CYBERSECURITY TIPS FOR SMALL BUSINESS

CPA AUSTRALIA

TIPS FOR MANAGING CYBERSECURITY RISKS

In today's increasingly digital, data-driven world, businesses of all sizes rely heavily on technology to carry out day-to-day operations and perform basic business functions. Increased adoption of technology, connectivity with third-party providers and other technology-led initiatives expose businesses to additional cyber vulnerabilities.

For most small businesses, it is not a matter of 'if' you will be attacked but whether you have already been attacked or will be attacked, without your realisation. Cyber-attacks often target client data. When client data is compromised, businesses may not only experience financial loss, but also reputational and relationship damage.

What measures should small businesses take to mitigate the risk of cyber-attacks? Here are **CPA Australia's recommendations** on safeguarding your small business from cybersecurity threats.

CULTIVATING CULTURE

1. INSTIL CYBER RISK AWARENESS IN ALL STAFF

A robust cyber security system is not just the responsibility of IT but of each and every employee. Cyber criminals always find new ways to access information, therefore, it is crucial to create a culture where all employees are aware of and understand the impact of new cyber threats.

You could invest a considerable amount in software to protect your business network only to find out that a simple error such as an inadvertent sharing of passwords by a staff member has provided provide access to cyber criminals. While technical controls are essential, you should also establish and enforce basic security protocols and train staff to follow them.[1]

As part of cybersecurity education and training,[2] staff should not only be informed about the mechanics of cyber-crime, i.e. how cyber criminals operate, but also about the scale and scope of risks and potential damages the organisation may be exposed to by cyber-attacks.

Education and training should give employees a reasonable sense of when a potential cybercriminal may be seeking confidential information from them. Perpetrators often use well-established communication methods, via email (known as phishing), phone (known as vishing), or even text message (sometimes called smishing).

Other important steps to ensuring that cybersecurity is part of the culture of your small business include:

- including it in your business planning and decision-making
- regularly testing employees, for example, to see how they would react to a phishing email
- assigning responsibility for communicating and training to one staff member.

You should also consider running cybersecurity awareness campaigns such as phishing campaigns to educate staff and suppliers about phishing emails and how to detect them.

2. ALLOCATE RESOURCES TO CYBER RISK IN YOUR BUDGET

When determining what resources to allocate to manage your cyber risk, you should be fully informed about how all the computing services your business utilises are provided and protected. As a smaller organisation, you may need to commit a larger portion of your budget to meeting new regulatory requirements and operational cyber needs.

Which aspects of cybersecurity you spend more or less on will depend on the nature of your business. For example, you may want to focus your spending on network security instead of identity access management where you have a limited number of people accessing your systems.

Depending on your budget, you may want to consider purchasing off-the-shelf cyber security software provided by third-party vendors (see Tip 8, below).

[1] For tips on how to create a cybersecurity policy, refer to **https://www.business.gov.au/Risk-management/Cyber-security/How-to-create-a-cyber-security-policy**

[2] For more information on this topic, see the Council of Small Businesses Organisations Australia (COSBOA's) cybersecurity management solutions for small businesses. In Singapore and Malaysia, the Cybersecurity Agency of Singapore and Cybersecurity Malaysia have related resources on their websites to support small businesses.

3. INCORPORATE CYBER RISK CONSIDERATIONS INTO YOUR BUSINESS PLANNING

If your business plan is focused on growth, you may need to add new platforms, products, apps and web capabilities. Cyber security considerations may multiply with the introduction of each new element.

Align your cyber security protection plans to your business plan. This will help you identify and respond to emerging exposures e.g. third-party and supply chain control deficiencies.

Including your cyber professionals at the start of a project will lead to better and cheaper security outcomes for your business as it is typically more expensive to solve security issues later.

These steps will assist the person or people responsible for cybersecurity in your business to better manage cyber risk across the organisation and foster greater collaboration and innovation.

4. SEPARATE RESPONSIBILITY FOR CYBERSECURITY FROM IT

Where possible, entrust cybersecurity management to a staff member who is not already responsible for IT matters. This will ensure objective consideration of security occurs when considering new IT service or extending existing IT services.

If responsibility for IT and cyber security must fall to one person, consider having IT and cyber security as independent goals for that employee or contractor.

OPERATIONAL TIPS

5. KEEP YOUR SOFTWARE UP TO DATE

Security vulnerabilities in applications can be used to execute malicious code on systems while vulnerabilities in the operating system can be used to further the compromise of systems.[3]

For smaller organisations, the simplest solution is turning on auto-updates and consistently ensuring key assets are connected to the internet for updates to be performed successfully.

Frequently patch applications such as Java, PDF viewers, Flash, web browsers, Microsoft Office, PDF viewers and operating systems to mitigate vulnerabilities. It is important to keep your computer's operating system patches up to date. Make sure you use the latest operating system version and don't use unsupported versions.[4]

Antivirus or endpoint security software is essential. Your antivirus software should be set to run a scan after each update. Enable automatic updates of such software and prevent employees from disabling these updates. Some antivirus solutions offer a streamlined update process.

Remember to install anti-virus software on your portable devices and keep them updated to block threats from entering your network.

Consider restricting user access permission, limiting employees from installing any application without the IT or security administrator's approval. Larger businesses could also use application 'whitelisting' to help prevent malicious software and unapproved programs from running.

6. MAINTAIN A FIREWALL

Make sure your operating system's firewall is enabled and prevent staff from disabling it. This goes a long way to preventing incoming external threats. If employees (or others with system access) work remotely, an appropriate and up-to-date firewall helps to ensure your systems are protected.

[3] **https://www.cyber.gov.au/acsc/view-all-content/essential-eight/essential-eight-explained**

[4] Patches are software and operating system (OS) updates that address security vulnerabilities within a program or product. Software vendors may choose to release updates to fix performance bugs, as well as to provide enhanced security features. (reference: Cybersecurity & Infrastructure Security Agency)

7. IDENTIFY ASSETS VULNERABLE

All your virtual and physical assets have intrinsic worth to you and your business. You should prioritise the protection of your most vital digital systems and those most likely to be attacked. For example, the systems that store customer records are likely be more important to you than a USB-powered coffee cup warmer.

When identifying the vulnerabilities that you should minimise first, consider not only the reported impact of a vulnerability (e.g. data loss) but also the likelihood of that vulnerability being exploited.

The **Center of Internet Security** often releases security bulletins that demonstrate the severity of vulnerabilities to help inform priorities. Businesses can refer to these resources when assessing their vulnerabilities, especially when doing this for the first time.

8. PERFORM REGULAR BACKUPS

Regular backups stored at a secure offsite location or in the cloud should enable you to get your business up and running very quickly after an attack. This has become more critical as the threat of ransomware attacks increases. There have been many reports of systems and even backups being maliciously encrypted, with hackers demanding hundreds and thousands of dollars for the 'privilege' of unlocking important data and systems.

Backups should be fully tested on a regular basis. If you are storing sensitive client information on a cloud-based backup service, this data should be encrypted and possibly password-protected beforehand.

9. CHECK THE SECURITY OF THIRD PARTIES ACCESSING YOUR SYSTEM

If your organisation’s IT system is entirely managed by a third-party vendor or supplemented by IT services provided by a third-party vendor, it is crucial to ensure your vendor has clear cyber security and data privacy policies in place. Where you allow suppliers or contractors to access your systems, ensure cybersecurity requirements are built into their contracts and that their cybersecurity processes align with your own. If they outsource your work to another provider, check the outsourced provider’s security processes and procedures.

Some questions you should ask the third-party vendor are:

- How and where is the (client) data stored?
- What cyber security measures do you have in place?
- Have you had any breaches or cyber security issues in the past?

Most services these days list their operational sub-processors. These details are often available on their corporate website’s privacy, security or trust pages. Make sure you review access on a regular basis and revoke accounts where necessary. Maintaining a register of these organisations and their employees will enable you to identify and disable access as circumstances change.

10. MOBILE DEVICES SECURITY

Significant risks are presented by employees, contractors, suppliers and customers who can access your network from personal devices. If you allow such access, you should apply limits. Require employees, contractors, and suppliers to password protect such devices and ensure appropriate security apps are installed.

Mobile device operating systems and applications should be required to be kept up to date. Consider enforcing restrictions by limiting access to known devices (known as 'whitelisting'). While this might seem overly prescriptive, sometimes cybersecurity is only as secure as its weakest link.

11. CONTROL NETWORK ACCESS

Establish separate user accounts for each employee and require strong passwords that expire at least every three months. Avoid using joint accounts that have shared passwords. Separate user accounts allow you to track individual users. This helps in scenarios where perhaps an employee's account has been compromised and you need to disable it. Consider restricting who can plug devices into your network to authorised personnel only. Most consumer and 'small business' grade routers provide options for this.

More businesses are adopting multi-factor authentication (MFA) or second-factor authentication (2FA) which allows for a second line of defence against your account being compromised. Some forms of MFA are available on Google or Microsoft Authenticator mobile applications. An example of 2FA can be enabling mobile phone SMS for security purposes when an account is accessed.

12. RESTRICTING ACCESS TO WI-FI NETWORKS

If your business has Wi-Fi available for employee use, make sure it is secure (password-protected) and is hidden. If you provide public Wi-Fi for customers, ensure it only allows users internet access, not business-critical network access. Never use public Wi-Fi hotspots to access your company network, as data can often be transmitted in plain text for potential Wi-Fi detectors to see.

13. SEPARATE YOUR POINT-OF-SALE SYSTEMS

Isolate point-of-sales systems from other, less secure systems. Speak to the provider of your point-of-sale systems, as they may be able to assist you better secure your system. This could include things like a non-network EFTPOS terminal device.

14. REGULATE EMPLOYEE ACCESS TO INFORMATION SYSTEMS

Employees should only be given access to systems they need to perform their duties. No employee should have access to your entire system and installation of non-standard software should only occur with specific permission. Consider requiring separate authority and passwords to access critical data.

When a person leaves your employment, their access to your system, including remote access must be disabled immediately. Limit the use of administrative or privileged user accounts except in limited circumstances where maintenance is required.

15. DISASTER RECOVERY PLAN

Have a disaster recovery plan in place to help you respond quickly in the event of an attack. Consider how long it might take you to get back up and running after a significant disruption, so your business is not out of action for a long period of time. This could include how long it would take you to acquire new hardware and to restore your data.

Your plan should include information on how you will communicate with customers and other stakeholders if their data has been accessed or lost. This can help protect your business' reputation and services.

16. REVIEW

Review your cybersecurity processes regularly. You may wish to engage with external party to review and advise on the effectiveness of your cybersecurity. This also includes your suppliers and insurance provisions.

17. REPORT ATTACKS

As with a physical break-in to your premises, you should report attempted and actual break-ins to your systems. Only if you report such violations can law enforcement agencies act against such criminals. To work out how to report a cybercrime in your location, Google search "report a cybercrime".

CONCLUSION

The digital economy has changed the way many organisations do business. Online technology services have become much more accessible and consumable by small and medium businesses. However, the frequency of hackers targeting small and medium businesses means this step has risks.

To mitigate the risks, it is important that your whole business is aware, responsible and accountable. Businesses need to continuously upgrade their capabilities – human and technological – to remain secure, vigilant, and resilient. Better education about current threats and their implications can galvanize increased engagement and help focus your business on the challenge, while assuring that adequate resources are allocated to the task.

Getting cybersecurity right not only protects your systems, it can help your business grow, as it will be better positioned to incorporate emerging technologies that improve efficiency and the customer experience.