# 11 KEY LESSONS FROM AUSTRALIA'S CYBER CRIME CHALLENGE

A rising list of ransomware attacks on Australian companies has caused financial and reputational damage, while traditional threats – phishing and business email compromise (BEC) – are growing ever more sophisticated.

**So, what have we learnt about cyber risks, and how can businesses stay safe?**

## A HIGH PRICE TO PAY

**AUD**
**3.35**
**MILLION**
The average cost of a data breach in Australia per breach
SOURCE

**AUD**
**42**
**BILLION**
The estimated annual cost of cyber crime in Australia
SOURCE

**AUD**
**2.59**
**BILLION**
The estimated annual cost of ransomware attacks in Australia
SOURCE

**USD**
**265**
**BILLION**
The global cost of ransomware attacks by 2031
SOURCE

> "As defenders of cyber attacks, you have to be right all of the time. An attacker only needs to be right once."

**ANDREW WEBSTER** Chief Security Officer, Transgrid

## HOW BUSINESSES CAN RESPOND

### #1 Design your applications defensively

Some recent breaches appear to have involved unprotected application components, which trusted whoever had access. Unfortunately, if accessible to an attacker, they can exploit that vulnerability to inappropriately access data.

**THE TAKEAWAY:**

Simon Brown, Westpac's Head of Cyber Strategy and Advice, advises companies to design their applications to be defensive: do not let any part of your systems or networks trust another part – instead, design systems to always explicitly authenticate. At the same time, rigorously collect historical systems data ("logs") so that it's easier to assess what data has been accessed in an attack.

### #2 Communicate clearly with customers and regulators

Fast and transparent communication is paramount when in incident response mode, says Shamela Gonzalez, Director and FSI Industry Lead at CyberCX.

Stakeholders will inevitably become disgruntled if there are delays or a lack of detail on the extent of a data breach. "We'll see more rigour around transparency because public expectations have increased," Gonzalez says.

**THE TAKEAWAY:**

Be explicit when a breach occurs, don't create a sense that you aren't doing anything or fall into radio silence.

### #3 Speed up software patching

The Australian Cyber Security Centre (ACSC) advises businesses that industry best practice is now to apply high-priority security patches within 48 hours. Previous average response times were up to 90 days. "That's a dramatic reimagining – from months to hours – for many organisations to consider," notes Westpac's Brown.

**THE TAKEAWAY:**

Vulnerability scanners can help organisations gather information on missing patches in their systems and networks.

### #4 Ramp up multi-factor authentication

Cyber criminals can often use a misconfigured firewall to gain a treasure trove of customer information. Many cyber security experts believe more rigorous use of multi-factor authentication (MFA) – requiring users to provide two or more verification factors to gain access to a network, and not just a password – is key to preventing attacks.

**THE TAKEAWAY:**

MFA should be non-negotiable, says Nadia Yousef, Country Manager New Zealand at CISO Lens, a peak body for cyber security executives. "A lot of the attacks we have seen would have been mitigated if MFA had been in place with good password hygiene."

### #5 Say goodbye to passwords?

Poor password management is blamed for many cyber attacks. David Lacey, Managing Director of cyber support service IDCARE, says "brave organisations" are opting not to rely on passwords. This can nullify the risk of inadequate passwords, or the tendency of people to forget to update them. "It takes the human frailty out of the scenario," Lacey says.

**THE TAKEAWAY:**

If passwords are not used, companies must deploy smart devices that can recognise users, and then use MFA as a complementary security layer.

### #6 Get up to speed with privacy rules

Recent cyber attacks, prompted changes to the penalty regime for serious or repeated breaches of the Privacy Act. Business leaders must understand the relevant Australian Privacy Principles (APPs), when to notify affected individuals and the Office of the Australian Information Commissioner of a data breach, CyberCX's Gonzalez recommends.

**THE TAKEAWAY:**

More boards should follow the lead of progressive directors who are now "seeking to understand the mechanics behind the risks, playing through actual cyber scenarios and want to see themselves in some of these playbooks", suggests Gonzalez.

### #7 Factor in supply-chain risks

Think about cyber crime as not only a direct risk to your organisation's operations, but as something that could happen in the supply chain. "A cyber attack for one of your key suppliers could become a business disruption event for you," Brown warns.

**THE TAKEAWAY:**

Improve resilience by avoiding dependence on one supplier for a critical function in case they experience a cyber crime event.

### #8 Beware of the next big threat

Artificial intelligence is being used in relationship scams to generate fake voices or videos of loved ones or other trusted people – and IDCARE's Lacey believes the corporate world is vulnerable, too. "CEOs or other senior staff may be impersonated so criminals can gain access to systems. Rather than using an email, it could be a fake audio or video call instead."

**THE TAKEAWAY:**

Never be complacent about cyber risks because hackers are perpetually seeking new ways to deceive victims.

### #9 Keep watching for phishing and other attack vectors

Email-based cyber breaches continue to grow. Business Email Compromise (BEC), where a scammer tricks someone into sending money or divulging confidential information, is becoming increasingly sophisticated.

"Everyone is worried about ransomware, but BEC is almost as common," Yousef says. Phishing (emails and links), smishing (texts) and vishing (voice calls and voicemails) attacks are also a constant threat.

**THE TAKEAWAY:**

Cyber training for staff is essential. Transgrid's Webster urges hyper-vigilance as AI tools like ChatGPT are helping hackers write more professional scripts for email scams making them harder to detect.

**74%**
of Australian organisations have fallen victim to at least one successful email attack in the past 12 months.
SOURCE

### #10 Finetune your cyber safety playbook

Discuss and document crucial cyber risk issues from staff training to employee roles in the event of an attack, and whether your business would pay a ransom.

The Australian Government recommends that a ransom should never be paid, and for an unprepared company, the consequences of losing control might be unacceptable; some companies fold when they try to hold out. If you don't want to be in that position, ensuring you have a great, tested backup-and-recovery plan in place is critical.

**THE TAKEAWAY:**

Boards and management teams should have a conversation about paying ransoms. CISO Lens' Yousef says: "It's worth testing what it would be like for your organisation if there were an attack."

**44%**
of businesses pay a ransom within 24 hours of being attacked, up from 29% in 2021.
SOURCE

### #11 Test backup-and-restore systems

Backup and restoration plans should be tested – before an attack, advises Transgrid Chief Security Officer, Andrew Webster. Testing your cyber security playbook can help safeguard important data, software and configuration settings.

"Many companies have backups, but they've never tried a restore because it's difficult to schedule while you're trying to run your business," Webster observes.

**THE TAKEAWAY:**

A focus on resilience should include having a backup and restoration plan – and a plan B and a plan C if the first strategy fails.

**69%**
The proportion of Australian businesses that have experienced a ransomware attack in the past five years.
SOURCE

## WHAT'S ON THE RADAR?



**Quantum computing**
could be used by malicious actors to attack previously unbreakable encryption codes, if it turns out to be possible.



**Data manipulation**
could see attackers edit and modify information without leaving a trace to destabilise an organisation or demand a ransom for the restoration of that data.

## SOME FINAL TIPS...

Offer incentives to cyber security champions in your broader team, to encourage a security mindset across your whole organisation.

Ensure there are no security gaps between legacy systems and new platforms.

Apply normal product and services rigour and testing when releasing customer support packages for cyber victims and do not rush their rollout.



Engage in polite paranoia with cyber risks, not just at work but with texts, messaging apps and emails sent from home.

## HOW WESTPAC CAN HELP

To safeguard businesses and customers, Westpac has rigorous internal and external cyber security measures in place. Our fraud and scam teams work 24/7, see **https://www.westpac.com.au/security/** for further information.

©Westpac Institutional Bank – A division of Westpac Banking Corporation ABN 33 007 457 141 AFSL and Australian credit licence 233714 (Westpac). The information provided is factual only and does not constitute financial product advice. Before acting on it, you should seek independent financial and tax advice about its appropriateness to your objectives, financial situation and needs. Information is current as at July 2023.