IT CHECKLIST FOR SMALL BUSINESS

INTRODUCTION

A small business is unlikely to have a dedicated IT Department or Help Desk. However, these businesses still have many of the needs of a large organisation. They still need to make sure those tasks are carried out by someone within the business, or by an outside service provider.

This checklist aims to provide small businesses with prompts for further action.

First, small businesses increasingly turn to an outside provider to manage their IT services as cloud computing becomes abundant[1]. By extension the concept of 'cloud computing' for small businesses ‘levels the playing field’ with bigger businesses[2], and is a popular option in delivering IT services in Australian small to medium enterprises (SMEs)[3]. In particular, Microsoft’s subscription-based Office 365 is disrupting the traditional concept of the software license as well as what using ‘the cloud’ means. Microsoft’s companion service, OneDrive, offers cloud file storage services that are very useful and applicable to smaller businesses. Similar prominent international providers include services such as Dropbox, Apple’s iCloud, and of course Google Drive.

Second, the use of online social media (Facebook, Twitter and so on) has increased exponentially. When this checklist was first released in 2005, social media was barely even a thing. Today, small businesses dread a bad Yelp review, and look to manage and react to their social media presence on demand[4].

Third, relatively recent mobile devices such as iPhones (2007), iPads (2010), and Android tablets (2011) have had a huge impact. These tools have allowed new services and products to be provided by small businesses[5].

[1] Kushida, Murray, & Zysman, 2015
[2] Al Isma’ili, Li, Shen & He, 2016
[3] Fakieh, Blount & Busch, 2016
[4] Whiting, Hansen & Sen, 2017
[5] Fani, Solms & Gerber, 2016

However, the adoption of 'Bring Your Own Device' (BYOD), where employees use their personal devices to store business data[6], opens up new concerns and issues.

Fourth, although viruses and Trojan horses very much existed in 2005, concerted ransomware attacks such as WannaCry, Cryptolocker and their related derivatives have adopted commercially-focused business models – to the cost of many small businesses[7]. In an inter-connected world of businesses, cybersecurity has become a key point of concern[8].

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 February 2017 Australia introduced mandatory data breach notification laws[9].

The following pages discuss each of these five issues: cloud computing, social media, mobile devices, cyber-security and the need to monitor business compliance needs.

At its heart, though, 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.

CLOUD COMPUTING

Cloud computing allows a business to pool and share hardware infrastructure resources on a massive scale, and it can be quickly applied to a business need with minimal effort and interaction with the service provider[10]. More simply, cloud computing is where your 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' – it might be anywhere in the world. For example, your business emails might be hosted 'in the cloud' with Gmail or Microsoft Outlook, or your data files might be on Microsoft OneDrive, Dropbox, Apple's iCloud, or Google Drive.

Cloud computing is increasingly abundant and cheap[11]. There are real advantages with cloud computing. You don't need to pay IT staff to look after new servers, you don't need to regularly buy new hardware every few years (or software, for that matter), and most cloud computing arrangements come with guaranteed availability. For instance, the Microsoft Office 365 offering now offers 99.9% guaranteed uptime – that's better than most small businesses experience with their own hardware and software. Cloud computing can be much, much cheaper and more reliable than 'traditional' arrangements.

[6] Thomson, 2012
[7] University of Kent, 2016
[8] Valach, 2016
[9] Abrahams & Griffin, 2017
[10] Jansen and Grance 2011; Kushida, Murray & Zysman, 2015
[11] Kushida, Murray, & Zysman 2015

There's also an old saying that, "You don't build a church to fit 1,000 people once a year". To stretch that analogy to breaking point, cloud computing is the marquee and white plastic chairs you can hire for that once-a-year event – except that the marquee looks remarkably like the church inside. For this reason, cloud computing offers the same opportunity for innovations to smaller businesses as large ones[12].

It's not all good news, of course. You do lose control over your IT – you may not be able to customise your IT solution perhaps as much as you'd like. That is, after all, how the costs are kept low – standardised technology. And, your data may be stored somewhere it oughtn't – if your business is affected by the *Privacy Act* (1988), Australian Privacy Principle 8 may be violated if you send private data offshore without proper safeguards in place[13]. And, of course, cloud computing requires internet access. If you lose access to the Internet (or the internet connection is 'iffy' at best), then your decision to use cloud computing might rain on your parade.

In 2014, Microsoft really put the cat amongst the pigeons with 'skyrocketing' usage of its Office 365 offering[14]. For less than the cost of a single-origin coffee in some of the more upmarket Melbourne laneway cafes each week, Microsoft will provide each user with a 50gb e-mail account, 1TB of file storage, video conferencing and multiple licensed copies of Microsoft Office on desktop computers, laptops, and mobile devices. Further, Microsoft now have Australian-based servers that ensure that the data stays in Australia. This ensures you can manage data sovereignty, and addresses some of concerns that exist regarding data privacy. This indicates just how far (and mature) such offerings have now become. Of course, Google Apps is another worthwhile competitor in this space worth considering, but Microsoft's Office suite has been king of the desktop computer for many years now.

Another big provider is the online accounting software Xero. Xero is accounting software stored in the cloud, and provides integration between the small business's accounting software and its accounting advisors. Xero has become very popular for small business accounting[15].

One big issue with cloud computing, though, is the fragmentation of where your files are stored. Your files may be stored on Dropbox, Google Drive, or OneDrive whereas your email might be on Google. To complicate matters, your accounting data might be stored with Xero. Backing up all this data from different locations, or moving from one provider to another, might become complex and difficult. For example, a better product may come along and you might find it difficult to move your data from one provider to another – this is called 'vendor lock-in'[16]. As well, using a traditional approach to ensure business continuity (for example, a UPS battery pack on your computer) won't do much to keep your applications available if they are stored in the cloud and your internet connection goes down.

For further reading on this topic download CPA Australia's guides to the cloud and an overview of its advantages and disadvantages. Similarly, several recent InTheBlack articles have 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.

[12] Al Isma'ili et al., 2016
[13] Office of the Australian Information Commissioner, 2015
[14] Bort, 7 March 2015
[15] Carter, Axelsen, Titman, Aggarwal & Fotheringham, 2016
[16] El-gazzar, 2014

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[17]. Increasingly, the small business needs to engage with customers online.

Social media can engender strong reactions. Some might say, 'these people should go outside and actually talk to people', or 'staring at a laptop screen isn't social!', and this view has some validity. However, undeniably online social media in some form is here to stay. This isn't about to change, and ignoring the influence of social media can be to the cost of the business.

One example of a small business using social commerce to take its product to the world through occasionally viral videos is the innovative Gidget Retro Camper. This is a 'Teardrop Camper' that expands from an easily-towed small camper to be able to accommodate a Queen-sized bed (with full kitchenette facilities). This small business has its own YouTube channel, a Twitter account and a Facebook page. One of their videos has more than 15.9m views, and they export their innovative product from Brendale in Brisbane across Australia and the world. They engage with existing and potential customers using these tools.

One issue to be aware of for all businesses is the risk of 'cyber-bullying' by your employees. Cyber-bulling 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*'[18]. 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, the 2015 case of a real estate agency in Launceston indicate that cyber bullying is a live issue for small businesses[19]. In that case, the cyber bullying was part of a wider pattern of bullying behavior in the workplace with legal consequences under the *Fair Work Act* (2009).

Similarly, sometimes the power of social media can spell trouble for small businesses. 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 or on Yelp[20]. 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).

However, most small businesses have a strong appreciation of the need to manage their online reputation, and manage it accordingly[21]. 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 respond if a comment is made about the business – good or bad! And, always be sure to count to 10 before you reply to a bad Yelp review.

For the record, Amy's Baking Company closed down in 2015. Apparently, there is such a thing as 'bad publicity'.[22]

[17] Fensel, Toma, García, Stavrakantonakis & Fensel, 2014
[18] Smith et al., 2008, p.376
[19] Han, M., 25 September 2015
[20] Clay, 2013
[21] Whiting et al. ,2017
[22] Bleier, 2015

MOBILE DEVICES

For some, recalling life before the smartphone is a distant memory. The first incarnation of this checklist did not address the smartphone – precisely because the iPhone did not arrive in Australia until 2007. Since then though, the use of mobile devices has increased exponentially[23]. Consumers have taken up these devices enthusiastically – and then looked wistfully at the mobile tools provided by their employer and expressed a desire to bring the same convenience and functionality to their workplace.

However, this concept of 'Bring Your Own Device' (BYOD) - where your employees use their personal devices to store business data[24] – opens up new concerns and issues for the small business. In addition to worries about where their data might be 'in the cloud', BYOD means that any small – and easily-lost – device can 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. Mobile devices can also 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.

However, there are real benefits. 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. Worryingly though, the same authors report that 36% of employees ignore their employers' IT policies and just use whatever tool they can bring to the task. So, it is very likely that your employees are already using mobile devices with your 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. You should also ensure that the data on the device can be deleted remotely when (not if!) these devices are lost, and all users 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 such password protection on a mobile device is often ineffective against even hackers with mediocre skills. A mobile device is not the appropriate place for your highly sensitive business information or the private personal data of your customers or employees.

CYBER SECURITY

The trends recognised in cloud computing, mobile devices, and social media all underpin the recognition of the fourth trend, 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.'[25].

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

[23] Rennhoff & Routon, 2016
[24] Thomson, 2012
[25] Craigen, Diakun-Thibaul & Purse 2014, p.17

Cyber attacks may be costly. PwC estimates that the worst breaches at small businesses cost on average $135,000 and $240,000[26]. 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.

First, there is the risk that a hacker might obtain sensitive information from your systems such as credit card data. There are open markets for such information on the 'dark web' – the seamier alleyways and byways of the internet. If others access such sensitive information, your business might find its credit card facilities withdrawn, as your business has likely violated the Payment Card Industry – Data Security Standard – or PCI-DSS. You agreed to follow this standard when you signed the merchant agreement with your bank. Any breach of this standard means the merchant agreement might be rescinded. High-profile issues to date include a salacious breach of the Brazzers website (790k email addresses), Yahoo (32m records), SnapChat (1.7m records), PayAsUGym (300k records), and the Daily Motion video-sharing website (18.3m email addresses with passwords). Your business might be subject to penalties under the merchant agreement, lose the ability to take credit card payments (which might alone be crippling for many businesses), or have to recompense customers that suffer losses from the security breach.

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 such lost data might cause. The damage to business reputation and goodwill might be more crippling than the actual data loss itself.

Third, and extending from the previous two issues, is that 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. A larger SME might also be subject to significant penalties and/or court action arising from breaches of the *Privacy Act* (1988) in Australia – this Act applies to health information or private information maintained by businesses with more than $3m turnover. 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* (1988) to implement mandatory data breach notification requirements[27].

However, the fourth, and most recent, aspect of cyber security that causes considerable problems for SME businesses is ransomware[28]. From about 2012, ransomware attacks such as Cryptolocker and Reveton[29] and, more recently, WannaCry[30] have adopted commercially-focused business models. That is, the virus has commercialised to turn a profit[31]. Since the last time this checklist was updated, such ransomware in particular has had a high impact upon SMEs[32].

With ransomware, a virus arrives via a Trojan horse – usually a 'phishing' email disguised as a funny video or perhaps purporting to be an emailed red light fine – and secretly installs the virus. This virus slowly encrypts your data with a secret 2,048-bit encryption key. For a time, your data continues to be accessible as the virus decrypts the data using the key. However, once all data is encrypted (and, likely, all of your backups too), you

[26] PwC, 2014
[27] Abrahams & Griffin, 2017
[28] Tuttle, 2016
[29] University of Kent, 2014
[30] Martin, Kinross & Hankin, 2017
[31] Valach, 2016
[32] University of Kent, 2016

will be contacted and asked to pay a ransom within a short period, or the criminal gang (usually, sophisticated enterprises operate these scams) will remove the encryption key and your data will be lost[33]. Literally, the criminal gang holds your data to ransom – hence, 'ransomware'. The key is sufficiently strong that 'cracking' the key instead of paying the ransom is uneconomic – some estimate that an average desktop computer would take thousands of years to decrypt the data without the key[34]. It is unlikely you have that kind of time.

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.

In 2017, an InTheBlack article drew on the Australian Signals Directorate guidance from 2017 to identify eight cybersecurity strategies to protect you and your business[35].

1. **Application whitelisting**
   Windows is 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.
2. **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.
3. **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[36].
4. **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[37].
5. **Disable untrusted Microsoft Office macros**
   Macros ("Visual Basic for Applications") in Microsoft 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.
6. **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[38].
7. **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.

[33] Valach, 2016
[34] Ku, 2017
[35] Rees, 2017
[36] Martin et al., 2017
[37] Australian Signals Directorate, 2017
[38] Australian Signals Directorate, 2017

8. **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 these strategies mitigate over 85% of targeted cyber intrusions.

Should you become the victim of a ransomware attack, you have three 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 your only pragmatic option is to pay.

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 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. Both Gillies and Broadbent provide simple templates for documenting the strategy 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.[39]

Privacy Act

A major compliance requirement is the *Privacy Act* (1988). As a general rule, the Privacy Act applies to all companies that manage health-related private information and companies of over $3,000,000 turnover that maintain private information only. The Privacy Act sets out 13 Australian Privacy Principles (APP)[40]:

- APP 1 — Open and transparent management of personal information
- APP 2 — Anonymity and pseudonymity
- APP 3 — Collection of solicited personal information
- APP 4 — Dealing with unsolicited personal information
- APP 5 — Notification of the collection of personal information
- APP 6 — Use or disclosure of personal information
- APP 7 — Direct marketing
- APP 8 — Cross-border disclosure of personal information
- APP 9 — Adoption, use or disclosure of government related identifiers
- APP 10 — Quality of personal information
- APP 11 — Security of personal information
- APP 12 — Access to personal information
- APP 13 — Correction of personal information

[39] Gillies and Broadbent (2005); Gillies (2008)
[40] Office of the Australian Information Commissioner, 2015

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

Although these principles do not apply to all SME businesses, 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.

Data breach notifications

In 2017 the Australian privacy legislation was changed to provide for mandatory data breach notification.

This means that businesses need to notify affected individuals in the case of eligible data breaches which are likely to result in serious harm to the individual.[41]

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).

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 draft fact sheet.

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.

[41] Abrahams & Griffin, 2017

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.

For more information on notifying individuals about an eligible data breach read the OAIC's draft fact sheet.

Key external service providers

Finally, you need to maintain a list of the key external service providers that you use – for example, an IT support business or a cloud service provider such as Office 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. As part of this, you should ask yourself whether the 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. You will appreciate that such an arrangement rarely provides best value for the customer.

ABOUT THE CHECKLIST

This checklist has two components.

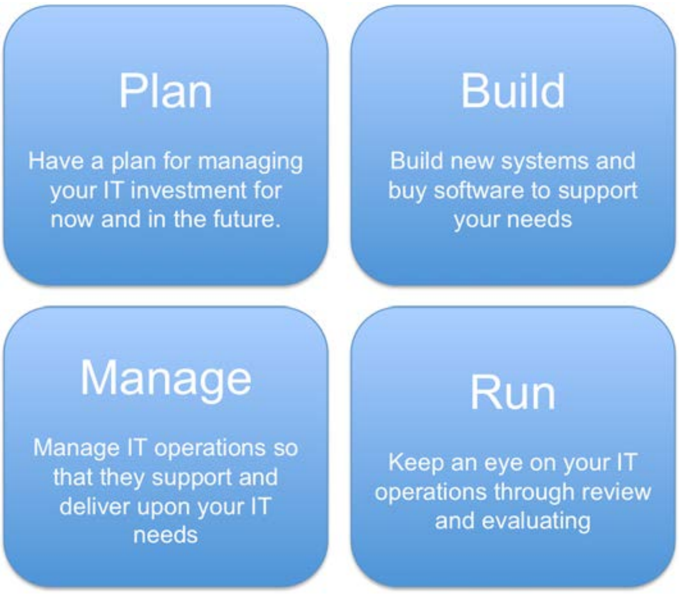
First, the **Top 10 Tasks** you must undertake for good information security.[42]

Second, a **Detailed Checklist** to ensure that your business delivers good ICT service delivery. On this list items marked with a star are *essential* for the good governance and delivery of IT.[43]

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

USING THIS CHECKLIST

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



Plan

Have a plan for managing your IT investment for now and in the future.

Build

Build new systems and buy software to support your needs

Manage

Manage IT operations so that they support and deliver upon your IT needs

Run

Keep an eye on your IT operations through review and evaluating

The checklist is designed for use by small businesses in the context of international best practice.

The 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.[44]

Supporting material is indicated for further research, however, the checklist is designed to be useful on its own.

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

[43] Drawn from the CPA Australia publication, Gillies and Broadbent (2005).

[44] The principal resources drawn upon are Gillies (2008), Gillies & Broadbent (2005), Axelsen (2008) and COBIT 5 (ISACA 20012). See the further reading list at the end of the checklist.

TOP 10 TASKS OF INFORMATION SECURITY

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

DETAILED CHECKLIST

Focus	IT checklist for small business	
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. [See COBIT 5 AP002, AP001 and EDM04 (ISACA, 2012); the CPA Australia publication, *Business Management of IT* (Gillies, 2008) may also be valuable]	
	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.	□
	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.	□
	You have an IT budget for the next 12 months that replaces out-of-warranty equipment and buys new technology you need.	★ □
	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. [See COBIT 5 APO12 (ISACA, 2012); see also the Risk Management Standard (AS/NZS ISO 31000: Risk management – Principles and guidelines) from Standards Australia (2009)]	
	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?	□
	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).	□
	You have a risk register detailing the worst of these risks, how they affect the key business function (e.g. sending invoices) and the tasks you need to do to reduce this risk.	□
	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?	★ □
	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. [See COBIT 5 BAI01 (ISACA, 2012); for extensive and complex guidance refer to the Project Management Body of Knowledge (Project Management Institute, 2008)]	

	Your IT projects are never done because they are ‘fun’ but because they support the business.	□
	Your IT projects have a rough business case before implementing.	□
	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.	★ □
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’. [See COBIT 5 BAI02, BAI05, and BAI06 (ISACA, 2012)]	
	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.	★ □
	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.	□
	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.	□
	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.	□
	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.	□
	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. [See COBIT 5 BAI01, BAI02, APO10, and BAI06 (ISACA); for a good overview also refer to the CPA Australia publication, *Delivering information and communications technology services to small to medium enterprises* (Axelsen, 2008)]	
	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.	□

	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.	□
	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.	★ □
	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. [See COBIT 5 BAI05 and BAI06 (ISACA, 2012)]	
	If you have an IT professional in-house then you have discussed how software is to be deployed and set up.	□
	If you do not have an IT professional in-house then you have established a working relationship with a professional who can guide you in deploying and setting up software.	□
	You have a firm understanding within the business of when tasks will be done in-house and when you will call in outside help.	□
	Your subscription software (e.g. Office 365, Adobe) is automatically downloaded and kept up-to-date.	□
	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 Microsoft Office macros where possible as such insecure software is a frequent source of cyber security vulnerabilities.	□
	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 COBIT 5 BAI07 (ISACA, 2012); Australian Signals Directorate (2016)]	
	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.	□
	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).	□

	Your desktop computers auto-update to implement patches that are provided by the operating system developer.	★ □
	You have a process in place (perhaps a routine security audit by an external person) to check that security patches are being deployed appropriately.	□
	Consider application whitelisting so only authorised software applications run on your computer.	□
	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. [See COBIT 5 BAI07 (ISACA, 2012); for a good overview also refer to the CPA Australia publication, *Delivering information and communications technology services to small to medium enterprises* (Axelsen, 2008)]	
	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.	★ □
	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).	□
	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.	□
	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).	□
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. [See COBIT 5 AP009, BAI04 and MEA01 (ISACA); for a good overview also refer to the CPA Australia publication, *Delivering information and communications technology services to small to medium enterprises* (Axelsen, 2008)]	
	You regularly review your IT for out-of-warranty equipment and replace such equipment when the technology is key to the business.	□
	You have an independent mentor to discuss your IT needs with from time to time.	□

	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.	□
	When staff expectations of IT service providers are not met, the staff know they have someone to raise the issues with.	□
	10. Meet your legal requirements	
	There are all sorts of requirements businesses have to meet. Be sure to meet yours or you may have unexpected fines when transgressions occur. [See COBIT 5 MEA02 and MEA03 (ISACA, 2012); also refer to the Office of the Australian Information Commissioner’s website]	
	You have reviewed your small business’s privacy obligations at the Office of the Australian Information Commissioner’s website and identified your legal obligations.	★ □
	You have policies to ensure that your privacy obligations are met.	★ □
	You have reviewed your small business’s record-keeping obligations as set out by the Australian Taxation Office and identified your record-keeping obligations.	★ □
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, and so a spam filter is required. [See COBIT 5 DSS04 (ISACA, 2012)]	
	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.	□
	If your business runs seven days a week, then there is a way to address alerts each business day.	□
	Your anti-virus software addresses viruses, Trojans, spyware, key-logging software and warns against suspect web pages.	★ □
	You have a spam filter in place to ensure most dangerous unsolicited email is not downloaded onto your network.	□
	Your users know to be vigilant for ‘phishing’ emails that may contain Trojan horses, and check suspect emails with others.	□
	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. [See COBIT 5 DSS04 (ISACA, 2012)]	

	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.	□
	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.	★ □
	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.	□
	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.	□
	You have practised your disaster recovery steps at least once with the current team of people.	□
	You are able to access passwords to online services that the business uses (e.g. through Evernote or LastPass for Business).	□
	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. [See COBIT 5 DSS05 (ISACA, 2012)]	
	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.	□
	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.	□
	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.	□
	You have developed a communications strategy and have allocated responsibility to someone in the office for ensuring that new employees know about the rules.	□
	You have allocated responsibility to someone in the office to keep the rules up-to-date.	□

	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. [See COBIT 5 DSS05 (ISACA, 2012)]	
	You have allocated responsibility to one or two people to add new users to the network (this will be the 'network administrator').	□
	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).	□
	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.	□
	You have a process in place to change online passwords when employees depart.	★ □
	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.	□
	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. [See COBIT 5 DSS05 (ISACA, 2012)]	
	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.	□
	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.	□
	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).	□
	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.	□
	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.	★ □

	16. Setting up shared folders, disk quotes, and granting / reducing access rights to data, systems and applications	
	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. [See COBIT 5 DSS05 (ISACA, 2012); also refer to CPA Australia's Cloud computing guide]	
	The business has appropriate rules in place so that people can see the data they need for their job, but data is generally secured.	✶ □
	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.	□
	Administrator privileges are provided on an as-needs basis, even to their own mobile devices.	□
	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.	□
	Permissions to access shared folders are reviewed regularly (quarterly?) and permissions are deleted when they are no longer needed (perhaps because someone changed roles).	□
	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.	□
	All business data should be stored on the server or managed cloud data service where it can be secured and backed up.	□
	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.	✶ □
	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. [See COBIT 5 APO07 (ISACA, 2012)]	
	You have talked with the staff of the business and written down what tasks they need to perform using their software.	□

	You have made plans to get appropriate information or training for them to perform those tasks effectively and efficiently.	□
	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.	□
	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.	□
	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). [See COBIT 5 APO07 (ISACA, 2012); Thomson (2012)]	
	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.	★ □
	The rules in place identify what personal use of computers and internet access is reasonable in the circumstances for this business.	□
	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.	□
	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.	□
	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.	□
	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.	□
	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.	□
	Your users know to be careful when using public wireless networks. Online transactions are not carried out using public wireless networks.	□

	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. [See COBIT 5 DSS02 (ISACA, 2012)]	
	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.	□
	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.	★ □
	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. [See COBIT 5 DSS02 and DSS03 (ISACA, 2012)]	
	You have allocated responsibility to one person (with a backup if necessary) to replenish stocks of paper, toner etc. for printers and fax machines.	□
	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).	□
	Everyone in the business knows the process and you encourage them to use that process by following it yourself.	□
	New employees are told about the system and encouraged to use it.	□
	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. [See COBIT 5 DSS04, DSS06, DSS05 and DSS01 (ISACA, 2012)]	
	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.	□

	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.	□
	Backup tapes and disks are routinely stored off-site in a secure location as 'cold' backups.	★ □
	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.	□
	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.	□
	Critical business data is not stored on easily-lost USB sticks or external hard drives.	★ □
	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.	★ □
	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. [See COBIT 5 DSS04 (ISACA, 2012)]	
	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.	★ □
	You have a documented restore process and you regularly (monthly? quarterly?) test that you can restore data from your backups.	★ □
	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.	□
	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.	□
	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.	

	[See COBIT 5 DS001, DSS05 and DSS06 (ISACA, 2012)]	
	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.	□
	You have appointed someone as responsible for undertaking those routine steps.	□
	You know what you can do in-house and when to call in an expert and have communicated this to staff.	□
	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.	□
	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. [See COBIT 5 DSS01, DSS05, and BAI09 (ISACA, 2012)]	
	In choosing an ISP you explore a wide range of possible vendors to get the services you need and the best value for money.	□
	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.	□
	Someone has been allocated responsibility for regularly checking competitive pricing and service offerings from ISPs.	□
	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.	★ □
	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. [See COBIT 5 DSS01 (ISACA, 2012)]	
	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.	□

	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.	□
	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.	□
	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.	★ □
	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. [See COBIT 5 BAI10, DSS01 and DSS01 (ISACA, 2012); CPA Australia (2012)]	
	You have considered whether a cloud equivalent to your existing servers (e.g. Office 365 – which would provide mail servers and file servers) would be more suitable for the business.	★ □
	You have consulted with an expert administrator of your servers to write out the routine steps to follow for good administration of the database.	□
	You have appointed someone as responsible for undertaking those routine steps.	□
	You know what you can do in-house and when to call in an expert and have communicated this to staff.	□
	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.	★ □

FURTHER READING

Abrahams, N., & Griffin, J. (2017). 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. (2016). Clearing the 'Cloud' Hanging Over the Adoption of Cloud Computing in Australian SMEs. In DIGIT 2016 Proceedings (p. 23).

Australian Signals Directorate. (2016). Implementing Application Whitelisting.

Australian Signals Directorate. (2017). Strategies to Mitigate Cyber Security Incidents.

Axelsen, M. (2008). *Delivering information and communications technology services to small to medium enterprises*. Available from the CPA Australia Library.

Bleier, E. (2017, September 7). 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.

Bort, J. (n.d.). Everyone is talking about how Microsoft Office 365 is suddenly beating Google Apps. Business Insider Australia.

Carter, D., Axelsen, M., Titman, T., Aggarwal, D., & Fotheringham, D. (2016). Outsourcing: Opportunity or Threat?

Clay, K. (2013). Lessons From Amy's Baking Company: Six Things You Should Never Do On Social Media - Forbes. Forbes, 1–5.

CPA Australia. Cloud Computing: Advantages and disadvantages.

CPA Australia. (2014). A Guide To The Cloud.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. Technology Innovation Management Review, 4(10).

Cyber Security Working Group. (2017). Security tips for business.

El-gazzar, R. (2014). Creating Value for All Through IT. In IFIP Advances in Information and Communication Technology (pp. 214–242).

Fakieh, B., Blount, Y., & Busch, P. (2016). 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. (2016). 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. (2014). *Enabling customers engagement and collaboration for small and medium-sized enterprises in ubiquitous multi-channel ecosystems*. Computers in Industry, 65(5), 891–904.

Gillies, C. (2008). *Business Management of Information Technology*. Melbourne, Australia: CPA Australia. Available from the CPA Australia Library.

Gillies, C., & Broadbent, M. (2005). IT Governance: A Practical Guide for Company Directors and Business Executives. Melbourne, Australia: CPA Australia. Available from the CPA Australia Library.

Han, M. (2015, September 25). Facebook unfriending constitutes “bullying”, says workplace tribunal. The Sydney Morning Herald. Sydney.

Harris, J., Ives, B., & Junglas, I. (2012). *IT Consumerization: When Gadgets Turn Into Enterprise IT Tools*. MIS Quarterly Executive, 11(3), 99–112.

ISACA. (2012). *COBIT 5 Enabling Processes*. Rolling Meadows, Illinois: ISACA.

Jansen, W., & Grance, T. (2011). *Guidelines on security and privacy in public cloud computing*. NIST Special Publication, 144(7), 800–144.

Kaspersky Lab. (2016). The cost of Cryptomalware: SMBs at Gunpoint.

Ku, J. (2017). A comprehensive study of hashing algorithms. Journal of Analysis of Applied Mathematics, 8(January), 5–27.

Kushida, K. E., Murray, J., & Zysman, J. (2015). Cloud Computing: From Scarcity to Abundance. Journal of Industry, Competition and Trade, 15(1), 5–19.

Macpherson, S. (2014). New doors open from the cloud. InTheBlack Digital.

Macpherson, S. (2014). Worried about cloud safety? InTheBlack Digital.

Martin, G., Kinross, J., & Hankin, C. (2017). Effective cybersecurity is fundamental to patient safety. Bmj, 2375, j2375.

Office of the Australian Information Commissioner. (2015). Australian Privacy Principles Guidelines.

Project Management Institute. (2008). *A Guide to the Project Management Body of Knowledge* (3rd ed.). London: Project Management Institute.

PwC. (2014). 2014 Information Security Breaches Survey: Technical Report.

Rees, G. (2017). 8 cybersecurity strategies to protect you and your business. InTheBlack, (April).

Rennhoff, A. D., & Routon, P. W. (2016). Can you hear me now? The rise of smartphones and their welfare effects. Telecommunications Policy, 40(1), 39–51.

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: its nature and impact in secondary school pupils. Journal of Child Psychology and Psychiatry, 49(4), 376–385.

Thomson, G. (2012). BYOD: enabling the chaos. Network Security, 2012(2), 5–8.

Tuttle, H. (2016). Ransomware Attacks Pose Growing Threat. Risk Management, 63(4), 4–7.

University of Kent. (2016). *2016 Kent Cyber Security Survey*.

University of Kent. (2014). Survey on Cyber Security: Executive Summary.

Valach, A. P. (2016). What to Do After a Ransomware Attack. Risk Management, 63(5), 12.

Whiting, R. H., Hansen, P., & Sen, A. (2017). A tool for measuring SMEs’ reputation, engagement and goodwill. Journal of Intellectual Capital, 18(1), 170–188.

About the author

Dr. Micheal Axelsen FCPA is a Postdoctoral Research Fellow (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 is a lecturer in IT governance and management in UQ's leading MBA program. His research interests include intelligent decision aids, information systems audit, and business process management.

Disclaimer

CPA Australia and the author have used reasonable care and skill in compiling the content of these materials. However, CPA Australia makes no warranty as to the accuracy or completeness of any information contained therein nor does CPA Australia accept responsibility for any acts or omissions in reliance upon these materials. These materials are intended to be a guide only and no part is intended to be advice, whether legal or professional. All persons are advised to seek professional advice to keep abreast of any legal or other reforms and developments. To the extent permitted by applicable law, CPA Australia, its employees, agents and consultants exclude all liability for any loss or damage claims and expenses including but not limited to legal costs, indirect special or consequential loss or damage (including but not limited to, negligence) arising out of the information in the materials. Where any law prohibits the exclusion of such liability, CPA Australia limits its liability to the resupply of the information.

CPA Australia has a range of services tailored to support public practitioners.

For further information please visit cpaaustralia.com.au/publicpractice or contact your local office on 1300 73 73 73.

July 2017