



**CYBER SECURITY PRIMER :
YOUR ORGANISATION'S GUIDE
TO IMPROVED CYBER RESILIENCE**

2023

EXECUTIVE SUMMARY

This guide seeks to simplify cyber security, by providing actionable tips and information for business leaders and executives. These tips can help balance the need to operate effectively and take advantage of innovative technology while managing cyber threats and risks.

To understand what needs to be done, we must build knowledge of the threats we face. This guide takes a look at the current cyber threat landscape, as well as the evolving tactics used by malicious actors to target organisations. Furthermore, we take a look at the principle of Defence in Depth, and why this layered, strategic approach is being utilised by many organisations as a way to manage their cyber risk exposure.

Lastly, there are a number of simple, actionable tips that organisations and employees can use to help improve their cyber security position. For your convenience a snapshot of these tips can be found below. For further details, please refer to page 21. At ANZ, we believe that cyber security is everyone's business, so we hope this guide provides some helpful insights and tips to help support you to protect your own information and that of your organisation.

SIMPLE ACTIONABLE TIPS FOR BUSINESSES

ACTIVATE MULTI-FACTOR AUTHENTICATION (MFA)

Multi-factor authentication should be implemented across all systems and applications where it is available.



RUN REGULAR BACK-UPS

Regular back-ups are necessary to recover from a cyber-attack that destroys data or prevents technology from functioning e.g. ransomware.



PATCH & UPDATE SYSTEMS AND SOFTWARE

Keep operating systems and software up-to-date with the latest versions to mitigate security vulnerabilities.



RESTRICT PRIVILEGED ACCESS

Privileged accounts should only be used for administrative purposes, and should be restricted and reviewed regularly.



SIMPLE ACTIONABLE TIPS FOR YOUR EMPLOYEES



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.



CYBER SECURITY

IS EVERYONE'S BUSINESS

Cyber security is a shared responsibility - businesses do not exist in isolation and we all rely on a complex web of suppliers, partners and customers which need to be considered as part of a holistic security risk management approach.

The world of cyber security has now remarkably evolved and the opportunities it presents continue to excite and fascinate me. As a data scientist with a background in artificial intelligence (AI), I'm always curious how new innovations can help us to be more strategic, collaborative and solve real-world problems.

At ANZ, we recognise that our digital world is constantly evolving, with both positive innovation and new threats. Indeed, cyberattacks continue to increase in sophistication, persistence, and impact. As a result, cyber security has shifted from solely a technical concern; it is now a pivotal element of business strategy and a core Board accountability. Not only must businesses be ready to defend against advances in threats, we must use capability like AI to our advantage – building it into our defences.

From ransomware attacks that paralyse businesses to supply chain breaches that disrupt the global economy. Threat actors, cybercriminals, and hackers are all vying for opportunities to exploit people and system vulnerabilities to gain access to sensitive data and/or reap financial benefits. Recent incidents have proven that no organisation, regardless of size, is immune to these threats.

But there are ways for us to mitigate common threats and it's achievable, particularly if we work together. This guide intends to encourage you as business leaders to adopt a strategic approach to cyber security that is anchored in risk management. Businesses will continue to benefit from the inclusion of cyber security basics like regular updates to software (patching), implementing multi-factor authentication, and restricting access to administrative or privileged accounts.

Employees are often an entry point for cyberattacks, so it is only fitting that employee cyber security education is also an on-going process. Fostering a culture of security where everyone is responsible for protecting customer information and/or organisation's assets is key.

Cyber security is a shared responsibility - businesses do not exist in isolation and we all rely on a complex web of suppliers, partners and customers which need to be considered as part of a holistic security risk management approach. One of the most profound aspects of supply chains in the digital age is their extensive reliance on technology. Interconnectedness allows for unprecedented efficiency and connectivity; on the other hand, it creates opportunities for cyber threats. The security of your supply chain and delivery partners directly impacts your organisation's resilience to cyber threats. Hence, the modern business landscape demands an approach to cyber security that extends beyond the boundaries of the organisation itself. Making cyber security a part of third-party assessments goes a long way in creating a more secure ecosystem.

This guide seeks to support business leaders to adapt a strategic approach to cyber security that is anchored in risk management. We hope to help equip you to lead your organisation into a future where cyber security is not a barrier but a competitive advantage.

DR. MARIA MILOSAVLJEVIC

Chief Information Security Officer
ANZ

Note: All information contained in this publication is based on information available at the time of publication. While the publication has been prepared in good faith, no representation, warranty, assurance or undertaking is or will be made, and no responsibility or liability is or will be accepted by ANZ in relation to the accuracy or completeness of this publication or the use of information contained in this publication.

CONTENTS

THE CYBER LANDSCAPE 4

- The impact of rapidly advancing technology 4
- Cyber attacks are becoming more frequent 4
- Increasingly adverse threat environment 5
- Complexity of systems and technology 6
- Phenomenal growth of data 7
- Increased connectivity with third parties 7
- Rapid adoption of transformative technology 8
- Remote Workforce and Hybrid Workplaces 8

THE ATTACK SURFACE 9

- Cyber criminal targets 9
- Internal factors 9
- System vulnerabilities 11
- External factors 12

CYBER ATTACK TACTICS 13

- Ransomware 13
- Malicious software 14
- DDOS 14
- Business email compromise 14
- Impersonation scams 16
- Impacts of cyber attacks 16

DEFENCE IN DEPTH 17

- The sum of all parts 17
- Getting the basic right 18
- Protecting the confidentiality, integrity and availability of your systems and information 19
- Making security an ongoing conversation 19
- Investing in people and processes 20
- Securing your supply chain and third parties 21

SIMPLE, ACTIONABLE TIPS AND INFORMATION 22

- Build a human firewall 22
- Make a P.A.C.T. 22
- Avoiding business email compromise 23
- Build a cyber incident response plan 23

IN CONCLUSION 24

- Cyber security is everyone's business 24

GETTING SUPPORT-YOU'RE NOT ALONE 25

- Cyber insurance 25
- A starting point of useful websites 25
- Key policy documents related to cyber security 25

THE CYBER LANDSCAPE

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.

CYBER ATTACKS ARE BECOMING MORE FREQUENT

These numbers demonstrate both the size of the challenge and the management factors which contribute.

95%

CYBER ATTACKS ARE DRIVEN BY FINANCIAL GAIN²

\$10.5T
USD

COST OF CYBER CRIME BY 2025³

74%

PERCENTAGE OF BREACHES THAT INCLUDES THE HUMAN ELEMENT THROUGH ERROR, PRIVILEGE MISUSE, USE OF STOLEN CREDENTIALS OR SOCIAL ENGINEERING²

\$63k
AUD

AVERAGE REPORTED COST OF A CYBER ATTACK FOR AUSTRALIAN SMB⁴

\$2.11M
AUD

AVERAGE COST OF RECOVERY FROM RANSOMWARE⁵

266
DAYS

AVERAGE TIME TO IDENTIFY AND CONTAIN A DATA BREACH GLOBALLY⁶

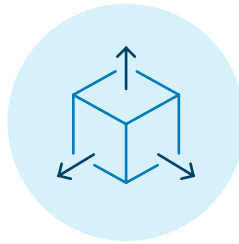
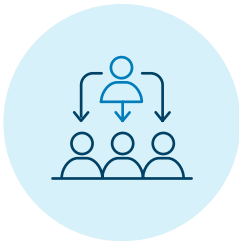
¹ <https://www.verizon.com/business/resources/infographics/2023-dbir-infographic.pdf>

² <https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/>

³ <https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022> <https://www.sophos.com/en-us/content/state-of-ransomware>

⁴ <https://www.ibm.com/reports/data-breach>

KEY DRIVERS BEHIND THE SURGE IN CYBER ATTACKS.

INCREASINGLY ADVERSE
THREAT ENVIRONMENTCOMPLEXITY OF SYSTEMS
AND TECHNOLOGYPHENOMENAL
GROWTH OF DATAINCREASED CONNECTIVITY
WITH THIRD PARTIESRAPID ADOPTION OF
TRANSFORMATIVE TECHNOLOGYREMOTE WORKFORCE AND
HYBRID WORKPLACES

INCREASINGLY ADVERSE THREAT ENVIRONMENT

Geopolitical dynamics are creating significant headwinds for global cooperation⁷. This gave way to better collaboration between the government and business sectors for cybersecurity best practices and industry regulations.⁸

Government agencies like the Australian Cyber Security Centre (ACSC)⁹, UK's National Cyber Security Centre (NCSC)¹⁰, SingCERT¹¹, CERT NZ¹², US CERT - CISA¹³ release regular alerts to remind organisations of the current heightened threat environment, and to be prepared and equipped to respond and recover from an attack that may impact business operations.

We are seeing governments around the world making amendments to legislation to widen the cyber security obligations of organisations that provide essential services. In Australia, recent amendments to the Security of Critical Infrastructure Act (SOCI)¹⁴ demonstrates the governments' recognition of the need for an enhanced regulatory framework to protect Australia's critical services.

In the UK, the Electronic Communications (Security Measures) Regulations come into force on 1 October 2022. The regulations are intended to address risks to the security of the UK's public telecoms networks and services¹⁵.

Unfortunately, cyber crime continues to pay well for criminals. Traditional methods used by criminals are evolving. The take-off of Ransomware as a Service (RaaS), means ransomware is more accessible than ever to those with ill intent. We're seeing the sophistication of Business Email Compromise (BEC) scams continue to grow and according to the ACSC, BEC scams have cost Australians over \$98 million between June 2021 - July 2022¹⁶. The total cost is even greater when the losses from ransomware, distributed denial of service (DDoS), and other attacks are included.

⁷ <https://www.weforum.org/reports/global-risks-report-2023/digest/>

⁸ <https://www.cyber.gov.au/acsc/view-all-content/advisories/russian-state-sponsored-and-criminal-cyber-threats-critical-infrastructure>

⁹ <https://www.cyber.gov.au/>

¹⁰ <https://www.ncsc.gov.uk/>

¹¹ <https://www.csa.gov.sg/singcert>

¹² <https://www.cert.govt.nz/>

¹³ <https://www.cisa.gov/uscert/>

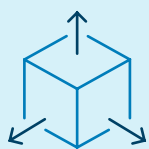
¹⁴ <https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/slacip-bill-2022>

¹⁵ <https://www.gov.uk/government/news/tough-new-rules-confirmed-to-protect-uk-telecoms-networks-against-cyber-attacks>

¹⁶ <https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022>

Organisations have been urged by the Australian Cyber Security Centre (ACSC) to increase their cyber resilience in light of the current heightened cyber threat environment.

Recent media coverage of events around the world serves as a reminder for commercial and institutional businesses to enhance their cyber security position by remaining vigilant, staying on top of the latest threats and trends, and practising good cyber security hygiene.



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. According to US government tracking, the number of security vulnerabilities distributed is increasing each year¹⁷.

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.

¹⁷. <https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time>



PHENOMENAL GROWTH OF DATA

Organisations can be targeted by cyber criminals not just for their financial assets, but also for the large volumes of personal and sensitive information¹⁸ they collect, generate, process, and store.

This information is regularly sold on the “dark web”¹⁹ as an enabler for identity theft, social engineering attacks such as phishing, and other criminal activity. So, while big data analytics present an enormous business opportunity to develop customer-centric products and services, the benefits of collecting large volumes of data comes with additional risk.

Increasingly, there is growing pressure from government entities and regulatory authorities for organisations to comply with regulations, such as Australian Prudential Regulation Authority’s (APRA) Information Security standard (CPS 234), Australia’s Notifiable Data Breach (NDB) scheme²⁰ and Europe’s General Data Protection Regulation (GDPR)²¹ and the upcoming changes to both the Australian Privacy Act²² and CPS 230 Operational Risk Management Standard²³.

This is enforced through significant financial penalties for non-compliance. However, the overall impact of a large-scale data breach is much higher, considering the customer devastation and associated remediation efforts, legal costs, reputational damage, impact on share price and credit rating, job loss, and even criminal charges.



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 actors²⁴. 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.

¹⁸ <https://www.cyber.gov.au/acsc/view-all-content/advice/personal-information-and-privacy>

¹⁹ <https://www.cyber.gov.au/acsc/view-all-content/glossary/dark-web>

²⁰ <https://www.oaic.gov.au/privacy/notifiable-data-breaches>

²¹ <https://gdpr-info.eu/>

²² <https://www.aq.gov.au/integrity/consultations/review-privacy-act-1988>

²³ <https://www.apra.gov.au/sites/default/files/2022-07/Draft%20Prudential%20Standard%20CPS%20230%20Operational%20Risk%20Management.pdf>

²⁴ <https://www.cyber.gov.au/acsc/view-all-content/news/joint-advisory-released-managed-service-providers-and-customers-mitigate-cybersecurity-risks>



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) attacks²⁵ through botnets²⁶.

With their focus on innovation and functionality, IoT developers can overlook security features that may increase manufacturing and maintenance expenses²⁷, potentially leaving businesses as well as their consumers exposed.

DIGITAL TRANSFORMATION OF SERVICES

Increasingly, consumer services like virtual health are changing the way we live and work. Whilst the pandemic brought about mixed changes, this is a welcome shift. With 50% of consumers voting likely or very likely to use virtual healthcare in a recent industry survey, meaning that it is likely to stay and therefore security considerations are essential²⁸.

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.



REMOTE WORKFORCE AND HYBRID WORKPLACES

The COVID-19 pandemic forced organisations to rapidly change to new tools which supported their remote workforce, and these tools also kept many businesses fully operational during the pandemic.

This has provided a lot of benefits for both employees and businesses, including increased flexibility, cost / time saving, and improved work / life balance. It is important for organisations to support and enable the workforce with secure technology and education, equipping them with the knowledge, capability and skills to operate securely from wherever they are working.

²⁵ <https://www.cyber.gov.au/acsc/view-all-content/threats/denial-service>

²⁶ <https://www.cyber.gov.au/acsc/view-all-content/glossary/botnet>

²⁷ <https://www.cyber.gov.au/acsc/view-all-content/advice/personal-information-and-privacy>

²⁸ <https://www.pwc.com.au/health/virtual-health/consumers-clinicians-move-towards-virtual-healthcare.html>

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 objective²⁹.

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.

²⁹ Social Engineering Definition, Australia Cyber Security Centre <https://www.cyber.gov.au/acsc/view-all-content/glossary/social-engineering>

COMMON SECURITY ATTACKS CAN INVOLVE SOME TYPE OF 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

Source: Verizon Data Breach Incident Report 2022



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 Australian Cyber Security Centre (ACSC) has developed a free tool³⁰ for organisations to use to help assess and strengthen their cyber maturity.

³⁰ <https://www.cyber.gov.au/acsc/small-and-medium-businesses/cyber-security-assessment-tool>



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 essential³¹.

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 date³².

³¹. <https://www.cyber.gov.au/acsc/view-all-content/publications/assessing-security-vulnerabilities-and-applying-patches>

³². <https://www.ncsc.gov.uk/guidance/vulnerability-management>

EXTERNAL FACTORS



THIRD PARTIES AND SUPPLY CHAIN

As interconnectivity grows, malicious actors are increasingly looking to compromise multiple victims across a range of sectors via a single entry point. The ACSC expects this trend to continue. For example, Managed Service Providers (MSPs) were targeted over 2021–22 as they are used by government, commercial and not-for-profit businesses of all sizes, making them an attractive target for malicious actors³³. Smaller third parties are increasingly being compromised as a way of gaining access to larger corporations.

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.

Third parties and supply chain partners are a valuable part of a business, and when approached with the same security-first mindset as a secure organisation they can allow an organisation to perform to its potential.



³³ <https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022>

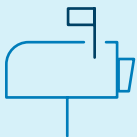
CYBER ATTACK TACTICS

Data breach is typically understood as a scenario where hackers (unauthorised to access or use a system) break into a system and steal sensitive information, but there is a lot more to a cyber attack.

A cyber attack is defined as an attacker gaining access to systems and compromising any element of the Confidentiality, Integrity or Availability (or CIA) of systems and data. So, in addition to stolen data (confidentiality), successful attacks can shut down operations or lock organisations from their data or systems (availability) or call into question the accuracy of data (integrity) by manipulating records. For example, an compromised social media account that a hacker used to post unauthorised posts is a failure of integrity.

For that reason, it's important to implement an approach that helps ensure data and system confidentiality, integrity, and availability (CIA). In other words an approach that helps ensure that data and applications are protected, accurate and available to those who need them.

SOME OF THE MORE COMMON APPROACHES TO GAIN ACCESS TO ORGANISATIONAL DATA AND SYSTEMS INCLUDE:



RANSOMWARE

Ransomware is a specific type of malicious software hackers use to deny access or availability to systems or data.

After gaining access to a network, the hacker encrypts data and denies access until the ransom is paid and may also threaten to publish it online as an extra "incentive" to pay the ransom. Once the demands are met, the hacker may provide a decryption key allowing the organisation to recover their data.

It's worth noting, when dealing with criminals, paying the fee does not guarantee a solution or removal of the ransomware. In some industry examples, the attacker lays dormant, following payment, ready to attack in the future.

Cybercriminals might also demand a ransom to prevent data and intellectual property from being leaked or sold online³⁴.

Supporting criminals by giving them money through a ransom payment may be illegal as well as ethically questionable as it promotes further crime.

Ransomware has grown in profile and impact over the last year, with the ACSC reporting a 75% increase from 2019-2020³⁵. This may be credited to a business model known as Ransomware as a Service (RaaS), which has taken off in recent years and involves the selling or renting of ransomware, making it easier for threat actors with little knowledge to deploy their own attacks. Cyber criminals often install it via phishing emails, or illicitly obtained user logins and credentials through spear phishing, or by directly exploiting known system vulnerabilities³⁶.

³⁴ <https://www.cyber.gov.au/ransomware>

³⁵ <https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022>

³⁶ <https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2020-june-2021>



MALICIOUS SOFTWARE

Malware (or malicious software) is a software used to cause damage to computer systems or organisational networks. Malware is the way cyber criminals typically gain access to devices. Malware can be installed via direct targeted attacks (e.g. targeted email/phishing/exploiting vulnerabilities in software) or through randomised broad attacks (e.g. infected websites).

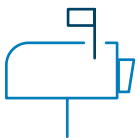


DDOS

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic.

Like ransomware attacks, DDoS is often used for extortion. For example an organisation is threatened with an attack against its website unless it makes a payment. Using services such as a Content Delivery Network (CDN) or a DDoS mitigation provider is an important control against the threat of DDoS.

These sit between the provider serving your content and the users /customers of your online service. Any traffic directed at your online service goes through the CDN or DDoS mitigation provider first, allowing any attack traffic to be dealt with before it hits your infrastructure. A good start is engaging your existing internet service providers for DDoS protection options³⁷.



BUSINESS EMAIL COMPROMISE (BEC)

Malicious emails (phishing) continue to be a common entry point of attacks on organisations. These emails can seek to gather information about an individual (e.g. credentials) or organisation, attempt to trick the recipient into an action, or deliver ransomware.

A specific type of phishing, business email compromise (BEC), is rapidly increasing in frequency, complexity and impact on company bottom lines. So much so that in 2021 the FBI indicated losses from BEC attacks between 2016 -2021 amounted to \$43 billion³⁸, accounting for almost half of all losses due to cyber crime. These emails typically purport to be from a significant stakeholder seeking urgent action, like funds transfer, or change of account details, and come in a variety of forms:

EXECUTIVE FRAUD

Scammer masquerades as an executive and sends an email to employees directing them to transfer funds to an account.

LEGAL IMPERSONATION

Scammer masquerades as a lawyer or legal firm representative and requests payment for an urgent and sensitive matter.

INVOICE FRAUD

Scammer masquerades as a trusted supplier and sends fake invoices.

DATA THEFT

Scammer masquerades as a trusted person to request sensitive information.

PAYROLL FRAUD

Scammer masquerades as an employee to update payroll information and funnel wages into a new account.

³⁷ <https://www.cyber.gov.au/acsc/view-all-content/threats/denial-service>

³⁸ FBI Internet Crime Complaint Centre Alert (I-050422-PSA)

EXPLOITING TRUST THROUGH 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.





IMPERSONATION SCAMS

Impersonation scam involves scammers impersonating a loved one or legitimate organisations instructing to make a payment, visit a website, or obtain personal or sensitive information.

Scam messages may even appear in the same thread of prior messages from the actual person or organisation. Government agencies, banks, insurance or telecommunication companies are commonly imitated organisations.

There are numerous impersonation scams circulating, which may be convincing as the impersonator preys on emotions such as trust, fear, panic, or curiosity.

IMPACTS OF CYBER ATTACKS



Reputational damage



Emotional distress



Financial loss



Business disruption



Loss of intellectual property



Customer devastation



Regulatory fines



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



Identity theft



Inability to access critical services / supplies (where Critical Infrastructure has been impacted)

DEFENCE IN DEPTH

A STRONG SECURITY POSITION - THE SUM OF ALL PARTS

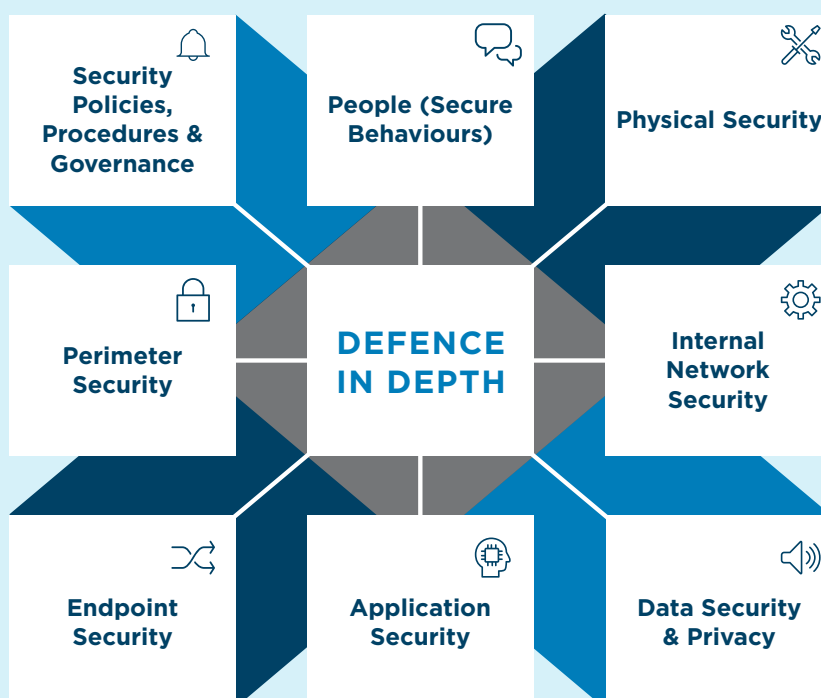
Cyber security isn't about a single function or component working in isolation, but a complex interconnection of equally important parts working together.

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

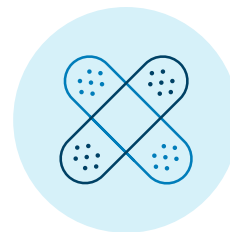
The Australian Signal Directorate's (ASD) Essential Eight framework is a great guide to consider when developing your cyber security model. It is a prioritised list of mitigation strategies developed to assist organisations to protect their systems against a range of cyber threats and can be customised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



APPLICATION CONTROL



CONFIGURE MICROSOFT OFFICE MACROS



PATCH APPLICATIONS



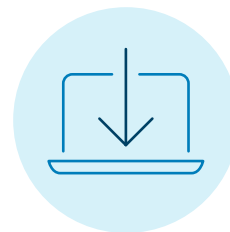
USER APPLICATION HARDENING



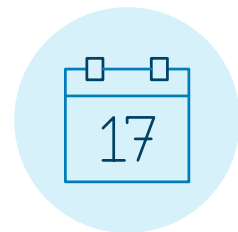
RESTRICT ADMINISTRATIVE PRIVILEGES



MULTI-FACTOR AUTHENTICATION



PATCH OPERATING SYSTEMS



DAILY BACK UPS

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 attack³⁹.

³⁹ <https://www.cyber.gov.au/acsc/view-all-content/products/essential-eight/strategies-mitigate-cyber-security/incidents-mitigation-details>



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 (if your third party is impacted by an attack it could have a direct impact on you and customers).



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 practicing 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 subcontractors 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. ACSC is encouraging all Australian individuals and businesses to strengthen their email security by taking the following steps:

- 1**  Set secure passphrases 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 for reference.

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. Whilst this was largely accelerated by the COVID-19 pandemic, we now know that to a large extent, the changes that have been made to business operations are here to stay.

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.

CYBER INSURANCE

Cyber insurance continues to grow in popularity as companies seek to mitigate the cost of potential cyber attacks, but it must be accompanied by investment in cyber security protection. As noted by the Australian Cyber Security Centre, any insurance pay out might not be able to repair damage to stolen intellectual property and the associated loss of long-term competitive advantages, damage to reputation, and lost customer loyalty.

As with any insurance, consideration should be given to the type, amount and suitability of cover for each business - including a review of opportunities for working with providers to ensure attack preparedness.

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-medium-businesses/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



ANZ works closely with industry and government partners to ensure robust controls are in place to protect our customers and systems. To find out more about the precautions we take to protect your company's data and money,

Nothing in this publication constitutes a recommendation, solicitation or offer by ANZ to you to acquire a product/service, or an offer by ANZ to provide you with other products or services. All information contained in this publication is based on information available at the time of publication. While the publication has been prepared in good faith, no representation, warranty, assurance or undertaking is or will be made, and no responsibility or liability is or will be accepted by ANZ in relation to the accuracy or completeness of this publication or the use of information contained in this publication. ANZ does not provide any financial,

investment, legal or taxation advice in connection with any product/service. This publication may not be reproduced, distributed or published by any recipient for any purpose. ANZ does not warrant the fairness, accuracy, fitness for any particular purpose, adequacy or completeness of any information contained, or referred to, in this publication. To the maximum extent permitted by law ANZ nor its directors, employees, agents or advisers will be liable in any way whatsoever for any loss, damage, claim, liability, cost or expense arising directly or indirectly (and whether in tort (including negligence), contract, equity or otherwise) from the use of, or reliance on, any information contained in and/or omitted from the material in this publication. All information contained in this publication is subject to change without notice. Notice of confidentiality

The information disclosed in this document is provided to you strictly on a commercial-in-confidence basis. Except where required at law or with ANZ's written consent, you may not disclose the information contained in this document to any person other than for the purpose of assisting you in assessing the possibility of purchasing ANZ's financial products and only if you have made such person aware of your obligations under this document before you disclose information to them.

© Copyright Australia and New Zealand Banking Group Limited (ANZ) ANZ Centre, 833 Collins Street, Docklands, VIC, 3008, ABN 11 005 357 522. ANZ's colour blue is a trademark of ANZ. This publication is distributed in Australia by Australia and New Zealand Banking Group Limited ABN 11 005 357 522 ("ANZBGL"), in New Zealand by ANZ Bank New Zealand Ltd; and in other countries by the relevant subsidiary or branch of ANZBGL (together ANZBGL, ANZ Bank New Zealand Ltd and all other relevant subsidiaries or branches of ANZBGL referred to as "ANZ").

