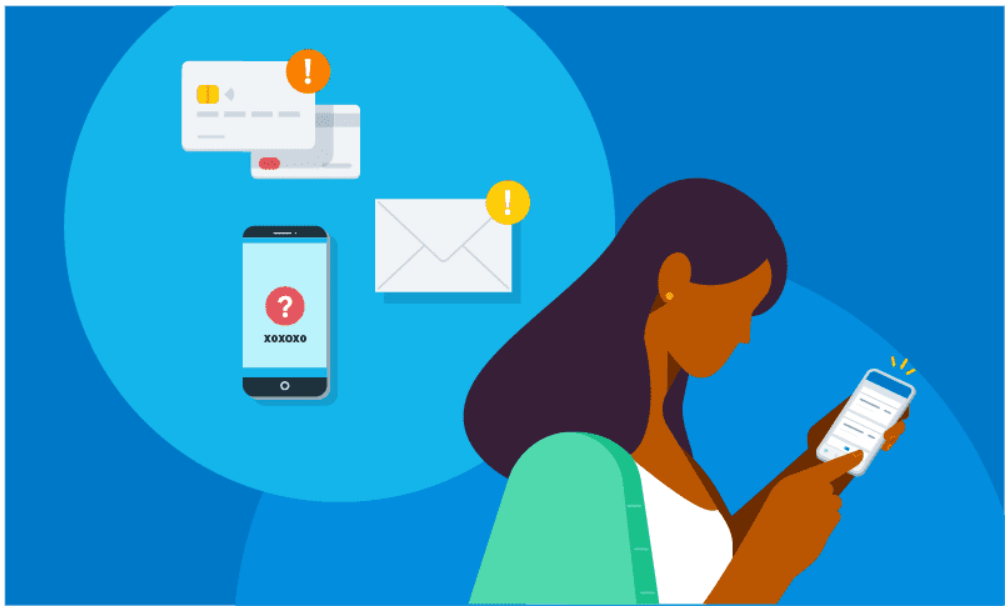

Over the last 12 months, millions of customers around the world have been impacted by some of the biggest data breaches in history.

As a small business or advisor working with sensitive personal and financial information every day, the stakes are high. If your business or practice experienced a data breach, it could have a serious impact on your livelihood. Aside from facing hefty fines and costs, you may never fully recover the trust of your customers and clients.

October is Cybersecurity Awareness Month and a timely reminder to stay secure online. Even if you feel pretty confident about your security processes, it's worth reviewing the basics. A good way to identify any gaps is to get into the mindset of a cyber criminal. Who are they? What are they looking for? Why are they stealing information? And how do they get it?

Who are the criminals behind a cyber attack?

Despite stereotypes you might have seen, cybercriminals aren't necessarily well-funded geniuses who lurk in the shadows building sophisticated hacking programs. The barrier to entry is actually much lower, with cybercrime tools and services available to anyone with the right motivation.

Stolen data is a valuable commodity on the dark web, and cyber criminals know they can make a quick buck by targeting businesses with lax security. They don't care what they damage they do, or who they hurt along the way.

There are four different kinds of cyber criminals:

- **Hackers**, who use their skills to break into vulnerable systems and networks
- **Cyberactivists**, who often have political or ideological reasons for exploiting a company and exposing their data
- **'Script kiddies'**, who don't have technical expertise and use off-the-shelf hacking tools to steal data
- **Malicious insiders**, who are employees using their position to steal sensitive information from their company

What do cyber criminals want?

Data is the ultimate prize for a cyber criminal. This could be anything from the personal information of staff and customers, to confidential business information like sales and inventory records, credit cards and banking information, or account credentials used to access company systems.

Personal information can be used to commit identity fraud like scam campaigns, or payment fraud like transactions on stolen credit cards. Business information can be sold to competitors or state sponsors, and used to gain access to company accounts.

Cyber criminals steal this data by gaining control of the accounts that access it. These might include email accounts, file storage accounts, or accounts that give you access to your company systems and networks. Once they have access to your accounts, cyber criminals can change your password and lock you out, then use this account to access other online services.

Imagine if a cyber criminal was able to access your email account. They could intercept a PDF invoice and edit the payment details, to trick your customers into paying a fraudulent bank account instead of you. Sending an e-invoice in Xero is one way to avoid this risk.

How do cyber criminals access your accounts?

Cyber criminals use a number of tactics to gain access to your accounts.

- **Direct attacks**, using tools that allow them to guess or break passwords that are weak. If you've used that password across multiple accounts, the damage could be wide ranging
- **Phishing and social engineering**, where cyber criminals trick people into handing over their details using links or requests in emails, texts, phone calls and other communications
- **Malware**, which is malicious software that can infect your device to monitor your activity, and provide backdoor access to your systems
- **Ransomware**, which spreads across your devices to lock them, so the cyber criminal can threaten to expose or erase your data unless you pay a ransom

How can you prepare and protect your business?

Being cyber wise in your business or practice doesn't have to be complex or expensive. It's about taking a layered approach, to make sure you have broad protection against a range of threats. You probably already do this with your home security. Aside from locking doors and windows, you might have additional deterrents like gates, cameras, alarms, and perhaps even a dog.

If you're not sure where to start, here are some strategies you can use to improve your business' resilience to cybercrime.

1. Do a risk assessment on your business or practice

Start by doing a risk assessment for your business or practice. This might involve thinking about:

- what data is stored by your business or practice
- which technology (such as hardware, software or cloud accounts) you're using to store data and where there might be vulnerabilities
- what obligations you have (such as the Australian Privacy Act 1988 or GDPR regulations) to manage data and disclose data breaches

2. Get your security basics sorted

It's important to get the basics right, like having strong and unique passwords on each account, and changing them often. Cyber criminals often use tools that scan dictionaries and social media to crack accounts, so it's important to make sure your passwords are complex and contain capitals, numbers and special characters.

Password managers are a good option — they'll do the hard work for you in terms of making up strong unique passwords for your accounts, and providing them for you so you don't have to remember them when you need to log in.

Multi-factor authentication (MFA) should be turned on wherever possible — especially for email accounts and other critical online services. MFA will prevent an imposter from accessing your personal and company accounts, even if the passwords have been exposed.

Xero Verify is an MFA tool that provides an extra layer of protection on your Xero account, allowing you to quickly authenticate yourself with the push of a button.

3. Develop strong policies and processes

Make sure your team are maintaining clear and consistent cybersecurity habits, by creating policies that outline how your business or practice handles account security (passwords and MFA), device security (antivirus and updates), and data security (storage and backups).

Your privacy policies should also be kept up to date and cover what data you collect, how you use that data, and how long you intend to hold the data. Also consider why you need this information and what your obligations are. Remember: if you don't need the information, don't collect it.

It's also wise to have a business continuity plan in place, with important contact details, information on what you have backed up and all the critical passwords you need. Of course, make sure you keep your business continuity plan secure too!

4. Buy secure products and services

Look for organisations that adhere to data security standards. For example, Xero is audited to be compliant with ISO 27001 and SOC2. If you're using a service that needs you to add or upload information, make sure they're providing a secure webpage (check the address begins with 'https' instead of just 'http').

It's also critical that you can store your data securely, and back it up regularly (either to the cloud or a local device). Access and sharing should be limited to those who need the data for their jobs.

5. Upskill your staff on cybersecurity

Don't forget to consider the human element of security. Everyone in your business or practice should understand how to safely use the accounts, devices and data that belong to your business.

Staff should also know who to ask for help when they need it, and feel confident about reporting risks or mistakes as soon as possible. It's important that these issues aren't buried and that someone is taking responsibility to resolve them.

Know where to go for help and support

Many countries have a government cyber agency that offers free resources, training materials and templates to help guide you. If you're not comfortable doing it yourself, you may like to hire a security consultant or IT professional to provide advice.

If the worst does happen, it's important to know how to respond. While you need to act quickly, making panicked decisions can make things worse. Report the incident to your cyber agency, and contact your bank if any money has been transferred. If there is any threat to harm people, call the police.

Cyber criminals are a growing threat to all of us. The best way to make sure you keep your data safe is to look at your business or practice through the eyes of a cyber criminal, and look at what gaps or vulnerabilities might exist. That way, you can enjoy peace of mind, knowing the data you're holding is safe and secure.

Popular this week