Cyber Audit TEAM

10 TIPS TO *ENHANCE YOUR INFORMATION SECURITY POSTURE*

Everyone wants to feel like their company's data is being protected – a recent **survey** of small business leaders suggested that 77% were confident their data was secure. How confident are you?

Your firm's reputation is intrinsically linked to your ability to demonstrate your company is protecting your clients personal, private or financial information, or protecting their brand and reputation within your supply chain.

Perhaps you've received reassurance from your internal or external IT team about your company's risk exposure and been advised that systems are in place to protect the business.

You may not know that almost all data breaches occur because of human error — not hacking. These breaches are often the result of staff being too trusting, too busy, untrained and/or complacent.

Can I really spot and stop attempted breaches of our data?

Unfortunately, many companies haven't progressed towards investing in next-generation information security. They are often over-reliant on their IT provider, who has only installed basic IT security such as Anti-Virus software and firewalls.

With independent support from information security specialists, utilising Security Information and Event Management (SIEM) and real-time monitoring, you can mitigate most attempts to breach your data.

Should I be concerned?

It is estimated that a data breach occurs every 14 seconds. The Australian Cyber Security Centre (ACSC) receives a **data breach report** every 10 minutes.

According to the **2019 IBM Ponemon Report**, the average time for an Australian business to identify a data breach was 200 days, with a further 81 days required to contain the threat. The report also identified the average cost of a data breach was in excess of $3 million.

What can I do to protect my business, its data, and our brand and reputation?

The good news is there are numerous practical and affordable solutions to reduce the likelihood your company suffers a data breach — and Cyber Audit Team (CAT) are here to help.

Our team of specialists have rich information security-focused backgrounds and possess highly sought after skills and experience, to assist businesses of all sizes, across all industries.

We'd like to share with you and your team our top 10 tips to help your business enhance your information security posture and reduce your risk.

01. Passwords Aren't Always the Answer

Poor password hygiene can be a key business risk, especially when staff are allowed to create their own passwords. This often leads to those same passwords being reused across multiple platforms.

Long and complex pass-phrases are preferable, but here are some other measures to consider:

- **Password managers**

  It's imperative that passwords are unique and complex for every account. Your employees will struggle to remember multiple complex passwords; that's why good practice is to use a recognised **password manager**. These generate unique, complex passwords and store them in an encrypted database.

- **Biometrics**

  Implementing biometrics — such as fingerprint and facial recognition — on sensitive platforms such as Office 365, financial programs and CRM systems adds an additional layer of security.

- **Physical tokens**

  Physical authentication methods can also assist in protecting your corporate information security. Devices such as **Yubico's YubiKey**, **Google's Titan** or **RSA devices** should also be considered for privileged access users.

02. Enforce Multi-Factor Authentication (MFA)

In today's interconnected world and rapidly evolving threat landscape, strong passwords are no longer considered sufficient alone.

Additional layers of security, such as Multi-Factor Authentication (MFA), ensures users are only granted access when two or more pieces of evidence or factors are present. MFA should be mandated by companies as an essential layer of security.

- Today, nearly all digital platforms or Apps support MFA. Authenticator Apps such as **Microsoft Authenticator**, **Google Authenticator** or **LastPass Authenticator** are all well regarded and should be considered.
- Physical tokens for highly sensitive information or privileged access users add stronger layers of security, whilst enabling 'passwordless' authentication.
- SMS is a more traditional **Two-Factor Authentication (2FA)** method. However, given its known **security weaknesses**, it should be the option of last resort.
- Other methods to enable security while reducing user friction include using contextual intelligence to prove identity, alerting and monitoring on abnormal logon activity and **Single Sign-On (SSO)**.

03. Keep Personally Identifiable Information (PII) Private

PII is extremely valuable to Threat Actors (criminals) who can use this information to steal your identity, impersonate you, or obtain credit cards or bank loans in your name.

- Take precautions to always protect your PII. Consider how much of your PII you freely provide on your social media accounts, or when signing up to new Apps, online accounts, or online shopping, etc.
- Never share your sensitive data such as date of birth, home address, mobile phone number or mother's maiden name with any third party suppliers.
- If you're contacted by someone claiming to be from a bank, Telstra, ATO, or other recognised agency or business, you are not obligated to divulge sensitive or personal information — especially as you don't really know whom you're speaking with. Don't ever feel intimidated or threatened by the caller, no matter where they claim to be from. If they are legitimate, they will understand your privacy concerns and allow you to call them back on their published number.

04. Be Cautious of One Time Password (OTP)

OTP is another form of authentication, which is sent as a text to the mobile device of the user. This can be from an App, a platform or provider to verify the user or grant access. Time-based OTP (TOPT) is only valid for a short duration, changing every 20-30 seconds.

- One of the issues with OTP is that it's sent through text or email. These forms of communications can be intercepted.
- Be aware of unsolicited support calls, especially from organisations such as Telstra, ATO, banks or companies like Apple, Samsung etc. who advise you that they will send you an OTP via text, and then request you repeat it back to them for security identification. It's quite possible the caller may be a Threat Actor socially engineering you.
- Also remember to protect your PII and don't divulge anything to the caller.
- One secure use of OTP is when used as an authenticator method through Google or Microsoft Authenticator applications.

05. Keep Security Questions Safe

It’s convenient to select security questions which are easy to remember, however, this makes it easier for a Threat Actor to compromise a system using social engineering.

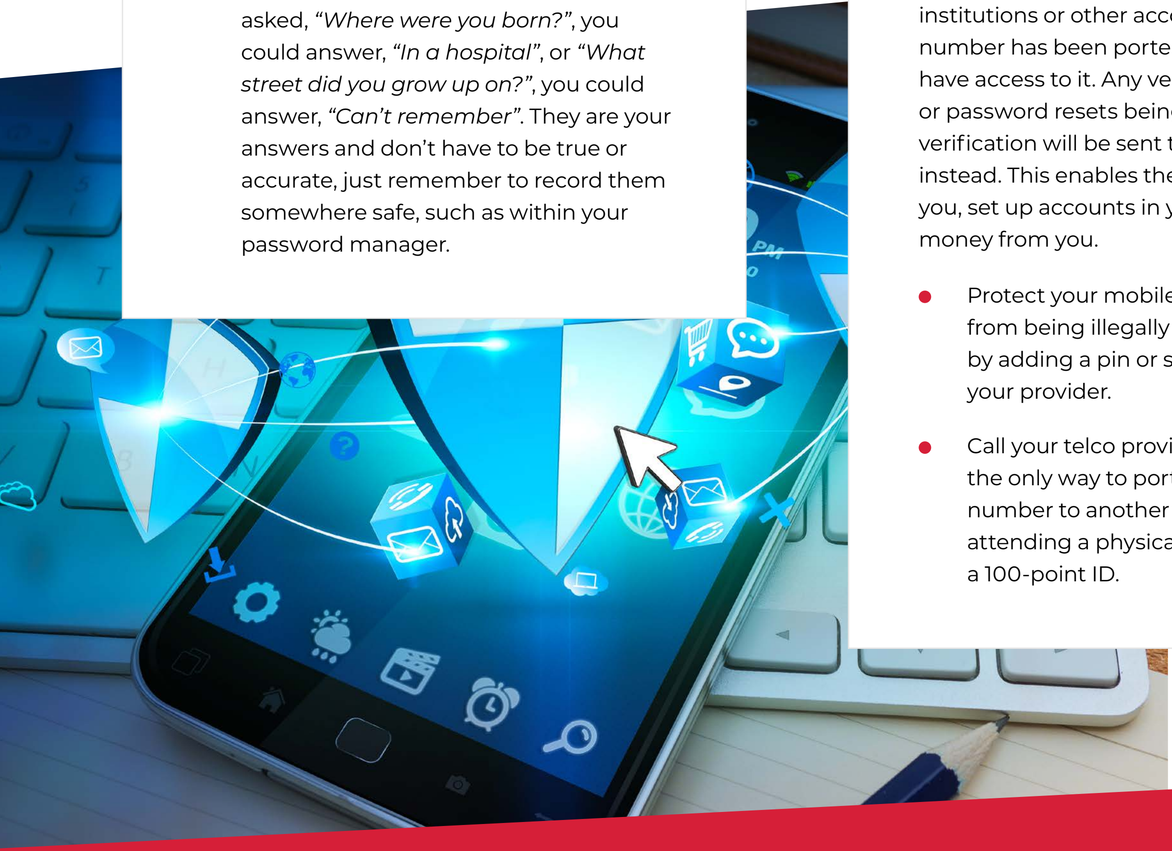
- Whenever you complete online security questions for third party providers, remember that you don’t have to provide the real answers such as mother’s maiden name, street you were born, etc.
- These security questions are only used by the provider to identify you. So if asked, “*Where were you born?*”, you could answer, “*In a hospital*”, or “*What street did you grow up on?*”, you could answer, “*Can’t remember*”. They are your answers and don’t have to be true or accurate, just remember to record them somewhere safe, such as within your password manager.

06. Beware of Mobile Porting Scams

Fraudulent **mobile number porting** happens when a Threat Actor pretends to be you and **ports your mobile number from one provider to another**. Threat Actors can often access your PII via your social media profiles.

Threat Actors then fraudulently use your mobile number to gain access to email accounts, superannuation, financial institutions or other accounts. Once your number has been ported, you no longer have access to it. Any verification codes or password resets being sent to you for verification will be sent to the Threat Actor instead. This enables them to impersonate you, set up accounts in your name or steal money from you.

- Protect your mobile phone number from being illegally ported away (stolen) by adding a pin or security question via your provider.
- Call your telco provider and request that the only way to port a mobile phone number to another provider must be by attending a physical store and providing a 100-point ID.



07.
Avoid Using Social Logins

While it may seem easier to sign in to accounts using your social login (such as Facebook or Google), the convenience comes at the expense of your **security** and **privacy**.

Facebook and Google are by far the two most frequently used services for social logins to other sites and are more interested in collecting excess data than serving a better user experience.

- Usually, companies who provide a social login are more interested in **collecting excess data** than serving a better user experience. This is primarily because more information is shared through social logins than necessary.
- It is commonly recommended that companies use their password manager as a secure alternative to social logins.

08.
Free Wi-Fi vs Hotspot

Free Wi-Fi access has its benefits including flexibility, mobility and expediency. But the risks can be far greater than the rewards.

- Our best advice is to advise your staff to **never use free Wi-Fi** - EVER!
- A safer alternative is to Hotspot from your phone. This is one of the major reasons most telcos have drastically increased our monthly data allowances.
- If you must urgently use free Wi-Fi, then confirm the 'official' hotspot name from venue staff and manually connect your device to it.
- Ensure your **VPN** is turned on before accessing any sensitive information such as emails, banking or social media.
- If you don't have a VPN, do not access corporate emails, online banking or shopping, or enter your passwords or credit card details on public Wi-Fi.
- Remember to turn off automatic connection to Wi-Fi in your device's settings and file sharing.

09. Update, Update, Update!

Providers and developers release regular updates/patches for their software, Apps and hardware solutions, primarily because of discovered vulnerabilities. If staff are given the option to 'postpone' these important updates then your business could be dangerously exposed to compromise and attack.

- Establish an enforceable policy that ensures systems are promptly updated/ patched to mitigate exposure and risk from an online attack.
- In addition to security fixes, updates can also include driver improvements, enhanced or new features, and better compatibility with different devices or applications.
- Updates can also improve software performance, eliminate known bugs, and remove outdated features taking up hard drive space.

10. Independently Assess for Awareness

If you're not sure where your company's information security weaknesses are, one thing is almost certain — a Threat Actor will find them and soon exploit them.

Threat Actors use numerous sophisticated and unsophisticated strategies to target companies of all sizes. One of the best defences to protect your company is to employ various mitigating solutions, based on your risk appetite and budget.

This is best achieved by conducting a robust and independent '**gap analysis**' of your company's information security posture. This will identify your company's specific exposure to risk.

Practical and **affordable solutions** can then be implemented and could include enhancement to policies and procedures, regular staff training, real-time monitoring of your digital environment, vulnerability assessments, and penetration testing, etc.

We hope you have found our tips helpful. If you'd like more guidance, Cyber Audit Team conducts fixed-fee information security assessments that are thorough, yet non-intrusive. We are then able to tailor a solution for your business that is both affordable and simple to implement.

Cyber Audit
TEAM

Cyber Audit Team is an independent Cyber Resilience Assessment and Managed Detection and Response Services provider.

The multi-disciplinary team of highly experienced industry specialists provide simplified end-to-end Information Security solutions as well as support and guidance to businesses of all sizes across various industries.

Cyber Audit Team
4 Helensvale Road
Helensvale QLD 4212
Australia

P: 1300 077 022
E: enquiries@cyberauditteam.com
W: cyberauditteam.com

Follow us on LinkedIn & Twitter
@cyberauditteam