Australian Government

Australian Small Business and Family Enterprise Ombudsman

Cyber Security: The Small Business Best Practice Guide

"Rule one: Do not own a computer. Rule two: Do not power it on. Rule three: Do not use it."

National Security Agency cryptographer Robert Morris

Manager
Communications and Marketing
Australian Small Business and Family Enterprise Ombudsman
02 6263 1500
media@asbfeo.gov.au

Primary Author Tom Eddie, Analyst

CONTENTS

1. INTRODUCTION AND APPROACH

Cyber security is a big problem for small business

- Small business is the target of 43% of all cybercrimes.[1]
- 60% of small businesses who experience a significant cyber breach go out of business within 6 months.[2]
- 22% of small businesses that were breached by the 2017 Ransomware attacks were so affected they could not continue operating.[3]
- 33% of businesses with fewer than 100 employees don't take proactive measures against cyber security breaches.[4]
- 87% of small businesses believe their business is safe from cyberattacks because they use antivirus software alone.[5]
- Cybercrime costs the Australian economy more than $1 billion annually.[6]

What is cyber security and how does it apply to my business?

Cyber security is the protection of information and digital assets from compromise, theft or loss, whether from a determined attacker outside, or an insider threat within your business. **It is security as it relates to the risks of being online**. For example, if you have commercial assets or personal information stored on smart phones, computers, hard drives or online, they are at risk. If you do business online, you could be the victim of hacking. If you or your staff use web-based software, you could be inadvertently putting your business and your customers at further risk.

Cyberattacks can occur in countless different ways, and they are multiplying daily, so **you can never be 100% safe**. Business is being conducted more digitally in all sectors, so cyber security must be made a priority. Think about cyber security in the same way you think about regular security such as locking the door when you leave the office, or not sharing trade secrets with your competitors.

Small business faces a unique risk when it comes to cyber security

Small business is such a diverse sector, and a small one-person artisan business is going to be connected to the internet in different ways to a 50 person social-marketing company. If you use the internet, and you have something of value on your computer or your phone, then you're at risk. This

[1] https://smallbiztrends.com/2016/04/cyber-attacks-target-small-business.html
[2] Testimony of Dr. Jane LeClair, Chief Operating Officer, National Cybersecurity Institute at Excelsior College, before the U.S. House of Representatives Committee on Small Business (Apr. 22, 2015), available at http://docs.house.gov/meetings/SM/SM00/20150422/103276/HHRG-114-SM00-20150422-SD003-U4.pdf & https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html
[3] https://go.malwarebytes.com/rs/805-USG-300/images/Second%20Annual%20State%20of%20Ransomware%20Report%20-%20Australia.pdf
[4] https://www.telstraglobal.com/images/assets/insights/resources/Telstra_Cyber_Security_Report_2017_-_Whitepaper.pdf https://www.myob.com/au/about/news/2017/cloud-security-the-silver-lining-for-smes
[5] https://www.myob.com/au/about/news/2017/cloud-security-the-silver-lining-for-smes
[6] http://acumeninsurance.com.au/2017/03/14/cybercrime-costs-the-australian-economy-over-4-5-billion-annually-and-is-now-in-the-top-5-risks-faced-by-businesses/

guide informs how small business owners might be at risk, and how they can make small changes to be cyber secure.

Small businesses may be less connected to online services, and as a result, believe they are more protected from cybercrime, or that cyber security doesn't concern them.

Small businesses often don't have dedicated IT teams or managers, so cyber security is out of sight – out of mind. This false sense of security puts small business at a high risk of exploitation, both from committed attackers, and from 'insider threats' (compromises, either accidental or deliberate, from people inside the business).

A best practice guide

The small business sector is becoming more aware of the dangers of cyber security, and the particular threat experienced by small business owners. Recent studies by Symantec and the New South Wales Small Business Commissioner's Office show interest in cyber security is growing as it becomes a higher priority for small business owners, but its complexity is stopping businesses from incorporating proper policies into day-to-day operations.[7]

To assist small business owners and decision makers, we have prepared a best practice guide on cyber security to:

- **expose the issue of cyber security**, as it affects small businesses;
- demonstrate the importance of a cyber security policy for **all small businesses using the internet**;
- recommend **best practice principles and actions** to protect your business; and
- highlight the best places to go for **more information**.

In preparing this guide, the ASBFEO reviewed over 60 guides, security resources and cyber advice documents to prepare a best of breed document. We have done extensive review of a wide spectrum of information, so small business owners don't have to. We have brought the full range of recommended cyber security principles into one place, and compared how the sources you may go to measure up for small business. In this guide, you will find a glossary resource for best-practice cyber principles, and all the best sources to get more information on each. You can read this document from start to finish or jump to the section you are interested in.

[7] https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf; http://www.smallbusiness.nsw.gov.au/__data/assets/pdf_file/0007/104857/cyber-scare-full-report.pdf

2. BEST PRACTICE PRINCIPLES

Cyber security is complex, but it isn't hard.

What you need to consider to secure your business

- You need to have **support from everyone** in the business from top to bottom to ensure your approach is employed.
  - Businesses with high cyber-resilience all consider support and oversight from **management as the most important factor**.
- When it comes to cyber-attacks, **it's not a matter of *if*, but *when***
  - **Cyber security is everyone's business**. All staff should know safe online practices.
- Although you can find countless approaches promoting many useful actions, there is **no single fix** for cyber security.
  - Aiming to implement many actions, even if only to a small degree, is the best long-term approach to maximise protection with limited resources. **Consider the full range of actions**, rather than selecting a few.

It starts at the top

Develop a business-wide policy so everyone knows that cyber security is a priority, and so the business owners can be seen to be actively engaging with cyber security. If cyber security is thought of as a strictly IT issue, it doesn't send the message that it's a top priority, and won't make your business or staff cyber secure. Because cyber attackers target people just as they target hardware, cyber security is for everyone at every level in the business. Establishing and communicating their responsibilities is vital to build a cyber aware business.

As the Australian Cyber Security Centre (ASCS) warns, business owners and managers must weigh investment in cybersecurity against other business needs and consider the overall level of cyber risk, the business's exposure to such risks, and the potential whole-of-business cost that could be incurred if a serious cyber incident were to occur on the network.[8]

Cyber Security isn't the job of the IT specialist

- Technology in small businesses is usually handled ad hoc, by a single person or a few individuals. It is important to separate cyber security from ICT, because it applies to everyone who uses the internet. Of all the following actions to protect against cyber threats, only a few should be limited to the resident IT expert. Management should actively communicate staff and stakeholder responsibilities.

[8] https://www.acsc.gov.au/publications/ACSC_Cyber_Security_Survey_2016.pdf

Understand your risks and you will know how to safeguard against them

- There is no one fix to cyber security, and there's not even a best-of-breed solution that everyone can apply to be cyber-safe. Cyberattacks are changing every day, so nobody is 100% secure. Cyber security is an ongoing pursuit to manage and minimise the risks of conducting business online. The approach you use should be designed around a strong understanding of your risks. You can then prioritise which actions to adopt most strongly to maximise protection.

Getting everyone on board

It is the responsibility of the decision maker in the business to develop cyber security rules and ensure they are followed. Emailing a list of rules to staff won't cut it; they need to build a culture of active participation to ensure the safest, most efficient online activity.

Build a cyber aware culture across the business

- As cyber security is a growing priority for small business, it should be considered along with day-to-day operations like finances and human resourcing. Making cyber security a cultural part of your business will make it easier to think about, and for your staff to engage with cyber security actions. Actively promote your cyber security rules, not just to staff, but to stakeholders and your professional network. Enhance the security of the environment you work in by encouraging people around you become cyber secure too.

Train and educate your staff and clients

- Survey results from businesses around the world show that the complicated nature of cyberattacks and how to defend against them is the biggest barrier for small business operators in adopting new cyber practices.[9] In the same way that purchasing a forklift will be useless until people are trained in its proper use, the training and education in cyber security is more important than any particular action such as using anti-virus security software.
- Develop a "security rules" document that explains what staff are allowed and not allowed to do with regards to cyber security. Include policies on appropriate internet, social media, email, and device use. This could include "you may not connect a personal computer or storage device to the business network", or "when accessing the business network remotely, you must use the approved security".[10]
- Ensure everyone is made aware of the business's cyber rules from day one. This can be through HR processes, or in meetings to communicate the results of regular Security Vulnerability Assessments.
- Train staff in what a potential attack looks like, so they know how to recognise them to avoid falling into phishing, malware and ransomware traps.

It's a hands-on job

- A mistake that most people make in thinking about cyber security is in treating it like other sorts of security like physical infrastructure security. You can't put up a wall to defend against

[9] https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf; https://staysafeonline.org/wp-content/uploads/2017/09/2012-NCSA-McAfee-Online-Safety-Study.pdf; https://www.telstra.com.au/content/dam/tcom/business-enterprise/campaigns/pdf/cyber-security-whitepaper.pdf
[10] https://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-en.aspx

cyberattacks, and you can't see them coming up to your gates. You can't even expect to know who *they* are, or what methods they will try to use against you. Therefore, the strategies you put in place need to include an ongoing, manual maintenance, to constantly check for vulnerabilities, and understand how your assets could be affected at a given time. This responsibility is more than the work of a single person or team, but extends to everyone in with power over the business' assets, and everyone using the internet.

Prioritise actions and save time and money

- Even the largest businesses cannot hope to be 100% safe from cyberattacks, so prioritising the actions you take to defend your business allows you to maximise protection with limited resources such as money, time, staff and technological know-how.
- The following **Actions to Defend Your Business** section starts with vital information that will help you understand the risks you face, and how to address them. This still applies even to businesses with a very limited online presence. Read the next **Become Cyber Secure** section for specific actions to apply. Not every action may be relevant to the smallest businesses, so read each and think how it could apply to your business.

Security software

Security software like paid anti-malware (or antivirus) software, has historically been the go-to solution for users wanting to protect themselves from cybercrime. In the many small business cyber security surveys, users consistently believe that a subscription to Norton by Symantec, Avast, Kaspersky etc. will be enough to protect them. This is not the case.

Benefits and limitations

- Anti-malware software may stop many of the malicious attacks on your computers (providing you keep them up to date), but it gives a false sense of security and does not educate you on how **your actions influence the cyberattacks made against you**. It also doesn't stop the insider threat of someone causing vulnerability or letting an attacker in.
- Cyber security involves more than just desktop software security, as more of your devices access the internet. This is what's known as the "internet of things"; televisions, household appliances and even lights are now connecting to the internet.
- PCs and mobile devices integrate security software as standard these days, so make sure your devices are regularly updated. If you use a Windows PC (which the majority of PC users do), use Windows Defender Firewall. Microsoft Windows has the free built-in Windows Defender Firewall, which is considered to be as good as any paid anti-malware platform.
- You shouldn't use multiple antivirus programs on one computer as they can conflict with each other.
- If you don't invest in anti-virus software, you still need to make sure Windows Defender is constantly running and updated, and is paired with a good anti-malware solution. There are good free anti-malware programs available online, but you should always be sure of the software you download and only download from a reputable, secure site.

3. KNOW YOUR RISKS AND VULNERABILITIES

The first step to becoming cyber secure is to review threat-prone parts of the business. Understand current weaknesses, current culture and gaps, benchmark against resilient similar-sized businesses, and use this information to build a list of required actions.

Secure your business from Risks and Vulnerabilities. At minimum:

- Perform an evaluation of your current exposure to cyber threats
- Survey your business to understand staff culture around safe ICT practices and cyber security knowledge
- Familiarise yourself with important actions as recommended by the trusted cyber security authorities
- Prioritise how, when and where you can apply the full range of recommended actions

Evaluate your exposure – Security Vulnerability Assessments

Start by conducting an assessment of how you are at risk. Do this by cataloguing all aspects of your internet connectivity, and then consider how secure your business, its assets and your staff are. Steps can then be identified to reduce the risk of compromise, educate staff on best-practice and implement actions to build security.

- Employing a cyber security expert or consultant to perform an initial security vulnerability assessment on your system will give you a more informed picture. New threats are always emerging so aim to repeat this process as often as you can.
- Various software solutions including anti-virus software can provide meaningful information and reports on the vulnerabilities of your system, as a snapshot or over time.
- Security Vulnerability Assessments will show how your vulnerabilities have changed over time. As your business changes, use this information to get a deeper understanding of assets, systems, its users, and the threats you have or expect to encounter.

Awareness and management of your assets

Information is often the most critical and valuable asset to a business. Physical assets are easy to account for, but digital assets are becoming more valuable as businesses become digital. Understanding and accounting for your assets is vital for knowing how to protect them. Performing regular audits on your digital assets will allow you to prioritise how you protect them, rather than applying an expensive and ineffective blanket approach.

- Think about your digital assets in the same manner as your physical assets. Maintain the integrity of the information you keep, keep it secured and confidential, and maintain its availability for use by the business or clients.

Evaluate your exposure

Know how you can be attacked by understanding the specific dangers of operating online, what types of attacks exist, and how they could affect your business. Reading this guide is a first step along the way to good threat analysis practices, but it pays to know more about each type of attack, and how the way you operate your business makes you more vulnerable at different times.

- Threat analysis is also important after you have identified a breach or a weakness, so you can patch up the vulnerability and secure yourself from future threats of that nature.

Prioritise protection of assets

Know what you need to protect, and you will save precious effort, time and money when it comes to protecting it. Prioritising the assets you protect is a strategy which can save small business a great deal when it comes to cyber security. The cost of cyber security is often prohibitive to small business, which means many business owners often make a token effort to become secure, picking and choosing certain actions. As a result, the business will have a patchy security, and attacks will still be able to get through. The Canadian Government has useful tips for each type of asset:

- Determine what assets you need to secure (anything of value managed or owned by your business).
- Identify the threats and risks that could affect those assets or your business overall.
- Identify what safeguards you should put in place to deal with threats and secure assets.
- Monitor your safeguards and assets to prevent or manage security breaches.
- Respond to cyber security issues as they occur (such as an attempt to break into business systems).
- Update and adjust to safeguards as needed (in response to changes in assets, threats and risks).[11]

Attacks to defend against

Security compromise – insider threats

When a security breach has occurred as the result of someone inside the business, it is called an insider threat. It can be brought about by a range of factors:

- **Accidental**: This is the human error category, accounting for about 30% of cyber incidents.[12] This threat is caused by staff mistakes or lack of education of correct practice. You can have an expensive anti-malware subscription, but when someone on the inside clicks on a phishing email, or doesn't lock a device, your defences are left open for waiting attackers.
- **Negligent**: This type of threat is caused by staff avoiding their responsibilities or the policies you've put in place. They are not being malicious, but their neglect of safe cyber practices and taking shortcuts in cyber security puts you at risk. Making cyber security practices a part of the business culture will build confidence and adherence to your rules.
- **Malicious**: Cyberattacks don't all come from invisible "black hats" around the world. Your staff members can be the source of a deliberate cyber breach. It is vital to consider malicious

[11] https://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-en.aspx
[12] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

insider threats in such events as disgruntled or financially motivated current or former staff who have access to confidential information. Maintain security of your information and keep administrator rights to select individuals will help protect your business from staff with bad intentions. Administrator accounts are recommended to not be used for email and web browsing.

Directed attacks – external threats

It is important to know what an attack from outside your business looks like. You may have heard about these things on the new or in the media. A directed attack can be in the following forms:

- **Phishing**: This is a specific type of spam that involves an attempt to get information such as credit card details, user names and passwords. The attack is disguised as a trustworthy entity, like a scam bank email. Everyone should be able to differentiate between legitimate and scam communication.
- **DoS/DDoS**: Denial of Service attacks intend to make your machine, network or software unavailable by flooding them with requests in an attempt to overload them and make them crash. Distributed Denial of Service attacks can be even more powerful and difficult to track, by using a network of infected computers and connections to carry out the attack.
- **Malware**: This term refers to malicious or intrusive software, including viruses, worms, Trojans, ransomware, spyware and adware. Security software will protect you from most malware, but it is recommended you educate everyone in proper software use. Limit access rights to install new software on your system so someone doesn't inadvertently install bad software and introduce malware to your machines.
- **Ransomware**: Widely publicised since the WannaCry and Petya global attacks, ransomware involves an attacker hijacking your files and demanding you pay for their return. It is recommended you never pay the attacker, as paying them seldom means you get access back. Small businesses will often pay this money, as not paying means they cannot run their business, so make sure you back up regularly so you can restore your system if a ransomware attack occurs. If you use Windows, Windows Defender consistently releases updates defending against ransomware, so make sure you download updates regularly.

Don't be fooled – Website cloning

Website cloning is becoming more prevalent, and more complex. The process involves replicating entire websites and functional online businesses, which are then passed off as legitimate sites. Pay close attention to the websites you visit, especially those that involve financial elements or require information to be entered, like online department stores, banks, or government websites.

- **Water holing** (Watering hole attacks): Attackers analyse your activities in order to predict the actions which leave you vulnerable to their attacks. Water holing involves an attacker infecting a website they know all your staff to frequent, which increases the likelihood that one of the visitors will become infected and introduce the infection to your system.

What to do when you've been attacked

The actions taken as soon as an attack or breach has occurred often determine the depth of its effect on your business, your ability to recover, and affect the likelihood of future breaches.

Stop further infection

When you feel an attack has occurred, or a computer has been compromised, stop the infection from spreading. Quarantine that computer or device by removing it from the network. Pull out the network cable from the computer, or turn off the device's wireless connection.

Report incidents

- Breaches should be reported immediately. Inform everyone in the business of the incident and how it occurred. Identify the behaviour that caused the incident and quarantine the affected machine or device by removing it from the network.
- You can report cyber incidents through the Australian Government channels listed below. Doing so will alert authorities to the incident, so that its effects can be minimised and investigated, and efforts to catch the attacker can be made. These channels also provide advice to help people recognise and avoid common types of cybercrime:
  - **Computer Emergency Response Team** (**CERT**) https://www.cert.gov.au/.
  - **Australian Cybercrime Online Reporting Network** (**ACORN**) https://www.acorn.gov.au.
- From 22 February 2018, all businesses with a turnover greater than $3 million which have a significant data breach are required to inform all concerned parties, and to inform the **Office of the Australian Information Commissioner**. If there is unauthorised access, disclosure or loss of personal information that could be seriously compromising to the person or people it relates to, you must report it. https://www.oaic.gov.au/.

Recover your data from compromise

When a breach does occur small businesses generally don't have the measures in place to recover, because they haven't taken the time to make a plan to deal with a potential breach.

- The best way to recover from a breach is by having backups of your information. Restoring recent backups can allow you to recover lost of compromised files and damaged systems.
- Conducting the backups is only half the job; you need to test the backups, in case they are corrupted. There is no value in saving backups that can't be restored.

Consider cyber insurance

- When budgeting for cyber security, there are many free tools and services, and you will save money on cyber security by knowing what you need to defend.
- Cyber insurance can help cover losses and ease recovery after a security breach. Discuss the ins-and-outs with your insurance provider, because many things aren't covered, and having insurance doesn't give you a better defence from attack. Many security software providers offer cyber insurance as part of a package, which you may want to consider.

4. BECOME CYBER SECURE

After acquiring a good knowledge of risks and responses, the next step is to incorporate actions, tasks and rules into the daily running of the business, to minimise both security compromises from occurring, and the extent to which they affect your business. This section provides directions on many specific actions to help you become cyber secure. Not all apply to every small business, but following these will increase your security. It is important you read and consider each section, to then decide which actions will be given priority in your business's cyber security rules.

Become Cyber Secure. At minimum:

- Backup regularly
- Patch applications and run security updates and scans
- Protect devices and accounts with complex, limited time passwords with multi-factor authentication
- Protect systems by limiting application control and limit administrative accounts

Backup regularly

Backups are used to restore lost, damaged or compromised data and the more up-to-date the backup, the quicker you can recover from the setback. Backing up your assets and information will protect you from losing information caused by accidental deletion, system failures, disasters (such as a fire), data corruption (such as from a failed update), or theft (such as ransomware).

- To perform a backup you can either use close storage or an external hard drive. Some security software has built-in backup capability.
- Start by performing a full backup. Your operating system can be scheduled to do this at intervals. Full system backups can be used to restore computers when the operating system is compromised and you can't get onto the system.
- Back up data to portable or external drives, which can be removed from the system, and stored separately and securely.
- Aim to conduct backups of valuable files and folders daily. This is considered a good benchmark for all backups.

Many businesses recommend using cloud services to back-up your data, and this has become the default for mobile devices, such as Apple's iCloud, or from Amazon or Microsoft. While the cloud is useful, remember that you are entrusting your data to another business outside of your control. This could put your data at risk, both in terms of the data itself, and the legal implications of doing so. You should assess these risks as part of your overall cyber strategy.

Patch your applications

According to Microsoft Australia, if you do one thing to reduce your cyber security risk, it is the patching (or updating) of security vulnerabilities in security software, applications and operating systems.[13] When trillions of attacks are directed at users and businesses daily, developers work hard to deploy patches to keep software secure.

Hackers seek to exploit vulnerabilities in existing software. New methods of exploitation are discovered daily. To combat this, you should regularly apply the patches developers release to all the applications you use.

- The majority of patches deployed for applications are not for the purpose of adding new features, but for securing the existing features against the many new attacks.
- Check for updates for applications you run, and perform security scans every day.
- Visit the software's webpage and check for patches and updates there.

Monitor remote internet usage (i.e. Cloud, unprotected Wi-Fi)

Cloud technology is a powerful tool for small business to store, access, secure and communicate using web-based technology. It works by services storing information on the internet so you can access it without having the files stored locally on your computer.

- Cloud services offer greatly increased flexibility in how you conduct business, but you need to be aware of the security risks involved. By removing your digital assets from your direct control, you can't control their security. It is important to be aware of all the security credentials of the cloud service you're using.
- Always keep your data backed up offline, in case the cloud service is unavailable or its security is compromised.

Wi-Fi (wireless fidelity) involves connecting to a network remotely. You can remotely access the internet, or files and devices attached to that network.

- While your modem and Internet Service Provider (ISP) will give you added Wi-Fi security in your office, you're at considerable risk when joining unsecured, public networks. You are most secure online when your device is plugged directly into the modem.
- Be especially cautious when connecting to Wi-Fi in places like airports or restaurants, because your laptop or device can be visible to any would-be attacker.

Don't forget security for your devices

Take care of your physical assets as you would your valuable personal belongings. When you store your information on devices, there are further steps to ensure its safety. The same applies for your devices.

- A useful way to store and backup assets is on external and removable storage, such as USB sticks and drives. They are small and can hold vast amounts of data, and are generally low-cost. They do, however, expose you to infection by malware, theft of unsecured, easily transferred information, or the loss of the device and all its contents. Safeguard against these

[13] https://blogs.msdn.microsoft.com/govtech/2015/04/21/if-you-do-only-one-thing-to-reduce-your-cybersecurity-risk/

risks with proper secure handling practices, including a safe place to store them, and reporting lost, stolen or damaged devices.

- Mobile devices should be treated in the same way as desktop computers. Private information is usually protected by a single passcode, which is the only thing protecting them against security compromise for the business. Ensure all mobile devices have passcodes and are locked when not in use.
- Encrypt all of your sensitive data on portable storage devices by using passworded folders or .zip archives, and store them securely out of sight.
- Take care when accepting devices like USB drives from other people as they may contain malware. You won't know for sure until it's on your system, so it is better to be safe.

Minimise your online footprint

Cybercriminals prey on businesses that put a lot of their assets online without adequately securing them. The simplest way to protect yourself from cyberattacks is summed up in National Security Agency cryptographer Robert Morris' three computer security rules: "Rule one: Do not own a computer. Rule two: Do not power it on. Rule three: Do not use it." While this is unrealistic in practice for businesses taking advantage of the digital age, minimising the exposure of your assets to the internet or internet-connected devices will make them more secure.

- If you don't feel confident in the security of certain assets, consider removing them from your network.
- Back-up valuable information on external hard drives and disconnect them from your computers and network. Keep them stored in secure – preferably offsite – locations.

Filter email and web content

Emails are part of the day-to-day landscape for most small businesses. Emails have also become the primary point of access for an attacker. Spam, phishing, and malware are introduced to systems when malicious or infected emails are opened by the recipient. According to a Symantec report, spam represents about 69% of all emails sent on the internet, so knowing how to avoid it is vital to your business.[14]

- The Australian Signals Directorate recommends email quarantining. This means emails from unknown sources can be established before staff are free to open them.[15] This kind of service is often included if you pay for security software or if your IT is managed by another company.
- Use a spam filter on your email hosting service to block recognised spam, keep employee emails confidential, educate everyone on potential spam, and be suspicious of the following traits in incoming mail:
  - Unknown sender
  - Misspelled words in the email (this is done to bypass your spam filter)
  - Unusual phrasing
  - Great offers or rewards
  - Requests for your information

[14] https://www.symantec.com/security-center/threat-report
[15] https://asd.gov.au/publications/protect/malicious_email_mitigation.htm

    - » Requests you click on a link in the email, even if the link claims to remove you from the mailing list.
- If something looks authentic but is out of place or doesn't feel right, talk about it, and investigate it. A call to the supplier or sender can save you a lot of embarrassment, time and money.

Web filtering follows the same approach as email filtering. You can use security software to block access to untrusted sites and educate yourself and staff on safe browsing practices.

- Browse safe sites. When on the internet, always look for the padlock symbol on the address bar, to show a secure site, and look for the *s* in the "*https*", preceding the website address. This means the website has a secure signature, and you will be better protected while browsing that site.
- Check the link address. A common method for luring victims is to have links on websites and emails that look recognisable and legitimate, but direct you somewhere else. Hover your mouse over the link, and a box should appear with the real destination address. If it's different, it may be malicious.

Shut it down – Disable extensions and macros

Do you use macros and extensions? If you do, do you know why? Macros and "extensions" are like small programs that run within other programs. They are often third-party programs that increase functionality, such as a payment portal in your web browser. They can also compromise the security of the applications running them, and of your system.

- A macro is a way of grouping commands and instructions into a single command, in order to automatically complete a range of functions. Microsoft Office makes use of "trusted" documents, locations or files to automate tasks, but attackers can create macros to take advantage of trusted files to infect your system. To protect against ransomware attacks, the ACSC and Australian Signals Directorate (ASD) recommend disabling Microsoft Office macros as they can be used to gain control of your system.[16]
- Add-ons like Java make web-applications more interactive, but are not built into your operating system. They can be exploited to gain access to your data. Be aware of which extensions, add-ons and macros you use, and consider disabling them if they're not necessary.
- While installing new software you are often offered third-party applications which require unnecessary access to your system. Consider avoiding these by unchecking the box when offered the software.

Monitor external services (Point of Sale (POS) / financial transactions)

A large number of small businesses – especially in retail – rely on external IT services like Point of Sale for their everyday business. These external financial services such as banking and POS platforms are frequent targets.[17]

- 95% of cyberattacks are financially motivated. You could follow all of the actions listed here to secure your systems, but if you access outside systems – or if outside systems are allowed to access you – you might be opening a backdoor for an attacker to reach you. If the bank you

[16] https://asd.gov.au/publications/protect/ms-office-macro-security.htm; https://www.acsc.gov.au/publications/ACSC_Cyber_Security_Survey_2016.pdf
[17] https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf

use experiences a breach or DDoS attack, it can have significant impact on your business. Be aware of attacks on your external services, and try to limit reliance on them.

- Make sure your POS system is behind a firewall with separate credentials and password.

Personnel security and insider threats

You're the boss – Protect administrator privileges

Administrator accounts have full access to operating systems, accounts and networks. They allow users to make changes to the entire system and the accounts of others. An *administrator* is a user who has the responsibility to manage these changes.

- Minimising the ability for users to make changes on computers is vital to keeping your computer systems secure. As a rule, no one should have access to anything they do not need. Consider disabling the local administrator accounts on office computers, meaning someone using that machine cannot change the operating system, the network, their own and others' privileges, and even change or delete files.
- Consider using unique admin passwords on each machine. If one is compromised you are not at risk of a wider security breach.
- Limit access to the programs you use, financial and client data on your systems, and also on your point of sale systems.

Need to know – Classify sensitive information

Similar to administrator privileges, the less access users have, the safer your information will be from compromise, either intentional or unintentional. Digital information is an asset to businesses, and should not be left lying around for anyone to see. As such, information security should be viewed on a "need-to-know" basis, limiting access to trusted, involved parties only. This extends beyond logon details and HR information, to things like accounts and working documents.

- Information security classification will be most relevant to small businesses with a large amount of assets like sensitive personal details or financial information.
- Limiting access to information will help protect it from accidental compromise.
- Set up a labelling system to communicate information security classification, and train employees in the handling of sensitive information. This involves determining where the information is stored, its value and risk of loss or theft, and the level of security required to protect it. Use words like *public*, *restricted*, or *confidential*, and limit access depending on the level.
- A simple system is to identify confidential information and label it '*confidential'* and instruct staff regarding its use. A key learning is not to assume staff will automatically understand how to treat sensitive information.

1ts_nøt_H@rD – Password complexity and lifecycle

A single password is often the only barrier protecting all your sensitive assets. If that password is discovered by a dedicated attacker, they have full access to everything protected by that password. Stay Smart Online records that 63% of small business cyber breaches occurred as a result of weak or

stolen passwords.[18] Everyone knows not to have their password as "*password*", but staying clear of dictionary words entirely, and using numbers and symbols is important.

There are programs that exist to guess trillions of different password combinations, so the more complex your password, the better. To further reduce the risk of password compromise, require passwords to be changed at regular intervals.

- The longer you use a particular password, the more likely it is to be compromised. It is recommended making resetting passwords mandatory for everyone every 1-3 months.
- Make sure staff don't write passwords down on paper.
- Do not communicate personal passwords to anyone, even among trusted colleagues or family members. Access to reset passwords should be limited to select individuals.
- Many small businesses report passwords are often written on sticky notes on the computer. If you do write down the password, consider writing a clue to it instead and keeping it hidden.

Go a step further – Two-step authentication

Often, a single password is all that stands in between an intruder and all your protected data. Having one strong password is good; having two is great. Two step (or multi-factor) authentication is like having an extra level of protection by forcing the user to prove they are who they claim to be beyond a single password.

- Online services frequently use token-based authentication factors, Captcha boxes, SMS instant message confirmations or voice-call authentication, which assist in verifying identity.
- Physical devices can also use two-step authentication. Secure USB drives are available which require passwords, keys or fingerprints to be usable.

Good app/bad app – Whitelist applications

You may wish to control what software and applications are allowed to be installed and used on work devices. This is especially important on devices that are used outside of work too, such as laptops that you or your staff take home on the weekend.

- Even without administration rights, users can install unapproved or malicious programs. An email could contain a link or an attachment that, when opened, installs malware.
- Whitelist applications which can be installed or accessed on your system. Have a list of all the appropriate programs which might be important for usage, and only add trusted programs to that list.
- For advanced users, you can prevent unapproved applications (.exe), scripts (.dll) and installers from running, using a "group policy". There are simple guides available to setting up a group policy.[19]

It is your business – Monitor network and mobile usage

Small businesses often set up networks to allow access off-site, in buildings with shared occupancy, at home, or even overseas. While having a flexible business network allows staff to take advantage of

[18] https://www.staysmartonline.gov.au/sites/g/files/net1886/f/Stay-Smart-Online-Small-Business-Guide_0.PDF
[19] This beginner's guide gives a step-by-step introduction to enforcing settings on your computers: https://technet.microsoft.com/en-us/library/hh147307(v=ws.10).aspx

more technology, it becomes harder to monitor security on the network. In these situations, your systems and information are at risk, such as when a work computer is connected to a new network with different security, giving malware a path into the work system.

- Establish network rules and mobile device rules. Staff will then know the sites they can visit, the things they can download, and the apps they can use on their work phone. It is vital that any devices you allow onto the work network adhere to a correct usage policy, including restricting certain sites. You need to find a balance between monitoring all staff activity and trusting your employees.
- It is unwise to remove or disable security software on business networks, while inside the office or not.

***Cyber Serenity* – Keeping you cyber safe.**

The following summary points can be used to help you implement the above rules into your business:

- **Evaluate**
  - Conduct an initial *Security Vulnerability Assessment* to review threat-prone parts of your business, understand current weaknesses and workplace culture, and benchmark against resilient similar-sized businesses.
  - Establish a list of the required actions to address the gaps.
- **Adopt & apply**
  - Implement, at very least, the **minimum recommended actions** listed at the start of each section of this guide, and keep them as a priority.
  - Apply the required actions in the form of rules which should be clearly communicated and trained into all staff and stakeholders using your systems and accessing your data. Conduct training to test knowledge and build confidence in your business's cyber security practices.
  - Consider how the full range of actions could apply to your business, and make every effort to adopt them.
- **Get everyone on board**
  - Build your staff's confidence in the rules you enact. Everyone using your systems and accessing your data is an active participant in keeping the business safe.
  - Show trust in staff by not monitoring their every action online. Instead, require them to use the same security principles and software as yourself.
  - Work with staff to ensure they are comfortable adopting your policies. Having too many restrictions and actions will alienate staff and will pose a difficulty to imposing rules. Monitoring all their internet usage and mobile devices will convince staff you don't trust them, and they won't trust you or your policies.
- **Monitor**
  - Continue to review the effectiveness of your cyber security rules, and update them when there are changes to your business or the environment you work in.
  - Conduct *Security Vulnerability Assessments* at ongoing intervals to get a detailed snapshot of your business's cyber health.
  - Pay attention to news and media covering small business cyber security issues

5. FOR MORE INFORMATION

Small businesses can find useful information around cyber security through State and Federal Government agencies whose main purpose is to be a point of reference and assistance.

The ASBFEO has conducted analysis and stakeholder engagement around the most visible and accessible agencies working on cyber security across governments, IT security vendors, industry associations and internet service providers (ISPs), both domestically and abroad. This was done to **highlight the simplest, but most effective ways of securing your business**.

The ASBFEO views these sources to be the most desirable for small businesses to visit for more information:

- For a comprehensive list of practical actions to make your computers, networks and systems more secure, the **Australian Signals Directorate's (ASD)** ***Essential Eight*** (https://asd.gov.au/infosec/mitigationstrategies.htm) aims to prevent malware from running, to limit the extent of an incident, and recover data.
- For useful statistics on how cyber security affects small business, the **Australian Cyber Security Centre** (https://www.acsc.gov.au/publications.html) produces and regularly reviews statistics from cyber security incidents.
- Familiarise yourself with the **Computer Emergency Response Team (CERT) Australia** (https://www.cert.gov.au/advice) for more information on what to do when you've been attacked.

There are also many excellent small business guides from outside Australia, especially the U.S., U.K. and Canada, with simple steps to follow. Australian and international sources are listed below:

Recommended information

Best practice principles

- **Stay Smart Online** is an Australian Government initiative aimed at educating people and businesses on cyber practice, using straightforward, accessible language. This guide highlights the areas where Australian small businesses go wrong in thinking about cyber security.
  - https://www.staysmartonline.gov.au/news/top-5-cyber-security-mistakes-small-businesses

It starts at the top

- The UK's **National Cyber Security Centre** offers excellent advice on how governance of cyber security within an organisation should be thought about, depending on the size of the organisation.
  - https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

Getting everyone on board

- The **European Union Agency for Network and Information Security** has developed a guide to help organisations of different sizes and types build a cyber security policy that suits their needs.
  - https://www.enisa.europa.eu/publications/ncss-good-practice-guide

It's a hands-on job

- **Cisco's** *Small Business Computer Security Checklist* highlights how important it is for cyber security to be seen as a
  - https://www.cisco.com/c/en/us/solutions/small-business/resource-center/secure-my-business/protect-your-network.html

Know your risks and vulnerabilities

- The **Australian Cyber Security Centre** (ACSC) is the Australian Government's leading cyber security authority, and conducts regular analysis of threats as they affect individuals and businesses of different sizes. The ACSC recommends the *Essential Eight* and CERT Australia for cyber best practice.
  - https://www.acsc.gov.au/publications.html
- The **NSW Small Business Commissioner** has conducted surveys on cybercrime as it affects small business, and an analysis of the sector's maturity in dealing with cybercrime. Knowing how attacks can affect you will inform how you deal with them.
  - http://www.smallbusiness.nsw.gov.au/resources/how-cyber-aware-is-your-small-business

Attacks to defend against

- **CERT Australia** has publications to inform you on the types of attacks you might encounter, informed by the data they receive from individuals and businesses who have been attacked.
  - https://www.cert.gov.au/guides
- **Symantec's** *Internet Security Threat Report* is a detailed look at the range of attacks their security software encounters, and how they recommend addressing each.
  - http://now.symassets.com/content/dam/content/en-au/collaterals/datasheets/cybersecurity-simplified.pdf

What to do when you've been attacked

- The **Australian Cybercrime Online Reporting Network (ACORN)** is the Government portal for you to report information about a cyber incident.
  - https://www.acorn.gov.au/
- **Stay Smart Online** has released the *Cyber First Aid Kit*, an online tool to help diagnose symptoms and prescribe treatments to cyberattack breaches.
  - http://www.idcare.org/cyber-first-aid-kit
- **Connectsmart's** *SME Toolkit*, a New Zealand Government initiative, walks you through a plan to develop actions for when you've been compromised by a cyberattack.
  - https://www.connectsmart.govt.nz/assets/Uploads/Connect-Smart-for-Business-SME-Toolkit.pdf
- The **Office of the Australian Information Commissioner** provides useful information about your reporting obligations in the event of a cyberattack, such as a data breach.
  - https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

Become cyber secure

- The **Get Cyber Safe Guide for Small and Medium Businesses** from the Government of Canada is an excellent resource for small businesses, set out in clear, descriptive language. Refer to it for more explanation on most points made here.
  - https://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-en.aspx
- The **Australian Signals Directorate's (ASD)** ***Essential Eight*** comes from the Australian Government's primary authority on cyber security, and provides the most detailed recommendations for the most advanced users and organisations. While not all of it will apply to small businesses, it is a handy benchmark when you're thinking about securing your business.
  - https://asd.gov.au/publications/protect/Essential_Eight_Explained.pdf

Personnel security and insider threats

- **Microsoft** promotes an organisation-wide approach to cyber security which promotes people management. While not specifically small business focused, you will find it a useful tool to consider threats that could affect your staff, and threats introduced by staff actions.
  - https://www.microsoft.com/en-au/security
- **CERT USA** has collated a list of guides on insider threats from think tanks and universities.
  - https://www.cert.org/insider-threat/publications/

Security software

- There are a range of anti-malware brands that can offer small business-focused tools. We recommend searching for reviews of each, to save money for your business, without compromising on security.

Sources

Information provided in this report was attained by collating data from cyber security surveys, commissioned reports, media and direct consultation with cyber security experts in Government and industry. Sources range from Australian and international organisations including (but not limited to) government agencies, government initiatives, industry associations, security providers, ICT and telecommunications companies, universities and think tanks. Source selection was based on sources advertised as small business-focused, and sources were rated by how accessible they are to untrained users.

Some sources prioritise certain sorts of actions over others, and some focus more on specific actions, while neglecting broad principles, and vice-versa. A select few rationalise the most effective approaches spanning the spectrum of actions, to provide the highest expectation of protection with the limited resources available to small business. In addition, a separate sample of over 60 major cyber security resources was reviewed in a matrix analysis to rank them against the broad and specific recommended actions they promote. All of the recommendations in this report are based on the most comprehensive and effectively small business-focused sources.

Online Reference Sources

- ASB Bank 'Keeping Your Business Safe Online', 2017 https://www.asb.co.nz/banking-with-asb/guide-to-small-business-cyber-security.html
- Australian Cyber Security Centre 'ACSC 2016 Cyber Security Survey', 2017 https://www.acsc.gov.au/publications/ACSC_Cyber_Security_Survey_2016.pdf
- Australian Cyber Security Centre 'Ransomware campaign impacting organisations globally', 13/5/2017 https://www.acsc.gov.au/ransomware-campaign-impacting-organisations-globally.html
- Australian Prudential Regulatory Authority '2015/16 Cyber Security Survey Results Information Paper', 9/2017 http://www.apra.gov.au/AboutAPRA/Documents/Information-Paper-Cyber-Security-2016-v4.pdf
- Australian Signals Directorate 'Cyber Security Incidents - Are You Ready?' 3/2014 https://www.asd.gov.au/publications/protect/cyber-security-incidents-are-you-ready.htm
- Australian Signals Directorate 'Implementing Application Whitelisting', 5/2016 https://www.asd.gov.au/publications/protect/application_whitelisting.htm
- Australian Signals Directorate 'Information Security Advice', 2/12017 https://asd.gov.au/publications/protect/essential-eight-explained.htm
- Australian Signals Directorate 'Strategies To Mitigate Cyber Security Incidents', 2/2017 https://www.asd.gov.au/infosec/top-mitigations/mitigations-2017-table.htm
- Australian Taxation Office 'Top cyber security tips for business', 10/5/2017 https://www.ato.gov.au/General/Online-services/Identity-security/Protecting-your-information/Top-cyber-security-tips-for-businesses/
- Beehive 'Cyber security credentials scheme proposed for SMEs', 10/12/2015 https://www.beehive.govt.nz/release/cyber-security-credentials-scheme-proposed-smes
- Business News Daily ' A 'Culture of Cybersecurity' Is Best Small Business Defense', 10/11/2014 http://www.businessnewsdaily.com/7432-small-business-hackers.html

- Business News Daily ’13 Security Solutions for Small Business’, 30/5/2017 http://www.businessnewsdaily.com/6020-cybersecurity-solutions.html
- Business News Daily ’Cybersecurity: ‘Best of Breed’ May Not Be Best for Small Businesses’, 12/6/2014 http://www.businessnewsdaily.com/6587-smb-custom-cybersecurity.html
- Business News Daily ’Cybersecurity: A Small Business Guide’, 2/6/2017 http://www.businessnewsdaily.com/6058-improve-small-business-cybersecurity.html
- Business.gov.au ‘Cyber Security Small Business Program’, 25/10/2017 https://www.business.gov.au/assistance/cyber-security-small-business-program
- Business.gov.au ‘Cyber Security’, 24/11/2017 https://www.business.gov.au/info/run/advertising-and-online/cybercrime
- CERT NZ ‘Guides’, 2017 https://www.cert.govt.nz/businesses-and-individuals/guides/
- CompuData ‘8 Cyber Security Tips for Your Small Business’, 27/3/2017 http://www.compudata.com/cyber-security-tips/
- Connect Smart ‘Connect Smart for Business SME Toolkit’, 6/2014 http://www.connectsmart.govt.nz/assets/SME-Toolkit/Connect-Smart-for-Business-SME-Toolkit.pdf
- Council of Small Business Australia ‘COSBOA Communique – Business Continuity & CyberSecurity’, 28/5/2017 http://www.cosboa.org.au/blog/cosboa-communique-business-continuity-cybersecurity/
- CSO ‘Australian Businesses should use ASD Essential Eight as a roadmap for proactive security’, 8/6/2017 https://www.cso.com.au/article/620382/australian-businesses-should-use-asd-essential-eight-roadmap-proactive-security/
- Cybertraing365 ‘Cyber Security Educationhttps://www.cybertraining365.com/
- Department of Innovation ‘Cyber Security Growth Centre’, 2017 https://www.innovation.gov.au/page/cyber-security-growth-centre
- Disrupt Africa ‘Small business security: three steps to prevent cybercrime’, 27/6/2017 http://disrupt-africa.com/2017/06/small-business-security-three-steps-to-prevent-cybercrime/
- Federal Communications Commission ‘Cybersecurity for Small Business’, 2017 https://www.fcc.gov/general/cybersecurity-small-business
- Forbes ‘Cyber Attacks: 5 Ways Small Businesses Can Protect Themselves’, 26/10/2015 https://www.forbes.com/sites/franksorrentino/2015/10/26/cyber-attacks-5-ways-small-businesses-can-protect-themselves/#31ece1563193
- Forbes ‘Cyber Security, Small Business And The 2015 Trends That Will Matter More In 2016’, 12/1/2016 https://www.forbes.com/sites/franksorrentino/2016/01/12/cyber-security-small-business-and-the-2015-trends-that-will-matter-more-in-2016/#223cd5c91a38
- GlobalSign ’31 Cybersecurity Tips for Business’ 3/10/2016 https://www.globalsign.com/en/blog/cybersecurity-tips-for-business/
- Gov.uk ‘Cyber Security Guidance for Business’, 16/1/2015 https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary
- Gov.uk ‘Small Businesses: What you need to know about Cyber Security’, 3/2015 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/412017/BIS-15-147-small-businesses-cyber-guide-March-2015.pdf

- Government of Canada ‘Get Cyber Safe Guide for Small and Medium Businesses’, 23/10/2017 https://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-en.aspx
- Iinet ‘Media Release - iiNet's Online Safety Series spreads the word on cyber security’, 30/5/2011 https://www.iinet.net.au/about/mediacentre/releases/110530-iinet-online-safety-series
- Inside Small Business ‘Five ways to protect your business from cyber security breaches’, 1/6/2017 https://insidesmallbusiness.com.au/planning-management/five-ways-to-protect-your-business-from-cyber-security-breaches
- Kaspersky ‘Small Business IT Security Practical Guide’, 2017 https://media.kaspersky.com/en/kaspersky-small-business-it-security-practical-guide.pdf
- KPMG ‘Cyber security: it’s not just about technology’, 2014 https://assets.kpmg.com/content/dam/kpmg/pdf/2014/05/cyber-security-not-just-technology.pdf
- Malwarebytes ‘Second Annual State of Ransomware
- Microsoft ‘Group Policy for Beginners’, 27/5/2011 https://technet.microsoft.com/en-us/library/hh147307(v=ws.10).aspx
- Microsoft ‘Security Guide for Small Business’, 2005 https://s0.yellowpages.com.au/7ffe4b9f-62ec-498b-92a3-98daef86eb41/guardian-security-holding-pty-ltd-balcatta-6021-document.pdf
- Microsoft ‘Top 10 data security tips for small business’, 18/4/2017 https://blogs.business.microsoft.com/en-us/2017/04/18/top-10-data-security-tips-small-business/
- Ministry of Communications and Information Singapore ‘Go Safe Online’, 24/10/2017 https://www.csa.gov.sg/gosafeonline/go-safe-for-business/smes
- Ministry of Communications and Information Singapore ‘Singapore’s Cybersecurity Strategy’, 10/10/2016 https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.ashx?la=en
- MYOB ‘Cloud Security the Silver Lining for SMEs’, 4/9/2017 https://www.myob.com/au/about/news/2017/cloud-security-the-silver-lining-for-smes
- National Cyber Security Centre ‘Ransomware: 'WannaCry' guidance for home users and small businesses’ 17/5/2017 https://www.ncsc.gov.uk/WannaCry-guidance-for-home-users-and-small-businesses
- National Institute of Standards and Technology ‘Small Business Information Security: The Fundamentals’ 11/2016 http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf
- National Security Agency ‘NSA Office of Small Business Programs’, 1/8/2017 https://www.nsa.gov/business/small-business-office/
- National Security Agency ‘NSA Set-Aside for Small Business (NSETS)’, 3/5/2016 https://www.nsa.gov/business/programs/nsets.shtml
- Office of the New South Wales Small Business Commissioner ‘How cyber aware is your small business?’, 10/2017 http://www.smallbusiness.nsw.gov.au/resources/how-cyber-aware-is-your-small-business

- Optus ‘5 Steps for cyber security in small business’, 2017 http://www.optus.com.au/business/optus-smart-shop/security-and-protection/cyber-security
- PM&C Library ‘ANZUS 2.0 cybersecurity and Australia–US relations’, 3/5/2017 http://library.pmc.gov.au/2012/05/anzus-2-0-cybersecurity-and-australia-us-relations/
- PM&C Library ‘Strategic Risks of Ambiguity in Cyberspace’, 9/7/2017 http://library.pmc.gov.au/2015/07/strategic-risks-of-ambiguity-in-cyberspace/
- PM&C Library ‘The Hacked World Order : How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age’, 5/6/2017 http://library.pmc.gov.au/2017/06/the-hacked-world-order-how-nations-fight-trade-maneuver-and-manipulate-in-the-digital-age-new-book/
- Protective Security ‘Risk Management Of Outsourced ICT Arrangements – Including Cloud’, 2017 https://www.protectivesecurity.gov.au/informationsecurity/Pages/RiskManagementOfOutsourcedICTArrangements-IncludingCloud.asp
- Real Estate Agents ‘Small Business Security Guide for Australian Real Estate Agents’, 2016 https://agent.realestate.com.au/wp-content/uploads/Stay_Smart_Online.pdf
- Report: Survey Results for Australia’, 6/2017 https://go.malwarebytes.com/rs/805-USG-300/images/Second%20Annual%20State%20of%20Ransomware%20Report%20-%20Australia.pdf
- Scamwatch ‘Watch out for scammers when going online’, 10/10/2017 https://www.scamwatch.gov.au/news/watch-out-for-scammers-when-going-online
- Singapore Business Review ‘5 cyber security measures Singapore SMEs should know’, 8/9/2014 http://sbr.com.sg/information-technology/commentary/five-important-cyber-security-measures-singapore-smes-0
- Small Business UK ‘Cyber security: What small businesses need to know’, 6/2/2017 http://smallbusiness.co.uk/cyber-security-small-businesses-2536683/
- Squarespace Security ‘Cyber Security Tips for Business’ 2015 https://static1.squarespace.com/static/587655a3e6f2e1ab23aa85c8/t/58f0daa5a5790a8991acca9d/1492179627958/SOeC.15-10_4pg-Brochure_BUSINESS_WEB.pdf
- Stay Smart Online ‘Protect Your Business in 5 minutes’, 2017 https://www.staysmartonline.gov.au/sites/g/files/net1886/f/Stay-Smart-Online-Small-Business-Guide_0.PDF
- Stop Badware ‘Preventing badware: Basics’, 2017 https://www.stopbadware.org/prevent-badware-basics
- Sydney Morning Herald ‘Government to provide $15 million as cyber criminals shift focus to small business’, 26/5/2017 http://www.smh.com.au/small-business/government-to-provide-15-million-as-cyber-criminals-shift-focus-to-small-business-20170525-gwcplh.html
- Symantec ‘2017 Internet Security Threat Report’, 2017 https://www.symantec.com/security-center/threat-report
- Telstra ‘Cyber Security Whitepaper’, 2017 https://www.telstra.com.au/content/dam/tcom/business-enterprise/campaigns/pdf/cyber-security-whitepaper.pdf
- The Conversation ‘The three ‘B's’ of cybersecurity for small businesses’, 18/4/2017 http://theconversation.com/the-three-bs-of-cybersecurity-for-small-businesses-76259

- University of Maine ‘Small Business Cyber Security Guide’, 2016 https://www1.maine.gov/ag/docs/Small-Business-Cyber-Security-Guide.pdf
- Verizon ‘How long since you took a hard look at your cybersecurity?’, 2017 http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/