

IT CHECKLIST FOR SMALL BUSINESS

INTRODUCTION

Very few small businesses have a dedicated IT Department or Help Desk. However, small businesses still have many of the needs of a large organisation and they still need to make sure those tasks are carried out by someone for the business. This checklist aims to provide small businesses with prompts for further action.

First, small businesses often use cloud computing instead of an IT contractor as cloud computing is now a commodity that can expand (and shrink) as required. No large initial investment in IT infrastructure is needed. Cloud services are more easily installed and are generally more reliable. Cloud computing is popular as it gives small businesses the same capabilities as larger businesses. Cloud computing 'levels the playing field'.

Second, the use of online social media (Facebook, Twitter and so on) has increased exponentially. Social media barely registered on our radar in 2005 when this checklist was first created. Today, small businesses rely on social media to 'spread the word' and definitely dread a bad Google review whilst valuing good reviews online. Small businesses look to manage and react to their social media presence on demand.

Third, mobile devices such as iPhones (2007), iPads (2010), and Android tablets and phones (2013) have had a huge impact. These tools have allowed new services and products to be provided by small businesses. However, the adoption of 'Bring Your Own Device' (BYOD), where employees use their personal devices to store business data, opens up new concerns and issues. These mobile devices – along with internet connectivity – have given businesses options in the face of the COVID-19 pandemic of 2020.

Fourth, although viruses and Trojan horses very much existed back in 2005, concerted ransomware attacks such as WannaCry, Cryptolocker and their related derivatives have now adopted commercially-focused business models. Literally, ransomware franchises exist. Small businesses in particular are vulnerable. In ensuring business survival during the COVID-19 pandemic, not all the remote devices used while 'working from home' were properly protected. These problems need to be addressed when these computers return to the workplace. In the interconnected world of businesses, cybersecurity has become a key point of concern.

Finally, though, the business needs to ensure that it is constantly addressing its own compliance needs, and monitoring changes to legislation. This means the business must keep its strategy for using IT current and ensure that arrangements with service providers address regularly changing business compliance issues. For example, in 2014 the Australian Privacy Principles received a major update, and in 2018, Australia's mandatory data breach notification laws came into effect.

The following pages discuss each of these five issues: cloud computing, social media, mobile devices, cybersecurity and the need to monitor business compliance needs. We end this discussion that considers how small businesses can navigate the minefield that is selecting key providers of these IT services.

CLOUD COMPUTING

Cloud computing allows the pooling and sharing of hardware infrastructure resources on a massive scale. The technology can be quickly applied to a business need with minimal effort. Cloud computing is where applications and data are stored on computers you don't own, but instead lease the computing power as you need it. Usually, you cannot identify a specific item of hardware that contains 'your data' – cloud service providers locate data centres around the world to ensure energy efficiency and sustainability.

Cloud computing is increasingly abundant, cheap, and commonly used. There are real advantages with cloud computing. You don't need to pay IT staff to look after new servers, and you don't need to regularly buy new hardware every few years (or software, for that matter). You pay predictable subscription payments, and most cloud computing arrangements come with guaranteed availability. For instance, the Microsoft 365 for Business plans¹ offer 99.9% guaranteed uptime, or approximately 9 hours downtime per year – that's better than most small businesses can manage on their own.

Cloud computing gives small businesses the power to innovate as well as the flexibility to grow - and shrink - as needed. Cloud computing changes the challenges of 'traditional' IT into a simple transaction. You need more computing power? You've got it – and it's about as difficult to set up as Netflix.

It's not all good news. You do lose some control over your IT – you may not be able to customise your IT solution as much as you'd like. Standardised technology keeps costs low. And, your data may be stored somewhere it oughtn't. Australian Privacy Principle 8 of the *Privacy Act 1988* (**Privacy Act**) requires those subject to the Act to only send private data offshore with proper safeguards – and the Act does apply to some small businesses. Finally, of course, cloud computing requires internet access. If you lose access to the Internet (or the internet connection is unstable), then your decision to use cloud computing might rain on your parade.

Microsoft 365 Business Standard – Microsoft's mid-tier offering - offers all the Office desktop applications, 1 terabyte of file storage, 50 gigabytes of email storage, and multiple licensed copies of Office on desktop computers, laptops, and mobile devices. All for the cost of coffee-and-cake, with upgrades to the software built into the price. Google's G Suite is priced similarly. For accountants, another big provider is the online accounting software Xero – 'accounting software in the cloud'.

One new management headache created by cloud computing is the fragmentation of where all of the business's files are stored. Cloud computing resources can easily grow like Topsy, with your data stored in many different places. Files may be stored on Dropbox, Google Drive, and OneDrive, whilst email is on Gmail. Accounting data might be stored with Xero whilst customer information is located on Salesforce.

For this reason it is easy to 'lose' data. Backing up data in different locations, or moving from one provider to another, becomes complex and difficult. For example, a better product may come along and moving your data from one provider to another becomes difficult – this is called 'vendor lock-in'. Or, you might abandon the data thinking that you'll come back to it and sort it out 'tomorrow' – but of course, tomorrow never comes.

Similarly, a traditional approach to keep your technology working (for example, an uninterruptible power supply) won't keep you working if your applications and data are stored in the cloud and you have no internet.

¹ Microsoft Office 365 was rebranded as Microsoft 365 in April 2020.

For further reading on this topic read CPA Australia's [guides to the cloud](#) and an overview of its advantages and disadvantages. Several [InTheBlack](#) articles have also looked at this topic.

SOCIAL MEDIA

Facebook, Twitter, Instagram and LinkedIn – not to mention BuzzFeed and Reddit - have become so ubiquitous they are now verbs in some circles. Social media connects people, and when people connect they share news. So it is not surprising that online social networking has led to fundamental changes in the way news is shared and how the 'word gets out' for small businesses. Increasingly, the small business needs to engage with customers online.

Social media can be key to getting new customers, with the social media page providing a way to engage with existing and potential customers. For example, Facebook pages that allow consumers to comment, provide suggestions, and discuss the small business's products and services are an important tool to the small business in marketing itself. Occasionally, small business ideas go 'viral', but really it's the connections made to customers through social media that makes the difference. A business does not need to go viral with its social media – it just needs to support and enhance relationships with actual customers.

There is a dark side to social media though if used poorly. Amy's Baking Company participated in the reality television series 'Gordon Ramsay's Kitchen Nightmares' and has become a by-word of how NOT to respond when a customer leaves a negative review on your business's Facebook page, Google Reviews or on Yelp. The episode did not end well (an online search tells more of this story - but since Gordon Ramsay is involved, you know the language might turn blue).

Unlike Amy, though, people in small businesses have a strong appreciation of the need to manage their online reputation. This means that you and your staff need to know what people say about your business in social media. Particularly, in a small business you need to be sure that your staff know how to (or whether to) respond if a comment is made about the business online – good or bad! And, always be sure to count to 10 before you reply to a bad Yelp or Google review.

For the record, Amy's Baking Company closed down in 2015. Apparently, there is such a thing as 'bad publicity', though the owners still spar with former customers on their Facebook page.

Regarding social media, there is one further issue for small businesses to be aware of. This is the risk that your employees might engage in 'cyber-bullying'. Cyber-bullying is defined as '*an aggressive intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself*'. That is, your employees might use social media to 'cyber-bully' their colleagues. As their employer, you have a responsibility to ensure a safe workplace, and cyber-bullying does not indicate a safe workplace. For example, in 2015 case a real estate agency in Launceston was found to have tolerated cyber bullying as part of a wider pattern of bullying behaviour in the workplace. There were legal consequences under the *Fair Work Act* (2009) for that small business. Your staff should be clear on the relationship between a safe workplace and cyber-bullying.

MOBILE DEVICES

The use of mobile devices has increased exponentially. Consumers have taken up these devices enthusiastically - some might say a little too enthusiastically.

It was probably to be expected that these consumers would want the same convenience in the workplace. Harris, Ives & Junglas noted in 2012 that 49% of employees felt they would get more tasks done on time if allowed to choose their own mobile tools – and even 23% of their skeptical bosses felt that the use of these consumer mobile devices in the workplace increases employee productivity.

This concept of 'Bring Your Own Device' (BYOD) - where your employees use their personal devices to store business data – opens up new concerns and issues for the small business. In addition to worries about where exactly the business's data might be 'in the cloud', BYOD means that any small – and easily-lost – device can easily contain vast amounts of relevant business information. Spreadsheets with pricing models, client lists, usernames and access can easily be stored on a mobile device such as an Android phone, iPhone, iPad or Surface Pro.

Worryingly though, 36% of employees ignore their employers' IT policies and just use whatever tool they can bring to the task. So, even if the 'skeptical boss' has forbidden the use of private technology inside the business, it is very likely their employees are already using private mobile devices with business data on them. You just don't know about it.

It is possible that for some businesses with sensitive data, BYOD is not appropriate at all. For those businesses that do allow their staff to use their own mobile devices, the business still needs to be particularly vigilant in the area of anti-virus protection and educating users on how to use them safely.

Mobile devices can be gateways for new viruses, Trojan horses, and other cyber-security problems to enter your business computers – and the business may not be well-equipped to address such problems.

It's also a good idea to make sure that you can delete the data on a device remotely when (not if!) the device is lost. All users also need to be very aware of what data they should put on the device. At its most basic, you must ensure that the mobile device has some basic levels of password protection.

Even then though, you must recognize that password protection on a mobile device is often ineffective against hackers with even mediocre skills. A mobile device is definitely not the appropriate place for your highly sensitive business information or private personal data.

CYBER SECURITY

The trends recognised in cloud computing, mobile devices, and social media all underpin the fourth trend, the need for more vigilance regarding cyber security. An official definition for cyber security is 'the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights.'²

More simply, cyber security is making sure your business data is safe from attack via the internet.

Cyber-attacks are costly. The Department of Home Affairs in 2019 pegged the costs of cyber security incidents in Australia as \$A29 billion each year. Cyber-attacks affect one in three Australian adults. PwC estimates that the worst breaches at small businesses cost on average \$135,000 and \$240,000. A Kaspersky Labs survey in 2016 found that the average amount of damage caused by a ransomware attack might be up to \$99,000 for small to medium businesses. There are therefore several means by which cyber security issues can affect (or even destroy) your business.

² Craigen, Diakun-Thibault and Purose, 2014.

First, a hacker might obtain sensitive information from your systems such as credit card data or personal, private information relating to customers. There are open markets for such information on the 'dark web' – the seamier alleyways and byways of the internet. Credit card information has obvious value, but so too does personal identification data as it allows identity theft to take place.

Small businesses often do not manage data securely, and small firms such as accountants and financial planners are attractive targets for identity theft as they often have lax security but have a great deal of precious information about real people. This information can be used to facilitate identity theft.

A second but related issue is that, when a hacker obtains sensitive information about the business, the business may find its reputation ruined. Few small businesses can survive the damage to its reputation that losing data that allowed identity theft to occur. The damage to business reputation and goodwill might be more crippling than the actual data loss itself.

A third aspect of cyber security that causes considerable problems for SME businesses is ransomware. From about 2012, ransomware attacks such as Cryptolocker, Reveton, and WannaCry (along with countless others) have adopted commercially-focused business models. That is, computer viruses have been commercialised to turn a profit with criminals holding business data to ransom. Ransomware such as this has had a high impact upon SMEs. Ransomware continues to be a business strategy for cyber-criminals, even to the extent of the development of the provision of 'Ransomware as a Service' franchise business models on the darknet, the internet's 'Wild West'.³

Be vigilant about anti-virus and not installing 'dodgy' software (e.g. screensavers, games) from 'dodgy' internet sites on business computers. Install reputable anti-virus software (e.g. Sophos), and keep devices (laptops, phones, voice recorders) and software up-to-date so that the latest software is managing your data. Many cyber breaches from third parties are because older software is being used - no-one quite got around to updating it.

Third, the data loss might result in court action against the business. A third party might sue your business as they have themselves made a loss. SMEs might also be subject to significant penalties and/or court action arising from breaches of the Privacy Act in Australia – in general, this Act applies to health information or private information maintained by businesses with more than \$3m turnover, but it can capture small businesses as well.

In these cases, even if the court action against your business ultimately fails, the cost of defending against the action – and the associated distraction that causes – is a significant problem and a cost. Data loss may also result in a need to notify affected individuals under changes to the Privacy Act to implement mandatory data breach notification requirements.

In our modern world, many of the old threats no longer exist. Few businesses need concern themselves with Bonnie-and-Clyde-style crime. However, new threats now exist, and your business needs to be sure it is equipped to deal with them.

Remote working

A recent and specific example for cyber security is the extensive 'pivot' to 'working from home' that has occurred during the COVID-19 pandemic. The urgent need to pivot and move tasks and technologies to employee homes means that these devices may no longer be properly secured, or the devices may never have

³ Meland, Bayoumy and Sindre, 2020.

been appropriately secured for the needs of the business. Rather, the driving force was the need to 'get back up and running'. Accordingly, these devices can become avenues for cyber-attack if they are brought back to the workplace without proper review, update, and patching by the business.

CPA Australia provides a number of resources on remote working:

- [Cyber security essentials for working remotely](#)
- [Remote working checklist](#)
- [Fact sheet: Setting up your virtual office](#)
- [Webinar recording: How to set up a virtual office](#)
- [Remote working templates and forms \(contained within COVID-19 employer's manual\)](#)
- [Data security in the age of working from home](#)
- [Stay safe: Practical tips to create a cybersafe environment](#)
- [Top tech tools to help you work from home](#)
- [8 essential tech tools for your home office](#)
- [Safe from harm – online security when working remotely](#)
- [7 tips for troubleshooting your remote work technology](#)
- [Secure your data - 6 cybersecurity solutions in the COVID-19 era](#)

In addition, the Tax Practitioners Board have a [webinar recording](#) and [FAQs](#) on being cyber aware.

Risk mitigation

There are several things you can do to reduce the risk of cyber-attack. Australian Signals Directorate guidance highlights eight cybersecurity strategies to protect you and your business.

- **Application whitelisting**

Windows (and Macs) are intended to be easy to use and, by default, the user can install and run almost any application. Application whitelisting allows only authorised software applications to run on your computer. No other software is allowed to run. This approach is restrictive for some power users, but most users use a small set of applications to complete their tasks. A wider selection is often simply not needed.

- **Patch applications**

Many applications are regularly updated to address security vulnerabilities as they become apparent – quickly and regularly updating (or 'patching') the software will remove a key means by which cyber-security attacks are carried out.

- **Patch operating systems**

As with applications, security weaknesses are often discovered in operating systems. Again, quickly and regularly updating the operating system defends against most cyber-security attacks. The WannaCry attack in 2017, for example, took advantage of a vulnerability that had been patched for nearly two months.

- **Restrict administrative privileges**

Again, Windows is intended to be easy to use, and often users have free reign of the computer. However, administrator privileges should only be provided on an as-needs basis, as otherwise exploits have the 'keys to the kingdom' and can corrupt the computer itself.

- **Disable untrusted Office macros**

Macros ("Visual Basic for Applications") in Office are useful, simple, and prone to abuse by cyber-attacks. Macros should be blocked so that only approved macros are run on the computer.

- **User application hardening**

One way different types of malware infect computers is to take advantage of weaknesses in popular tools such as Flash and Java. These should be blocked or uninstalled completely.

- **Multi-factor authentication**

Although having a strong password is an assumed requirement, multi-factor authentication means that the user requires another 'factor' in addition to the password for their account (particularly for 'privileged actions' on the computer such as installing software). These factors might include, for example, a separate PIN, a physical token, or a fingerprint scan.

- **Daily back-up of important data**

Off-line, incorruptible, and disconnected backups – that cannot be encrypted by the malware – is a key corrective control that stops the malware from encrypting your 'live' data as well as the backed-up data.

Although these eight strategies are not a complete vaccine against cyber-attack, the Australian Signals Directorate considers that the 'Top 4' strategies (application whitelisting, patching applications, patching operating systems, and restricting administrative privileges) mitigate over 85% of targeted cyber intrusions.

One problem with implementing cyber security is that people often - wrongly - think that they are secure as they haven't been breached. In fact, many have been breached without knowing it. It's so easy to lose data - how much of the business's data is secured with strong passwords?

Many rely the 'She'll be right' strategy. However, hope is not a strategy. Cyber criminals know that many people use the same password in many different places. Even when that password is known to be compromised, people often do not change the password on all the sites they use.

You should check out whether your password has been comprised with the haveibeenpwned.com website. Using a password manager rather than sticky notes with your password written down is important. And, in particular, you should stop using the same password on all your accounts!

A good password manager works with your phone, tells you which of your passwords are weak or have been compromised. A good password manager also helps you create more secure passwords than 'password123'. It's hard to remember all those passwords - so stop trying and use a properly-secured password manager instead. You should also stop sending sensitive data by email. Instead, use an authenticated sharing service and a secure portal, and ensure that sensitive data shared by email is encrypted or has strong access controls through a strong and secure password.

If, despite your precautions, your business is the victim of a ransomware attack, you have three basic options:

1. Use a recent, uncorrupted back-up to restore your data
2. Try one of the decryption websites for information and decryption tools, such as No More Ransom
3. Pay the ransom.

When it comes to ransomware, sometimes it may seem that your only pragmatic option is to pay the ransom. That, however, tends to place you on a 'sucker list' and you will likely receive even more attacks into the future.⁴

MONITORING BUSINESS COMPLIANCE NEEDS

The regulatory environment your business faces is constantly changing. You must know the business's compliance requirements and be aware of recent legislative changes. This means you must keep the IT documentation and IT Strategy current and ensure your service providers continue to meet business needs.

You should document your strategy, at least with a hardware plan and basic software roadmap. Simple templates for documenting your IT strategy are available and, once documented, you should be sure to review the strategy at least once a year and compare it to your overall business strategy and compliance requirements.

Privacy Act

A major compliance requirement is the Privacy Act. As a general rule, the Privacy Act applies to all companies of over \$3,000,000 turnover, as well as companies that manage health-related private information and other specific types of activities. The Privacy Act sets out 13 Australian Privacy Principles (APP).

These privacy principles set out the fundamental requirements of entities in Australia that manage private and/or sensitive information.

Data breach notifications

In 2018, Australian privacy legislation came into effect that required certain businesses to notify affected individuals where an eligible data breach occurred. This scheme required notification for eligible data breaches likely to result in serious harm to the individual.

Not all data breaches are eligible. For example, if an entity acts quickly to remediate a data breach, and as a result of this action the data breach is not likely to result in serious harm, there is no requirement to notify any individuals or the Office of the Australian Information Commissioner (**OAIC**).

From its commencement in February 2018 to 30 June 2018, this scheme had 305 notifications made. 59% of these breaches were malicious or criminal attacks, 36% arose through human error, and 5% arose through system faults. Most of these breaches (61%) reported affected 100 or fewer people. The majority of malicious or criminal breaches related to compromised passwords, and 32 of the 88 human errors resulting in a notifiable data breach related to the use of email. From 1 January 2020 to 30 June 2020 there were 518 notifications of eligible data breaches, of which 317 (61%) were malicious or criminal attacks and 176 (34%) arose through human error. System faults were the source of 25 (5%) of these notifications. It is apparent that the source of eligible data breaches have remained remarkably stable during the period of the scheme.

⁴ Saunders 2017.

What is an eligible data breach?

An eligible data breach arises when the following three criteria are satisfied:

1. there is unauthorised access to, or unauthorised disclosure of, personal information, or a loss of personal information
2. this is likely to result in serious harm to one or more individuals
3. the entity has not been able to prevent the likely risk of serious harm with remedial action.

For more information on eligible data breaches read the OAIC's [guide to managing data breaches](#).

What does serious harm mean?

In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm.

In making an assessment of harm you need to consider the nature and sensitivity of the personal information, who has obtained or accessed the information, or who could obtain or access the information and the nature and consequences of the harm.

Notification process

In the event of an eligible data breach you need to:

1. complete an assessment within 30 days of becoming aware of the breach
2. notify affected individuals and the Australian Privacy Commissioner as soon as is practicable.

The notification to individuals should include:

- the identity of the organisation
- the description of the breach
- the kind of information concerned
- any response the individual should make as a result of the breach.

You have a choice about how many individuals to notify. You may:

1. notify all individuals to whom the relevant information relates or
2. notify only those individuals at risk of serious harm or
3. publish a notification on your website and take proactive steps to publicise it.

If the requirements of the mandatory data breach notification scheme are not met, then significant penalties may apply - in 2018, the penalty is \$2.1 million for businesses and \$420,000 for individuals.

Small business and the Privacy Act

The Privacy Act does not apply to all SME businesses, but its application can be surprisingly broad. First, although the Privacy Act applies to businesses with \$3m turnover or more, that level of turnover is not necessarily all that big a business. Many businesses operate with slim profit margins, and such businesses would be caught as they might have a sizeable turnover even though their profit is not particularly large.

Some other small businesses - particularly accountants or financial advisors - might be caught by the little-known '[TFN rule](#)', or they might store health-related information. In both cases, the Privacy Act applies irrespective of the business's turnover. This rule means that [some smaller businesses](#) can be caught by the Privacy Act, at least for the management of certain types of information such as Tax File Numbers or health records.

These businesses can have professional obligations, and regulators (e.g. ASIC, ATO) may apply fines on companies or directors. The Tax Practitioners Board has good advice for accountants, and with that advice available as an example an accounting firm cannot ‘hope and pray’ and leave data privacy ‘to the Techheads’. You are still responsible. So, you need to take steps to reduce your risk of data breach.

Even if your small business is not subject to the Privacy Act, you may wish to treat these principles as ‘best practice’ for how you should manage private information. That is, you may wish to voluntarily comply with these principles to demonstrate that your business manages customer information according to best practice. Without wanting to preempt and predict future developments, the long term trend has been toward the tightening – not loosening – of the data privacy standards that businesses have to meet.

The OAIC has a [checklist](#) that will assist in determining whether the Privacy Act applies to your business.

KEY EXTERNAL SERVICE PROVIDERS

Selecting an external service provider

At the start of this checklist it was noted that few small businesses have the resources for their own dedicated IT support staff. CPA Australia can provide some assistance with selecting different types of IT service providers, specifically, selecting a [cloud service provider](#) and selecting an [outsourced service provider](#).

At a high level, it remains important that you understand what is needed from ICT and know what types of services can be done by a service provider and which need to be done in-house. It is good to keep the ability to direct your IT to meet your strategic needs in-house, but clearly many commodity services can be provided more effectively and efficiently by a dedicated service provider.

It is also important to consider whether you should have more than one service provider. A single service provider can more easily be held accountable than multiple service providers but presents a risk to your business if that provider fails as you leave access to all of those services at once.

Some of the issues to consider when selecting a service provider include the service provider’s background, whether you can work with the provider and the staff that they want you to work with, their ability to address your needs securely, and how they will go about implementing the system. Your own legal requirements are also an important consideration. Finally, in these days of social media it is important that you consider the service provider’s ‘digital footprint’ on social media in the same way that your clients evaluate your business. Search online for reviews of the service provider.

Using the above as a guide, the below could be your starting point in selecting a service provider:

- a clear and enforceable service agreement
- clear scope and acceptable performance of services over the long term (for example, are software updates and hardware upgrades considered - what is appropriate in 2020 will likely not be appropriate at the end of an agreement in 2025)
- a process for extension of the contract as well as variation of the services (and service levels) provided
- pricing and fee structure that is realistic without ‘hidden’ costs for out-of-scope and unforeseen services
- payment terms that align the benefits with the costs of the agreement
- clear representations and warranties
- outline your respective obligations (for example, how will you address the need for interruptions to the working day and manage the ongoing relationship)

- ascertain their service availability (for example, can you contact them 24/7 if you are the subject of a cyber-attack?)

It is also important that any contractual arrangement you do put in place aims to maintain a strong relationship with the service provider. Frequently, relationships such as these start out strongly, but over time the relationship can be taken somewhat for granted.

If the relationship deteriorates over time, problems that arise can become much bigger if the relationship is not good to start with. It is important that you maintain a strong professional relationship in the good times so that when things are not going well, you have a level of understanding and trust to draw upon.

In CPA Australia's [Guide to the Cloud](#), it is considered essential that you proceed cautiously with your choices, consider the location of the service provider, and place an emphasis on selecting a provider you can work with rather than just considering price alone. You should also give thought to your own clients' needs with how you manage their data and understand your service provider's proposed disaster recovery arrangements and data backup approach. Finally, you need to have an eye to how you might 'divorce' your service provider if and when the relationship is no longer working for the both of you.

As a concluding consideration, you should keep a list of the key external service providers that you use – for example, an IT support business or a cloud service provider such as Microsoft 365 or Xero. Be sure to meet with these service providers regularly to discuss how that service is performing and whether there are improvements that can be easily achieved. You should also satisfy yourself that your business could download its data and applications and move to another service provider easily. If your business is 'locked in' with the service provider, you will be unable to change providers easily if they fail, or you wish to get better value with a different service provider when you 'divorce'.

ABOUT THE CHECKLIST

The following checklist has two components.

First, the **Top 10 Tasks** you must undertake for good information security.⁵

Second, a **Detailed Checklist** to ensure that your business delivers good ICT service delivery.

In both cases, a business owner should consider each checklist item in accordance with their own needs.

At its heart this checklist remains focused on the issues you face so you do not forget the important items. Each item on the checklist aims to ensure that you think clearly about your own requirements and prompts you for further action.

⁵ Based upon the security tips for business identified by the Cyber Security Working Group (2017) and the Australian Signals Directorate (2017).

TOP 10 TASKS OF INFORMATION SECURITY

TASK	DESCRIPTION
1. Passwords	<p>Ensure your passwords are strong and secure and use multi factor authentication where possible.</p> <p>Regularly change passwords, and do not share them.</p>
2. System Access	<p>Remove system access from people who no longer need it, and limit access to only those needed to do their role.</p> <p>Administrator privileges are provided on an 'as-needs' basis.</p>
3. Secure Wi-Fi & Devices	<p>Secure your wireless network and be careful when using public wireless networks with mobile devices.</p> <p>Avoid transacting online where you are using public or complimentary Wi-Fi.</p> <p>Never leave your information physically unattended – secure your electronic devices.</p>
4. Legitimate Software	<p>Only download/install programs from a trusted source.</p> <p>Consider using application whitelisting so only authorised software applications run on your computer.</p> <p>Disable untrusted Office macros and block or uninstall Flash and Java.</p>
5. Patches and Anti-Virus	<p>Ensure all mobile devices/operating systems/software have the latest available security updates and run weekly anti-virus/ malware scans.</p>
6. 'Clean' devices	<p>Do not use USB or external hard drives from an unfamiliar source.</p>
7. Social Media	<p>Be vigilant about what you share on social media – try to keep personal information private and know who interact with online.</p>
8. Email	<p>Use a spam filter for your email and use email carefully - be wary of downloading attachments or opening links in emails you have received in case it is a 'phishing' attempt.</p>
9. Secure Snail Mail	<p>Use a PO Box, or ensure your mail is secure.</p>
10. Daily backup	<p>Use off-line, incorruptible, and disconnected backups.</p>

DETAILED CHECKLIST

There are four activities a small business needs to focus on to keep IT working: how to *plan, build, manage* and *run* IT.







The below detailed checklist considers areas of IT management by looking at each focus activity in turn. Each activity identifies related items for the business to consider.



On this list items marked with a star are *essential* for the good governance and delivery of IT.





FOCUS	IT CHECKLIST FOR SMALL BUSINESS ⁶	
PLAN	1. Set out a general strategic direction for your IT	
	It is hard to get to where you are going if you don't have a roadmap to get there. Make sure that you have at least a rough direction of what your IT needs to do, how this is to be achieved, and when it will be done.	
	You have a short plan that outlines why you need IT, what it is for, and how it is to be used in support of the business.	<input type="checkbox"/>
	You know what sort of technology you need to have, what it needs to be compatible with, and what you might need in the future. Don't just buy what another company wants to sell you.	<input type="checkbox"/>
	You have an IT budget for the next 12 months that replaces out-of-warranty equipment and buys new technology you need.	<input type="checkbox"/>


⁶ Primary resource: ISACA COBIT 5 Enabling Processes.



	2. Manage and mitigate IT risks	
	Like all aspects of business, IT has risks to be dealt with. Be sure to have at least thought about the major risks to your business and how you might cope with them.	
	You know how long your business can survive without IT before you can't catch up – is it a week? 3 days? 1 day? 1 hour?	<input type="checkbox"/>
	You have written down the risks that might occur (from likely to unlikely) and how bad they might be if they do occur (from insignificant to catastrophic).	<input type="checkbox"/>
	You have a risk register detailing the worst risks, how they affect the key business function (e.g. sending invoices) and the tasks you need to do to reduce this risk.	<input type="checkbox"/>
	You know what your compliance risks are for your industry – does the law mean that you have to manage your data in a particular way, and does everyone working in your business treat your data with appropriate respect?	 <input type="checkbox"/>
	3. Deliver upon the IT projects you set yourself	
	A wish list is not sufficient, make sure the IT projects you sign up for are ones you need and can achieve.	
	Your IT projects are never done because they are 'fun' but because they support the business.	<input type="checkbox"/>
	Your IT projects have a rough business case before implementing.	<input type="checkbox"/>
	IT projects have an outline of how they are going to be achieved, when they are to be achieved, and what they need to deliver.	 <input type="checkbox"/>
BUILD	4. Installing new equipment (servers, PCs, laptops, printers, scanners etc. along with their related drivers)	
	In a small business, it is tempting to buy new equipment without having thought about how it will be installed. You don't want the entire business to come to a stop as five people try to install a new scanner 'just like the one we have at home'.	
	Make sure that the equipment you buy is suitable for a business network environment. Not all equipment suitable for home use will run on a business network.	 <input type="checkbox"/>
	Make sure that new equipment has an appropriate warranty – while not always good value, extended warranties can reduce the impact on your business if equipment does break unexpectedly.	<input type="checkbox"/>
	If you don't have an onsite IT professional, when you buy new equipment consider arranging for the vendor to install it. While it may cost a little, it may be cheaper than having your staff fumbling at a task that is not their area of expertise.	<input type="checkbox"/>
	To reduce complexity, consider limiting your purchases to a few brands and types of equipment that you trust and are familiar with. Try to have a common operating system (e.g. Windows 10) on all computers to make maintenance easier.	<input type="checkbox"/>



	Make sure that new drivers (e.g. printer drivers) are installed when you buy new equipment. Even if the new printer seems to work with the old drivers make sure that everyone is using the same drivers for the same printer.	<input type="checkbox"/>
5. Customising software to suit the needs of the business		
	'Customising' can mean lots of things: writing a quick macro in PowerPoint; creating a stand-alone application based on Excel; or writing customisations that live within your line of business application or accounting system. Sooner or later most small businesses will do one of these. Some can be done in-house by 'power users' but if it's something that is important to the business (and not just important to the user) you need a professional.	
	You have decided what customisations are appropriate for your business and decided, in general terms, how they will be created. Consider whether it is appropriate to let the in-house 'power user' have a week or two to work on some Word macros and when you will call in an expert.	<input type="checkbox"/>
	You have clear and exclusive rights to the intellectual property of software developed by third party contractors where that software is key to your business.	<input type="checkbox"/>
	Before customising software and 'building your own', you ask a mentor to be sure that you really need this customisation as you know that software customisations are often more expensive and take longer than initially thought and can quickly be outdated.	 <input type="checkbox"/>
6. Deploying existing software to new users, setting up new software and deploying new software to existing users		
	This task needs to be undertaken with some care. First, to ensure that the software is installed and set up appropriately and second, to ensure that licensing arrangements are followed.	
	If you have an IT professional inhouse then you have discussed how software is to be deployed and set up.	<input type="checkbox"/>
	If you do not have an IT professional inhouse then you have established a working relationship with a professional who can guide you in deploying and setting up software.	<input type="checkbox"/>
	You have a firm understanding within the business of when tasks will be done in-house and when you will call in outside help.	<input type="checkbox"/>
	Your subscription software (e.g. Microsoft 365, Adobe) is automatically downloaded and kept up-to-date.	<input type="checkbox"/>
	Software is only installed from a trusted source or from the original shrink-wrapped products. Block, uninstall or at least limit the use of Flash, Java and Office macros where possible as such insecure software is a frequent source of cyber security vulnerabilities.	<input type="checkbox"/>


7. Downloading, assessing and deploying security patches to ensure secure mobile devices, operating systems and applications		
As long as malicious users continue to try to breach systems through security holes in software, software vendors will be issuing security patches. Modern operating systems have the option to 'auto-update' the machine with security patches. Application whitelisting is also considered a strong control against cyber security attacks. [See also Australian Signals Directorate (2017)]		
You have considered and decided on a policy for installing security patches. For example, you may decide to install all security patches as soon as they are made available. Or, if your line of business or back office systems are old, uncommon or heavily customised, you may have a policy of testing each security patch against your software to ensure that it will still work properly.		<input type="checkbox"/>
You have allocated responsibility to one person for downloading, assessing (if necessary) and deploying security patches for the operating system and applications (line of business applications, back office systems and desktop applications).		<input type="checkbox"/>
Your desktop computers auto-update to implement patches that are provided by the operating system developer.		 <input type="checkbox"/>
You have a process in place (perhaps a routine security audit by an external person) to check that security patches are being deployed appropriately.		<input type="checkbox"/>
Consider application whitelisting so only authorised software applications run on your computer.		<input type="checkbox"/>
8. Administration: maintaining records of software licences, domain names, service contracts for peripherals like printers, liaising with vendors		
Your software licences are valuable. It's easy to install software on a machine and 'forget' that it is there. It is also easy to forget what service contracts you have in place for your equipment. Finally, it is easy to forget to renew a domain name. Domain names are cheap, but very valuable. If you don't renew your domain name someone else can register it and you will struggle to get it back.		
You have allocated responsibility to someone to keep a list of what software is installed on every machine, with what licence to ensure that the business is complying with the licence agreements and is protecting the business's assets.		 <input type="checkbox"/>
You have allocated responsibility to someone to keep a list of what domain names and web hosting arrangements you have, with expiry dates. You have a system in place to remind you of when to renew domain names (you should renew them about three months in advance of the deadline).		<input type="checkbox"/>
You have allocated responsibility to someone for maintaining a list of all service contracts. Only one person is permitted to call a vendor for service.		<input type="checkbox"/>
You have allocated responsibility to someone for maintaining all usernames and passwords for the online services your business uses in a password protected database that you can access from any PC with internet access in the case of disasters (e.g. Evernote or LastPass for Business).		<input type="checkbox"/>



MANAGE	9. Manage your IT – is it adequate?	
	Much as we'd like it to be, IT is not 'set and forget'. Keep an eye on IT to be sure that the hardware you have is up to the task, and that your service providers continue to perform. Regularly review whether your IT needs are better met by an external IT service provider, a cloud solution provider, or in-house, depending on your business growth.	
	You regularly review your IT for out-of-warranty equipment and replace such equipment when the technology is key to the business.	<input type="checkbox"/>
	You have an independent mentor to discuss your IT needs with from time to time.	<input type="checkbox"/>
	You regularly (at least every three years) 'test the market' to be sure that your IT service providers are still the best 'fit' for your business.	<input type="checkbox"/>
	When staff expectations of IT service providers are not met, the staff know they have someone to raise the issues with.	<input type="checkbox"/>
	10. Meet your legal requirements	
	There are all sorts of requirements businesses have to meet. If you don't meet them you may have unexpected fines when transgressions occur. [See OAIC]	
	You have reviewed your small business's privacy obligations at the OAIC's website and identified your legal obligations.	 <input type="checkbox"/>
	You have policies to ensure that your privacy obligations are met.	 <input type="checkbox"/>
	You have reviewed your small business's record-keeping obligations as set out by the Australian Taxation Office and identified your record-keeping obligations.	 <input type="checkbox"/>
RUN	11. Downloading and deploying hourly data files for anti-virus software and maintain a spam filter on email	
	Viruses are invented daily so you need to ensure that data files for your anti-virus software are downloaded and installed daily. Viruses in this context include all forms of malware, viruses, Trojans, spyware etc. Such viruses commonly infect networks through the use of email so a spam filter is required.	
	You have set up the anti-virus software to update hourly, run a full scan each week and send an email alert to the responsible person or, if that person is away on leave or for illness, alerts go to someone else.	<input type="checkbox"/>
	If your business runs seven days a week, then there is a way to address alerts each business day.	<input type="checkbox"/>
	Your anti-virus software addresses viruses, Trojans, spyware, key-logging software and warns against suspect web pages.	 <input type="checkbox"/>
	You have a spam filter in place to ensure most dangerous unsolicited email is not downloaded onto your network.	<input type="checkbox"/>
	Your users know to be vigilant for 'phishing' emails that may contain Trojan horses and check suspect emails with others.	<input type="checkbox"/>





12. Disaster recovery (e.g. after prolonged power failure, fire, flood, theft)		
	Your business may depend on your IT system and so you need to know that the business will survive even if the IT system is destroyed or damaged.	
	You have acted to prevent disasters by installing surge protectors, power conditioning and uninterruptible power supplies. You have software in place to enable a controlled shutdown of servers and you have tested these systems.	<input type="checkbox"/>
	You have a plan in place for how to get your business up and running again. For example, some businesses make an arrangement with a similar business to act as a 'warm site' so that there is at least one computer in their office that you could use to restore your backups.	 <input type="checkbox"/>
	You have written out the steps to be followed after a disaster. Remember that as owner or manager you may not be available after a disaster to perform work like this, or even direct it.	<input type="checkbox"/>
	You have ensured that the relevant employees in the business know where to find the disaster recovery instructions and how to follow them. Procedures are printed out at a different location.	<input type="checkbox"/>
	You have practised your disaster recovery steps at least once with your current team.	<input type="checkbox"/>
	You are able to access passwords to online services that the business uses (e.g. through Evernote or LastPass for Business).	<input type="checkbox"/>
13. Creating and maintaining in-house rules about access, permissions, passwords and other safety, security and administrative rules		
	Intruders, former employees and kids hacking for fun can access your business's information unless you have rules for who can access what data.	
	You have written rules (perhaps only one page) on who is allowed to access what data, how passwords or pass phrases are to be formatted, how often they expire, at what intervals they can be recycled and other security issues.	<input type="checkbox"/>
	Your rules mean that no-one ever has to share their password with another user. If users share a computer each person has an individual profile, user name and password. People in the office know that using someone else's password is like forging their signature.	<input type="checkbox"/>
	The business's rules address safety issues such as ensuring that cables do not run across hallways or walkways, appropriate numbers of power outlets are available for IT equipment and that staff follow appropriate practices in using IT equipment to prevent accidents or injury.	<input type="checkbox"/>
	You have developed a communications strategy and have allocated responsibility to someone in the office for ensuring that new employees know about the rules.	<input type="checkbox"/>
	You have allocated responsibility to someone in the office to keep the rules up-to-date.	<input type="checkbox"/>



14. Creating, maintaining and deleting users from the network		
	New employees need to be added as new users to the network, and just as importantly, former employees need to be removed as soon as they leave the business.	
	You have allocated responsibility to one or two people to add new users to the network (this will be the 'network administrator').	<input type="checkbox"/>
	You have a system in place where a new user can be added to the network so they can be productive from the day they start work (without having to use someone else's password to access the network).	<input type="checkbox"/>
	You have a process in place to maintain a central registry of passwords to business-critical files, online services, or applications, or to retrieve passwords from departing employees. For example, an accounts clerk may have passwords to the online banking, or employees may have password-protected individual documents that the business will need.	<input type="checkbox"/>
	You have a process in place to change online passwords when employees depart.	 <input type="checkbox"/>
	The person who calculates the final pay for an employee leaving the business is responsible for informing the network administrator that the employee is leaving. The network administrator is responsible for disabling that user from the network as soon as they receive notice.	<input type="checkbox"/>
15. Creating and re-setting the network passwords		
	All new users on the network will need a password that they can change for their own needs. And whether we like it or not, users often forget passwords and can be locked out of the network.	
	The network has a 'three strikes and you're out' policy: if a user gets the password wrong three times in a row, the user is locked out of the network.	<input type="checkbox"/>
	The network administrator can re-set the password of someone who is locked out within a very short time (say, 10 minutes). Someone is allocated as backup for this task to cover meal breaks, leave and other absences.	<input type="checkbox"/>
	The network operating system is set up so as to require users to change their network password regularly (say, every month or every three months).	<input type="checkbox"/>
	Password rules (e.g. how long a password must be, and how frequently it must be changed) are appropriate to the circumstances but are not so difficult that users are tempted to write them down.	<input type="checkbox"/>
	Secure your wireless network. You have changed the default password on your Wi-Fi network's equipment (e.g. routers/wireless hubs) and have implemented encrypted security channels rather than an open Wi-Fi connection.	 <input type="checkbox"/>



16. Setting up shared folders, disk quotes, and granting / reducing access rights to data, systems and applications		
	<p>Shared folders allow groups of employees to access the same files. Disk quotas restrict the amount of data that one employee can store on a server or a cloud service. Ensure system and application access addresses what employees need to undertake their role, and no more. These tasks have security and performance implications.</p> <p>[See CPA Australia's Cloud computing guide]</p>	
	The business has appropriate rules in place so that people can see the data they need for their job, but data is generally secured.	 <input type="checkbox"/>
	System and application access rights are reviewed and removed from people who no longer need it due to changed roles – limit system and application access rights to what is needed.	<input type="checkbox"/>
	Administrator privileges are provided on an as-needs basis, even to their own mobile devices.	<input type="checkbox"/>
	Someone (the 'network administrator') has been allocated the job of managing shared folders and granting permission to individuals or groups to see the files in those shared folders.	<input type="checkbox"/>
	Permissions to access shared folders are reviewed regularly (quarterly?) and permissions are deleted when they are no longer needed (perhaps because someone changed roles).	<input type="checkbox"/>
	If appropriate, disk quotas are in place that limits the space that employees' files can take up on servers and cloud services. Employees should not store large files unless needed.	<input type="checkbox"/>
	All business data should be stored on the server or managed cloud data service where it can be secured and backed up.	<input type="checkbox"/>
	Cloud data services such as DropBox, iCloud and Google Drive are implemented in full awareness of the potential risks and benefits of such services – do not implement these lightly.	 <input type="checkbox"/>
17. Training users in how to use new software and hardware		
	The more your users know about the software they use every day, the more productive they can be. You don't want office staff wasting time on page numbers every time they have to produce a Word document when a few hours of training would teach them how to do it once and for all. Few users manage to teach themselves anything beyond the basics but sending people to generalist 'Introduction to X' or 'Intermediate Y' courses often don't help. To be effective you have to be specific.	
	You have talked with the staff of the business and written down what tasks they need to perform using their software.	<input type="checkbox"/>
	You have made plans to get appropriate information or training for them to perform those tasks effectively and efficiently.	<input type="checkbox"/>

	You have a way of checking back with employees soon after training about whether they can now perform the relevant tasks. If skills learned in training are not used on the job immediately they may be lost and the training will have been wasted.	<input type="checkbox"/>
	You have considered using a private YouTube channel to create videos of how to perform tasks using your current software – this way a new employee can use these videos to understand how to carry out tasks essential to your business if the usual person is on leave or departs the business. Free software is available but check that this free software does not itself introduce malware. Be sure that no passwords are included on the video.	<input type="checkbox"/>
18. Acceptable use policy		
	Computers are powerful tools and increasingly their use for purposes unrelated to your business may affect you. Be clear to all your staff what they may use your computers for (and what they may not).	
	You have an acceptable use policy that has been reviewed by, or provided by, an industrial relations expert that sets out what users can and cannot do with your IT equipment.	 <input type="checkbox"/>
	The rules in place identify what personal use of computers and internet access is reasonable in the circumstances for this business.	<input type="checkbox"/>
	Do not use USB or external hard drives from an unfamiliar source without the device being scanned on a known secure machine that is disconnected from the network.	<input type="checkbox"/>
	Online Social Media tools such as Facebook and Twitter may be used by employees and inadvertently affect your business reputation. Your acceptable use policy makes it clear to employees what they can and cannot do when using online social media like Facebook and Twitter.	<input type="checkbox"/>
	Online Social Media tools may be used by employees to 'cyber-bully' co-workers. Your responsibility to maintain a safe workplace means that your acceptable use policy makes it clear to employees that such behaviour is unacceptable.	<input type="checkbox"/>
	All staff must be vigilant regarding the information shared on social media – try to keep personal information private, and ensure employees are aware that such data may be used to 'socially engineer' access to your data or to undertake 'spear phishing' attacks.	<input type="checkbox"/>
	Your acceptable use policy also addresses what people can do with business data (e.g. copy it, share it) on their 'BYOD' devices such as iPads, iPhones, and Android devices.	<input type="checkbox"/>
	Your users know to be careful when using public wireless networks. Online transactions are not carried out using public wireless networks.	<input type="checkbox"/>
19. Cleaning up machines that have been infected with viruses, Trojans, worms or other malware		
	In spite of your best efforts some machines will get infected with viruses or other malware (laptops are more vulnerable than desktop machines). You need them cleaned up properly, and in the case of severe infection, this is a job for an expert.	

	You have decided how you will isolate infected machines from the network and employees know when to tackle the clean-up job themselves and when to call in an expert.	<input type="checkbox"/>
	If you don't have an IT professional on staff you have established a working relationship with an IT professional who can be available to clean machines at relatively short notice.	 <input type="checkbox"/>
20. Answering basic questions from users about how to use the software and hardware and troubleshooting minor problems		
	Your investment in desktops, laptops and software licences is significant. It is no use investing in these unless your people can make use of the hardware and the software. And, while support and advice from colleagues is a good way to learn, you don't want the entire office to stop work while everyone crowds round one person's desk as they try to create a table of contents in Word.	
	You have allocated responsibility to one person (with a backup if necessary) to replenish stocks of paper, toner etc. for printers and fax machines.	<input type="checkbox"/>
	You have devised a process for users to get help in using software and hardware and troubleshooting minor problems (such as a printer not working). For example, the process might be that an employee first asks your in-house 'power user' for advice and, if that person can't help, the employee seeks free help (from online newsgroups) or paid help (e.g. from an external advisor or trainer).	<input type="checkbox"/>
	Everyone in the business knows the process and you encourage them to use that process by following it yourself.	<input type="checkbox"/>
	New employees are told about the system and encouraged to use it.	<input type="checkbox"/>
21. Maintaining physical security over IT equipment, backup tapes or disks etc.		
	If someone steals your computers or your backup tapes you lose not only the equipment but all the data on it. Physical threat is as likely to come from careless or malicious staff as well as outsiders. Make sure you have your hardware and backup tapes or disks secured.	
	You have a secure, locked, air conditioned or well-ventilated space for servers and other equipment that does not have to be out in the open. As few people as possible have access to this space.	<input type="checkbox"/>
	Someone in the office has been allocated responsibility for locking up the area where servers and backup tapes are stored. A backup person is organised to cover times when the primary person is unavailable because of holidays, illness etc.	<input type="checkbox"/>
	Backup tapes and disks are routinely stored off-site in a secure location as 'cold' backups.	 <input type="checkbox"/>
	Where equipment is out in the open, or is left unattended for periods of time, desktop machines are locked to the desk or to a portion of the building structure.	<input type="checkbox"/>
	The business has a policy on security of laptops and mobile devices when out of the office (for example, employees may not leave laptops in a car). This policy includes the security of mobile data devices such as iPads and iPhones that have business data on them. Devices are not left unattended.	<input type="checkbox"/>

	Critical business data is not stored on easily-lost USB sticks or external hard drives.	 <input type="checkbox"/>
	You are able to remotely 'wipe' any mobile device your business owns that has your business's data on it. You are also able to remotely 'wipe' your employees' mobile devices where they have sensitive business data you do not want others to find.	 <input type="checkbox"/>
22. Making, testing and restoring backups (from whole servers to single files)		
	What is your data worth? If you lost everything how long would it take the business to be up and running again? What would it cost, in time or money, if your business lost the last month's data? A backup is only as good as what you can restore.	
	You have a documented backup process that provides for off-line, incorruptible and disconnected backups. You have allocated responsibility to someone for backing up data from servers every day. This includes reviewing the backup log for any issues relating to the success or failure of the backup and responding to those issues. Someone is available, and is trained, to cover for your main person if they are away for a day.	 <input type="checkbox"/>
	You have a documented restore process and you regularly (monthly? quarterly?) test that you can restore data from your backups.	 <input type="checkbox"/>
	At least some backup media are stored off-site. For example, if you back up every day you might store every second day's data off-site. It may be appropriate to keep regular permanent backups off-site, such as a backup of financial data after each end-of-month procedure is completed.	<input type="checkbox"/>
	You have a policy that requires users to store data that is crucial to the business on the server. If a user stores a file on a desktop computer, that file will not be backed up during the normal backup process.	<input type="checkbox"/>
23. Database administration (e.g. SQL server)		
	Very small, or micro, businesses may not run a significant database but most line of business applications and medium-to-large accounting systems rely on an underlying database. Database administration is a specialist skill and few small businesses would have an in-house expert.	
	You have consulted with an expert administrator of your database (e.g. Microsoft SQL Server, MySQL etc.) to write out the routine steps to follow for good administration of the database including securing the database and backing it up.	<input type="checkbox"/>
	You have appointed someone as responsible for undertaking those routine steps.	<input type="checkbox"/>
	You know what you can do in-house and when to call in an expert and have communicated this to staff.	<input type="checkbox"/>
	You have established a working relationship with an external specialist who is familiar with your business and your database set up. You have arranged for that specialist to run brief regular (quarterly? six monthly?) check-ups and be available to fix urgent database problems.	<input type="checkbox"/>

24. Setting up and maintaining the connection to the internet and liaising with the ISP when there are connection problems		
For most businesses, the connection to the Internet is vital. The market remains volatile and ISPs are routinely dropping prices, increasing service speeds and broadening service offerings. You may not want to change ISP every six months but you should stay aware of changes in this market.		
In choosing an ISP you explore a wide range of possible vendors to get the services you need and the best value for money.		<input type="checkbox"/>
Someone has been allocated responsibility of managing the technical aspects of connecting to the Internet. This might be the 'network administrator'. This person deals with the ISP about problems with the connection.		<input type="checkbox"/>
Someone has been allocated responsibility for regularly checking competitive pricing and service offerings from ISPs.		<input type="checkbox"/>
If you use cloud computing, you have a backup means of accessing the internet (for example, an iiNet broadband account as well as a Telstra Wi-Fi hotspot) in case one provider's services become unavailable.		 <input type="checkbox"/>
25. Troubleshooting network problems involving the WAN or LAN (including routers, firewalls, bridges, switches, cabling, wireless access points and devices etc.) and setting up and maintaining systems for remote users to log in to the network from home or while travelling		
Perhaps the most frustrating IT problem is when 'the network goes down'. It can be difficult to pin point the source of the problem and unless you have a networking expert in-house you may need external help.		
You have consulted with an expert in security related to your operating system and are confident that your network is secure. This is especially important if you have a wireless network.		<input type="checkbox"/>
The network administrator has written down all the user names, passwords and settings for all network-related equipment. That information is kept securely but is available to those who may need it to repair network problems.		<input type="checkbox"/>
You have arranged that at least one person is available at all times with basic knowledge of how the network operates. You have arranged for a network expert to write down basic trouble-shooting steps for your in-house person to follow in the case of problems.		<input type="checkbox"/>
You have established a working relationship with an external specialist who is familiar with your business and how your network is set up and can be available at short notice to fix urgent network problems.		 <input type="checkbox"/>
26. Server management (e.g. mail server, web server)		
Even micro businesses may run a server to manage mail but many small businesses will run print servers, mail servers and maybe web servers for intranet or internet sites. Server administration is a specialist skill and few small businesses would have an in-house expert. However, many of these services are available as 'cloud' utilities and should be considered by most small businesses.		

	You have considered whether a cloud equivalent to your existing servers (e.g. Microsoft 365 – which would provide mail servers and file servers) would be more suitable for the business.	 <input type="checkbox"/>
	You have consulted with an expert administrator of your servers to write out the routine steps to follow for good administration of the database.	<input type="checkbox"/>
	You have appointed someone as responsible for undertaking those routine steps.	<input type="checkbox"/>
	You know what you can do in-house and when to call in an expert and have communicated this to staff.	<input type="checkbox"/>
	You have established a working relationship with an external specialist who is familiar with your business and your server set up and can be available at short notice to fix urgent server problems.	 <input type="checkbox"/>

REFERENCES AND FURTHER RESOURCES

- Abrahams, N., & Griffin, J. Privacy law: The end of a long road: Mandatory data breach notification becomes law. *Law Society of NSW Journal*, (32), 2017–2018.
- Al Isma'ili, S., Li, M., Shen, J., & He, Q. "Clearing the 'Cloud': Hanging Over the Adoption of Cloud Computing in Australian SMEs." In *DIGIT 2016 Proceedings* (p. 23).
- Attaran, M. and Woods, J. "Cloud Computing Technology: Improving Small Business Performance Using the Internet," *Journal of Small Business & Entrepreneurship*. 2018: 1-25.
- Australian Signals Directorate. *Implementing Application Whitelisting*. 2016.
- Australian Signals Directorate. *Strategies to Mitigate Cyber Security Incidents*. 2017.
- Axelsen, M. *Delivering information and communications technology services to small to medium enterprises*. 2008. Available from the CPA Australia Library.
- Axelsen, M. "[Why Even Small Practices Are Cybercrime Targets](#)." *InTheBlack Digital*. 2 March 2018.
- Axelsen, M. "[When it comes to ransomware, it's sometimes best to pay up](#)." 30 May 2017.
- Bleier, E. [Amy's Baking company is no more : Notorious Kitchen Nightmares restaurant closes after owners threatened to stab customers , stole from their own staff and broke iron-willed Gordon Ramsay](#). *Daily Mail*. 7 September 2017.
- Bort, J. [Everyone is talking about how Microsoft Office 365 is suddenly beating Google Apps](#). *Business Insider Australia*. 2015.
- Carrigan, D., Gallagher, J., & Di Marco, B. "Australia's New Mandatory Data Breach Notification Regime: How to Prepare Your Business," *Governance Directions* 69, no. 5. 2017: 280-282.
- Chen, C. et al. "Understanding Compulsive Smartphone Use: An Empirical Test of a Flow-Based Model," *International Journal of Information Management* 37, no. 5. 2017: 438-454.
- Clay, K. [Lessons From Amy's Baking Company: Six Things You Should Never Do On Social Media - Forbes](#). *Forbes*, 2013: 1–5.
- CPA Australia. [Cloud Computing: Advantages and disadvantages](#).
- CPA Australia. [A Guide to the Cloud](#). 2014.
- CPA Australia. [Outsourcing: Opportunity or Threat?](#) 2016.
- Craigien, D., Diakun-Thibault, N., & Purse, R. [Defining Cybersecurity](#). *Technology Innovation Management Review*, 4, No. 10. 2014.
- Cyber Security Working Group. *Security tips for business*. 2017.
- El-gazzar, R. [Creating Value for All Through IT](#). In *IFIP Advances in Information and Communication Technology* (pp. 214–242). 2014.
- Fakieh, B., Blount, Y., & Busch, P. SMEs and cloud computing: The benefits to the national economy and global competitiveness. In *European, Mediterranean & Middle Eastern Conference on Information Systems 2016*.
- Fani, N., Von Solms, R., & Gerber, M. [Governing information security within the context of bring your own device in SMMEs](#). 2016 IST-Africa Conference, IST-Africa 2016, 1–11.
- Fensel, A., Toma, I., García, J. M., Stavrakantonakis, I., & Fensel, D. Enabling customers engagement and collaboration for small and medium-sized enterprises in ubiquitous multi-channel ecosystems. *Computers in Industry*, 65, No. 5, 2014: 891–904.
- Gillies, C. *Business Management of Information Technology*. Available from the CPA Australia Library.

- Gillies, C., & Broadbent, M. IT Governance: A Practical Guide for Company Directors and Business Executives. 2005.
- Han, M. [Facebook unfriending constitutes “bullying”, says workplace tribunal](#). The Sydney Morning Herald. 25 September 2015.
- Harris, J., Ives, B., & Junglas, I. IT Consumerization: When Gadgets Turn Into Enterprise IT Tools. MIS Quarterly Executive, 11, No. 3, 2012: 99–112.
- ISACA. COBIT 5 Enabling Processes. 2012.
- Jansen, W., & Grance, T. Guidelines on security and privacy in public cloud computing. NIST Special Publication, 144, No. 7, 2011: 800–144.
- Keogh, K., Gordon, C., & Marinovic, P. "Cyber Security: Global Developments in Cyber Security Law: Is Australia Keeping Pace?," LSJ: Law Society of NSW Journal, no. 42. 2018: 82.
- Kushida, K. E., Murray, J., & Zysman, J. [Cloud Computing: From Scarcity to Abundance](#). Journal of Industry, Competition and Trade, 15, No. 1, 2015: 5–19.
- Macpherson, S. [Cloud Accounting: What You Need to Consider](#). InTheBlack Digital. 2017.
- Mahony, T. et al. "If We Post It They Will Come: A Small Business Perspective of Social Media Marketing" (paper presented at the Proceedings of the Australasian Computer Science Week Multiconference, 2018).
- Martin, G., Kinross, J., & Hankin, C. [Effective cybersecurity is fundamental to patient safety](#). Bmj, 2375, j2375. 2017.
- Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. The Ransomware-as-a-Service economy within the darknet. [Computers & Security](#) 92: 101762, 2020.
- Office of the Australian Information Commissioner. [Australian Privacy Principles Guidelines](#).
- Office of the Australian Information Commissioner. [Data Breach Preparation and Response — a Guide to Managing Data Breaches in Accordance with the Privacy Act 1988](#) (Cth)."
- Office of the Australian Information Commissioner, "[Does My Small Business Need to Comply with the Privacy Act?](#)".
- Office of the Australian Information Commissioner, "Notifiable Data Breaches Quarterly Statistics Report 1 April - 30 June 2018".
- PwC. 2014 Information Security Breaches Survey: Technical Report. 2014: 22.
- Rees, G. [8 cybersecurity strategies to protect you and your business](#). InTheBlack Digital. 2017.
- Rennhoff, A. D., & Routon, P. W. [Can you hear me now? The rise of smartphones and their welfare effects](#). Telecommunications Policy, 40, No. 1, 2016: 39–51.
- Saunders, J. Tackling cybercrime – the UK response. Journal of Cyber Policy, 2(1), 2017: 4-15.
- Shuja, J. et al., "Sustainable Cloud Data Centers: A Survey of Enabling Techniques and Technologies," Renewable and Sustainable Energy Reviews 62, 2016: 195-214.
- Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. [Cyberbullying: its nature and impact in secondary school pupils](#). Journal of Child Psychology and Psychiatry, 49, No. 4, 2008: 376–385.
- Thomson, G. [BYOD: enabling the chaos](#). Network Security, 2012 (2), 5–8.
- Tuttle, H. [Ransomware Attacks Pose Growing Threat](#). Risk Management, 63, No. 4, 2016: 4–7.
- University of Kent. 2016 Kent Cyber Security Survey.
- University of Kent. Survey on Cyber Security: Executive Summary. 2014.
- Valach, A. P. [What to Do After a Ransomware Attack](#). Risk Management, 63, No. 5, 2016: 12.

Wash, R. et al. "Understanding Password Choices: How Frequently Entered Passwords Are Re-Used across Websites" (paper presented at the Symposium on Usable Privacy and Security (SOUPS)). 2016.

Whiting, R. H., Hansen, P., & Sen, A. [A tool for measuring SMEs' reputation, engagement and goodwill](#). Journal of Intellectual Capital, 18 No. 1, 2017: 170–188.

Zuchetti, A. "[Cyber Criminals' Secret Weapon: Fear of Forgetting](#)".

About the author

Dr. Micheal Axelsen FCPA is a Senior Lecturer (Business Information Systems) at the University of Queensland (UQ). Dr. Axelsen was a member of the then CPA Australia Centre of Excellence which was instrumental in the creation of this checklist in 2005. Since then Micheal has continued to partner with CPA Australia to educate members about IT management. Micheal lectures in IT governance and management in UQ's leading MBA program as well as the Master of Commerce program. His research focus is on the role of technological decision aids in information assurance and governance.

Copyright © CPA Australia Ltd ("CPA Australia") (ABN 64 008 392 452) 2020.

DISCLAIMER: CPA Australia Ltd has used reasonable care and skill in compiling the content of this material. However, CPA Australia Ltd makes no warranty as to the accuracy or completeness of any information in these materials. The above material is only general in nature and not intended to be specific to the reader's circumstances. Further, as laws change frequently, all practitioners, readers, viewers and users are advised to undertake their own research or to seek professional advice before making any decisions or relying on the information provided.

August 2020