SIMPLIFYING CYBER

FOR BUSINESS

2021

ANZ

CYBER SECURITY

IS EVERYONE'S BUSINESS

It's exciting to see the opportunities available to people and business today – opportunities made possible by technology that makes work and life in general easier, faster, more accessible and more flexible.

While modern technology offers businesses a range of opportunities, the benefits of technology can carry risk. Advantages like increased speed and reach are equally appealing to those with ill intent. So it's little wonder why cyber security has become such a vital part of business.

Many companies have enhanced their security capability in response to the increased volume and sophistication of cyber attacks globally. Every company is different and has a different risk appetite, but those who have responded with proactive partnerships between their business, technology and security teams will be better prepared and equipped to manage cyber threats.

Creating this sense of shared responsibility can be achieved through clear communication between security and technology teams and the business. This ensures that business leaders are empowered to make informed decisions that balance operational benefits with risk implications. Cyber security is ultimately a business issue and requires focus from everyone in an organisation.

Cyber security can be perceived as overly complex, but doing cyber security well is not as hard as people think - many risks can be reduced simply by improving the basics. If we all play our part right, we can unlock the full potential of the digital age, whilst ensuring risks are understood and managed. A collaborative approach works because cyber security is not just a technology matter - it is everyone's business.

Keeping systems and applications up to date (patching), ensuring working backups are in place, allowing only the right people access to information and systems, and educating teams on the risks and their roles can improve an organisations' cyber security capability. Modernising general security capability and increasing the use of cloud computing with the right security controls in place can also significantly improve organisations' cyber security position.

As the lines between work and home become increasingly blurred, the need for companies to ensure employees are equipped with the knowledge, tools and mindset to work safely, and share information securely, takes on even greater urgency.

This guide sets out to simplify cyber for business, providing the context C-suite executives require, and sharing some everyday tips that can provide defence against cyber threats to allow an organisation to operate effectively, take advantage of innovative technology and remain secure.

LYNWEN CONNICK

Global Chief Information Security Officer
ANZ Banking Group

CONTENTS

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.

All of this has enabled people to be more connected virtually, at a time where we have become more distanced physically. New technology, more data, use of third parties, and complex systems are all factors that can help companies perform better.

But leaders should contemplate how these factors, if not well managed, could change their security posture. Unsurprisingly, regulatory and legislative coverage has also shifted with the changing environment at both a country and industry sector level.

CYBER ATTACKS ARE GROWING IN FREQUENCY AND SOPHISTICATION

These numbers share both the size of the challenge and the organisational factors which contribute.

39S
UNTIL THE NEXT MALICIOUS ATTACK

$6T
COST OF CYBER CRIME BY 2021

100B
SPAM EMAILS EVERY DAY

90%
CYBER ATTACKS ARE PHISHING EMAILS

87%
SMALL BUSINESSES THINK ANTIVIRUS SOFTWARE ALONE WILL PROTECT THEM

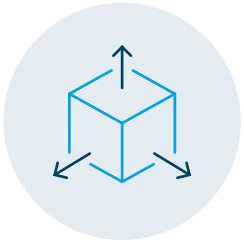
$3.9M
AVERAGE COST OF A DATA BREACH

70%
COMPANIES AREN'T PREPARED FOR AN ATTACK

Source: enterprise.verizon.com/en-au/resources/reports/dbir/

FIVE KEY DRIVERS BEHIND THE SURGE IN CYBER ATTACKS

INCREASINGLY ADVERSE THREAT ENVIRONMENT



COMPLEXITY OF SYSTEMS & TECHNOLOGY

PHENOMENAL GROWTH OF DATA

INCREASED CONNECTIVITY WITH THIRD PARTIES

RAPID ADOPTION OF TRANSFORMATIVE TECHNOLOGY

INCREASINGLY ADVERSE THREAT ENVIRONMENT

Traditional methods of attack are evolving. Business Email Compromise (BEC) scams alone cost Australians $132 million per annum[2]. The total cost is even greater when the likes of ransomware, distributed denial of service (DDoS), and other attacks are included.

Cyber crime is big business. Just as improved tools, information and revenue is appealing to business, the production and sale of tools and services that hackers use, as well as the potential proceeds of cyber crime are attractive to criminals. Options once only available to nation states are now widely available to low-level criminals. Attackers are also using automation and artificial intelligence to amplify the speed and scale of attacks.

Everyone should be prepared for an attack. Regardless of how well positioned you think you are - it's a question of when, not if your organisation will experience a cyber attack.

2. www.accc.gov.au/media-release/business-email-compromise-scams-cost-australians-132-million

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 ensuring systems remain up to date (patched), to guard against new vulnerabilities.

There can be a high price to pay when businesses fail to prioritise patching and vulnerability management, including data and financial loss leading to reputational, regulatory and legal impacts. 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 more than doubled between 2016 and 2018.[3]

PHENOMENAL GROWTH OF DATA

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

This information is regularly sold on the "dark web" 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 come with additional risk.

The introduction of regulation such as the Australian Prudential Regulation Authority's (APRA) information security standard (CPS 234), Australia's Notifiable Data Breach scheme and Europe's General Data Protection Regulation (GDPR) adds another driver to this.

Increasingly, this is enforced through significant financial penalties for non-compliance. However, the overall impact of a large-scale data breach is likely 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.

3. www.securitymagazine.com/articles/89783-set-a-new-record-for-security-vulnerabilities

INCREASED CONNECTIVITY WITH THIRD PARTIES

Third party suppliers are valuable partners that support and uplift business performance. Still, where they have access to your systems and information it is important to ensure they are equipped to protect your business and customer information.

Companies sharing data with third parties need to ensure both their own data and systems, and data held, or systems used to manage information on their behalf, is 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, active and ongoing monitoring is critical to ensure your information is protected wherever it may be.

RAPID ADOPTION OF TRANSFORMATIVE TECHNOLOGY

Technologies such as cloud computing have the potential to solve many security challenges. For instance, managed cloud-based IT (Information Technology) infrastructure can include automatic updates and maintenance (patching) for security vulnerabilities to ensure operating systems are always up to date.

Capitalising on the opportunities of emerging technology, including Cloud, requires a commitment to building in security from the beginning. Sometimes the speed of change can mean security requirements can be overlooked.[4] Embedding security skills within development teams is a great way to ensure security keeps pace with the change.

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, they also serve as a primary resource from which attackers can launch distributed denial-of-service (DDoS) attacks through botnets.

With their focus on innovation and functionality, IoT developers often overlook security features that can significantly increase manufacturing and maintenance expenses[5], leaving companies as well as consumers exposed.

4. www.reuters.com/investigates/special-report/china-cyber-cloudhopper
5. www.iotforall.com/bringing-shadow-iot-devices-into-the-light-on-corporate-networks

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 are 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 the risks in the environment. 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 by enabling it to 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.

SYSTEM VULNERABILITIES

Applications and operating systems require ongoing maintenance (or patching), to ensure any vulnerabilities identified in code cannot be exploited by hackers to gain system access. Often, the bigger the organisation, the bigger the attack surface, due to the sheer number of applications and operating systems.

Patching is important to update applications and operating systems to close newly identified vulnerabilities that could be leveraged by cyber criminals. Every time an application or operating system requires a patch, the developer releases an explanation of why the update is required. This transparency can also provide cyber criminals with the necessary information to reverse engineer a compromise or way into a network, so fast patching is essential.[6]

Some organisations 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 applying patches and exploit vulnerabilities in older versions of applications to access networks before the 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 updates are released usually means that changes are simpler, take less time and are less disruptive compared to trying to apply a large backlog of changes at once.

Typically, newer versions of operating systems and applications are designed with more features and security built in, including the latest patches. So, installing the latest version of software as well as applying patches as soon as they become available is important. In addition, up to date and well patched systems are not only more secure, they are also likely to be more reliable – so there are lots of good business reasons to keep systems up to date.

6. The Australian Cyber Security Centre has information on what patching involves and how to approach it: www.cyber.gov.au/acsc/view-all-content/publications/assessing-security-vulnerabilities-and-applying-patches.

PEOPLE

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

People are also human, and fallible - just like any vulnerability in a system, people can also be exploited. Developing the right skills across a workforce is inherently complex and requires sustained, culturally appropriate focus. Cyber criminals understand this and take advantage of skills gaps and human error.

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

A HIGH PROPORTION OF SUCCESSFUL SECURITY ATTACKS INVOLVE SOME TYPE OF HUMAN ERROR SUCH AS:


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

THIRD PARTIES & SUPPLY CHAIN

Cyber criminals will look for the easiest targets and the easiest ways to exploit that target. As a result, a direct attack on an organisation may not be the most attractive option. Smaller third parties are increasingly being compromised as a way of gaining access to larger corporations.

Cyber supply chain risk increases whenever companies introduce a third party to the delivery of products and services. Effective management of this risk will go a long way to ensuring secure supply throughout the product lifecycle, from design through to manufacture, delivery, maintenance and disposal.

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

Similarly, the COVID-19 pandemic forced companies to rapidly adopt new tools to support their remote workforce. In the effort to enable fast remote collaboration, employees and companies may be rapidly adopting new collaboration tools without considering the security implications. Online conference tools are just one example where security vulnerabilities have been observed.

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 applies to the rest of its operations, they can allow a company to perform to its potential. Introducing new components into your supply chain introduces more opportunities for a cyber criminal to find a weakness in systems, processes and people, so companies are wise to implement governance, processes and education controls.

CYBER ATTACK TACTICS

The phrase "data breach" is typically understood as a scenario where hackers 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 companies from their data or systems (availability) or call into question accuracy of data (integrity) by manipulating records. A compromised social media account that a hacker uses to post unauthorised posts is an example of a failure of integrity.

For that reason, it's important to implement an approach that ensures data and system confidentiality, integrity, and availability (CIA), in other words an approach that ensures that data and applications that provide services are protected, accurate and available to those who need them.[7]

IMPACTS OF CYBER ATTACKS


Reputational damage


Financial loss


Loss of intellectual property


Regulatory fines


Identity theft


Emotional distress


Business disruption


Customer devastation

7. www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples

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

MALICIOUS SOFTWARE

Malware (or malicious software) is software used to cause damage to computer systems or organisational networks. Malware is typically the way cyber criminals gain access to devices and can be achieved by direct targeted attacks (e.g., targeted email/phishing) or through randomised broad attacks (e.g., infected websites).

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 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, however dealing with criminals can mean paying the fee does not guarantee a solution or removal of the ransomware, which can lay dormant ready for attack in the future. Supporting criminals by giving them money through a ransom payment may also be illegal, and is certainly unethical as it promotes further crime. Prevention is certainly better than this unpalatable cure.

Ransomware has become one of the most significant threats given the potential impact on the operations of businesses and governments. Cyber criminals often install it via phishing emails, or illicitly obtained user logins and credentials through spear phishing, or by directly exploiting known system vulnerabilities.

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 a business 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 options.[8]

8. www.cyber.gov.au/acsc/view-all-content/threats/denial-service

BUSINESS EMAIL COMPROMISE

Malicious emails (phishing) are one of the most common forms of attack on organisations. These emails can seek to gather information about an individual or company, attempt to trick the recipient into an action, or deliver ransomware.

A specific type of phishing, business email compromise (or BEC), is rapidly increasing in frequency, complexity and impact on company bottom lines. So much so that in 2019 the FBI indicated losses from BEC attacks amounted to $1.7 billion[9] (almost half of all losses due to cyber crime). These emails typically purport to be a significant stakeholder seeking urgent action, like funds transfer, and come in a variety of forms:

EXECUTIVE FRAUD

Scammer masquerades as an executive and sends 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 invoice.

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.

TRUST AND ITS MISUSE

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

- Sending email using near identical domains (e.g., @azn.com instead of @anz.com).
- Sending email 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 company 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).

All in the 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 programs and spam filters without detection. Where emails do include a malicious attachment or link, well managed anti-malware and spam filters should quickly identify and remove a high proportion of these emails, but not all can be detected automatically.

9. news.microsoft.com/on-the-issues/2020/07/23/business-email-compromise-cybercrime-phishing

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.

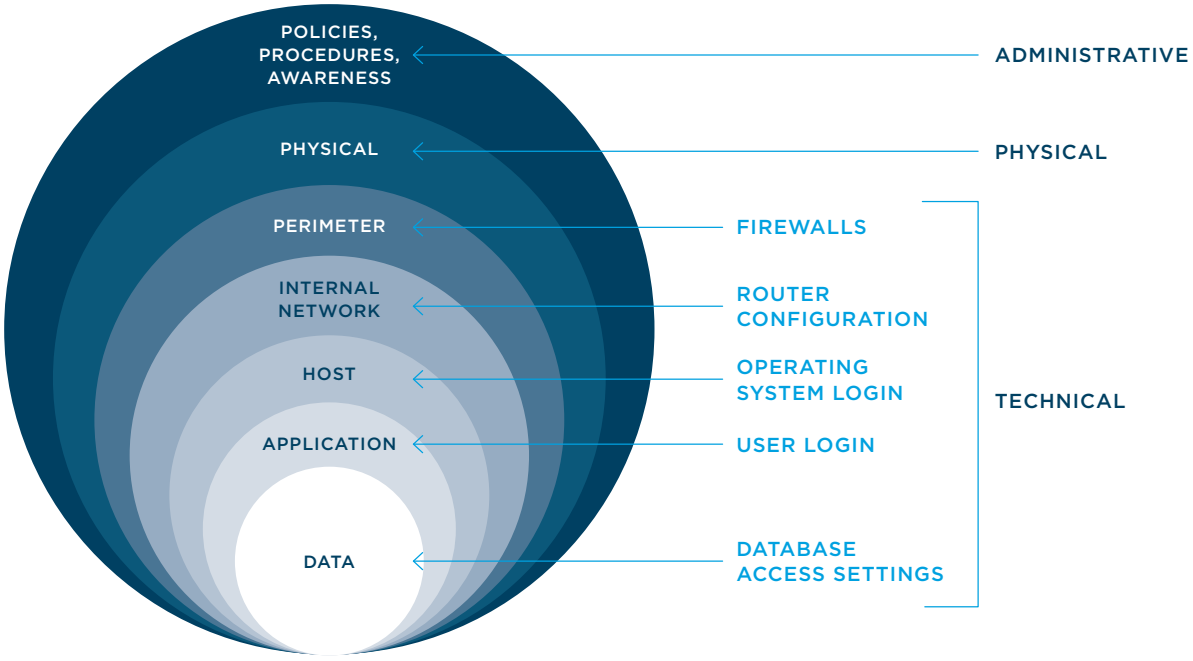
By understanding the threat landscape in which we operate, the opportunities that a cyber criminal may look for, and how they go about exploiting an identified vulnerability, we can develop a comprehensive security strategy. This includes controls to both address potential risks and empower your organisation to succeed by securely taking advantage of the opportunity technology presents.

A defence in depth approach anticipates the security considerations across all areas of an organisation from technology to processes to people and applies multiple layers of security controls to prevent the distinct types of attacks.

For example, a company could issue employee security passes to access office buildings and insist on user authentication requirements to enter the technical network.

After controlling access to the physical premises and system log ins, 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 also become invaluable.

These controls can then be reinforced with a cyber security education and behaviour influence program that educates and enables people to meet their specific security responsibilities, a threat intelligence capability, plus integrated security tools and systems to monitor and protect information. Robust governance, processes and standards also need to be understood and owned by everyone across your organisation.



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

CONTROL ACCESS

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

- Apply a virtual private network (VPN) that allows remote users to securely access information on your network, such as email and file services.
- Secure remote working and collaboration tools.
- Ensure employees understand the risks of leaving their own or their organisation's devices unattended, encourage them to keep devices somewhere safe and to lock them when they're not being used, to prevent unauthorised access.
- Ensure employees only use approved software and applications (it can be tempting for them to trial different software outside of the office environment).
- Enable two layers of protection against unauthorised access by enforcing multi-factor authentication on sensitive and critical systems.

SEGMENTATION

Having protective measures in place to prevent breaches of network perimeters is important, but not enough. It's 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 antivirus software and other detection capability to 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 add another layer of protection and support for managing and storing credentials. Importantly they also support more secure behaviour of people – by offering an easier way to apply complex and unique passwords.

KEY ELEMENTS OF CYBER SECURITY EDUCATION

ACCOUNTABILITY
Be clear that cyber security is a whole of business issue.

EMPLOYEE AWARENESS AND EDUCATION
Create a strong culture that encourages positive behaviours around cyber security.

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

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

NETWORK
Leverage relationships with trusted third parties (if your third party is impacted by an incident it could have a direct impact on you and customers).

INCIDENT RESPONSE
Know in advance who you will contact, what communication channels you'll use, who will help you respond, and what you'll say - and practice through drills and exercises.

POLICIES AND PROCEDURES
Make 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.

MAKING SECURITY AN ONGOING CONVERSATION

Have the conversation about cyber security companywide to ensure 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

An organisation's people are one of its strongest defences against cyber attack. Well informed, vigilant and resourced people can complement technical security systems to help identify, draw attention to, and prevent security threats.

A consistent and regular program of education and engagement can transform cultural norms and promote a security first mindset across the organisation. Effective education and influence programs extend well beyond employee on-boarding to ensure targeted security messages are delivered to the right audiences, at the right time, via the right communication channels.

SECURING YOUR SUPPLY CHAIN AND THIRD PARTIES

Engaging partners form 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 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 very tangible 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

- Ensuring your company's third party on boarding process reinforces roles and responsibilities when it comes to storing, sharing and accessing your company's information.
- Establishing clear cyber incident reporting and response requirements in the case of a security or information 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 third party have in place to protect information and systems?
- Conducting periodic assessments to ensure third parties are meeting their contractual obligations and have appropriate security controls.
- Reviewing the third party off boarding process so that your organisation's information stored or managed by the third party is appropriately purged and no longer accessible or discoverable.

EDUCATION

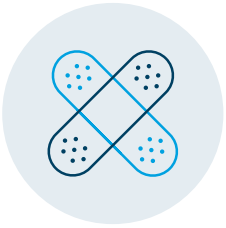
- Confirming third parties implement their own cyber security education program, so that employees know how to manage and protect information.
- Providing education to staff who engage third parties, so they understand and know how to manage third party risk.

THE ESSENTIAL EIGHT

The Australian Signal Directorate's 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



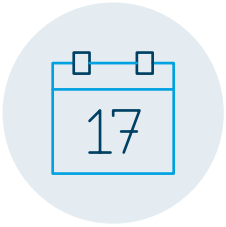
PATCH APPLICATIONS

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 incidents, but companies will go a long way to protecting themselves by implementing these steps as a baseline to make it much harder for cyber criminals to compromise systems. What's more, implementing the "Essential Eight" proactively is money well spent when applied according to the risk and when considered against the cost and impact of a major cyber incident.[10]

10. www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

SIMPLE ACTIONABLE STEPS

BUILD A HUMAN FIREWALL

Employees can be a company's most important defence in blocking cyber threats, and as more people work remotely the importance of 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. WORKING FROM HOME SECURELY

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

Turn on multi-factor authentication 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.

1. Seek supplier confirmation by phone rather than email if you receive a change of banking details from a supplier.
2. Request two authorisations for payments to create an extra level of security, particularly for large transactions or those that are sensitive or urgent.
3. Review how you update supplier details making sure employees are aware of the new or updated policies.
4. Be alert to phishing scams by not providing sensitive information about your company or employees to callers, and not publishing sensitive information online.
5. Protect employees' emails with two-factor authentication on emails, and blocks on spoofed emails if you own your domain.
6. Report scams to your bank and then the Australian Cyber Security Centre (ACSC) as soon as possible.

Although companies 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 significant proportion of malicious emails, providing another control layer to your organisation's security capability.

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 than ever, with access to more information. We can now collaborate easily, effectively and securely with colleagues and friends across the world, which we have seen with the shift to remote working in response to the global COVID-19 pandemic.

The changing landscape presents myriad opportunities; however cyber criminals can take advantage of the increased opportunities as well. The tools they use, the chances 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 ensuring its 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 – will completely shield companies from cyber crime. Our security team works with the business to help embed a security first approach that secures our foundations, embeds security across the organisation, enables transformation and embraces 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.

COMPANIES WITH THE MOST ROBUST CYBER DEFENCES WILL LIKELY:

- 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 company including Finance, IT, Risk
- Implement strong governance, processes and tools to protect systems and information
- Leverage relationships with trusted third parties
- Be prepared for incidents 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

RESOURCES

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 incident preparedness.

A STARTING POINT OF USEFUL WEBSITES

- Australian Cyber Security Centre
- ANZ Security Centre
- New Zealand National Cyber Security Centre
- Australian eSafety Commissioner
- Scam Watch
- The US National Institute of Standards and Technology (NIST)

KEY POLICY DOCUMENTS RELATED TO CYBER SECURITY

- Australia's Cyber Security Strategy outlines the federal government's overall vision.
- Australian Government Information Security Manual (ISM) assists in the protection of information that is processed, stored or communicated by companies' systems.
- Strategies to Mitigate Cyber Security Incidents complements the advice in the ISM and contains a complete list of strategies.
- Essential Eight Maturity Model complements the advice in the Strategies to Mitigate Cyber Security Incidents.

DISCLAIMER

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, email yourfeedback@anz.com.

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").

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.

Australia and New Zealand Banking Group Limited (ANZ) ABN 11 005 357 522. ANZSecSOII_CyberBrochureEd3_Feb2021_97713

anz.com