THE FIGHT AGAINST NON-STOP FRAUD

Stay up-to-date with the latest cyber threats and get tips to protect your organisation.

Cyber criminals are relentless in finding new ways to infiltrate and exploit organisations and their data. They will use any vulnerability they can find – and increasingly that is through weaknesses in supply chains and payment ecosystems. By compromising smaller vendors who may be easier to target, criminals can get inside the ecosystems of larger organisations and launch large-scale cyber attacks with devastating consequences.

No organisation can afford to let their guard down.

Recent reports of cyber attacks are a stark reminder to all organisations that they need to stay alert to new threats.

"Criminals are becoming increasingly sophisticated. We're seeing fraud and scams evolve at a staggering rate. Most have a cyber component to them so it's important that businesses make sure their cyber security policies and procedures are up-to-date and regularly tested to keep pace with changing security requirements," says Lizel Foord, Fraud Analytics Manager at Westpac New Zealand.

Supply chain attacks are a growing problem.

Ray Chow, Senior Manager of Cyber Security Advisory at Westpac, says his team are seeing concerning new trends that organisations need to be aware of.

"Cyber criminals have figured out that it's easier to gain access to a large organisation by targeting their ecosystems. In many instances the smaller vendors in the organisation's supply chain may not have the resources or knowledge to protect themselves from security breaches. In fact, they may not even consider themselves a target for cyber criminals. And therein lies the danger."

If a criminal gets access to a vendor's email system for example, it's much easier to trick people into falling for old tactics like phishing emails. The criminal can send an email from the vendor's inbox to the organisation the vendor usually deals with, and no red flags will be raised. The receiver won't think twice about clicking on a link in the email – unwittingly exposing them to risk and potentially giving the cyber criminals access to the organisation's systems or even the ability to lock staff out until they pay a ransom.

Ray says: "As we've seen in the media, this type of cyber attack has the potential to cripple organisations and result in serious or even life-threatening consequences for the people who use their services."

Protection of customer data has never been more important.

Once an organisation has been breached, customer data like passport numbers and credit card details can be accessed and sold on the dark web. This can cause serious reputational damage to an organisation. There are also legal ramifications to consider. The Privacy Act in New Zealand has recently been updated, giving affected individuals or groups the ability to take class action against organisations that have failed to keep their data safe.[1]

Every organisation in the supply chain is responsible for managing risk.

Large organisations can have hundreds of vendors connected to their systems, so there needs to be clear policies, processes and regular training in place around who in the organisation is responsible for identifying vendors, what level of risk they pose to the organisation and how that risk is managed.

Vendors need to make sure they understand the vulnerabilities in their security systems and take steps to mitigate those risks.

How to prevent a breach and keep your systems safe.

Lizel says: "Understand the risks to your organisation and plan ahead. Implement controls and regularly test their effectiveness. Create an organisational culture that takes security seriously, protects sensitive data and reports things that don't look right. Make sure staff understand the different ways that things may go wrong and what they can do to protect themselves and the organisation. Scams are not always obvious and can lead to serious security breaches."

[1] justice.govt.nz/justice-sector-policy/key-initiatives/privacy

Top tips for vendors and smaller organisations

Back up regularly.

- Identify what needs to be backed up such as documents, emails, contacts and calendars.
- Ensure the device containing your backup is not permanently connected to the device holding the original copy physically or over a local network.
- Consider backing up to the cloud. This means your data is stored in a separate location from your office/devices and you'll be able to access it from anywhere.
- If automatic backup is available, consider taking advantage of the 'set and forget' function as an effective back up method.
- Test your backup data periodically by accessing them to ensure they are accessible and active.
- If USB or removable media is used as a backup solution, consider making copy at least six-monthly, in case the original backup media has become faulty.

Keep mobile phones and devices safe.

- Switch on PIN/password/fingerprint recognition.
- Ensure devices can be tracked and remotely wiped or locked if they are lost or stolen.
- Keep your devices and all installed apps up-to-date and enable the automatic update option if available.
- Don't connect to public wifi hotspots, use 3G or 4G connections or VPNs instead.
- Replace devices that are no longer supported by manufacturers.

Create a cyber security awareness culture.

- Treat cyber security as 'health and safety' for your technology and online presence.
- Create a simple plan of 'DOs' and 'DON'Ts' around technology usage, including tips.
- Remind staff of the tips on a regular basis.

Protect your organisation from malware.

- Use antivirus software on all computers and laptops.
- Only install approved software on mobile phones and devices and prevent users downloading third party apps from unknown sources.
- Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors use the 'automatically update' option where available.
- Consider disabling ports so that staff can't use removable media like SD cards and USB sticks. Transfer files via email or cloud storage instead.
- Switch on your firewall to create a buffer between your internet and network.
- Make sure all laptops, Macs and PCs use encryption products that require a password to boot.
- Use two factor authentication for important websites like banking and email.
- Use a separate login for privileged activities versus everyday use to minimise exposure.

Avoid phishing attacks.

- Make sure staff don't browse the internet or check emails from an account with administrator privileges.
- Scan for malware and change passwords as soon as possible if you suspect you've been the victim of an attack.
- Check for obvious signs of phishing like poor spelling and grammar or low quality versions of recognisable logos. Double-check email addresses to check they are legitimate.
- When in doubt, contact the sender to confirm the request is genuine using a different communication method or draft a new email instead of using "reply to".
- Create a strong culture of cyber security awareness.
- Run compulsory cyber security awareness training sessions for all staff.
- Update your staff regularly about new threats.
- Ensure staff know how to report risks and feel comfortable speaking up if something doesn't seem right.
- Get more tips at westpac.co.nz/assets/Business/institutional/documents/Thought-Leadership-Articles/Financial-Crime-is-Everyones-Business-Westpac-NZ.pdf

Plan for an attack.

- Know who to contact in your business and externally. If you're dealing with a banking or payment ecosystem compromise, your bank should be at the top of your list. Westpac customers can contact their relationship manager, local branch or our call centre.
- Keep detailed notes about the event including dates and times. This will be important if you need to make an insurance claim and can also be used in staff training.

File a police report.

- Report a breach at privacy.org.nz

Top tips for large organisations

Identify and maintain visibility of all your suppliers.

- Think about who and what is connected to your organisation.
- Take into account all internet-enabled devices, equipment, systems and cloud-based services.
- This could include plant machinery, building systems and physical security systems.
- Don't forget your everyday commodity suppliers use technology to run their business too.

Determine which suppliers are the most critical.

- Categorise your suppliers into levels of risk and classification of data they are accessing, processing and storing.
- Consider the potential harm to your organisation caused by failures, outages or other disruptions to each of the assets and services you use.
- Create business continuity plans and arrange for contingencies in the event that a critical supplier is disrupted.
- Continuously evaluate the criticality of your suppliers.
- Maintain regular communication with your suppliers about issues, risks and changes that could impact your organisation.

Understand your suppliers' security measures.

- Make sure you know who your suppliers' own suppliers and contractors are and be aware of the access your suppliers grant to their own subcontractors, where it impacts your own information and assets.
- Ensure you have cancellation policy in your supplier's contract that includes the return or disposal of your assets and information if you need to terminate their services.

Make sure every supplier has an owner.

- Use a RASCI chart to determine who is Responsible, Accountable, Supporting, Consulted and Informed to capture key accountabilities and responsibilities.
- Ensure your cyber security teams know who the owner of each supplier is and agree who will keep them informed of any additions or changes in suppliers.

Communicate your security expectations.

- Clearly state your minimum security requirements for suppliers when drafting RFPs or contracts.
- Consider the security implications of allowing suppliers to use their own subcontractors.
- Where necessary, include provisions for exercising the right to audit the supplier's security, and for regular reports on security performance to be provided to you.
- Provide suppliers with the specific regulatory compliance mandate your organisation needs to adhere to – this will ensure you are continuing meeting your obligations.

Regularly review supplier risk.

- Consider the security implications for your organisation if a critical supplier experiences a change of ownership or major shareholding or undergoes a merger. A disruption such as a natural disaster, crisis or major event could also change their level of risk.

Establish reporting metrics.

- Clearly communicate how you expect your supplier to meet your security requirements e.g. incident response times, patching cycles and maintenance schedules.
- Consider how you'll measure their compliance e.g. internal or external audits, self-assessment questionnaires or participation in cyber security simulation events.

Sources:

ncsc.govt.nz/assets/NCSC-Documents/NCSC-Supply-Chain-Cyber-Security.pdf

ncsc.gov.uk/files/Small%20Business%20Guide%20Infographic%202.pdf

Supply chain security guidance: ncsc.gov.uk

ncsc.gov.uk/files/NCSC_SBG_Actions.pdf

zdnet.com/article/cybersecurity-your-supply-chain-is-now-your-weakest-link

Find out more

Visit cert.govt.nz or netsafe.org.nz

Visit westpac.co.nz/business-base or go to westpac.co.nz/safety-and-security for tips from our Financial Crime team.

Things you should know. All intellectual property in this document, any trademarks or brands represented in this document or on systems, services and products described in this document are the property of Westpac. Nothing in this document will transfer or shall be deemed to transfer title to that intellectual property. The content of this document is intended for information purposes only and you should use your own judgment regarding how such information should be applied in your own business. We make no warranty or representation, express or implied, regarding the accuracy of any information, statement or advice contained in this document. We recommend you seek independent legal, financial and/or tax advice before acting or relying on any of the information in this document. All opinions, statements and analysis expressed are based on information current at the time of writing from sources which Westpac believes to be authentic and reliable. Westpac issues no invitation to anyone to rely on this material.