1st EDITION 2023

The Software Alliance
BSA

Secure Your Business, Secure Your Future

An Australian CEO's Guide to Surviving Cybersecurity Threats

How business leaders in Australia can protect their businesses and society with common-sense cybersecurity

CONTENTS

INTRODUCTION

Australia is no stranger to cyber attacks. Over 76,000 cybercrime reports were made to the Australian Cyber Security Centre (ACSC) via its ReportCyber website during the 2021–22 financial year, representing an increase of nearly 13% from the previous financial year.

And these are just the cyber incidents reported to the ACSC, which, according to its Annual Cyber Threat Report for the financial year ending June 2022, occurred every seven minutes, on average, during the period. In the prior year, the average was one every eight minutes.[1]

Moreover, the average cost per cybercrime report jumped 14% to over $39,000 for small businesses, $88,000 for medium businesses, and over $62,000 for large businesses, according to the Australian cyber agency's annual report.

The actual number of cyber incidents, including those that go unreported, is likely to be much higher than the ACSC's official figures.

Cyber attacks can be launched for any number of reasons: monetary gain, nation-state espionage, business competition, activist causes, or even plain old cheeky fun. But whatever the motivations of an attack may be, the consequences of such incidents can be devastating for any organisation.

In Australia, a series of high-profile cyber attacks and subsequent data breaches dominated news headlines in the first few months of 2023 alone, with nationally recognised brands and major government entities caught up in the actions of cybercriminals and left cleaning up the fallout.

As a nation, we've seen first-hand how such incidents can lead to costly brand damage, disruption of business operations, the loss or theft of valuable business data and sensitive customer information, and legal or regulatory penalties.

This guide is designed to provide practical tips and resources to help you safeguard your organisation from cyber attacks and legal risks due to unsafe network policies. It covers everything from basic cybersecurity hygiene practices to advanced strategies that can help you stay one step ahead of cyber criminals. It also highlights the different types of cyber threats and how they can impact your business.

Perhaps most importantly, this guide discusses how to reduce the risk of becoming a victim of a successful attack and how to mitigate the damage such an attack can cause.

Our goal is to help you develop a comprehensive cybersecurity plan that aligns with your business goals and needs. After reading the guide, you'll have a better understanding of the best practices and strategies you can implement to safeguard your organisation against cyber threats.

STRENGTHENING AUSTRALIAN BUSINESSES AGAINST CYBER ATTACKS

As technology continues to proliferate in every part of business, so too does the risk of cyber threat.

Cyber attacks are becoming more frequent and sophisticated, and Australian businesses are far from immune to such threats. The need for robust cybersecurity measures has never been greater. It is crucial for businesses to understand the evolving risks and take proactive steps to protect their systems, their data, and their brand reputation.

With this in mind, I'm pleased to present our latest guide on cybersecurity for Australian businesses, which provides a comprehensive overview of the current cybersecurity landscape across the country. The guide covers the cyber threats facing Australian businesses, including ransomware attacks, phishing scams, and insider threats. It also outlines the best practices for protecting businesses against cyber attacks and the importance of using licensed software. Additionally, it provides guidance on how to comply with regulatory requirements and foster a cybersecurity culture within your organisation.

Cybersecurity and the ongoing fight against cybercrime more generally is a key focus of the Australian Government. In December 2022, Australia's Minister for Cyber Security, Clare O'Neil, officially announced the development of the 2023-2030 Australian Cyber Security Strategy.[2]

The strategy aims to make Australia, in the words of the government, the "most cyber secure nation in the world" by 2030. To realise this goal, "the government is developing cybersecurity policies and initiatives under four key areas: a thriving a thriving cyber ecosystem, a resilient critical infrastructure and government sector, a sovereign and assured capability to counter cyber threats, and the positioning of Australia as a trusted and influential global cyber leader."

Similarly, BSA believes that cybersecurity is not just an IT issue, but a broader issue that requires attention from all levels of an organisation as well as the wider business community. As such, this guide is designed to provide information for executives, IT professionals, and other stakeholders to understand the importance of cybersecurity and take proactive measures to protect their businesses.

Tarun Sawney

Senior Director, BSA TheSoftware Alliance

I encourage all Australian businesses to read this important resource and take action by enhancing their cybersecurity approaches. Together, we can build a safer and more resilient digital ecosystem for all.

UNDERSTANDING CYBERSECURITY THREATS

Australian organisations face a variety of cybersecurity threats that have the potential to significantly harm their businesses and impact their customers. Some of the most common types of cybersecurity threats include phishing, malware, ransomware, and denial-of-service (DoS) attacks.

Phishing is a type of social engineering attack in which cyber criminals send fraudulent emails, text messages, or instant messages designed to trick the receiver into divulging sensitive information such as usernames, passwords, and financial data. These attacks can have a devastating impact on businesses by allowing cyber criminals to gain access to confidential data, steal money, or compromise computer systems.

Malware – a portmanteau of 'malicious' and 'software' – is, as its name suggests, a class of software that can be installed on a computer system, without the user's consent, for malicious purposes. Malware can lead to issues such as data theft, system crashes, and unauthorised access to sensitive information.

Ransomware, like malware, is a kind of software that can be installed on a computer system without the user's consent. However, it is typically used to encrypt a victim's data, demanding payment in exchange for a decryption key. These attacks can have a significant impact on businesses by causing disruption to operations and potentially leading to data loss.

DoS attacks involve overwhelming a network or website with digital traffic, with the intent to disrupt or shut down the system. These attacks can cause significant downtime for businesses that leads to lost revenue. A distributed denial-of-service (DDoS) attack achieves this when multiple online devices flood the resources of the targeted system.

The rise of remote work in the wake of the COVID-19 pandemic has vastly extended the corporate network and expanded the potential attack surface for many businesses. With more employees working from home, there is an increased risk of cyber attacks targeting personal devices that may lack the same level of security as office-based devices.

Moreover, the adoption of cloud-based work collaboration solutions, along with other cloud-based services, has led to a more complex IT environment, introducing new cybersecurity challenges for Australian organisations and making it harder for businesses to ensure that their data is securely stored and protected from cyber attacks.

AI-powered scams are on the rise

Generative artificial intelligence (AI) technology, such as ChatGPT is being increasingly used by cyber criminals to carry out sophisticated scams by emulating and impersonating real people. As reported by ABC News, large language models, like the one used by the popular ChatGPT chatbot, are able to better emulate human-like responses than traditional systems as AI systems improve, providing cyber criminals with new tools with which to mount attacks.[3]

Indeed, scammers are using the generative AI technology made possible by large language models in a variety of ways. Voice cloning technology, for example, is making it possible for criminals to use the voices of high-profile individuals to create convincing deepfake videos or audio recordings. Meanwhile, AI chatbots are being used to create convincing phishing messages that can trick victims into giving out their personal information or clicking on malicious links.

To protect against these types of scams, authorities suggest businesses and individuals remain wary of unsolicited messages or calls, especially if they ask for personal information or money. They also emphasise the need for increased awareness and regulation of AI technology to prevent it from being misused for fraudulent purposes.

BY THE NUMBERS: CYBERCRIME IN AUSTRALIA

The ACSC's Annual Cyber Threat Report for July 2021 to June 2022 provided an in-depth snapshot of how threat actors across the world continue to find innovative techniques and exploits with which to target and attack Australians. It also revealed the toll such attacks are taking on local businesses.[4]

Some of the report's key findings include:

Over 25,000

calls were made to the Cyber Security Hotline during the reporting period, an average of 69 per day, representing an increase of 15% over the prior financial year.

Fraud, online shopping, and online banking

were the top reported cyber crime types, accounting for 54% of all reports.

The 2021-22

financial year saw a 25% increase in the number of publicly reported software vulnerabilities worldwide.

Anywhere from 150,000 to 200,000

small office or home office routers in Australian homes and small businesses were vulnerable to compromise, including by state actors.

The average cost per cybercrime

reported to the ACSC rose to over $39,000 for small business, $88,000 for medium business, and over $62,000 for large business, representing an average increase of 14% across all business sizes.

The financial

losses due to business email compromise attacks (BEC) increased to more than $98 million, an average loss of $64,000 per report.

The ACSC

responded to 135 ransomware incidents during FY21-22, representing an increase of over 75% compared to the year prior.

CYBERCRIME MAKING HEADLINES IN AUSTRALIA

Cyber attacks have become a major threat to brands in Australia. However, it's not only big business and government entities that are being targeted. Cyber criminals frequently target small and medium-sized organisations in both the private and public spheres.

Below are just a few examples of successful cyber attacks on organisations in Australia:

1. Westmead Hospital:

In May 2023, it was reported that hackers had threatened to release data stolen from the Crown Princess Mary Cancer Centre, part of Westmead Hospital, unless administrators agreed to pay a ransom. Medusa, the group claiming responsibility for the attack, had been actively targeting organisations in Australia and New Zealand since the beginning of 2023.[5]

2. Tasmanian Government:

In April 2023, the Tasmanian Government said it was investigating the theft of data from a third-party file transfer service used by the Tasmanian Department for Education, Children and Young People, with the state's Minister for Science and Technology, Madeleine Ogilvie, revealing that 16,000 stolen documents had been released by the hackers behind the attack.[6]

3. Latitude Financial:

In March 2023, Latitude, an Australian company that issues consumer loans and runs a "buy now, pay later" scheme used by major retailers, disclosed that hackers had stolen the personal information of over 14 million customers, including driver's licences, passport numbers, and financial statements.[7]

4. Medibank:

In October 2022, local health insurer Medibank revealed it had detected unusual activity on its network after a cyber criminal accessed its systems with a stolen Medibank username and password used by a third-party IT service provider. The records of millions of customers were compromised in the attack.[8]

5. Optus:

In September 2022, the internal network of telecommunications carrier Optus was breached in a cyber attack, with the data of nearly 10 million customers leaked, including names, dates of birth, phone numbers, email addresses, and, for a subset of customers, addresses and sensitive ID documents.[9]

As these examples highlight, the consequences of a cyber attack can be devastating for organisations and their customers, and can result in financial losses, reputational damage, and the loss or release of highly sensitive data.

Financial losses in Australia from business email compromise attacks alone came to nearly $100 million in the twelve months ending June 2022, the ACSC revealed in its Annual Cyber Threat Report.

Moreover, the damage from data theft specifically can go well beyond reputation alone, with a number of high-profile brands facing potentially expensive class actions following the breach and subsequent theft of sensitive customer data.

According to the Office of the Australian Information Commissioner (OAIC), of 40 data breaches that affected over 5,000 Australians in the six months to June 2022, the vast majority – 33 – were the result of cyber security incidents.

Against this backdrop, it is clear that there is a real need for businesses of all sizes to prioritise cybersecurity and invest in robust security measures to protect against cyber threats.

DEVELOPING A COMPREHENSIVE CYBERSECURITY STRATEGY

Developing a comprehensive cybersecurity strategy is critical to protect your organisation from the growing number and sophistication of cyber threats. A comprehensive strategy should include risk assessment, an incident response plan, and a security awareness program.

Assess Your Risk

Conducting a thorough risk assessment is essential for identifying the potential cybersecurity risks that a business may face. This process involves evaluating the organisation's assets, identifying vulnerabilities, and determining the potential impact of a cybersecurity breach. This information is critical in developing an effective cybersecurity strategy that addresses the most significant risks.

Plan Ahead

Developing an incident response plan is important to ensure that the business can quickly and effectively respond to a cybersecurity incident. This plan should outline the steps to be taken in the event of a breach, including how to contain the incident, notify stakeholders, and recover from the breach.

Spread the Word

Finally, establishing a security awareness program is critical for building a cybersecurity culture within the organisation. This program should involve all employees in the process of protecting the organisation's assets, including training on best practices for password management, safe browsing, and social engineering awareness.

Additionally, encouraging employees to report security incidents and providing a clear reporting process can help identify potential threats and minimise the impact of a cybersecurity breach. It may also be necessary to restrict access to certain software, especially that which uses cloud storage, exclusively to employees who have been trained on it as a preventative measure against potential system-wide damages resulting from errors made by untrained personnel.

Building a cybersecurity culture within the organisation is crucial for the success of any cybersecurity strategy. Business leaders should involve all employees in the process and encourage them to take an active role in protecting the organisation's assets. This includes providing regular training, promoting awareness of cybersecurity threats, and encouraging employees to report security incidents.

USING LICENSED SOFTWARE AND ENSURING COMPLIANCE

One highly effective measure businesses in Australia can take to reduce the risk of cybersecurity threats is to exclusively use licensed software. Not only does this help to ensure software being used by a business and its employees is up-to-date with the latest security patches to avoid the exploitation by cyber criminals of zero-day vulnerabilities, but it also helps to ensure compliance with Australian law.

The use of unlicensed software can lead to both cybersecurity and legal risks, with the potential for serious financial and organisational consequences such as malware extortion, data breaches, and reputational damage.

Below are some best practices for businesses to adopt and manage licensed software assets:

Obtain it legitimately.

It's important to buy software from legal vendors with genuine licences. Unlicensed software is often distributed through unofficial channels and can contain viruses, trojans, and other types of malware. This malware can then infect the organisation's network and cause significant damage, including data theft, system crashes, and ransomware attacks.

Maintain it.

Software maintenance is critical to ensuring the security and optimal performance of software. Software updates frequently fix bugs and vulnerabilities, so keeping your software updated to the latest version can prevent cybersecurity risks and ensure compliance with vendor requirements. This includes renewing licences as needed for service-based software.

Centralise it.

Software procurement should be managed through a centralised process to ensure that only licenced software is purchased, which means conducting due diligence on software vendors to ensure that they are reputable and compliant with Australian intellectual property (IP) law, in which software piracy features prominently.

For example, it is an offence to knowingly possess a computer program that has been copied illegally in infringement of the Copyright Act 1968. Corporations are liable for penalties of up to $585,000 and a possible imprisonment term for infringing the law.

This is why it is essential for business leaders in Australia to be aware of the terms and conditions of software licences to ensure compliance with vendor requirements. Software deployment should also be managed through a centralised process to ensure that software is installed only on authorised devices. This includes creating a software inventory to keep track of licences and ensure that they're not overused.

Take advantage of free tools.

The BSA Legalise and Protect campaign is an initiative that aims to raise awareness of the importance of using licensed software and reduce the use of unlicensed software in Australia.

Using licensed software is not only important for preventing cybersecurity risks, but also for ensuring compliance with Australian law. The use of unlicensed software is illegal and can lead to significant consequences, including hefty fines and legal action due to IP infringement. It is important that business leaders take steps to ensure compliance by conducting regular audits of software licences, keeping accurate records, and maintaining up-to-date software inventories.

UNDER-LICENSING

Legal, licensed, and updated software can provide the first line of defence against cyber criminals seeking access to corporate data or information about a business' customers.

As such, using under-licensed and unsupported software poses significant cyber risks for businesses. Unsupported software, for example, does not receive updates or security patches to protect against known vulnerabilities. Moreover, cyber criminals can take advantage of out-of-date software to install malware or collect data, as it's much easier for them to exploit known weaknesses than it is to search for new ones.

You may have under-licensed software and not know it. Some IT professionals fail to use the licensed software that their companies purchase, or continue to use software after its licence has expired. Both practices have the potential to put organisations at significant risk.

Furthermore, cyber criminals often exploit unlicensed or unsupported software as a means to access a wider network. They can use known vulnerabilities in older versions of software to penetrate a system, then use that access to move laterally through the network in search of valuable data to steal or systems to compromise.

One of the simplest ways for businesses to mitigate these risks is to ensure that they have properly licensed software that is up to date with the latest patches and security updates. Regular software audits can help ensure compliance and identify any unsupported or under-licensed software.

BUILDING A CYBERSECURITY CULTURE

Building a strong cybersecurity culture is critical to protecting organisations in Australia against cyber threats. While government efforts are being undertaken at both the federal and state levels to help foster a stronger cybersecurity culture in Australia, business leaders can also play a role by implementing strategies that promote a cybersecurity culture within their organisations.

Here are some effective strategies that can help to build a strong cybersecurity culture:

Raise Awareness

Regular training and awareness programs are essential to educate employees on the importance of cybersecurity and the risks associated with cyber attacks. This includes educating employees on safe internet practices, identifying phishing emails, and creating strong passwords. Training and awareness programs can be delivered in various formats, such as in-person training, online training, and company-wide emails.

Form a Team

Establishing a security committee or team can help create a security-conscious culture within the organisation. The security team can provide guidance, resources, and support to employees on cybersecurity-related issues. It can also conduct regular security assessments and provide recommendations for improving security protocols.

Clarify the Process

Business leaders should establish a reporting process that empowers employees to report issues and ensures the reports are investigated and addressed. Open communication about security issues is crucial to building a cybersecurity culture. Encourage employees to feel comfortable reporting security incidents and raising security concerns, and make sure they know to whom or on which platform they should report such issues. Recognition and rewards, such as congratulating the employee who finds the most vulnerabilities each quarter and/or offering a bonus for top reporters, can go a long way towards inspiring people to care about the business' cybersecurity.

Set an Example

Leadership plays a crucial role in promoting a culture of cybersecurity and software compliance within the organisation. Business leaders are in a prime position to lead by example and make cybersecurity a top priority. This can be achieved by regularly communicating about cyber risks and the importance of compliance, allocating resources to support cybersecurity initiatives, and encouraging employees to report security incidents.

PRACTICAL STEPS TO MAKE YOUR BUSINESS SAFER

A proactive and comprehensive approach by business leaders can help to protect their organisations – and themselves – against cyber threats.

Here are some practical steps that CEOs and top decision makers can take to achieve such an approach:

1. Conduct Regular Security Audits

Conducting regular security audits can help businesses identify potential vulnerabilities in their systems and networks. Businesses that can identify and assess potential risks can prioritise security improvements based on their criticality.

2. Establish a Security Budget

Establishing a dedicated budget for cybersecurity can help businesses allocate resources to the most critical areas. It is important to ensure that the budget is adequate to meet the organisation's needs, and that it is reviewed regularly.

3. Partner with Trusted Security Providers

Partnering with trusted security providers can help businesses improve their cybersecurity posture. Security providers can offer a range of services such as network security, threat detection and response, and training for employees.

4. Implement Software Compliance

Implementing software compliance can help businesses avoid legal and financial risks associated with using unlicensed software. Organisations should keep track of software assets, implement regular software updates and patches, and conduct regular audits to ensure compliance.

5. Establish an Incident Response Plan

Establishing an incident response plan that outlines the steps to be taken in the event of a security breach can help businesses minimise the fallout after an attack. An incident response plan should include steps for reporting incidents, investigation procedures, and communication protocols.

CONCLUSION

As noted by the ACSC in its FY2021-22 Annual Threat Report, Australia has seen an increase in the number and sophistication of cyber threats, with crimes like extortion, espionage, and fraud becoming easier to replicate at a greater scale.

However, Australian businesses and their leaders, regardless of size and industry, can better protect themselves by prioritising cybersecurity and taking proactive measures to minimise the danger that cyber threats pose. Indeed, in today's environment, such an approach is a necessity.

> “For businesses these days, cybersecurity is as important and essential as the shop having a lock on the door. We need all Australian businesses to be able to protect themselves and – just as importantly – protect their customers.”
>
> ***—Australian Prime Minister Anthony Albanese at a government-led cyber security roundtable event in early 2023.***[10]

Likewise, we should all recognise that cybersecurity is an essential part of doing business today. As such, we hope that this guide provides a helpful starting point from which to implement an effective cybersecurity strategy that can underpin and strengthen your business into the future.

1 Conduct regular cybersecurity audits to identify potential vulnerabilities.

2 Establish a cybersecurity budget and review it regularly.

3 Partner with trusted cybersecurity providers for services such as network security, threat detection and response, and employee training.

4 Promote a culture of cyber responsibility within your organisation.

5 Educate your employees on what cybersecurity threats look like and how they can avoid them.

6 Create an easy method for employees to report cybersecurity issues and incentivise them to do so.

7 Keep all of your software licensed and up to date.

8 Plan ahead for how you will respond in the event of a security breach.

These steps are a good start, but they are only the beginning of a cybersecurity journey. It is important to remember that cybersecurity is an ongoing process that requires continuous monitoring, assessment, and improvement.

Staying informed about the latest cybersecurity trends and threats is vital to ensuring that your organisation's security measures remain effective over time. The evolution of cybersecurity threats is ongoing, so the measures taken to defend against them also need to be ongoing and constantly evolving.

But by taking proactive measures today and promoting a culture of cybersecurity going forward, you can protect your organisation and customers from both cyber threats and the legal, financial, and reputational risks arising from them.

REFERENCES

1,4 Australia Cyber Security Centre. (2022). *Annual Cyber Threat Report,*
https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf

2 Australian Government Department of Home Affairs. (2023). *2023-2030 Australian Cyber Security Strategy,*
https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy

3 ABC News. (2023). *Experts say AI scams are on the rise as criminals use voice cloning, phishing and technologies like ChatGPT to trick people*
https://www.abc.net.au/news/2023-04-12/artificial-intelligence-ai-scams-voice-cloning-phishing-chatgpt/102064086

5 ABC News. (2023). *Crown Princess Mary Cancer Centre in Westmead Hospital in cyber attack, hackers threatening to release stolen data,*
https://www.abc.net.au/news/2023-05-04/crown-princess-mary-cancer-centre-being-hacked/102305996

6 Tasmanian Government. (2023). *Update on cyber investigation,*
https://www.premier.tas.gov.au/site_resources_2015/additional_releases/update-on-cyber-investigation3

7 The Guardian. (2023). *Latitude Financial cyber-attack worse than first thought with 14m customer records stolen,*
https://www.theguardian.com/australia-news/2023/mar/27/latitude-financial-cyber-data-breach-hack-14m-customer-records-stolen

8 Medibank. (2023). *Cyber event timeline,*
https://www.medibank.com.au/health-insurance/info/cyber-security/timeline/

9 Optus. (2023). *Latest updates & support on our cyber response,*
https://www.optus.com.au/support/cyberresponse

10 Australian Government. (2023). *Prime Minister's Cyber Security Roundtable,*
https://minister.homeaffairs.gov.au/ClareONeil/Pages/prime-minister-cyber-security-roundtable.aspx