Cyber security basics *for small businesses*

Produced by BizCover
May 2018

BizCover

Contents

Introduction

WITH SMALL BUSINESSES BEING THE TARGET OF FORTY THREE PERCENT OF ALL CYBERCRIMES IN AUSTRALIA, GONE ARE THE DAYS WHEN SMALL BUSINESS OWNERS CAN SIMPLY IGNORE THE IMPORTANCE OF CYBER SECURITY ISSUES.[1]

As cyber breaches continue to emerge as one of the top risks for businesses of all shapes and sizes, it's time for SME's to put cyber security on the agenda and develop strategies to minimise their risk of becoming the next victim of cybercrime.

However, before implementing a sound cyber security strategy, it is important to understand the types of cyber threats that exist, and how they can affect your industry and business operations.

No business is considered too small to avoid being a target for cybercriminals. As we continue to become more reliant on technology, the more we create, collect and share information online, and the more our vulnerability increases.

Our aim is to increase cyber security awareness among small business owners to assist you in identifying

ways to protect your business

what is at stake

what you can do

to ensure your business recovers in the event of a cyber attack or data breach.

CYBERCRIME CAN BE DESCRIBED AS ANY DECEPTIVE OR CRIMINAL ACTIVITY IN WHICH A COMPUTER OR NETWORK-CONNECTED DEVICE SUCH AS A MOBILE PHONE, IS USED AS A TOOL TO COMMIT A CYBER OFFENCE, FOR EXAMPLE, GAINING UNAUTHORISED ACCESS TO PERSONAL AND BUSINESS INFORMATION FOR EXPLOITIVE OR MALICIOUS PURPOSES. THOSE WHO TAKE PART IN CYBERCRIME ARE OFTEN REFERRED TO AS 'HACKERS'.

Demystifying ***cybercrime and cyber attacks***

There are many ways in which hackers commit cybercrime, including: [2]

- the deliberate distribution of malicious software or viruses, such as malware, spyware and ransomware which can cripple or halt access to your systems
- online phone scams
- theft of critical business information and data, or hacking of a business' system to obtain customer details or gain access to a supplier's network
- fake over payments
- fake invoicing

In recent years, there has been a significant growth in the number and severity of cyber attacks, both globally and in Australia. There is no common motive in cybercrime, and victims of cyber attacks can be random or targeted. Cyber criminals may be an individual or a group of people, and their intentions can be driven by political, religious, economic, and in some cases socio-cultural reasons.

It is a common misconception that cyber criminals focus their actions on government and larger organisations because they have more information to steal and bigger profits to tap into. When in fact, reality is that SME's have fast become the preferred target for many hackers due to their lack of resources to invest in robust security and limited expertise in understanding their cyber exposures. SME data is also more valuable than people assume, especially considering the type of personal information they may store about their customers, such as contact details, birth dates and credit card or bank account details. They may also be used as a pivot point into the integrated supply chain of their valued partners and suppliers.[3]

Nearly half of all Australian cyber attacks are aimed at small and medium sized businesses, with research showing that of those who are hacked, a further sixty percent go out of business within six months due to the financial implications that the attack has on their business.[4]

Who could be a ***threat to your business?***

Criminals

who illegally access your systems and disrupt your business for financial gain or other information, including personal information about your customers or clients

Clients

those you do business with who compromise your information with malicious intent

Competitors

looking to obtain inside information to gain advantage over your business

Employees

Current or former employees – who accidentally or intentionally compromise your information or data

Opportunistic hackers

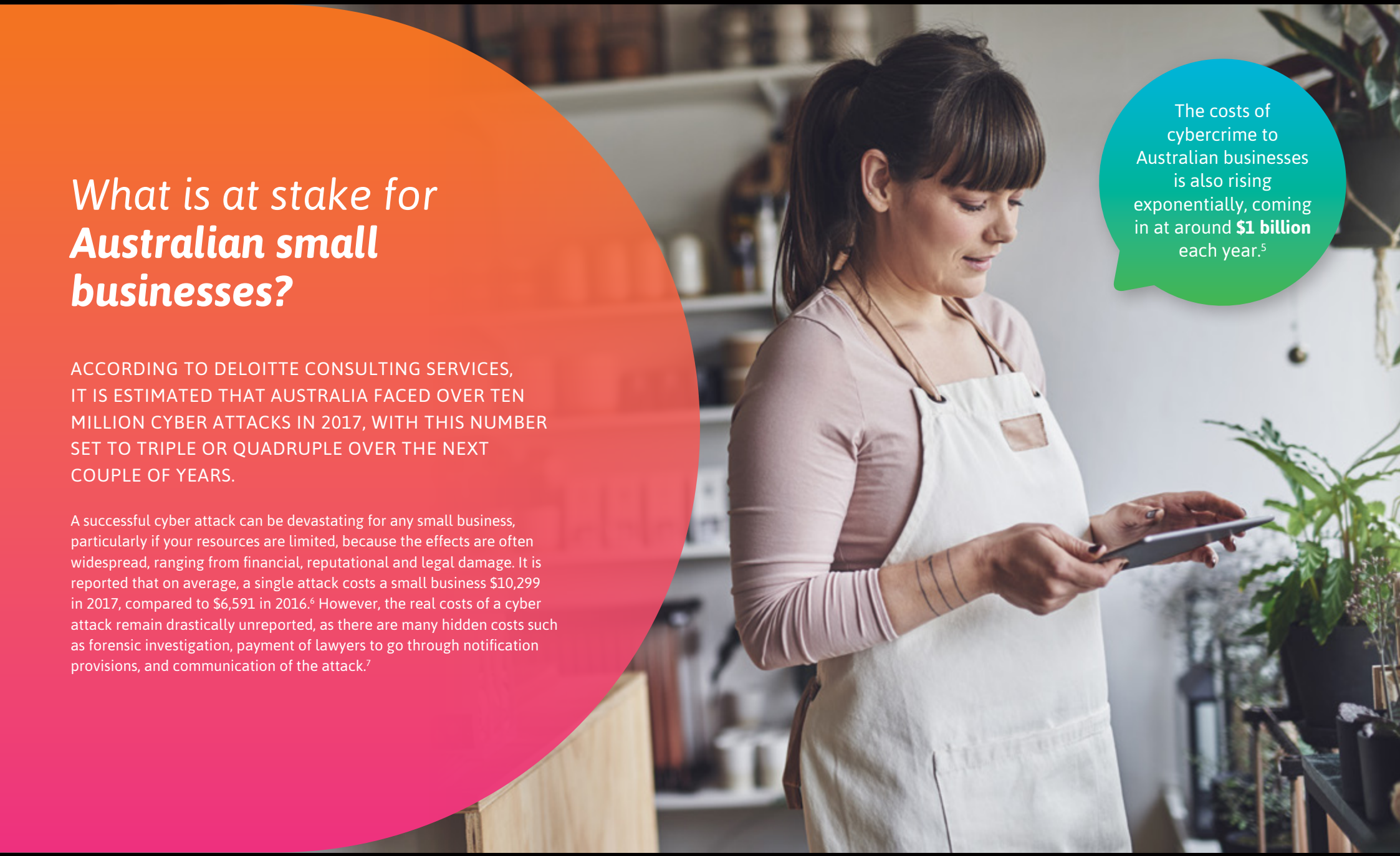
that may gain access to your information via lost or stolen devices, such as laptops or mobile phones

Source: www.business.gov.au/info/run/cyber-security

What is at stake for ***Australian small businesses?***

ACCORDING TO DELOITTE CONSULTING SERVICES, IT IS ESTIMATED THAT AUSTRALIA FACED OVER TEN MILLION CYBER ATTACKS IN 2017, WITH THIS NUMBER SET TO TRIPLE OR QUADRUPLE OVER THE NEXT COUPLE OF YEARS.

A successful cyber attack can be devastating for any small business, particularly if your resources are limited, because the effects are often widespread, ranging from financial, reputational and legal damage. It is reported that on average, a single attack costs a small business $10,299 in 2017, compared to $6,591 in 2016.[6] However, the real costs of a cyber attack remain drastically unreported, as there are many hidden costs such as forensic investigation, payment of lawyers to go through notification provisions, and communication of the attack.[7]



The costs of cybercrime to Australian businesses is also rising exponentially, coming in at around **$1 billion** each year.[5]

The impact of a cyber attack can be divided into three main categories:

Economic costs

Financial loss arising from a cyber attack can include:

- theft or extortion of money
- theft of business information, such as business and marketing plans, intellectual property, employee records and customer data
- theft of financial information, such as financial records, bank details or payment card details
- disruption to business operations resulting in lost productivity, including time involved in notifying the relevant authorities those whose information has been compromised
- loss of business contracts
- costs incurred with getting your affected systems up and running, such as forensic investigation, repair and restoration of affected systems, networks and devices

Reputational damage

A data breach can damage your business reputation and can even impact relationships you may have with suppliers, investors and other third parties, potentially leading to:

- loss of customers
- loss of business partnerships
- loss of sales
- reduction in profits

Legal consequences

The handling of personal information and data in Australia is governed by both federal and state legislation. If this data is compromised, whether accidentally or deliberately, you may face fines and penalties, as well as other legal action that can result in legal costs and compensation.

Startling Statistics

Australia faced over **10 million cyber attacks** in 2017

(Deloitte Consulting Services Study, 2017)

88% of targeted malware (i.e. a virus) remains undetected by traditional anti-virus software.

(Inside a Hacker's Playbook, Trustwave, 2013)

19% or **40,000** Australia's 2.1 million SME's have suffered a cyber attack.

(Norton SMB Cyber Security Survey, 2017)

The cost of cyber crime to **Australian businesses** is estimated at

$1b

per year, and rising exponentially.

(Cyber Scare Report, NSW Small Business Commissioner, May 2017)

79%

1

79% of businesses consider reputational damage as their most significant risk from a cyber attack...

75%

2

...followed by business interruption (75%)...

60%

3

...and increased legal and regulatory costs (60%).

(How to limit reputational cyber damage, Insurance Business Australia, 2018)

ONLY **38%** of SME's would contact IT forensic consultants for assistance following a cyber attack

(Cyber Scare Report, NSW Small Business Commissioner, May 2017)

$10,299 is the average cost of a cyber attack for an Australian small business

(Norton SMB Cyber Security Survey, 2017)

60% **of small businesses** who experience a significant cyber breach go out of business within 6 months.

(The Small Business Cyber Security Best Practice Guide, Australian Small Business and Family Enterprise mbudsman, 2018)

Over **one million** pieces of malware are created everyday.

(Symantec Internet Security Report, April 2015)

Small businesses are the target of **43% of all cybercrimes** in Australia.

(Australian Small Business and Family Enterprise Ombudsman, 2018)

23% of recipients open a phishing email and **11% click on attachments.**

(Verizon Data Breach Investigations Report, 2015)

How do cyber criminals ***gain entry?***

Cyber attacks come in many different forms and cyber criminals are increasingly developing more creative and sophisticated ways to gain access to confidential business and customer data.

The type of attack is typically driven by the type of information the hacker is after. However, internal breaches can also occur as a result of someone inside your business, whether accidental or deliberate. Some of the more common ways in which small business can be compromised are outlined below.

Internal Threats

An internal or 'insider' threat can be defined as "*a current or former employee, contractor or business partner with access to the organisation's network, system or data who intentionally or inadvertently misuses them*".[8]

According to Ernst & Young, an international accounting firm, most internal breaches are due to accidental or negligent actions whereby employees make honest mistakes, lack education in cyber security best practice, such as opening a phishing email, or taking shortcuts for convenience, including emailing sensitive information or using file sharing services.[9]

Malicious attacks occur when disgruntled current or former employees gain access to systems and confidential information with the intent to carry out a personal vendetta or steal intellectual property for financially motivated reasons.

It is important to note that whether a breach is malicious or unintentional, the effects it has on a business are parallel.

External Threats

External hackers look for ways to enter your system to acquire information that they can then either sell on the black market to make a profit or hold to ransom, for usually a large specified amount. An external attack can take place in the following forms:

Phishing Scams

Phishing or Whaling scams have become one of the most common methods that cyber criminals use to gain access to sensitive information, such as bank account numbers, credit card details, usernames and passwords, due to the ease and minimal effort required to execute them.

Typically, a user receives an email, text or phone call claiming to be from a legitimate organisation that the business uses, for example a telephone or internet provider, directing them to a fake website to either "verify" or "re-submit" their information. Once the information is provided, the criminals use it to gain access to personal or business accounts.

Malware

Malware (short for malicious software) is a program, such as a virus, worm or trojan or spyware, that is specifically designed to infect a digital device, with the intention of disrupting, damaging or gaining unauthorised access to a computer system (cyber espionage).[10]

Depending on the type of malware, it has the potential to destroy your system operating files, allow another user access to your computer, or track your activity, monitor your browsing activity or even record your keystrokes.

Ransomware

Ransomware is another type of malware which is used for digital extortion. Like other types of malware, it can infect your system by clicking on a malicious link in an email or opening an attachment. Once downloaded to your computer or other digital device they make your system inoperable by blocking access to your files and programs and demand that a ransom is paid. However, it is generally advisable not to pay ransoms as there is no guarantee that the defendant will restore systems and data upon payment.

Denial of Service (DoS)

To conduct a Denial of Service attack, the perpetrator attempts to prevent legitimate users from accessing the service by flooding the network with requests to overload it and ultimately make it crash. However, these kinds of attacks usually target larger companies and organisations.

Password Attacks

A Password Attack, also known as 'Brute Force Attack', is the penetration of a network or system whereby the attacker gains access by searching for vulnerabilities, such as cracking a user's password.[11]

Rather than infecting the victim's network with malicious software, the hacker often uses specifically designed software on their own system to try to crack your passwords with a trial-and-error method, usually with a good success rate.

Payment Card Skimming & Point of Sale Intrusions

Payment card skimming is where cybercriminals fit an additional card reader to physical point-of-sale equipment which then reads and records data from the magnetic strip, including the primary card number, security code, and other information such as the types of charges that are permitted.

A point of sale (POS) intrusion, on the other hand, is a remote attack involving memory scraping malware on point-of-sale systems that looks for data in the correct format, i.e. credit card information, and gathers it instantly when detected. The information is then sent to the attacker's computer.

Both methods aim to steal payment card information to then sell on the black market as opposed to using it directly. However, point-of-sale malware is a much simpler way of obtaining payment card information, hence why it is now one of the biggest sources of stolen payment card data for cybercriminals.[12]

Physical Theft & Loss

Loss of devices (laptops, tablets, mobile phones, and storage devices), whether accidental or through malicious intent, combined with the lack of encryption on those devices, can pose a significant security threat if they get into the hands of someone with ill intent. Confidential information, including intellectual property, business data or customer data, may be accessible on these devices resulting in a data breach that costly, both financially and reputationally.

Most common types of cyber incidents by industry

Accommodation & Food Services

- Point of sale intrusions
- Phishing scams (malicious emails)
- Insider/ privilege misuse

External threats account for 96% of breaches where cyber criminals are looking for payment data, e.g. credit card information.

Educational Services

- Targeted phishing campaigns
- Malware / cyber espionage
- Internal breaches (accidental/ negligent actions)

Around 70% of all breaches come from external threats where 56% of data compromised is of a personal nature and 27% inside secrets.

Financial and Insurance Services

- Denial of service attacks (DoS)
- Web application attacks
- Payment card skimmers

These account for 88% of data breach incidents, mostly from external threats looking for financial information.

Healthcare

- Insider/ privilege misuse and accidental errors
- Physical theft and loss
- Malicious emails

Alarmingly, 68% of all breaches come from internal sources where employees access patient data out of curiosity, or to commit identity fraud.

Information Technology

- Denial of service attacks (DoS)
- Web application attacks
- Malware

90% of all breaches within the information technology sector come from external threats, with 75% being financially motivated.

Manufacturing

- Cyber espionage
- Insider/ privilege misuse

The majority of breaches (96%) within the manufacturing industry are related to strategic advantage gains, i.e. theft of intellectual property and trade secrets, with 93% coming from external sources.

Retail

- Denial of service (DoS)
- Web application attacks
- Payment card skimming

Retailers are consistently targets of DoS and payment skimming attacks, accounting for 92% of all threats due to financial motivations.

Source: Verizon '2017 Data Breach Investigations Report: 10th Edition

How can ***small businesses protect themselves?***

AT THE VERY LEAST, MOST SMALL BUSINESSES HAVE A WEBSITE AND USE EMAIL, CONSEQUENTLY EXPOSING THEMSELVES TO CYBER ATTACKS AND DATA BREACHES.

Fortunately, there are a few simple steps you can take to limit your exposure and protect your business. Getting the basics right can have a great impact on the survival of your business, before and after a cyber attack. See what you can do on the following pages.

1. Understand your risks

With the nature of cyber attacks changing every day, knowing the various types of threats and how they could impact your business is the first step in minimising and managing a potential attack.

The next step is to try to understand your risks and the security gaps within your business by carrying out a comprehensive cyber risk assessment, so you can then prioritise which actions to adopt. Start by asking yourself the following questions:

- What are the top cyber risks within your industry?
- Who would benefit from having access to your systems and the information you hold?
- What information about your business is publicly available?
- What types of confidential and sensitive information and data do you hold?
- Who in your business has access to certain types of data?
- What digital assets in your business could you not operate without?
- What are the potential effects of downtime and the costs involved if you were to suffer a serious cyber incident?

2. Secure your network

Use a firewall and encrypting information to protect your internet connection and set up your Wi-Fi connection so that it does not broadcast your network name, or Service Set Identifier (SSID). Always ensure access to your router is protected with a password.

3. Update IT equipment and software

Regularly updating your IT equipment, operating systems and software is crucial. Outdated computers and operating systems can pose a huge risk as they are easily compromised by cyber criminals.

In addition, most apps have bugs that make you vulnerable to hackers, so ensure you keep up to date with the latest versions and patches.

4. Install security software

One of the best ways to protect your business from malware is to install anti-virus software to recognise and prevent unauthorised connections and update it regularly to detect the latest threats.

It's a good idea to run a full scan of your system when you first install anti-virus software to ensure there are no pre-existing viruses.

5. Back up

No small business should be without a reliable backup solution. Protect your important files and data by backing it up and storing it in a secure off-site location, or to a cloud-based service.

Either set up automatic back-ups, or do it daily or weekly, and conduct regular checks to verify that it has been done correctly.

6. Educate staff

Educate your staff about online threats and cyber security best practices, such as how to spot phishing scams and ransomware attacks, being aware of suspicious websites, and to never open email attachments from unknown sources.

7. Implement cyber security policies and procedures

Establish a formally written "security rules" document and ensure it is adhered to. You can include things such as the following:

- only allowing strong passwords to be used such as catchphrases or passphrases to access all computers, devices and applications, and making sure they are changed regularly
- appropriate internet and social media use. For example, no sharing of business information via personal social media sites
- not allowing personally owned devices to be connected to the business network
- rules for handling and storing sensitive and personally identifiable information
- reporting of all suspicious or scam emails.

In addition, establish seniority and only provide access to sensitive business information to those who require it to carry out their job.

8. Adopt a cyber incident response plan

Make it a top priority to prepare a cyber response plan so that you can respond to an incident fast and effectively. Incidents that aren't responded to quickly further expose your business to major disruptions and legal issues.[13]

The Australian Government has published some great resources on how to create a **Cyber Incident Response Plan**.

9. Have a safety net

In addition to the above steps, consider obtaining Cyber Liability insurance to further mitigate any loss and risk to your business in the event of a cyber attack or security breach.

Policies vary, but can reduce financial losses incurred, and can also provide a dedicated cyber breach response team to provide expert assistance in the event of a claim.

What is the ***Notifiable Data Breaches Scheme?***

AUSTRALIA'S NEW NOTIFIABLE DATA BEACHES (NDB) SCHEME CAME INTO EFFECT ON 22ND FEBRUARY 2018, AND ESTABLISHED REQUIREMENTS FOR ENTITIES THAT ARE GOVERNED BY THE PRIVACY ACT TO REPORT ANY DATA BREACH WHICH IS LIKELY TO RESULT IN SERIOUS HARM TO THE OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER (OAIC), AS WELL AS NOTIFYING ALL AFFECTED INDIVIDUALS.

What is the purpose of the NDB scheme?

The purpose of the NDB scheme is to strengthen the protection afforded to everyone's personal information and provide greater confidence within the community that their personal information is respected and handled with care.

It also aims to encourage Australian organisations to implement a higher standard of information security and improve transparency in the way that serious data breaches are responded to.[14]

Who does it apply to?

The NDB laws apply to all businesses, government agencies and not-for-profit organisations that have an annual turnover or have had an annual turnover in any financial year since 2002, of over $3,000,000.

It also applies to any small business operator (SBO), including sole traders, with an annual turnover of $3 million or less if they have obligations under the Australian Privacy Principles (APPs), such as health service providers, credit providers, credit reporting agencies, tax file number recipients, those operating a residential tenancy data base, and any business that has voluntarily opted in to be covered by the Privacy Act.[15]

To assess whether your business needs to comply with the Australian Privacy Principles the OAIC has provided a handy **checklist**.

What is an eligible data breach?

A data breach is defined as "*unauthorised disclosure of, access to or loss of personal information which a reasonable person would believe would likely result in serious harm to the person whose information has been affected*".[16]

Serious harm may be in the form of physical, psychological, emotional, financial or reputational harm, and can include but not limited to, identity theft, financial loss, threats to physical safety and reputational damage.

An eligible data breach occurs when the following criteria are met: [17]

- There is unauthorised access to or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- This is likely to result in serious harm to any of the individuals to whom the information relates.
- The entity has been unable to prevent the likely risk of serious harm with remedial action.

Examples of an eligible data breach include:

- Hackers accessing a database containing personal information
- An email containing personal information is inadvertently sent to the wrong recipient
- An employee or contractor access personal information or makes their own copy without any legitimate purpose
- Any device, such as a laptop or phone, containing personal information is lost or stolen.

What is considered 'Personal Information'?

Defined by the OAIC, personal information is "*information or an opinion that identifies or could reasonably identify an individual, whether true or not, and whether recorded in a material form or not*".[18]

Some examples of personal information are:

- Name
- Signature
- Home address
- Email address
- Telephone number
- Date of birth
- Driver's licence
- Passport
- Tax file information
- Bank account details
- Credit information
- Medicare card details
- Medical records
- Employment details
- Commentary or opinion about a person, e.g. employment referee's comments

Who needs to be notified?

Following an eligible data breach, The Privacy Commissioner and all individuals affected by the breach must be notified as soon as reasonably possible.

If it is not possible to notify individual directly, for example, the entity does not have up-to-date contact details, a statement can be published on the business' website and other reasonable steps to publicise the statement must be made, such as via newspapers, television or digital media.

What needs to be notified?

The notification must include:

- Details of the business, including contact details
- A description of the breach and the type of information affected
- Recommendations that individuals should take in response to the breach, such as cancelling payment cards that have been compromised.

Are there any consequences following an eligible data breach?

If a business fails to notify a data breach, the NDB laws state that a civil penalty can be applied for serious or repeated interferences of an individual's privacy, which attract a maximum fine of $420,000 for individuals and $2,100,000 for businesses.

Further information can be found in the **'Data breach preparation and response'** document on the OAIC website.

Following an eligible data breach, **The Privacy Commissioner and all individuals affected** by the breach must be notified.

What to do in the event of a ***cyber attack or data breach***

What is Cyber Liability insurance *and why do small businesses need it?*

DESPITE THE MEASURES PUT IN PLACE TO AVOID A CYBER ATTACK OR DATA BREACH THE REALITY IS, THAT AS BUSINESSES RELY MORE ON TECHNOLOGY AND CYBER CRIMINALS BECOME MORE SOPHISTICATED, IT'S NOT A CASE OF *IF* YOUR BUSINESS WILL SUFFER A CYBER SECURITY INCIDENT, BUT *WHEN* – PARTICULARLY IF YOUR BUSINESS REQUIRES THE COLLECTION OF CUSTOMER OR CLIENT INFORMATION, INCLUDING PERSONAL DETAILS, CREDIT CARD OR BANK DETAILS.

Even if you do not collect or store personal or financial information, almost every business uses a computer or network leaving it open to being infected by malware or viruses, despite having the latest anti-virus protection and firewalls. Prevention strategies are not fool-proof. Without a reliable safety net in place, such incidents can seriously threaten the financial state of your business and your ability to continue trading.

SME's of any size, including those not bound by the NDB scheme, can be exposed to a cyber incident. Depending on the type and severity of an attack, you may be up for the costs of IT support to unlock and repair your systems, ransoms and legal claims, as well as the costs associated with remediating losses suffered by your customers and the costs of reporting the breach to the OAIC and affected individuals. A study conducted by Clyde & Co found that 18.3 percent of the total costs incurred from a cyber claim are related to Notification costs alone, with the average cost of managing and rectifying a breach being $140 per compromised record[19]. This cost increases significantly for businesses within the financial services and healthcare industries, at $221 and $355 per compromised record respectively[20]. Furthermore, a cyber attack can cost more than just money – it can compromise your intellectual property, jeopardise your customer's private information and cause serious reputational damage to your business.

Whilst Cyber Liability insurance is no substitute for good risk management, it can play a vital role in mitigating losses incurred in the event of a cyber incident by covering your business against the expense and legal costs associated with data breaches and being hacked.

What is covered?

Cyber Liability Insurance can vary between insurers, however, typically, policies cover both first party losses and third-party liabilities that your business can incur as a result of a cyber incident, as well as losses that are incurred due to interruption caused to your business, for example, due to a network or system shutdown.

First Party Losses

Costs your business would incur in the event of a cyber attack or data breach, including::

- ✓ Loss of data and the costs of repairing and restoring systems and data that has been damaged or lost
- ✓ IT forensic investigations to identify the source and nature of an attack, and the extent of the damage
- ✓ Credit monitoring services for affected individuals
- ✓ Cyber extortion costs, i.e. paying ransoms to cyber criminals to unlock and restore your systems
- ✓ Notification costs to alert affected individuals and comply with Notifiable Data Breaches Scheme
- ✓ Legal representation costs
- ✓ PR or crisis management team to mitigate reputational damage

Third Party Liabilities

Claims for compensation by third parties such as customers and suppliers, following a data breach, including:

- ✓ Compensation claims arising from failing to protect personal (customer) information against cyber attacks or misuse
- ✓ Costs of appointing a legal defence team
- ✓ Fines and penalties imposed by regulators, such as the OAIC or ASIC

Business Interruption

Loss of profits your business would incur as a result of a cyber incident, including:

- ✓ Reimbursement for lost profits due to a network or system shutdown
- ✓ Necessary expenses incurred to maintain operation of the business as a result of the interruption

Importantly, taking out Cyber Liability cover can not only provide financial assistance for your business, it offers a dedicated response team of expert cyber specialists who will assist you in the event of a claim, from the initial notification through to a resolution to ensure the best possible outcome for your business.

References

[1] Eddie, T. (2018) *'The Small Business Cyber Security Best Practices Guide'*. [online] Australian Small Business and Family Enterprise Ombudsman. Available at: http://www.asbfeo.gov.au/sites/default/files/documents/ASBFEO-cyber-security-guide.pdf

[2] Industry.nsw.gov.au (2017). *'Cyber Aware: Report into the perceptions of, attitudes to and preparedness for cybercrime amongst Australian small and medium-sized enterprises'*. [online] Available at: https://www.industry.nsw.gov.au/__data/assets/pdf_file/0005/134933/Cyber-Aware-full-report.pdf

[3] Dual Australia (2018). *'Cyber Liability & Privacy Protection'*. [online] Available at: https://cdn2.hubspot.net/hubfs/2597761/DUAL%20Australia/AUS%20Assets/Docs/Cyber_Liability__Privacy_Protection_Profile_0914_V2.pdf

[4] Steadfast (2018). *'Cyber Protection Insurance at a Glance'*. [online] Available at: https://broker.steadfast.com.au/au/news/20170518/new-fact-sheet.aspx

[5] Industry.nsw.gov.au (2017). *'Cyber Scare: A look at small to medium-sized business and the emergence of cybercrime in Australia'*. [online] Available at: https://www.industry.nsw.gov.au/__data/assets/pdf_file/0003/134931/cyber-scare-full-report.pdf

[6] Symantec (2017). *'Norton SMB Cyber Security Survey Australia'*. [online] Available at: http://now.symassets.com/content/dam/content/en-au/collaterals/datasheets/cybersecurity-simplified.pdf

[7] Moorcraft, B. (2017). *'Cyberattack reports just 'tip of the iceberg' says QBE'*. [online] Insurance Business. Available at: https://www.insurancebusinessmag.com/au/news/breaking-news/cyberattack-reports-just-tip-of-the-iceberg-says-qbe-84263.aspx

[8] Cytex Cyber Security (2018). *'Internal vs. External Cyber Threats: what you need to know'*. [online] Available at: http://www.cytex.co.za/internal-vs-external-cyber-threats-need-know/

[9] Ernst & Young (2016). *'The internal cyber threat: employees'*. [online] Available at: https://consulting.ey.com/the-internal-cyber-threat-employees/

[10] Norton (2015). *'What is Malware?'*. [online] Available at: https://uk.norton.com/norton-blog/2015/10/mobile_malware_eve.html

[11] Sullivan, M. (2018). *'8 Types of Cyber Attacks Your Business Needs to Avoid'*. [online] Quickbooks. Available at: https://quickbooks.intuit.com/r/technology-and-security/8-types-of-cyber-attacks-your-business-needs-to-avoid/

[12] Symantec (2014). *'Security Response: a special report on attacks on point-of-sale systems'*. [online] Available at: https://www.symantec.com/content/dam/symantec/docs/white-papers/attacks-on-point-of-sale-systems-en.pdf

[13] Australian Government (2017). *'Prepare a cyber security incident response management plan'*. [online] Available at: https://www.business.gov.au/Info/Run/Cyber-Security/Prepare-a-cyber-security-incident-response-management-plan

[14] Office of the Australian Information Commissioner (2017). *'Mandatory data breach notification'*. [online] Australian Government. Available at: https://www.oaic.gov.au/media-and-speeches/statements/mandatory-data-breach-notification

[15] Office of the Australian Information Commissioner (2017). *'Entities covered by the NDB scheme'*. [online] Australian Government. Available at: https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/entities-covered-by-the-ndb-scheme

[16] Richardson, B. (2017). *'Out of the Shadows: Data breach mandatory reporting and cyber insurance'*. [online] QBE Insurance. Available at: https://www.qbe.com.au/about/contact-alerts/media-centre/press-releases/qbe-releases-white-paper-on-cyber-risk

[17] Office of the Australian Information Commissioner (2018). *'Data breach preparation and response: a guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)'*. [online] Australian Government. Available at: https://www.oaic.gov.au/resources/agencies-and-organisations/guides/data-breach-preparation-and-response.pdf

[18] Office of the Australian Information Commissioner (2015). *'Privacy business resource 10: Does my small business need to comply with the Privacy Act?'*. [online] Australian Government. Available at: https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-10

[19] Pokarier, M. & Di Macro, B. (2017). *'What are the financial exposures for organisations following Australia's Data Notification Law?'*. [online] Clyde&Co. Available at: https://www.clydeco.com/insight/article/what-are-the-financial-exposures-for-organisations-following-australias-dat

[20] Ponemon Institute (2018). *'The Third Annual Study on the Cyber Resilient Organisation (Australia)'*. [online] Available at: http://public.dhe.ibm.com/software/au/pdf/Ponemon_Cyber_Resilient_Study_Australia.pdf

BizCover

In a nutshell, your customer data is sacred.

GET INSTANT CYBER LIABILITY INSURANCE QUOTES TODAY

1300 249 268 bizcover.com.au