Strengthening your Cyber Security.

Simple strategies to help protect your business and reputation.

"Cyber attackers are sophisticated and cyber security can seem complicated. The good news is there are simple things you can do to help mitigate the risk. Thinking it's too hard and **doing nothing is just not an option**."

David Lister, Senior Manager ISG, Information Technology at Westpac New Zealand

Every business should be prepared for a cyber attack.

There's a saying in cyber security – "it's not if, but when". Businesses are constantly looking for faster and smarter ways to complete tasks – whether that's automating processes like payments, using cloud-based technology or communicating online instead of face-to-face. While this helps improve their productivity, it also increases their risk of becoming a target for cyber crime.

Cyber attackers are constantly evolving their methods to infiltrate business systems.

In the past cyber attackers were focused on causing damage to governments or large organisations to make a point. These attackers would typically do things like hack into systems to release sensitive information, or redirect visitors to questionable websites. Now they've moved onto causing disruption in businesses and trying to monetise that. One recent example of this is attackers delivering malware to computers that encrypts them, then demanding a ransom to unencrypt the computer. This particular type of malware is referred to as ransomware and has caused significant problems to some major organisations.

Your customers are at risk too.

Large businesses like banks have a lot of controls in place to protect themselves from fraud or theft – but often customers don't. So cyber attackers have figured out that it's easier to try and get money out of customers rather than trying to circumvent all the controls put in place by a business. A good example of this is business email fraud where cyber criminals gain access to the email systems of businesses and send out invoices to customers with altered account details – duping the customer into paying the amount owed into the wrong account.

According to the NZ Herald, business email compromise scams are costing Kiwis $8,000 a day. And globally the FBI estimates these types of scams are costing US$10 million a day.

Know your enemies.

People who carry out cyber attacks are commonly known in the security business as 'threat actors'. The main group a business is most likely to encounter – and that we deal with as a bank – is the cyber criminal.

Cyber criminals are a significant threat to businesses.

There are two things they want to do: Scam you to get your log-ons for internet banking so that they can defraud you and get money out of your account. Or get access to your email usernames and passwords in order to get into your email system and scam your customers and your business out of their money.

Nation state attackers can also pose a risk.

The other threat actor a business might encounter is a nation state attacker. These are secret organisations of governments that find exploits in operating systems like Windows, then use these to infiltrate other countries' organisations in order to steal secrets or undermine that country's stability.

Generally nation state attackers are not after legal firms, real estate companies or any other types of businesses. So why should you be concerned? The danger is that your business can get caught in the crossfire. If a nation state decides to hack into a cloud provider for example, all the businesses that use the services they provide will be affected by the security breach and be in danger of having their sensitive company data stolen or exposed.

The "WannaCry" cyber attack affected 300,000 computers in 150 nations.

This hacking tool was reportedly stolen from the National Security Agency (NSA) and used by North Korea to launch a cyber attack against the US. Delivered through a zip file attachment in an email, it exploited a vulnerability in Microsoft Word that locked up the victim's computer and demanded a ransom to unlock it. Once inside the computer system, it self-replicated quickly – causing it to spread like a virus.

The attack caused billions of dollars of damage to hospitals, banks and businesses around the world – with unconfirmed reports from the NZ government's Computer Emergency Response Team (CERT) that a small number of Kiwi businesses were caught in the crossfire.

Understanding the Cyber Kill Chain® can help you thwart an attack.

The Cyber Kill Chain® is a framework developed by global security company Lockheed Martin that identifies the seven steps a cyber attacker needs to complete in order to breach their target's security system and launch an attack. Knowing how an attacker typically operates can help you prepare a defence for each stage of the attack.

1. Reconnaissance

The attacker gathers as much information as possible about your business and employees from publicly available sources like your website, social networks, staff email addresses and your IT structure to look for vulnerabilities.

2. Weaponisation

Once the attacker has identified your vulnerabilities, they select malware or devise a strategy to get access to your system.

3. Delivery

The attacker delivers the malware by targeting your vulnerabilities – for example by sending your employee a link in an email.

4. Exploitation

Your employee falls for the scam – for example by clicking on a link in an email.

5. Installation

The malware is activated – installing the access required by the attacker to get into your system.

6. Command and control

The attacker takes control of your system – sending out a legitimate looking invoice to your customers with a changed account number, or locking your computer so that no-one can access it.

7. Actions on objective

The attacker achieves their aim – this could be duping your customers into sending them money, getting a ransom from you to unlock your systems or stealing your valuable data.

Top tips to protect your business

Understand your environment.

Think about how your business operates and the type of data you have that could be valuable to others. Then think about who is likely to target you. If you're dealing with financial transactions, you're more likely to be a target for scammers.

Protect your information.

Be careful about the business details you make available online and the information you and your people give away. Think about who can access your log-in page and the controls you have in place to protect that page. Use the two factor authenticator option available on most systems like Microsoft Office 365 and Google instead of relying solely on staff-created passwords.

Ask more questions.

Make sure you look at things with a critical eye – before you pay a large sum of money into a bank account, verify the account number first by calling the company and checking the details are correct. Don't believe everything your customer or supplier tells you. If someone calls up with a story about their account number changing, check it out. Be especially aware if these changes are made at the last minute or outside of normal business hours. Remember that banks pay to account numbers – not names. This means an invoice could look legitimate because it has the right name on it, but the account number has been changed.

Limit your admins and log them.

In order to install software on a PC or a server you generally need administrative access. So if your employees don't normally have administrative access then it will be much more difficult to have malware and other software installed on your devices that you're not aware of. By limiting the amount of administrative people and accounts you have, the easier they are to manage.

Patch all your stuff all the time.

If you have old or out of date software, you're making it easy for cyber criminals to attack you or you could be vulnerable if you're caught in the crossfire of a nation state attack. Make use of auto update options on mobile devices.

Test your staff.

Test your defences and see where you need to make changes by testing your staff. Ring up your call centre and see if they'll give you the information that you've said they shouldn't be giving out. See if you can get to the CFO to request a payment be made. Check that your staff are asking for the correct identification when you call and request information.

Stay up to date.

Cyber attackers are constantly adapting their methods, so make sure you're up to date with the latest scams. Government websites like **netsafe.org.nz** and **cert.govt.nz** have the latest information on cyber security. Subscribe to their newsletters and stay aware.

Restrict your software.

One of the things that causes computer systems to become increasing vulnerable is all of the applications that get added on top. So every time you add an application or install some software on your machine you are increasing the size of the attack space. This means cyber criminals can take advantage of a vulnerability in a piece of software that you've downloaded and installed, that you've maybe used once and won't ever use again. Ask yourself how many different PDF readers, Word processors and web browsers do you actually need? If you take a critical look at it you can seriously reduce the number of those applications that you have which means you can reduce the number of potential vulnerabilities in your system.

Back up, back up, back up.

Will your business be able to operate without the information you have in your systems? Probably not. And the cost of retrieving it may be significantly more than you expect – especially when you factor in the impact of business disruption and damage to your reputation.

If you've got critical data your business can't function without, make sure you have a back up of it – whether it's on another server or even printed copies that are stored in an offsite safe. That means if you become a victim of ransomware and your documents get encrypted or your system is damaged as a result of an attack, you can get your data back. What actually matters is not that you got compromised, but that you can recover from it.

What to do when the worst happens.

First and foremost: Don't panic. If you don't have people who can help you, go to **netsafe.org.nz** or **cert.govt.nz**. If you're a Westpac customer and the victim of a financial crime, your first port of call is the call centre or your local branch. We have a specialist fraud team who can help you. If it's a criminal offence, the police can help in some circumstances. There are specialists in this area who will likely have seen the scam you're reporting, so you do have options available to you.

GTS10192-0319