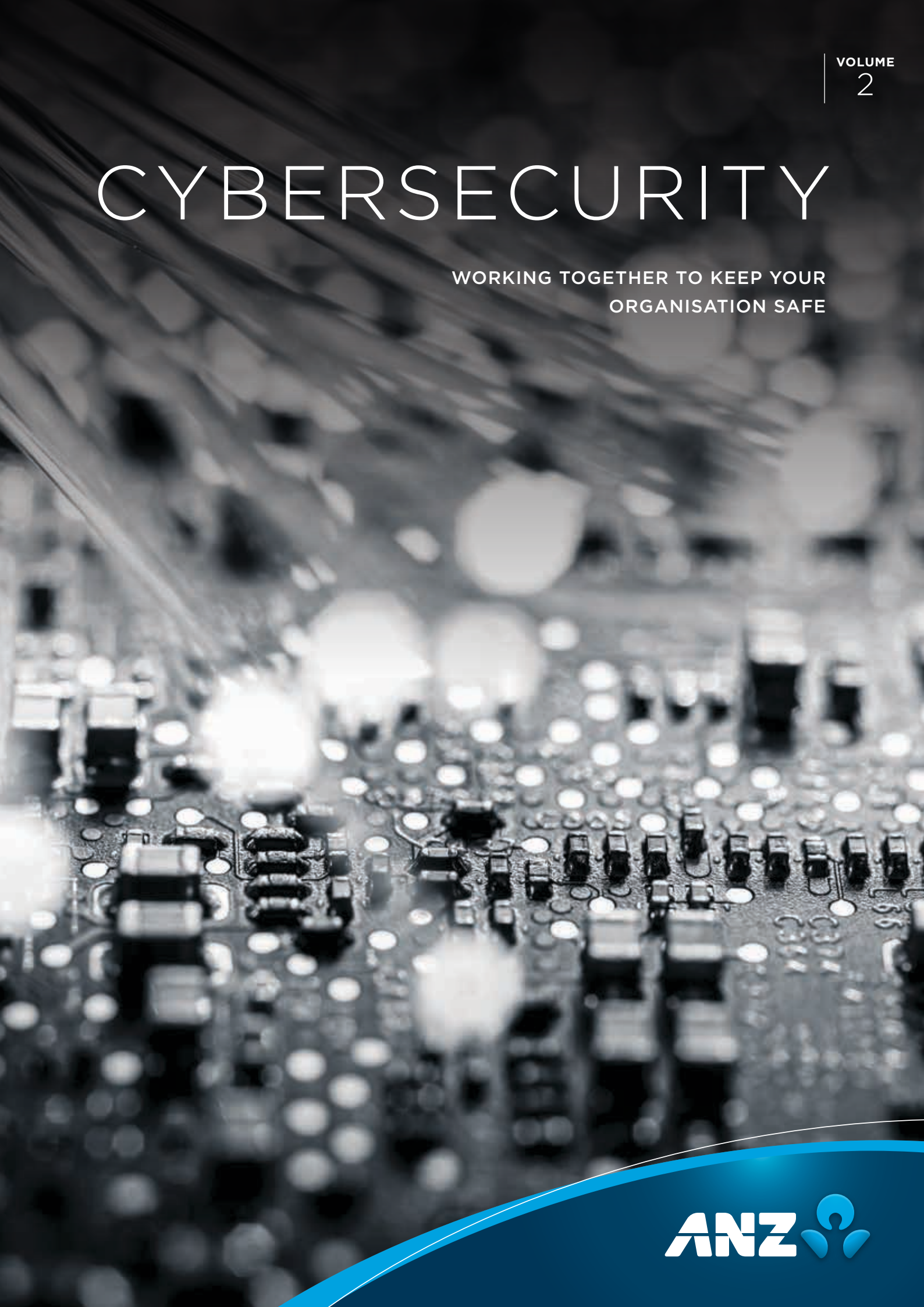
VOLUME
2

CYBERSECURITY

WORKING TOGETHER TO KEEP YOUR ORGANISATION SAFE



ANZ

A GUIDE TO PROTECTING YOUR ORGANISATION FROM CYBERCRIME

Cybersecurity incidents occur through a range of approaches and elements each designed to impact confidentiality, integrity, availability of information and systems and/or gain access to funds illegally.

Knowing how criminals try to compromise a system gives you greater clarity as to what their motivators are. Put simply, criminals attempt to compromise an organisation's information and systems to:

1. Cause business disruption (e.g. bringing down websites or databases via an attack critical to running a business)
2. Obtain sensitive/valuable information (e.g. steal IP or information on critical business deals that may give a competitor a market advantage)
3. Obtain funds (e.g. defraud them of funds)

Malware, for example, is just one method of attack which can be used to:

1. Access information (i.e. confidentiality)
2. Change information (i.e. integrity)
3. Limit access to systems or services (i.e. availability)
4. Simply gain access to funds (fraud)

Although these elements are not new, the way in which cybercriminals can now do this has changed. No longer are geographic boundaries or skill sets a barrier to entry to commit crime online.

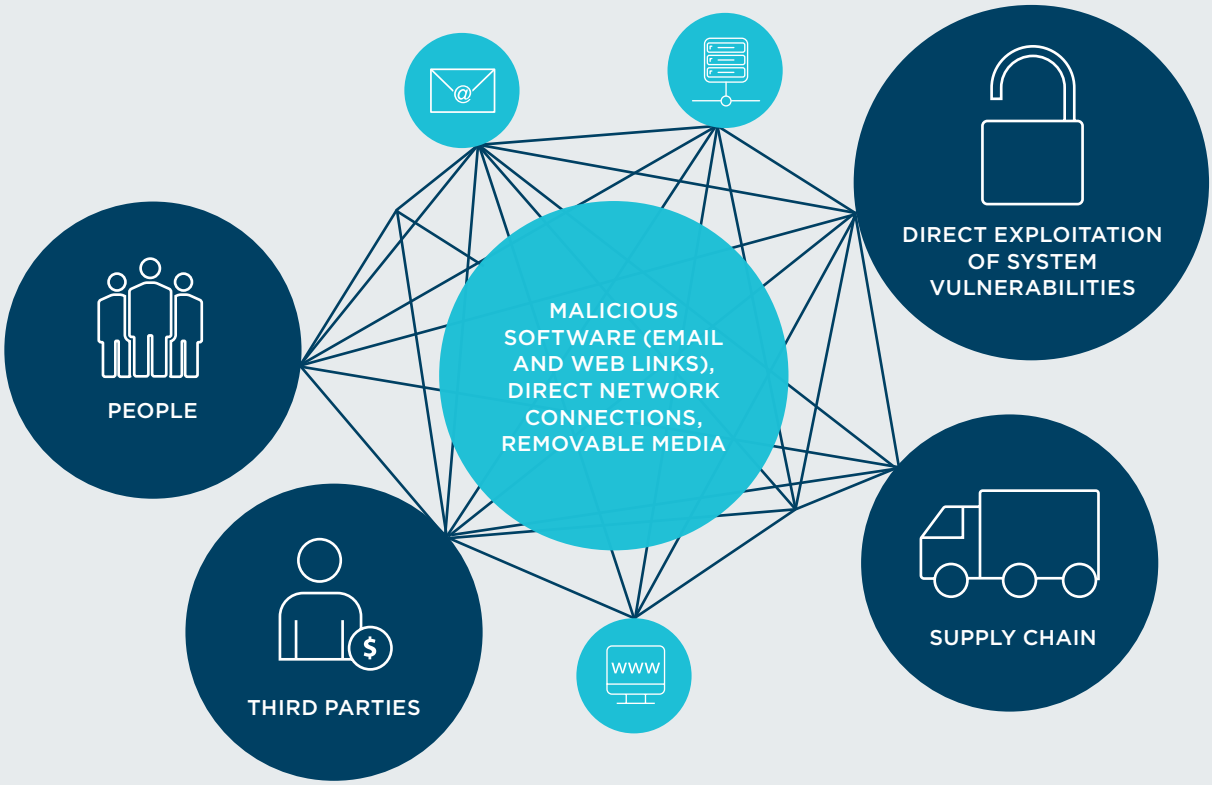
With business and consumer interactions moving to digital formats, there is a world of opportunities before us. Unfortunately this also brings increased risks and vulnerabilities for organisations regardless of their size, industry or location in the world. Digital development is making it very easy for others to intercept many aspects of people's professional and personal lives. It is no surprise that banks and corporates are ready targets for cybercrime, and we must continue to work together to prevent and mitigate the impacts of cybercrime.

At ANZ, we are committed to preserving the trust that our clients have in the quality and security of our banking services.

This guide 'shines a light' on some practical recommendations for keeping your organisation safe and secure, and together with the robust security practices we implement to help protect our clients, aims to minimise the chance of your organisation falling victim to cybercrime.

THE CHANGING CYBER THREAT LANDSCAPE

COMMON ATTACK VECTORS



AT A GLANCE

- Cybercriminals exploit any weakness in an organisation's people, process or technology infrastructure
- Using humans to infiltrate organisations is a common factor in most current cybercrime attacks
- Effective processes together with a risk management approach are crucial
- Organisations benefit from a multi-layered risk management strategy – 'defence in depth'
- The agility to know, control and adapt to new cyber threats will differentiate the strong from the weak
- Cyber resilience plans are essential – expect cyber disruption and prepare to deal with it while continuing to operate your business
- ANZ works with our clients to help keep them safe

CYBERCRIME INNOVATION

Cybercrime continues to threaten the Australian business landscape, with cybercrime expertise improving and adapting to target specific businesses. The ACSC (Australian Cybersecurity Centre) reports the changing environment has seen more diverse and innovative attempts to compromise government and private sector networks, increasing numbers of DDoS incidents, deliberate targeting, and changes in the frequency, scale, sophistication and severity of cyber incidents.[1]

Cybercriminals are increasingly sophisticated in their execution and can be equally opportunistic in who they target – from individuals through to large multi-national corporations, no one is immune from being attacked. This sophistication reflects the innovative methods used and speed of the execution. Cybercriminals innovate, make decisions and execute faster than many organisations are equipped to deal with. Moreover, cybercrime is now a business in every respect, with services that mirror those of multi-national organisations including customer support and technical helplines to ensure their criminal products and services work as intended.

In order to protect your business, you must understand this changing landscape and adapt.

Any modern corporate finance function is comprised of three main elements – people, process and technology. Cybercriminals look for and exploit any weakness in one or more of these elements to infiltrate the business to gain access to either information or syphon money, often millions of dollars at a time, into their international network.

CYBERCRIMINALS INNOVATE, MAKE DECISIONS AND EXECUTE FASTER THAN MANY ORGANISATIONS ARE EQUIPPED TO DEAL WITH.

CYBERCRIME IN ACTION

In March 2017, a Lithuanian man was arrested for duping two unnamed multinational internet companies via an email phishing attack. Google and Facebook later confirmed they were the two companies that fell victim to the scam costing them $100 million USD. He allegedly posed as a manufacturer in Asia and defrauded the companies from 2013 until 2015, stashing the money in bank accounts across Eastern Europe.

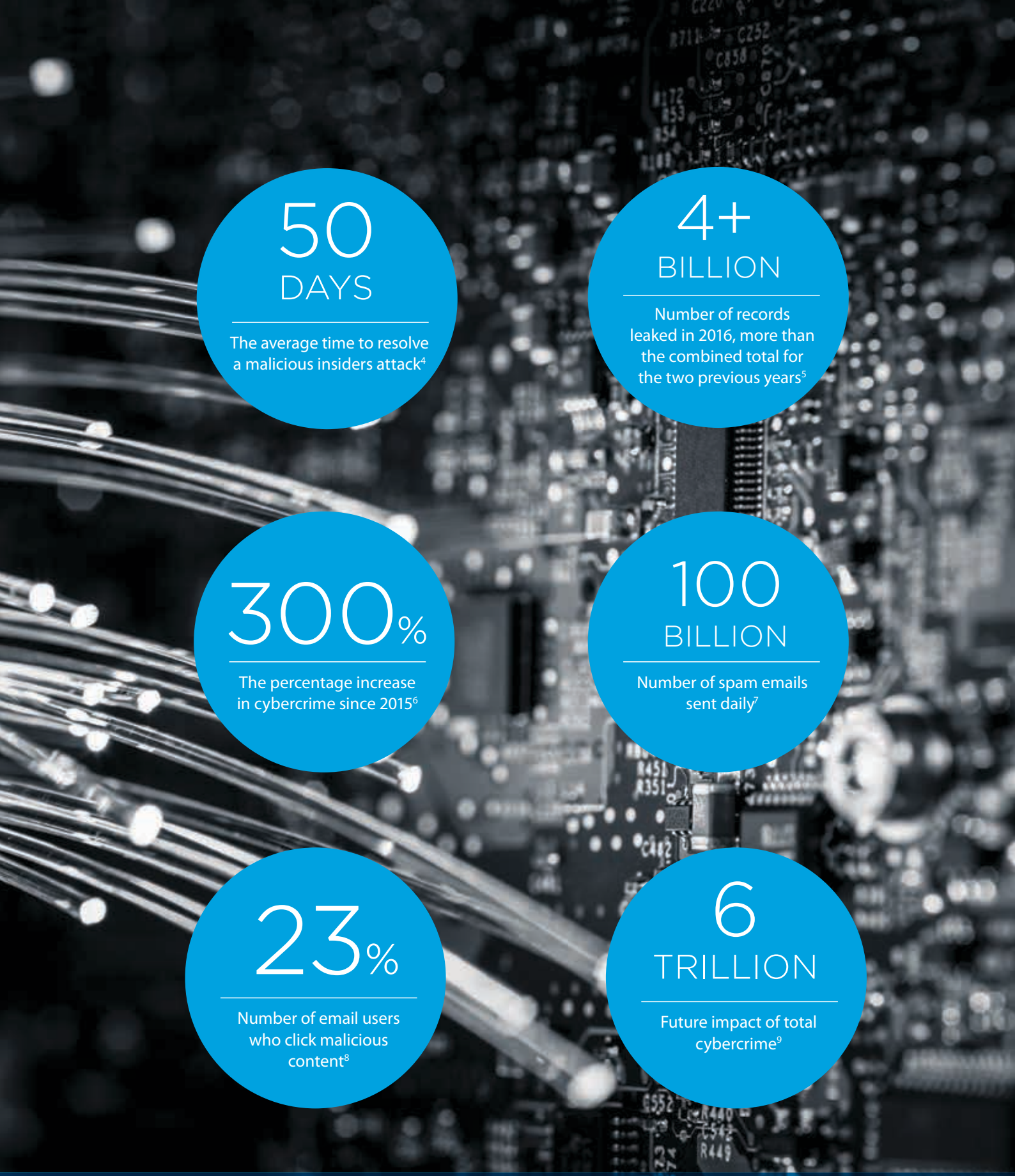
The emails were sent from accounts designed to look like they had come from an Asian-based manufacturer, but they did not. He used methods such as forging invoices, corporate stamps and email addresses to impersonate this Asian-based manufacturer with whom Facebook and Google regularly did business with.

This attack highlights how sophisticated cyber enabled fraud scams can fool even the biggest technology companies.[2]

On Friday, 12 May, 2017, the world was alarmed to discover that cybercrime had achieved a new record. In a widespread ransomware attack that hit organizations in more than 100 countries within the span of 48 hours, the operators of malware known as 'WannaCry' were believed to have caused the biggest attack of its kind ever recorded. Hospitals, rail systems, telecommunications and courier services were all impacted by WannaCry but many other organisations and individuals were affected as well.

According to an IBM report, ransomware was the most prevalent online threat in 2016. IBM researchers tracking spam trends noted that the rise in ransomware spam in 2016 reached an exorbitant 6,000 percent, going from 0.6 percent of spam emails in 2015 to an average of 40 percent of email spam in 2016. The situation is only worsening in 2017. The FBI estimated that ransomware is on pace to become a $1 billion source of income for cybercriminals by the end of 2016, a number that is expected to continue to rise in 2017.[3]

[1] https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf
[2] https://www.scmagazineuk.com/facebook-and-google-confirm-falling-victim-to-77m-phishing-scam/article/653837/
[3] https://securityintelligence.com/wannacry-ransomware-spreads-across-the-globe-makes-organizations-wanna-cry-about-microsoft-vulnerability/



50 DAYS

The average time to resolve a malicious insiders attack[4]

4+ BILLION

Number of records leaked in 2016, more than the combined total for the two previous years[5]

300%

The percentage increase in cybercrime since 2015[6]

100 BILLION

Number of spam emails sent daily[7]

23%

Number of email users who click malicious content[8]

6 TRILLION

Future impact of total cybercrime[9]

[4] https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017
[5] IBM Threat Intelligence Index 2017
[6] http://www.riskmanagementmonitor.com/ransomware-threats-jump-300/
[7] https://www.digicert.com/blog/dont-get-caught-phishing-scams/
[8] http://gizmodo.com/the-number-of-people-who-fall-for-phising-emails-is-st-1697725476
[9] https://www.csoonline.com/article/3110467/security/cybercrime-damages-expected-to-cost-the-world-6-trillion-by-2021.html

HOW DO THESE CYBER ATTACKS TAKE PLACE?

Methods used by cybercriminals are constantly evolving, and although too varied and numerous to list here, below are some of the most common methods.

SOCIAL ENGINEERING

Social engineering involves targeting an individual to facilitate the fraudulent transaction or data breach. During 2016 there was an aggressive increase in attacks that relied on humans rather than exploits of vulnerable software. By December, more than 99% of attachment-based email attacks were enabled by the user clicking something rather than an automated exploit. This trend extended to URL-based threats, where more than 90% of messages led users to credential phishing pages which trick victims into entering their usernames and passwords, rather than to exploits.[10]

Cybercriminals are often experts in human psychology and social engineering. They will send a bogus 'last minute crucial payment instruction' email at 5pm on a Friday just as people are going home in the hope that shortcuts will be taken to get the job done. Under the disguise of suppliers or colleagues, cybercriminals will send emails with links to fake e-Christmas or e-birthday cards in the hope that it will install malware on computers and retrieve banking credentials.

Increasingly social engineering is a prerequisite in the cybercriminals' success. People must be empowered and knowledgeable to spot and challenge the unusual, and then follow clearly defined response protocols. Continuous education and awareness are crucial[11].

MALICIOUS SOFTWARE

Malicious emails were the weapon of choice for a wide range of cyber attacks during 2016, used by everyone from state sponsored cyber espionage groups to mass-mailing ransomware gangs. One in 131 emails sent were malicious, the highest rate in five years.[12] Malicious software or 'malware' involves tricking individuals into opening infected files so that the cybercriminal can either introduce spyware, ransomware, viruses, trojans or any type of malware that would allow them to gain access to data, devices or systems.

PHISHING

Some of this activity is highly targeted phishing (or spear phishing). Phishing is when a malicious link to an authentic looking website is delivered via email, tricking the recipient to enter their security credentials or download malware. Spear phishing is more sophisticated by targeting a specific organisation or individual and appearing to come from a trusted source.

Phishing attacks leverage information gained from social media or other publicly available information, such as annual reports or company registers, to create legitimate looking emails to be sent to specific individuals, often purporting to come from friends or colleagues. Spear phishing can trick even the savviest of users, and as we have seen in previous examples, often has significant consequences.

RANSOMWARE

Ransomware continues to plague businesses and consumers with indiscriminate campaigns pushing out massive volumes of malicious emails. Attackers are demanding more and more from victims with the average ransom demand in 2016 rising from $1077, up from $294 a year earlier.[13]

Cybercriminals can go to extraordinary lengths to infect target computers. Legitimate websites can be compromised to host malware that then infect user devices. Fake surveys, free gift offers, 'must see' videos are just some of the ways criminals attempt to lure their unsuspecting victims.

EXISTING SYSTEM VULNERABILITIES

Cybercriminals often rely on known, but unpatched exploits, to gain access to IT systems to commit their crimes. Unchanged default root passwords are easy pathways into corporate IT systems. Cybercriminals know that large organisations are slow to react to patch upgrades. A patch release often describes the vulnerability that is being resolved in detail. If a cybercriminal failed in a past attack, but in their efforts, gathered information about a company's infrastructure, now knowing exactly how that infrastructure is vulnerable enables them to succeed in any future attempt until the patch is applied.

The Equifax data breach, disclosed in the United States in September 2017, was caused by vulnerabilities in the Apache Struts framework not being patched, even though the fix was available since March.[14] This oversight led to the exposure of personal records of over 145 million people.[15]

Organisations battling these threats must ensure that they have a robust approach to tackle them.

[10] https://www.proofpoint.com/us/human-factor-2017
[11] https://www.fbi.gov/news/stories/2014/april/understanding-school-impersonation-fraud/understanding-school-impersonation-fraud
[12] Symantec 2017 Internet Security Threat Report
[13] Symantec 2017 Internet Security Threat Report
[14] https://www.scmagazine.com/apache-struts-vulnerability-led-to-earlier-breach-at-equifax/article/689863/
[15] https://www.scmagazine.com/equifax-adds-25m-to-total-affected-by-breach-as-its-former-ceo-heads-to-washington/article/697471/

CURRENTLY, WE ARE SEEING SOCIAL ENGINEERING AS A PREREQUISITE IN THE CYBERCRIMINALS' SUCCESS.

CYBERCRIME IN ACTION

In 2017, the Australian Cybersecurity Centre[16] observed an increase in business email compromise through targeted phishing emails. Small businesses in particular were targeted by themed phishing emails from known contractors whose systems had been compromised by malicious adversaries. The adversary would gain access to small businesses through malicious PDF files or credential phishing. Within hours of the initial network compromise, new email rules would be implemented that forwarded new emails with certain subjects such as 'invoice' to the adversary's email address. These would then be deleted from the compromised business' email. The adversary would then create new invoices for clients and contractors using the business' branding but containing different banking details. In some cases, the adversary would send out emails advising that bank details would be changing for the next invoice.

In one instance, a cybercrime adversary posed as a Chief Executive Officer (CEO) and Chief Operating Officer (COO) of a large business and obtained fraudulent payments of over US$500,000. The adversary sent a spoofed email, purporting to be from the CEO (who was travelling at the time), requesting a large payment from the financial controller. A second email, purporting to be from the COO, was then sent to the financial controller. This email contained a false email trail approving the CEO's request for payment.

Not realising the request was fraudulent, the business made two payments to the cybercriminal, one for over US$200,000 and one for almost US$300,000. Both payments were made to bank accounts in overseas jurisdictions.

[16] https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf

KNOW, CONTROL AND ADAPT

Those who perpetrate these cyber attacks have a vested interest in ensuring their methods are innovative and covert. However, while cybercrime seems a new threat, a risk based approach allows focus on what is important.

UNDERSTAND YOUR PROCESSES AND YOUR RISKS

Knowing your organisational processes is crucial to understanding the cybersecurity risks they present. With this in mind, reviewing the maturity of your transactional processes is the first and most fundamental step in protecting against cybercrime. This includes the identification of gaps or weaknesses in process or controls, such as user access management and payment authorisation, which present a risk.

Risk professionals can help in defining the risks associated with those processes, the people who execute those processes and the technology that enables them. After they have identified the risks that pose the highest threat to your business objectives, clear plans must be set in place to mitigate them. Organisations can reduce the likelihood and impact of risks by implementing effective controls.

MONITOR THREATS

Controls are all those activities that detect or prevent undesirable events. Controls, much like processes, must be actively reviewed to make sure they are designed and operated in a way that reduces risk.

Remember all controls are not equal: they reduce in effectiveness over time. Process or technology change and time allows cybercriminals to adapt and change their tactics. This is where the controls to respond and recover from cyber incidents (as part of a cyber resilience plan) become even more imperative.

In the cybersecurity world we can also learn from other security principles such as 'defence in depth', making sure that we do not depend on a single control; and taking an end-to-end view that acknowledges how threats can enter at any point in our processes.

There are many different layers of people and process controls, from company level leadership to employee activities, behaviours, and culture. A robust, well documented and actively managed control environment is crucial. Any system is only as strong as its weakest link.

MONITOR AND ADAPT

During the ongoing governance of your organisation's process and controls, one core factor to take into account is the agility to change. As mentioned previously, cybercriminals are innovative and constantly change their approach, behaviour and tools to create new ways of stealing assets. Vigilance is key. The time to act is now.

Organisations must monitor security news, identify new best practices and source intelligence about the methods and tools used by cybercriminals. The flexibility to react to an ever-changing environment will differentiate the strong from the weak.

Governments are certainly taking the threat seriously. In 2013, the UK's National Cybercrime Unit became operational[17] and in 2014, The Australian Government opened the Australian Cybersecurity Centre to co-locate cybercrime intelligence units[18].

Certain industries have already begun to create intelligence sharing groups, some of which have government representation. It is expected that this trend will continue to expand as more and more companies, industries and governments realise that cyber threats are here to stay.

ADDITIONAL ACTIONS USING THE ESSENTIAL EIGHT

The Australian Signals Directorate's (ASD) Strategies to Mitigate Cybersecurity Incidents is a prioritised list of practical actions organisations can take to make their computers more secure. The actions are customisable to each organisation based on their risk profile and the threats they are most concerned about[19]. Admittedly these controls focus largely on technical components within your organisation, however the 'defence-in-depth' approach relies on organisations using multiple layers of security to make itself significantly more resilient in the face of a cyber event.

These strategies, which are collectively known as the 'Essential Eight', are highly recommended to help mitigate the growing threat of cyber events within your organisation.

For further information visit the Australian Signals Directorate site (https://www.asd.gov.au/publications/protect/essential-eight-explained.htm)

[17] http://www.computerweekly.com/news/2240206747/UK-National-Cyber-Crime-Unit-becomes-operational
[18] http://www.abc.net.au/news/2015-04-23/cyber-attacks-on-australian-businesses-rise-20-per-cent/6415026
[19] https://asd.gov.au/publications/protect/essential-eight-explained.htm

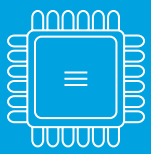
A ROBUST, WELL DOCUMENTED AND ACTIVELY MANAGED CONTROL ENVIRONMENT IS CRUCIAL. ANY SYSTEM IS ONLY AS STRONG AS ITS WEAKEST LINK.

KEY CONTROL CONSIDERATIONS

PEOPLE

Staff education: Invest in staff awareness on cyber risks and in particular new social engineering and phishing techniques. Your staff are the first and last line of defence against cyber attacks.

Build Relationships: Develop and leverage your relationships, both within your organization and with third parties to get insights into current threats, best practices and remember it is an ecosystem for all of us.



TECHNOLOGY

Network/ IT security controls: Consider robust logical access controls, new system strengthening, network and endpoint firewalls, up to date malware and anti-virus protection, intrusion detection systems, regular patching, vulnerability scans and penetration tests.

PROCESS

Governance and monitoring: Place cybersecurity on the agenda of senior executive and management meetings to ensure risks are regularly reviewed and appropriate proactive and reactive measurers are in place.

Insist on a robust security policy: Maintain clear protocols on segregation of duties, and controls for the use of all technology including mobile/portable devices. It should also explicitly define employee security screening processes, acceptable use of IT assets and staff training.

User access management: Ensure that only staff with the right responsibilities and security credentials has access to your systems and financial data, including two factor authentication for transaction signing/payment approvals. Regularly monitor and update user access privileges, and check that staff are protecting and not sharing their security credentials. Removing access when no longer required is equally important, including when staff move to new roles within the organisation.

Define a coordinated response to security events: expect a cyber incident, plan for and practice your response and resolution to minimise the impact of a loss.

Control payment authorisations: Consider strict procedures over all changes to customer/supplier bank details, key contacts and all other master data including identity verification and change accuracy controls.

Reconcile and review: Ensure reconciliations do not just serve as a rubber stamp activity but detect and escalate a leakage in funds whether small or big as a once off or over a period of time.

What is valuable? Consider what you have that may be valuable to others in your organization. This may be money, customer information, corporate intelligence etc and then plan ways to ensure it is protected.

CYBERCRIMINALS ARE INNOVATIVE AND CONSTANTLY CHANGE THEIR APPROACH, BEHAVIOUR AND TOOLS TO CREATE NEW WAYS OF STEALING ASSETS. VIGILANCE IS KEY. THE TIME TO ACT IS NOW.

PARTNERING WITH ANZ TO MINIMISE CYBER THREATS

Before implementing the strategies, organisations need to identify their assets and perform a risk assessment to identify the level of protection required from cyber threats. Organisations need to:

1. Identify which assets require protection – do they hold important, sensitive or other information with a need for immediate and continuous access?
2. Identify which adversaries are most likely to compromise their information – cybercriminals, nation-states or malicious insiders?
3. Identify what level of protection is required – use the Essential Eight strategies[20] as a baseline and then select other relevant strategies based on the risks to their business.

Our world is one occupied by a broad range of financial management activities – we get that. We also understand that financial transactions are only as secure as the link between your organisation, your business partners and your bank.

Our digital security encompasses a combination of hardware and software solutions, as well as best practice business process, experienced people and technology controls. Interfaces between ANZ and clients, and ANZ and other financial institutions use encryption and network security infrastructure to help protect your business.

Working together with ANZ, you get peace of mind from knowing that we are securing important links in the financial supply chain.

ANZ provides information on cybersecurity practices, which includes a mix of resources, information and software from third party suppliers, government departments and trends ANZ observes as a financial institution.

[20] https://asd.gov.au/publications/protect/essential-eight-explained.htm

A GLOSSARY OF USEFUL CYBER TERMS

Adware

Software that is covertly installed on your computer and designed to deliver advertisements or other content which encourages you to purchase goods or services.

Catfish

Internet predators who create fake online identities to lure people into emotional or romantic relationships for personal or financial gain.

CryptoLocker

A particularly malicious type of ransomware which, once installed on your computer, encrypts and locks all of the files on the infected computer including documents, photos, music and video. A pop up window will then display on the computer screen requesting payment of a ransom in return for a CryptoLocker key to unlock the encrypted files. Paying the ransom does not guarantee removal of the CryptoLocker.

Defence in Depth

Defence in depth (or layered defence) which really means that we recognise that no single control alone can prevent an intrusion. It is the sum of multiple controls that increase the difficulty and enhances the ability for us to detect an attacker.

Exploit

Exploiting is the act of trying or successfully using a vulnerability to perform an action which the system or application was not originally programmed to perform. This is often referred to as a 'breach'. A vulnerability can therefore be 'exploited' to turn it into viable method to attack a system.

Keylogger

A keylogger is a program that records the keystrokes on a computer. It does this by monitoring a user's input and keeping a log of all keys that are pressed. The log may be saved to a file or even sent to another machine over a network or the internet. Keylogger programs are often deemed spyware because they usually run without the user knowing it.

Malicious software (malware)

A catch-all term used to describe software designed to be installed into a computer system for the purpose of causing harm to you or others. This would include viruses, spyware, trojans, worms, etc.

Phishing (email/website)

Fraudulent email messages or web sites used to gain access to personal information for illegal purposes such as transferring funds or purchasing goods over the internet.

Ransomware

Malware which locks out computer functionality, for example, encrypting personal data, and offers to restore the functionality for a fee, which is extortion. Paying the fee does not guarantee removal of the ransomware, which can lay dormant ready for attack in the future (e.g. the impact of WannaCry)

Scam

A commonly used term to describe a confidence trick, relying on email or a website to deliver the trick to unsuspecting users.

Scareware

Malware that causes frightening messages to appear (for example, that your computer is infected with malware or that you are guilty of a crime), and attempts to extort money from you to resolve the alleged issue. Similar to ransomware)

Spam

Unsolicited email. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or illegal services. Users are advised that if an offer in an email appears too good to be true then it probably is and should not be actioned in any way.

Spyware

Software that is covertly installed on a computing device and takes information from it without you consent or the knowledge of the user.

Trojan horse

Malicious code that is hidden in a computer program or file that may appear to be useful, interesting, or at the very least harmless to you when using your computer. When this computer program or file is run, the malicious code is also triggered, resulting in the setup or installation or malware.

Virus

Malware designed to infect and corrupt a computer and to copy itself. Viruses can disrupt programs installed on a computer.

Vulnerability

A vulnerability (or finding) is a flaw in a system, or in some software that could provide an attacker with a way to bypass the security infrastructure of the host operating system or of the software itself. It isn't an open door but rather a weakness which if attacked could provide a way in.

Water-holes

Malware placed on a legitimate website to compromise website or users.

Weaponisation

Weaponisation is the use of an exploit to deliver malicious payload to the target system.

Worm

A self-replicating virus that does not alter files but resides in active memory and duplicates itself.e.g. this was responsible for the WannaCry spread). Typically a worm does not require user interaction to continue propagation within a computing environment and relies on exploiting vulnerabilities to spread.

Zero Day

A zero day (0-day) is an exploit that a software or manufacturer is not aware of. Organised Crime / Nation states and sophisticated adversaries will pay a considerable amount of money to obtain these zero day items. For example, a means to be able to unlock an iPhone without knowing the unlock code to the phone.

Zombie or bot

A single compromised computer(a robot computer), called a zombie or a bot.

IMPORTANT NOTICE

Australia and New Zealand Banking Group Limited (ACN 005 357 522) ("ANZ") and its related bodies corporate and affiliates are represented in various countries (together, "ANZ Group").

1. Country specific information: This document is distributed in: Australia by ANZ. ANZ holds an Australian Financial Services licence no. 234527; New Zealand by ANZ Bank New Zealand Limited; United States by the New York branch of ANZ; Indonesia by PT Bank ANZ Indonesia ("PT ANZ"). PT ANZ is incorporated and licensed in Indonesia with limited liability; Vietnam by ANZ Bank (Vietnam) Limited ("ANZ VN"). ANZ VN Is a wholly-owned foreign bank incorporated and licensed in Vietnam; China by the People's Republic of China by Australia and New Zealand Bank (China) Company Limited ("ANZ China"), which is a subsidiary of ANZ. ANZ China is incorporated and licensed in PRC. This document may not be distributed, re-distributed or published in the PRC, except under circumstances that will result in compliance with any applicable laws and regulations; Hong Kong by the Hong Kong branch of ANZ, which is registered by the Hong Kong Securities and Futures Commission; Singapore by the Singapore branch of ANZ. ANZ is licensed in Singapore under the Banking Act Cap. 19 of Singapore; Taiwan by ANZ Bank (Taiwan) Limited, which is a wholly-owned subsidiary of ANZ incorporated and licensed as a bank in Taiwan; Japan by the Japan branch of ANZ which is awarded a banking license in Japan; South Korea by the South Korea branch of ANZ, which is licensed in South Korea; Cambodia by ANZ Royal Bank (Cambodia) Limited ("ANZ Royal Bank"), which is a subsidiary of ANZ. ANZ Royal Bank is incorporated and licensed in Cambodia; India by the India branch of ANZ which is licensed in India. The information provided herein is solely for informational purposes, and does not constitute an offer or solicitation. The availing of any products from ANZ India is subject to the completion and execution of, the requirements and documentation prescribed by ANZ India, and any requirements prescribed under applicable law; Laos by ANZ Bank (Lao) Limited, which is a subsidiary of ANZ. ANZ Lao is incorporated and licensed in the Leo People's Democratic Republic; Malaysia (other than Labuan) by the Malaysian representative office of ANZ. As a representative office, ANZ cannot provide any banking services to clients in Malaysia. In Labuan, this document is distributed by the Labuan branch of ANZ which is licensed as a Labuan bank; Philippines by the Philippines branch of ANZ, which is licensed in the Philippines; Thailand by the Thailand representative office of ANZ. As a representative office, ANZ cannot provide any banking services to clients in Thailand; Papua New Guinea by Australia and New Zealand Banking Group (PNG) Limited (Company Registration No. 1-6419); American Samoa by the American Samoa branch of ANZ Guam Inc (operating as Amerika Samoa Bank); Cook Islands by the Cook Islands branch of ANZ; Fiji by the Fiji branch of ANZ. For Fiji regulatory purposes, this document and any views and recommendations are not to be deemed as investment advice; Guam by ANZ Guam Inc; Kiribati by ANZ Bank (Kiribati) Limited; New Caledonia by the New Caledonia representative office of ANZ. As a representative office, ANZ cannot provide any banking services to clients in New Caledonia; Samoa by ANZ Bank (Samoa) Limited; Solomon Islands by the Solomon Islands branch of ANZ; Tonga by the Tonga branch of ANZ; Timor-Leste by the Timor-Leste branch of ANZ; Vanuatu by ANZ Bank (Vanuatu) Limited; United Kingdom ANZ is authorised in the United Kingdom by the Prudential Regulation Authority ("PRA") and is subject to regulation by the Financial Conduct Authority ("FCA") and limited regulation by the PRA. Details about the extent of our regulation by the PRA are available from us on request. This document is distributed in the United Kingdom by ANZ solely for the information of persons who would come within the FCA definition of "eligible counterparty" or "professional client". It is not intended for and must not be distributed to any person who would come within the FCA definition of "retail client". Nothing here excludes or restricts any duty or liability to a customer which ANZ may have under the UK Financial Services and Markets Act 2000 or under the regulatory system as defined in the Rules of the PRA and the FCA; Germany by the Frankfurt Branch of ANZ solely for the information of its clients; Other EEA countries by ANZ Bank (Europe) Limited ("ANZBEL") which is authorised by the PRA and regulated by the FCA and the PRA in the United Kingdom, to persons who would come within the FCA definition of "eligible counterparty" or "professional client" in other countries in the EEA. This document is distributed in those countries solely for the information of such persons upon their request. It is not intended for, and must not be distributed to, any person in those countries who would come within the FCA definition of "retail client".

2. Information relevant to all countries: The distribution of this document may be restricted by law in certain jurisdictions. Persons who receive this document must inform themselves about and observe all relevant restrictions. This document has been prepared for information purposes only and does not take into account the specific requirements, investment objectives or financial circumstances of any recipient. The recipient should seek independent financial, legal, tax and other relevant advice and should independently verify the accuracy of the information contained in this document. Under no circumstances is this document to be used or considered as an offer to sell, or a solicitation of an offer to buy, or a recommendation or advice to buy or sell or not to buy or sell any product, instrument or investment, to effect any transaction or to conclude any legal act of any kind whatsoever. If, despite the foregoing, any services or products referred to in this document are deemed to be offered in the jurisdiction in which this document is received, no such service or product is intended for nor available to persons resident in that jurisdiction if it would be contradictory to local law or regulation. Such local laws, regulations and other limitations always apply with non-exclusive jurisdiction of local courts. To the extent permitted by law, ANZ Group does not accept any responsibility or liability arising from a recipient's use of this information. This document may not be reproduced, distributed or published by any recipient for any purpose. ANZ recommends you contact your ANZ Manager for further information before acquiring the product and refer to the product Terms and Conditions for full information relating to the product and services mentioned in this document.

Australia and New Zealand Banking Group Limited (ANZ) ABN 11 005 357 522. Item No. 92941 02.2018 W586398