] Organisations may greatly benefit in robust cyber security protocols. Regular audits, employee training, and threat detection systems are essential to help safeguard digital assets while often enhancing productivity and value creation.[29]

Remote workforce and hybrid workplaces

The shift to remote and hybrid workplaces has significantly impacted cyber security. With employees working from various locations, the attack surface for cyber threats has expanded, making it easier for attackers to exploit vulnerabilities.[30]

Remote workers often use personal devices and unsecured networks, increasing the risk of data breaches and cyberattacks.[31] Additionally, the lack of physical security measures in home environments makes it challenging to monitor and protect sensitive information.[32] Organisations must adapt by implementing robust security protocols, such as multi-factor authentication, regular security training, and advanced threat detection systems.[33] Despite these challenges, the transition also presents an opportunity to enhance cyber security practices and foster a culture of security awareness among employees.[34]

The attack surface

Cyber criminal targets

With a cyber landscape the likes of which we've never seen, creative cyber criminals continually develop new ways to exploit the evolving environment. They can be encouraged by increasing opportunities to profit (financially or politically) substantially from a cyber attack.

Security can play a valuable role in the way an organisation identifies and responds to risks. These risks can be made up of internal factors, such as system vulnerabilities, insecure processes and people. However, it's important not to forget that there are also external factors such as an organisations' supply chain and their third parties.

Far beyond being a reactive function, whose sole purpose is to stop hackers when they attack, a security team can contribute to the improved performance of an organisation. It can help take advantage of new opportunities in a secure way that builds confidence and trust in the resultant services. In much the same way as a car can go faster when it has better brakes, an organisation can operate more effectively when it has a robust security function.

Internal factors

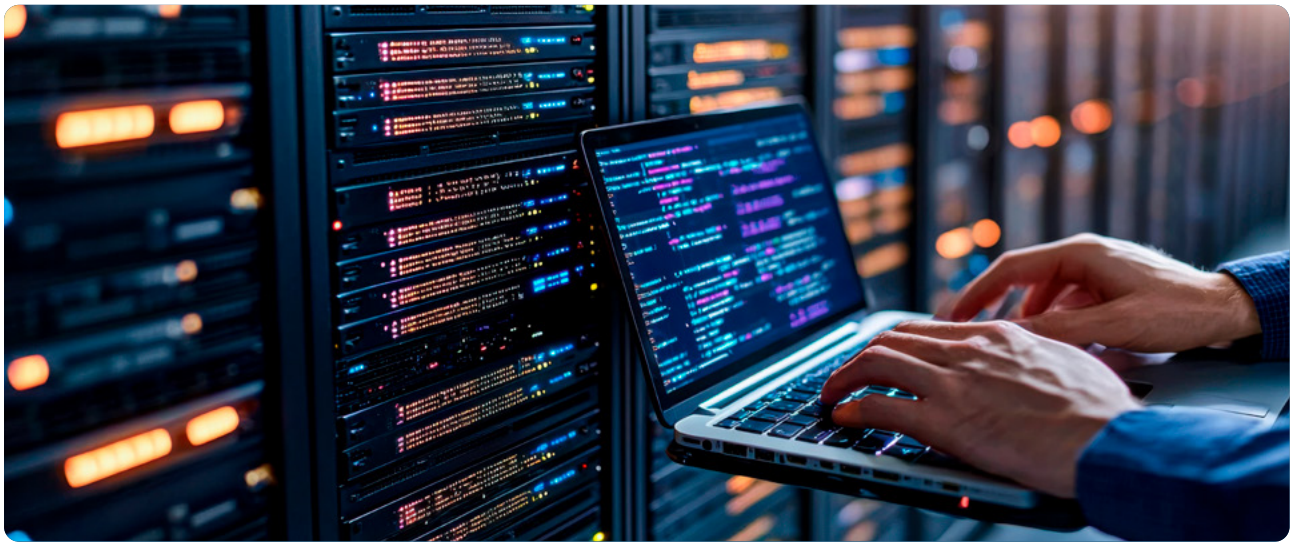
People

People are a key component of any organisation and should be valued and supported just the same as any other security control. They can provide a first and last line of defence, detecting and reporting malicious emails, suspicious phone calls, anomalous activity on the network or poor security practices. Often, people are also the target.

Social engineering is the process of using human behaviour to manipulate a person into inadvertently sharing information, clicking links, or other behaviours that can help a criminal meet their objective.[35]

However, with the right education and training along with technology and process based controls, employees can be an important defence mechanism against social engineering. Developing the right skills across a workforce however is inherently complex and requires a sustained, culturally appropriate focus.

Cyber criminals understand this complexity and look to take advantage of skill gaps and human behaviours such as our natural desire to help others.



Common security attacks

Common security practices prone to human error:

- Clicking on phishing links or attachments
- Downloading malicious software
- Inadvertently sharing organisational or customer information to unauthorised callers
- Using the same or a weak password across multiple systems or applications
- Storing user IDs and passwords in plain text on computers
- Sharing sensitive information on social media platforms or cloud solutions with inadequate security
- Failing to prioritise the latest software updates (patching) or other security remediation
- Engaging third parties without reviewing their security
- Acting on an unexpected or unusual invoice without validating its legitimacy

Processes

Having the right processes in place is critical to an organisation's cyber security.

The cyber threat landscape is constantly changing, and organisations should be regularly reviewing their existing processes to adapt to the changing environment.

Cyber security requires a combination of tactics across people, technology and process to be effective and provide a layered approach. Processes can provide an organisation with controls to help proactively prevent and respond to cyber security attacks.

Organisations could start to protecting what's most important to them by prioritising their assets, assessing what cyber threats can impact them, and developing controls to protect those assets against the possible threats.

The following tools provide guidelines and benchmarks to help companies identify areas for improvement and prioritise cyber security initiatives.

NIST Cyber security framework (USA)

Developed by the National Institute of Standards and Technology, this provides a policy framework of computer security guidance for how private sector organisations can assess and improve their ability to prevent, detect, and respond to cyber attacks.[36]

Cyber essentials (UK)

A government-backed scheme that helps organisations protect themselves against a range of the most common cyber attacks. It provides a clear statement of the basic controls all organisations should implement to mitigate the risk from common internet-based threats.[36]

Essential eight (Australia)

Developed by the Australian Cyber Security Centre, this is a set of baseline strategies to mitigate cyber security incidents. It includes recommendations for application whitelisting, patching applications, and restricting administrative privileges.[36]

Digital ready assessment tool (Australia)

Launched by the Australian Government, this free online tool helps businesses assess their digital maturity, compare themselves against their peers, and access government support programs.[37]

Cyber security maturity model certification (CMMC) (USA)

A unified standard for implementing cyber security across the defence industrial base. It aims to protect sensitive information and improve the cyber security posture of companies in the defence supply chain.[36]

CERT NZ's critical controls (New Zealand)

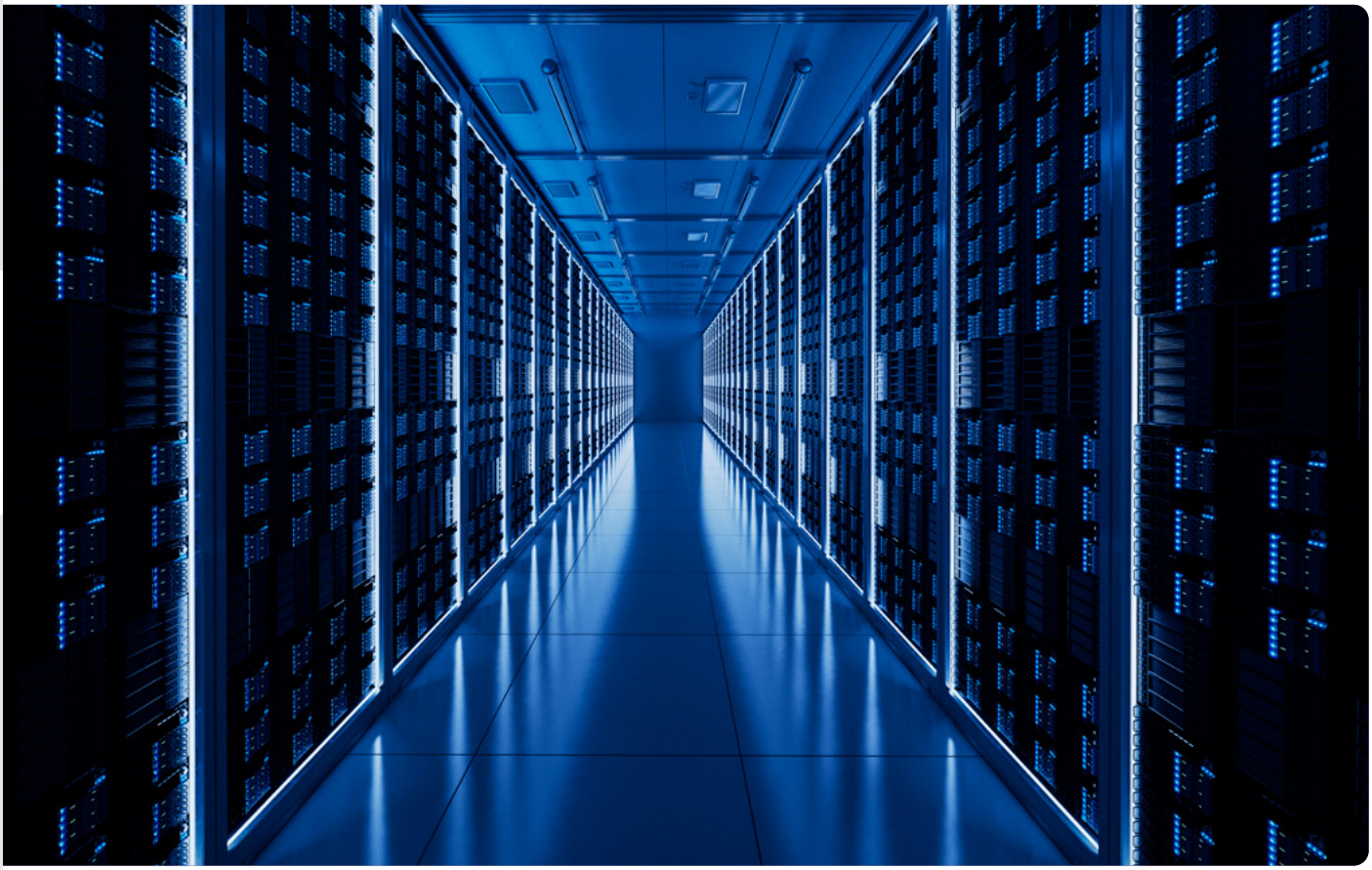
While not government-specific, this international standard is widely adopted and provides requirements for an information security management system (ISMS).

It helps organisations manage the security of assets such as financial information, intellectual property, employee details, or information entrusted to third parties.[38]

ISO/IEC 27001 (International)

While not government-specific, this international standard is widely adopted and provides requirements for an information security management system (ISMS).

It helps organisations manage the security of assets such as financial information, intellectual property, employee details, or information entrusted to third parties.[36]



System vulnerabilities

Applications and operating systems require ongoing maintenance (or patching) to prevent vulnerabilities identified in code from being exploited by hackers to gain system access.

When an application or operating system requires a patch, the developer releases an explanation of why the update is required. This transparency can also provide cyber criminals with the necessary information to reverse engineer a compromise or way into a network, so fast patching is essential.[39]

Some organisations might delay applying updates for lack of time, fear of changing a known tool, or doubt that the latest updates will work with their existing processes. Cyber criminals understand this tendency to delay patching, and exploit vulnerabilities in older versions of applications to access networks before vulnerabilities have been patched.

This is why application testing and a robust change management approach should be applied as soon as patches are released. Additionally, patching your systems as soon as updates are released typically means that changes are simpler, take less time, and are less disruptive compared to applying a large backlog of changes at once.

Typically, newer versions of operating systems and applications are designed with more features and security built in. In summary, up to date and well patched systems can be more secure, and are likely to be more reliable – so there are a lot of good business reasons to keep systems up to date.[40]

External factors

Third parties and supply chain

As interconnectivity expands, malicious actors are increasingly targeting multiple victims across various sectors through a single entry point. According to a 2025 report, 54% of organisations identified supply chain challenges as the biggest barrier to achieving cyber resilience.[41] This lack of visibility has tangible consequences: it is reported that third-party involvement in breaches has doubled to 30%.[42]

The growing requirement to share data and integrate information systems with third and fourth parties increases the attack surface for information breaches and compromises, either from deliberate attacks or by accident.

Cyber supply chain risks can change whenever organisations introduce or decommission a third party. Effective management of supply chain risks can go a long way to help secure supply throughout the product life cycle, from design through to manufacturing, delivery, maintenance and disposal.

Organisations can support strengthening their third and fourth-party risk management through continuous monitoring, well-defined contractual obligations for data protection, incident response, and compliance, and protocols for timely threat intelligence exchange and coordinated recovery efforts.

54%

54% of organisations identified supply chain challenges as the biggest barrier to achieving cyber resilience.[41]

30%

Lack of visibility: It is reported that third-party involvement in breaches has doubled to 30%.[42]

Cyber attack tactics

Artificial intelligence is reshaping the threat landscape. While it enhances defence capabilities, it also enables attackers to scale and automate operations.

AI-driven phishing now mimics tone, timing, and context challenging traditional detection methods. Deepfakes can bypass video verification and erode trust in digital communications. Generative AI can craft highly convincing messages tailored to individuals, while deepfakes are used to impersonate executives and manipulate recipients into taking action.

Organisations may adopt tactics to help counter these threats, such as AI-powered defences that can detect anomalies and respond in real time. As attackers evolve, defenders must match their pace with intelligent, adaptive strategies.

Some of the more common approaches to gain access to organisational data and systems include:

Ransomware

Malicious software

Distributed Denial of Service

Business Email Compromise

Impersonation scams

Ransomware

Ransomware attacks involve encrypting an organisation's data or systems and demanding payment, often in cryptocurrency, for their release. Ransomware-as-a-Service (RaaS) platforms have also lowered the barrier to entry, enabling less technical criminals to launch sophisticated campaigns.[43]

Malicious Software

Malware encompasses a wide range of harmful software, including viruses, trojans, spyware, and rootkits. These programs are designed to infiltrate systems, steal data, monitor user activity, or disrupt operations. AI is now being used to create polymorphic malware code that constantly changes its signature to evade detection. Some malware variants are also capable of autonomous propagation, spreading across networks without human intervention.

Distributed-Denial-of-Service (DDoS)

DDoS attacks overwhelm systems, servers, or networks with excessive traffic, rendering them inaccessible to legitimate users. With the proliferation of Internet of Things (IoT) devices and botnets, attackers can now launch multi-vector DDoS campaigns that target multiple layers of infrastructure simultaneously. The impact can range from temporary service outages to long-term reputational damage.

Business Email Compromise (BEC)

BEC attacks involve impersonating trusted individuals such as executives, suppliers, or partners to convince employees into transferring funds or sensitive information. These scams are increasingly enhanced by AI-generated emails and voice deepfakes, which mimic tone, style, and even speech patterns. Attackers often monitor email threads and time their messages to appear legitimate, making detection more difficult.

Impersonation and Deepfake Scams

Impersonation scams have evolved beyond simple email spoofing. Cybercriminals now use deepfake technology to create realistic audio and video content that impersonates individuals in real-time meetings or calls.[44] These tactics can be used to authorise fraudulent transactions, manipulate negotiations, or spread disinformation. As generative AI tools become more accessible, the sophistication and frequency of these attacks are expected to rise.

Exploiting trust through Business Email Compromise (BEC)

For business email compromise to be successful, a sense of trust must be established. To this end, cyber criminals employ various techniques:

- Sending emails using near identical domains (e.g. @azn.com instead of @anz.com)
- Sending emails from authentic email accounts (after gaining control via phishing or theft of staff email credentials)
- Purporting to come from (or spoofing) suppliers' or creditors' email addresses.

But that's not all. They may also:

- Pretend to be someone else, either a known third party, employee or person of significance to the person being scammed.
- Suggest everyone else within the organisation is doing something similar.
- Use hierarchy to suggest the request is from a senior stakeholder within the organisation (e.g. Head of Human Resources or Payroll).
- Indicate they can't be contacted for further information due to travel or personal circumstances.
- Create a sense of urgency in stating requests to avoid negative impacts (e.g. prices or terms may change).

Criminals hope that victims will update bank account details, share sensitive personal records, click on a link or download a document. In many cases, business email compromise doesn't include a malicious hyperlink or attachment, so they sneak past anti-virus and spam filters without detection. Where emails do include a malicious attachment or link, well managed anti-malware and spam filters should help identify and remove a high proportion of these emails, but not all can be detected automatically.

Impacts of Cyber Attacks

Reputational damage

Emotional distress

Financial loss

Business disruption

Loss of intellectual property

Customer devastation

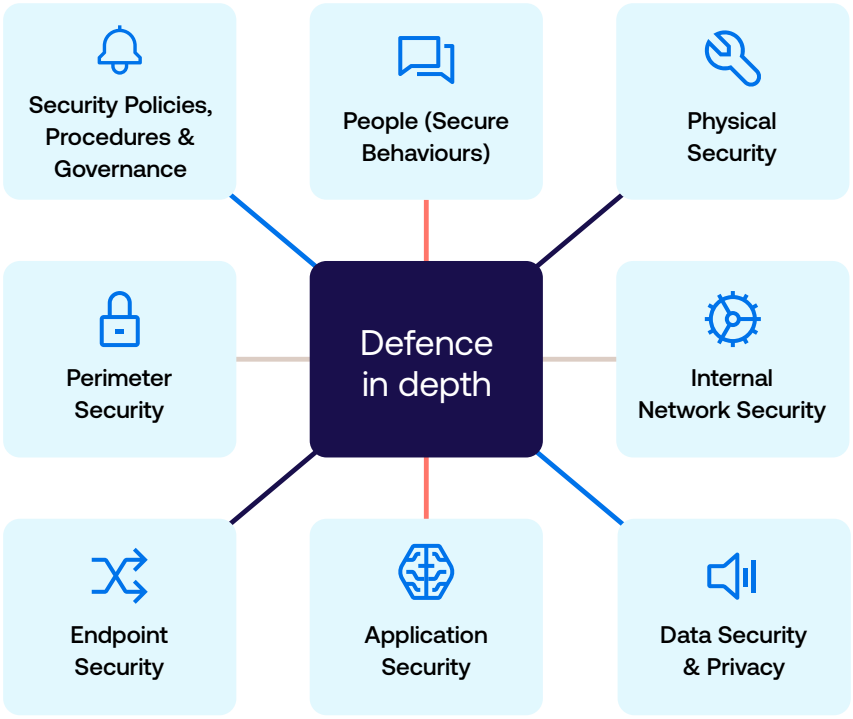
Regulatory fines

Identity theft

Physical damage (if the attack involves Operational Technology (OT) and Industrial Control Systems (ICS))

Inability to access critical services / supplies

Defence in depth



A strong security position - the sum of all parts

Cyber security isn't about a single function or component working in isolation, but a complex interconnection of equally important parts working together.

By understanding the threat landscape the opportunities that a cyber criminal may look for, and how they go about exploiting an identified vulnerability, organisations can develop an informed response to cyber threats and issues. This includes implementing relevant controls, processes and procedures so that security risks are managed to an acceptable level. Controls need to be reviewed regularly, so that they can stay aligned to the changing technology landscape.

A defence in depth approach anticipates the security considerations across all areas of an organisation from technology to processes to people. It also applies multiple layers of security controls to prevent distinct types of attacks. For example, an organisation could issue employee security passes to access office buildings and apply user authentication requirements to enter the technical network.

After controlling access to the physical premises and technical network, the organisation could also restrict users' access to only the systems and functions they require to perform their role - this is where network segmentation and privileged access management becomes valuable.

These controls can then be reinforced with a cyber security behaviour influence program that educates and enables people to meet their specific security responsibilities.

Such a program should be integrated with and informed by a threat intelligence capability. Robust governance, processes and standards also need to be understood and owned by everyone across your organisation.

Getting the basics right - Essential 8

The Australian Signal Directorate's (ASD) Essential Eight framework is a great guide to consider when developing your cyber security model.[45] It is a prioritised list of mitigation strategies developed to assist organisations to protect their systems against a range of cyber threats and can be customised based on an organisation's risk profile as well as the threats they are most concerned about.

No single mitigation strategy is guaranteed to prevent cyber security attacks, but organisations can go a long way to protecting themselves by implementing these tips as a baseline to make it much harder for cyber criminals to compromise systems. Implementing the "Essential Eight" proactively can be money well spent when applied according to the risk and when considered against the cost and impact of a major cyber attack.[46]

> Implementing the "Essential Eight" proactively can be money well spent when applied according to the risk...

Protecting the confidentiality, integrity and availability of your systems and information

It's important to know where your information is stored, who has access to it, who can change it, and how it is shared, to protect it from potential data loss or cyber compromise events.

Managing the Confidentiality, Integrity and Availability (CIA) of your information and systems can be achieved by applying the basic principles of information security, including:

Back up information

Regularly backing up information so that if something does go wrong you can quickly recover and reduce disruption to your business by reverting to a recent backup.

Control access

There's a range of ways to help manage who can access your systems and when.

- Applying a Virtual Private Network (VPN) that allows remote users to securely access information on your network, such as email and file services. Securing remote working and collaboration tools.
- Supporting employees to understand the risks of leaving their own or their organisation's devices unattended, encouraging them to keep devices somewhere safe and to lock them when they're not being used, to prevent unauthorised access.
- Reinforcing that only approved software and applications are to be used.

Segmentation

Having protective measures in place to prevent breaches of network perimeters is important, but not enough. It is equally important to limit attackers' ability to capitalise on any initial breach by splitting a computer network into subnetworks (network segmentation) so that if attackers do manage to breach your network in one place, they cannot move into other areas of your network.

Logging and monitoring

Monitoring your networks can be achieved by implementing integrated security tools and processes such as the use of a Network-based Intrusion Detection System (NIDS) and other detection capabilities to help detect and prevent malicious activity. Large organisations may have a dedicated Security Operations Centre (SOC), whose function is to constantly scan and monitor the network for malicious or unusual activity and prevent or respond to any identified threats. Smaller organisations might consider using a managed security service to perform this logging and monitoring function for them.

Password managers

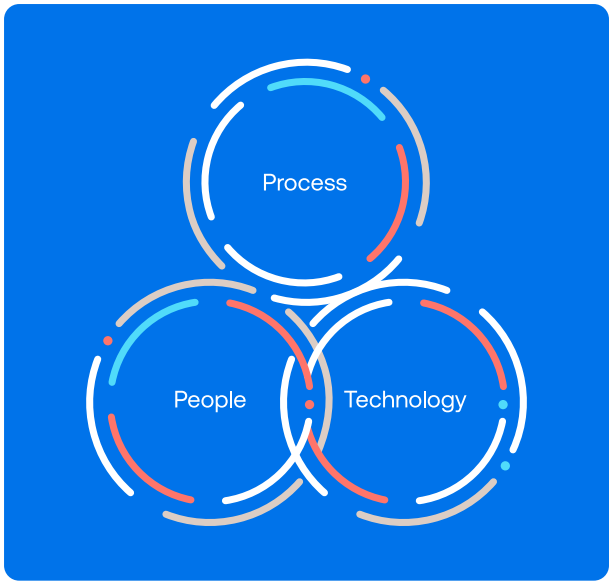
Password managers are not infallible, but they do add another layer of protection and support for managing and storing credentials. Importantly, they also support secure human behaviours - by offering an easier way to apply complex and unique passwords.

Making security an ongoing conversation

Have the conversation about cyber security organisation-wide, to help ensure that everyone understands the threats and how they may apply to their role. This conversation could include a discussion about prioritising the need for broader security controls such as keeping systems up to date and including a security perspective when considering new tools and systems.

Investing in people and processes

People are one of the strongest defences against cyber-attacks. Well informed, vigilant and resourced people can complement technical security controls to help identify, draw attention to, and prevent security threats.



A consistent and regular program of education and engagement can help transform cultural norms and promote a security first mindset across the organisation.

Effective education and influence programs extend well beyond employee on-boarding to help ensure that targeted security messages are delivered to the right audiences, at the right time, via the right communication channels.

Key elements of cyber security education

Accountability

Being clear that cyber security is a whole of business issue.

Employee awareness and education

Creating a strong culture that encourages positive behaviours around cyber security.

Speak out

Encouraging employees to act if they detect anything unusual in a call, email or text.

Collaborate

Partnering with key areas within your organisation to drive meaningful change, including human resources, communications, risk and customer facing business functions.

Network

Leveraging relationships with trusted third parties. When partners work together to uphold shared standards, the entire network becomes stronger and more secure.

Incident response

Knowing in advance who you will contact, what communication channels you'll use, who will help you respond, and what you'll say - and practising through drills and exercises.

Policies and procedures

Making it easy for employees to know, understand, and apply the organisation's security policies, standards, and procedures, including legal and regulatory responsibilities. This extends beyond publishing documents on an intranet. Help your organisation be secure by providing the context of how the security policy relates to specific work functions, and what each staff member can do to ensure they are compliant.

Securing your supply chain and third parties

Engaging partners from outside your organisation is an effective way to scale and bring in skills and resources. Just like introducing any new tool or people into your organisation, third parties (and your third parties' suppliers) have a vital role to play in protecting your information and business.

Establishing a list of all suppliers, such as software and hardware vendors, managed services providers, and where possible, their sub-contractors is a good place to start.

Implementing a trusted third-party cyber risk management program that is robust can take time, change scope and impact commercial contracts. However, adopting a risk- based approach to third parties that manage systems or sensitive information is one way to reduce cyber risk.

Implementing clear governance, processes and education can secure your relationships and help your third party suppliers integrate into your environment.

Governance

- Working with internal procurement teams to obtain commitment and understanding of the trusted third party program (for example, by completing a third party supplier assessment).
- Updating existing third party / supplier contracts to articulate the roles and responsibilities in storing, sharing, accessing, and purging information and data.

Processes

- Helping to ensure that your company's third-party onboarding process reinforces the roles and responsibilities when it comes to storing, sharing, and accessing your organisation's information.
- Establishing clear cyber incident reporting and response requirements in the case of a security or data breach.
- Undertaking a fourth party discovery program with your third party. What products and services do they outsource? Do they use third parties to store and protect information? What controls does the fourth party have in place to protect information and systems?
- Conducting periodic assessments to help ensure that third parties are meeting their contractual obligations and have appropriate security controls.
- Reviewing the third-party offboarding process so that your organisation's information stored or managed by the third party is appropriately purged and no longer accessible or discoverable.

Education

- Confirming third parties implement their own cyber security education program, so that employees know how to manage and protect information.
- Providing education to staff who engage with third parties, so that they understand and know how to manage third party security risks.

Simple, actionable tips and information

Build a human firewall

Employees can be an organisation's most important defence in blocking cyber threats, and as more people work remotely, having vigilant and well-prepared employees who can identify and act on cyber threats becomes increasingly important.

At a time when working from home has become the new norm, it's never been more important to work securely and maintain visibility over how corporate and customer information is used, stored and shared. So how can you protect your business, people, information, and family when working from home?

Make a P.A.C.T.

Pause before sharing information

Ask your employees to always think first before sharing sensitive information. And help them understand what is sensitive.

Activate multi factor authentication (MFA)

Turn on MFA for important tools such as remote access systems and resources (including cloud services).

Call out suspicious messages

Let employees know what to do if their device is lost or stolen, or they observe anything suspicious.

Turn on automatic updates

Ensure systems including phones, laptops, servers, virtual private networks and firewalls are updated with the most recent security patches.

Avoiding business email compromise

Given the sheer volume of emails, text messages, instant messages and social media messages we all send and receive, it's not surprising we tend to act on things straight away, and sometimes overlook inconsistencies in correspondence.

Preventative and protective measures are simple, cost effective and immediately beneficial. The Australia Cyber Security Centre (ACSC) is encouraging all Australian individuals and businesses to strengthen their email security by taking the following steps[47]:

Tips for avoiding business email compromise

1. Set secure pass phrases for each email account.
2. Set-up multi-factor authentication.
3. Exercise caution when opening attachments or links.
4. Think critically before actioning requests for money or sensitive information.
5. Businesses should establish clear processes for employees to verify and validate requests for payment and sensitive information, such as:
   - Seeking supplier confirmation by phone rather than email if you receive a change of banking details from a supplier.
   - Request two authorisations for payments to create an extra level of security, particularly for large transactions or those that are sensitive or urgent.
   - Review how you update supplier details making sure employees are aware of the new or updated policies.

Although organisations can't control what emails are sent by cyber criminals, they can introduce education programs to help staff recognise and report a range of suspicious emails - including Business Email Compromise. There are also many security tools available to detect a proportion of malicious emails, providing another control layer to your organisation's security capability.

Build a cyber incident response plan

The Australian Cyber Security Centre (ACSC) encourages organisations to have a cyber incident response plan to help ensure an effective response and prompt recovery in the event security controls don't prevent an incident occurring. This plan is ideally to be tested and regularly reviewed. To help you get started, they've provided readiness checklists and guidance.[45]

In conclusion

Cyber security is everyone's business

The pace, scale and sophistication of technology development has opened a world of new opportunities for people and organisations. We are more connected however, more remote than ever.

We can now collaborate easily, effectively and securely with colleagues and friends wherever we are in the world. The changing landscape presents a myriad of opportunities; however cyber criminals can take advantage of the increased opportunities as well. The tools they use, the opportunities they have and the potential rewards for a successful cyber-attack have never been more attractive.

This is why the role of cyber security teams across organisations continues to grow, not just as a defence function, but as expert advisors that can empower organisations to seize the opportunities of new technology whilst helping to ensure that it's information, customers, and people are protected. Security is what enables the business to operate effectively and scale rapidly and safely.

At ANZ, we often talk about cyber security as a team sport given no single control – be it software, process or people – can help shield companies from cyber-crime. Our security team works with the business to help embed a security first approach that secures our foundations and, helps to enable transformation and embrace innovation. Understanding the security environment, what that means for your organisation, how cyber criminals may try to exploit those opportunities and what you can do to protect yourself and your organisation all leads to a defence in depth approach that best prepares your organisation for the inevitability of a cyber-attack.

Forward moving organisations with cyber defences are likely to:

- Make it clear to their entire workforce that cyber security is a whole-of-business issue.
- Create and invest in a strong culture that encourages positive behaviours around cyber security.
- Empower employees to speak out and act if they see or hear anything unusual.
- Collaborate across key areas of the organisation including Finance, IT and Risk.
- Implement strong governance, processes and tools to protect systems and information.
- Leverage relationships with trusted third parties.
- Be prepared for attacks with a practiced response process.
- Embed security into culture, sourcing and third party arrangements.
- Use security to make the most of new opportunities to innovate and improve customer experience.

Getting support – you're not alone

There are a range of resources and government organisations, specifically designed to help you navigate your way through the world of cyber security.

A starting point of useful websites

- Australia Cyber Security Centre (ACSC) https://www.cyber.gov.au/
- ANZ Security Centre https://www.anz.com.au/security/
- eSafety commission https://www.esafety.gov.au/
- Australian Competition & Consumer Commission (ACCC) SCAMWATCH https://www.scamwatch.gov.au/
- ACSC Small and Medium Businesses Cyber Security Assessment Tool https://www.cyber.gov.au/acsc/small-and- mediumbusinesses/cyber-security-assessment-tool
- New Zealand National Cyber Security Centre https://www.ncsc.govt.nz/
- Hong Kong's Office of the Government Chief Information Officer (OGCIO) https://www.govcert.gov.hk/
- Cyber Security Agency of Singapore (CSA) https://www.csa.gov.sg/
- The US National Institute of Standards and Technology (NIST) https://www.nist.gov/
- Pacific Cyber Security Operational Network https://pacson.org/
- National Cyber Security Centre UK https://www.ncsc.gov.uk/

Key policy documents related to cyber security

- Australia's Cyber Security Strategy outlines the federal government's overall vision https://cybersecuritystrategy.homeaffairs.gov.au/
- Australian Government Information Security Manual (ISM) assists in the protection of information that is processed, stored or communicated by companies' systems. https://www.cyber.gov.au/acsc/view-all-content/ism
- Strategies to Mitigate Cyber Security Incidents complements the advice in the ISM and contains a complete list of strategies. https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents
- The Essential Eight Maturity Model complements the advice in the Strategies to Mitigate Cyber Security https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model
- The Australian Institute of Company Directors Cyber Security Governance Principles provide guidance to assist Australian directors oversee and engage with management on cyber security risk. https://www.aicd.com.au/risk-management/ framework/cyber-security/cyber-security-governance-principles.html

If your country is not listed, kindly consult your relevant local government's official website.

References

1. BetaNews. 2025. “AI-Powered Attacks, Zero-Days, and Supply Chain Breaches: The Top Cyber Threats of 2025.” https://betanews.com/2025/08/07/ai-powered-attacks-zero-days-and-supply-chain-breaches-the-top-cyber-threats-of-2025/

2. CyberProof. 2025. 2025 Global Threat Intelligence Report. https://go.cyberproof.com/hubfs/CyberProof_2025_Global_Threat_Intelligence_Report.pdf

3. ANZ. n.d. “ESG Reporting.” https://www.anz.com.au/about-us/esg/reporting/

4. Office of the Director of National Intelligence. 2025. Annual Threat Assessment of the U.S. Intelligence Community. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf

5. World Economic Forum. 2025. Global Cyber security Outlook 2025. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/.

6. The Hill. 2025. “AI-Powered Misinformation Poses Largest Short-Term Global Threat: World Economic Forum.” https://thehill.com/business/4400057-ai-powered-misinformation-poses-largest-short-term-global-threat-world-economic-forum/

7. Cloud Security Alliance. 2024. “Threat Report: BEC and VEC Attacks Continue to Surge, Outpacing Legacy Solutions.” https://cloudsecurityalliance.org/blog/2024/11/08/threat-report-bec-and-vec-attacks-continue-to-surge-outpacing-legacy-solutions

8. World Economic Forum. 2025. Global Risks Report 2025. https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf

9. Cyber security and Infrastructure Security Agency (CISA). 2025. FY2025–2026 International Strategic Plan. https://www.cisa.gov

10. Department for Science, Innovation and Technology. 2025. Telecommunications Security Code of Practice Consultation. https://www.gov.uk

11. Australian Government. 2025. Security of Critical Infrastructure Amendment (2025 Measures No. 1) Rules. https://www.legislation.gov.au

12. European Commission. 2025. Cyber Solidarity Act (Regulation 2025/38). https://digital-strategy.ec.europa.eu

13. Cyber Security Agency of Singapore. 2025. Singapore Cyber security Strategy 2025. https://www.csa.gov.sg

14. Ministry of Economy, Trade and Industry (METI). 2025. Strategy for Vitalization of the Cyber security Industry. https://www.meti.go.jp

15. World Economic Forum. 2025. “Global Risks Report 2025: Conflict, Environment, and Disinformation Top Threats.” https://www.weforum.org/press/2025/01/global-risks-report-2025-conflict-environment-and-disinformation-top-threats/

16. Cyber security and Infrastructure Security Agency (CISA). 2024. “CISA, FBI, NSA, and International Partners Release Joint Advisory: 2023 Top Routinely Exploited Vulnerabilities.” https://www.cisa.gov/news-events/alerts/2024/11/12/cisa-fbi-nsa-and-international-partners-release-joint-advisory-2023-top-routinely-exploited

17. European Commission. 2025. “General Data Protection Regulation (GDPR) Overview.” Accessed September 2, 2025. https://ec.europa.eu/info/law/law-topic/data-protection_en

18. Ministry of Electronics and Information Technology, Government of India. 2025. Digital Personal Data Protection Rules, 2025. Accessed September 2, 2025. https://www.meity.gov.in

19. State of California Department of Justice. 2025. California Consumer Privacy Act (CCPA) Updates 2025. Accessed September 2, 2025. https://oag.ca.gov/privacy/ccpa

20. Cyberspace Administration of China. 2025. Personal Information Protection Law Enforcement Actions. Accessed September 2, 2025. https://www.cac.gov.cn

21. Office of the Australian Information Commissioner. 2024. Privacy Act 1988 Amendments. Accessed September 2, 2025. https://www.oaic.gov.au/privacy/privacy-act

22. Office of the Privacy Commissioner, New Zealand. 2025. Privacy Act 2020 Overview and Updates. Accessed September 2, 2025. https://www.privacy.org.nz

23. World Economic Forum. 2025. Global Data Governance: Cross-Border Data Flows and Trust. Accessed September 2, 2025. https://www.weforum.org

24. ScalableOS. 2025. “Cyber security Threats MSPs Face.” https://scalableos.com/blogs/cybersecurity-threats-msps-face/

25. CyberPress. 2025. “New IoT Botnet Launching Large-Scale DDoS Attacks.” https://cyberpress.org/new-iot-botnet-launching-large-scale-ddos-attacks/

26. Center for Internet Security. 2025. “Critical Infrastructure Caught in Botnet.” https://www.cisecurity.org/insights/blog/critical-infrastructure-caught-botnet

27. U.S. House Committee on Oversight and Accountability. 2025. “Timmons Announces Hearing to Examine State-Sponsored Cyber Attacks Targeting Critical U.S. Infrastructure.” https://oversight.house.gov/release/timmons-announces-hearing-to-examine-state-sponsored-cyber-attacks-targeting-critical-u-s-infrastructure/

28. Inc. 2025. “AI-Powered Misinformation Is World’s Biggest Short-Term Threat, Davos Report Says.” https://www.inc.com/associated-press/ai-powered-misinformation-is-worlds-biggest-short-term-threat-davos-report-says.html

29. European Commission. 2025. “Contents Code for Generative AI.” https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai

30. Bank of America. 2025. Securing Hybrid and Remote Workforces. https://business.bofa.com/content/dam/flagship/global-transaction-services/cyber-security-journal/cyber-security-for-remote-workforce/securing-hybrid-and-remote-workforces.pdf

31. McKinsey & Company. n.d. “A Dual Cyber security Mindset for the Next Normal.” https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-dual-cybersecurity-mindset-for-the-next-normal

32. MIT Sloan Management Review. n.d. “Cyber security for a Remote Workforce.” https://sloanreview.mit.edu/article/cybersecurity-for-a-remote-workforce

33. Reciprocity. n.d. “Cyber security Risks in Hybrid Working Environments.” https://reciprocity.com/blog/cybersecurity-risks-in-hybrid-working-environments

34. TechRadar. n.d. “Are Remote Workers at Greater Risk of Cyber security Threats?” https://www.techradar.com/pro/are-remote-workers-at-greater-risk-of-cybersecurity-threats

35. Australian Cyber Security Centre. n.d. “Social Engineering.” https://www.cyber.gov.au/acsc/view-all-content/glossary/social-engineering

36. McKinsey & Company. n.d. “Organizational Cyber Maturity: A Survey of Industries.” https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/organizational-cyber-maturity-a-survey-of-industries

37. Security Boulevard. 2023. “Cyber security Maturity Assessment and Measurement Guide.” https://securityboulevard.com/2023/12/cybersecurity-maturity-assessment-and-measurement-guide/

38. CERT NZ. n.d. “10 Critical Controls.” https://www.cert.govt.nz/information-and-advice/critical-controls/10-critical-controls/

39. Australian Cyber Security Centre. n.d. “Assessing Security Vulnerabilities and Applying Patches.” https://www.cyber.gov.au/acsc/view-all-content/publications/assessing-security-vulnerabilities-and-applying-patches

40. UK National Cyber Security Centre. n.d. “Vulnerability Management.” https://www.ncsc.gov.uk/guidance/vulnerability-management

41. World Economic Forum. 2025. Global Cyber security Outlook 2025. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.

42. Verizon. 2025. 2025 Data Breach Investigations Report (DBIR). https://www.verizon.com/business/resources/Tc4e/reports/2025-dbir-data-breach-investigations-report.pdf

43. IBM. n.d. “Ransomware-as-a-Service.” https://www.ibm.com/think/topics/ransomware-as-a-service

44. TechRadar. 2025. “AI Impersonation Scams Are Skyrocketing in 2025, Security Experts Warn—Here’s How to Stay Safe.” https://www.techradar.com/computing/cyber-security/ai-impersonation-scams-are-sky-rocketing-in-2025-security-experts-warn-heres-how-to-stay-safe

45. Australian Cyber Security Centre. n.d. “Essential Eight.” https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/essential-eight

46. Australian Cyber Security Centre. n.d. “Strategies to Mitigate Cyber Security Incidents: Mitigation Details.” https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/strategies-mitigate-cyber-security-incidents/strategies-mitigate-cyber-security-incidents-mitigation-details

47. Australian Cyber Security Centre. n.d. “Preventing Business Email Compromise.” https://www.cyber.gov.au/protect-yourself/securing-your-email/email-security/preventing-business-email-compromise

This brochure is current as at October 2025 and it's details are subject to change.
Australia and New Zealand Banking Group Limited (ANZ) ABN 11 005 357 522.

anz.com.au/security/business/