October 2022

MARKET REPORT

The state of Cyber Resilience in Australia 2022

Five cybersecurity risks facing the hybrid workplace — and how to address them.

Barracuda
Your journey, secured.

Table of Contents

Introduction

Australia has embraced a hybrid work culture following the global pandemic. However, from the start there have been some cybersecurity 'red flags' with remote work arrangements. Within months of organisations asking employees to work from home, we saw security teams worried about stopgap measures taken for business continuity reasons; about the rising opportunism of attackers; and about workers' preparedness to face new or increasing cyber threats.

A lot has happened in the two years since the pandemic began. But what have Australian security teams learned about operating in hybrid and remote work environments? Our new research shows that Australia's CISOs and security teams were right to be wary of the work-from-home revolution.

Among other things, the research reveals that when it comes to IT and security for hybrid working, special rules apply for senior (and middle) managers; BYOD (Bring Your Own Device) brings new security challenges; and individuals and teams are having to 'flex' beyond reasonable constraints in the name of business continuity and productivity – at the expense of security. Additionally, passwords and IT systems are expected to fill any gaps left by inadequate cybersecurity training.

In this study, we identify and explore the cybersecurity controls and protections that were ignored, downplayed or side-stepped during the past two years. In addition, we examine what it will take for organisations to improve overall cyber resilience.

Methodology

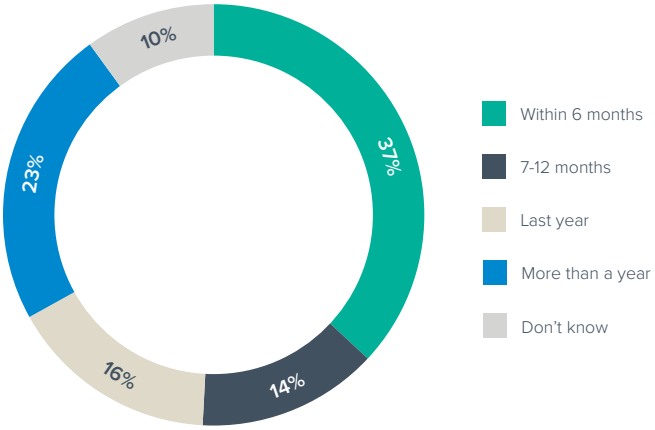
Barracuda commissioned independent market research firm StollzNow Research to conduct an Australian survey of IT decision-makers and non-IT workers in organisations of at least 50 employees that use a computer for work. There were 504 respondents across all organisational sizes and levels, including about 16% in senior management and 63% in mid-level roles. All states and territories in Australia, except the Northern Territory, are represented. The survey was fielded in May 2022.

Overview

Organisations are prone to security incidents

Australian organisations are succumbing to the increased threat landscape they now find themselves in. Overall, one-in-five (23%) of the Australian businesses surveyed say they have experienced a security breach, with just over half (51%) of them hit in the last 12 months.

If you have suffered from a cybersecurity breach, when was the most recent one you are aware of?



Base: respondents who experienced cybersecurity breach, n=115

The high level of security breaches is likely to reflect the challenges of securing a hybrid operating environment, with IT teams unsure how to combat the myriad threats and security challenges that hybrid workers now routinely face.

Over one-quarter (27%) of all respondents said they experience cybersecurity challenges while working from home. Respondents in senior management roles (41%) or working in small and medium enterprises with between 50 and 99 employees (56%) — which may have less IT support on hand — are more likely to say they encountered problems.

There is no single specific cybersecurity problem experienced in work-from-home environments. Rather it is a range of niggles that all make working from home a security challenge.

The top IT problems and security challenges are VPN issues and remote access (14%), phishing emails and malware (14%) and general cyberattack concerns (14%). However, home-based workers also report having problems with juggling too many access credentials (9%), unsecured home networks or personal devices (8%) and lack of access to existing systems (3%). The list goes on, but the short of it is that users are presenting to IT with a wide range of issues.

What are the cybersecurity challenges you experienced working from home?

VPN issues	14%
Phishing / malware	14%
Cyberattack concerns / security breaches	14%
Too many codes (MFA)	9%
Unsecured home networks / unsecured devices	8%
Hard to reset password remotely	8%
Spam	6%
Don't have access to all usual systems	3%
Authentication issues	3%
New communications systems	2%
Online scams	2%
Concerns about websites	2%
Other	25%

Base: all research participants, n=504

If the challenge is this complicated for employees, imagine the impact it is having on the team(s) tasked with securing this environment. Security in the hybrid work era clearly needs to be tightened up.

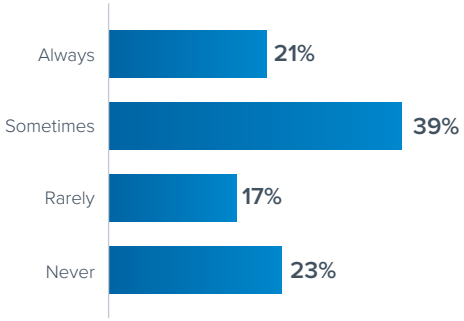
FINDING #1

Phishing is the top threat in the workplace

More than two years into hybrid work, warnings about the associated rise in phishing attacks and malicious links are not getting through. The risk increases when, as our survey shows, employees are inclined to think all emails are safe.

Our research finds that 60% of all respondents assume a link is safe if it comes through office IT systems. In addition, 52% of mobile users will click on a link if it comes from a "sender" that they trust.

When you receive a link in an external email, do you assume that IT systems will make sure the link is safe to click on?



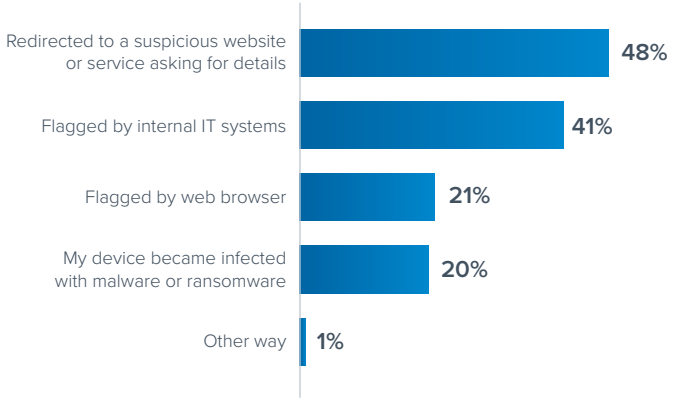
Base: all research participants, n=504

Today, email-based attacks are increasingly complex and often use customised social engineering tactics to trick users, such as impersonation. Clicking a link without making any attempt to verify it can leave users — and the organisations they work for — vulnerable to email compromise and account takeover, or worse.

Inserting malicious links or attachments is another common tactic to evade email security. The research shows that one-quarter (25%) of office staff have clicked on a malicious link, while 11% 'don't know' if they had or not.

Almost half (48%) of those who clicked on a malicious link only discovered it was malicious when they landed on a suspicious website and/or it was flagged by internal IT systems (41%). A fifth (20%) say they learned of their mistake when their machine was infected with what they believe to be malware or ransomware.

If you have clicked on a malicious link, how did you know the link was malicious?



Base: respondents who have clicked on a malicious link, n=124

All these point to ineffective email or web filtering protection and a gap in security-awareness training, which help to make phishing emails a top threat vector. The findings provide further evidence that human error often remains the weakest link in the chain that exposes corporate networks.

All users need to be part of a layered protection approach against phishing attacks and malicious links. There is a risk that many home-based workers put their faith in IT and security systems to recognise and block any threats they mistakenly engage with. They cannot simply outsource that responsibility to IT.

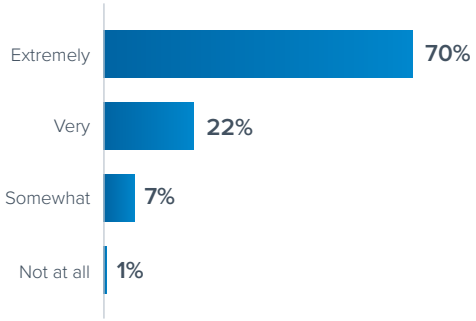
Traditional email gateways or web browsers can struggle to keep pace with the evolution of attacks. Mitigating the email risk with investment in advanced technology including AI-powered email protection against complex email threats such as account takeover or business email compromise (BEC) and security awareness training is crucial.

FINDING #2

A gap in security awareness training

The rise of data breaches, up 6% year-on-year according to the Office of the Australian Information Commissioner, and their often costly consequences has reminded organisations of the importance of cybersecurity. In Australia, businesses overwhelmingly care about cybersecurity — 92% of the organisations surveyed for this study think it is extremely or very important — but the findings also suggest they may not be getting the tools or training time needed to translate care and concern into security posture improvements.

How important do you think cybersecurity is to the organisation you work in?

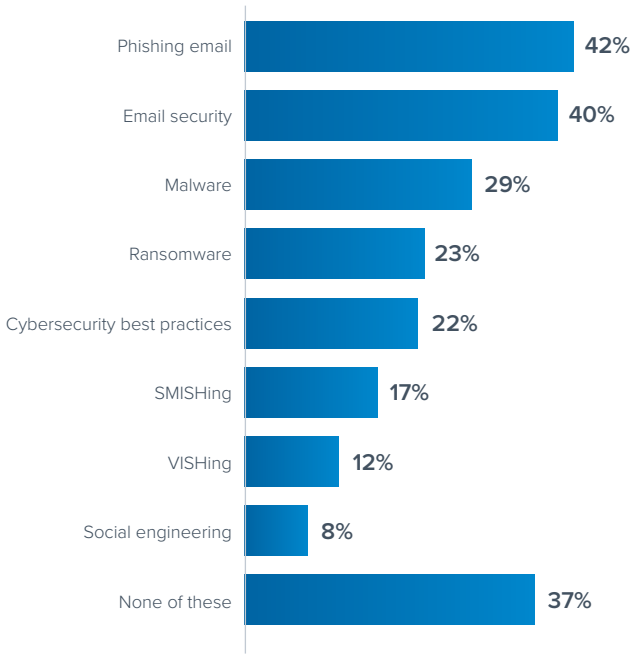


Base: all research participants, n=504

Our research suggests that many may have forgotten their cybersecurity awareness training — or perhaps more to the point, did not get enough of it in the past year. Just over a third (37%) have not had training in any of the main areas of cybersecurity awareness, and 14% have had no training at all.

For those that did receive training, it was mostly about phishing (42%) and general email security (40%), as well as all forms of social engineering (8%). But awareness of different types of phishing varies. Only 17% of respondents have received SMISHing training, and that falls to 12% for VISHing.

Have you had any training in any of these aspects of cybersecurity?

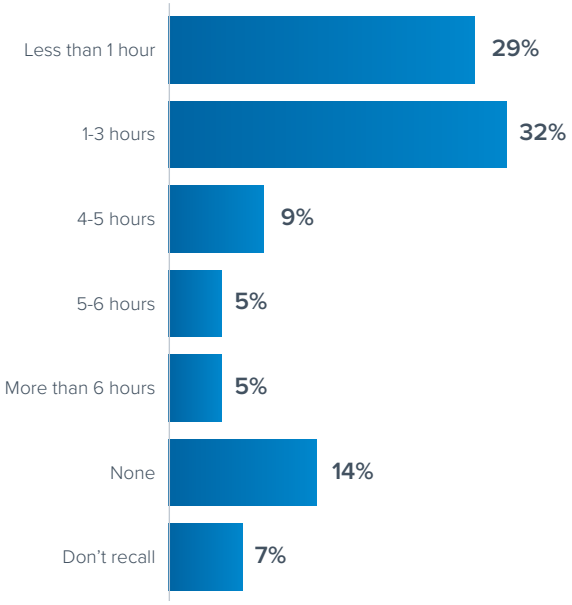


Base: respondents who are aware of cybersecurity terms n=480

Examining the hours of training they received, the results show that 61% received three hours or less a year, and 14% did not receive any security awareness training at all in the last year.

To effectively educate users on cybersecurity hygiene, organisations should ideally provide around 30-minutes of security awareness training per month. This regular approach helps to build and maintain a cybersecurity culture in the workplace and turn employees into a line of defense.

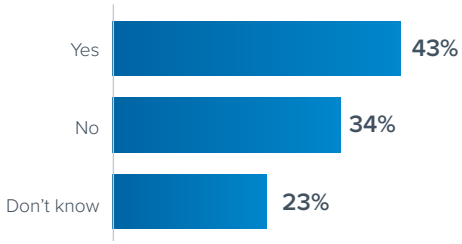
Time spent completing security awareness training in a year:



Base: all research participants, n=504

The survey found that just over two-in-five organisations (43%) share results of security awareness training with staff; the remaining 34% say results are not shared and 23% do not know if results are shared. Sharing results can be a good way of reinforcing employee awareness and understanding of the scale of a shared challenge that everyone faces together. Training is an investment in staff and capability. It should not be treated as a checkbox exercise. In some cases it may even be worth integrating security awareness into performance goals.

Are the results of security awareness training shared?



Base: all research participants, n=504

If staff lack training and refreshers on cybersecurity hygiene basics, how is that being reflected in their system use? To put it simply, our results suggest there may be a lot of blind trust and good faith that cybersecurity protection measures and technologies will cover any mistakes.

FINDING #3

The extended network needs stronger access controls

The rush to equip and enable employees to work-from-home during the COVID-19 pandemic, combined with chip shortages that made bulk device supplies harder to come by, meant that many organisations allowed employees to use personal devices and even personal email accounts to conduct company work as a transitionary measure.

BYOD is a common practice

Two years later, our survey shows that almost two-thirds (63%) of Australian organisations allow staff to use a personal mobile device for work-related activities. This is more likely for senior management (77%), but even 59% of middle management and 58% of other staff use personal devices for their work.

The most common use is for email (54%), but the devices are also being used to access organisational resources and data (31%), and to store organisational data (22%).

What do you use your personal mobile device for?

Base: all research participants, n=504

Security rules were always much harder to enforce on BYOD. As these devices generally sit outside the traditional corporate network perimeter or other fleet controls, the ongoing use of these devices can expose entire corporate networks to external threats. Security-conscious organisations offer corporate-issue devices and apply security controls for this reason.

The research shows that a significant number of organisations allow employees to perform their own IT admin tasks. For example, almost one-third of the respondents say they carry out their own computer system updates (32%) and backup (29%). Without proper monitoring or controls this could significantly increase risk.

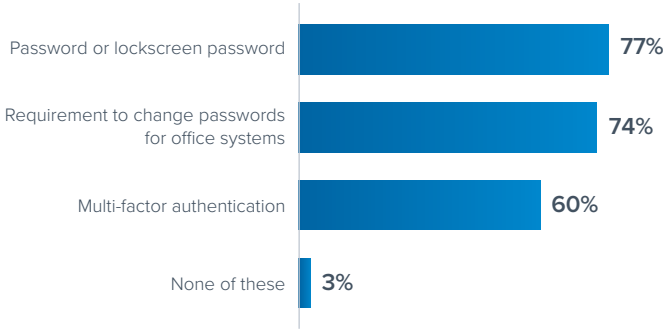
Limited use of MFA

It is not just about BYOD – it is also about protecting access credentials, applications and data being accessed through these devices.

The findings show that critical enterprise data and systems running in the cloud are accessed remotely with password-only protection – without having multi-factor authentication (MFA) in place – in 40% of cases.

In other words, despite everything we know about name-and-password login credentials being phished by attackers to access corporate accounts and data, use of MFA remains at 2019 levels, if that.

Security systems used in daily workspace?



Base: all research participants, n=504

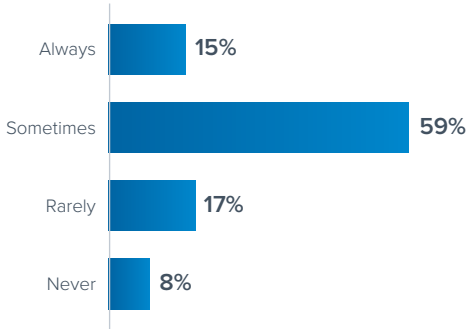
Of organisations that do have MFA enabled, some are clearly let down on implementation: 'too many MFA codes' is the fourth most complained about cybersecurity-related issue for home-based workers.

Where passwords are used as an authentication method, 87% of organisations require regular changes and have requirements for complex passwords in place

But complex passwords can be a challenge for users and reduce workplace efficiency. Almost three-quarters (74%) of users 'always' (15%) or 'sometimes' (59%) have trouble remembering complex passwords.

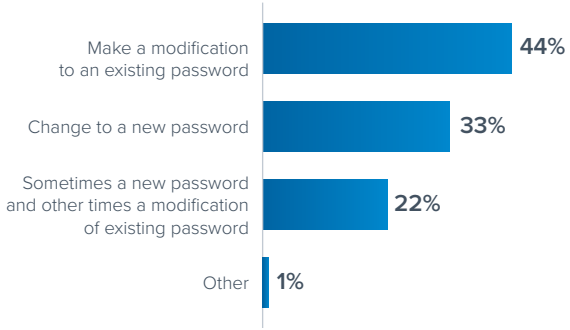
Given the difficulty of remembering a complex password, only 33% create a new complex password when prompted; most just make a small modification to the existing one, which makes them susceptible to breaches with similar password patterns.

Have trouble remembering new complex passwords?



Base: respondents who are required to change to complex password, n=383

Use a new password or modify an existing password?



Base: respondents who are required to change to complex password, n=383

The findings show that alternatives to complex passwords that are regularly changed are needed in business as this process impedes productivity and is ineffective.

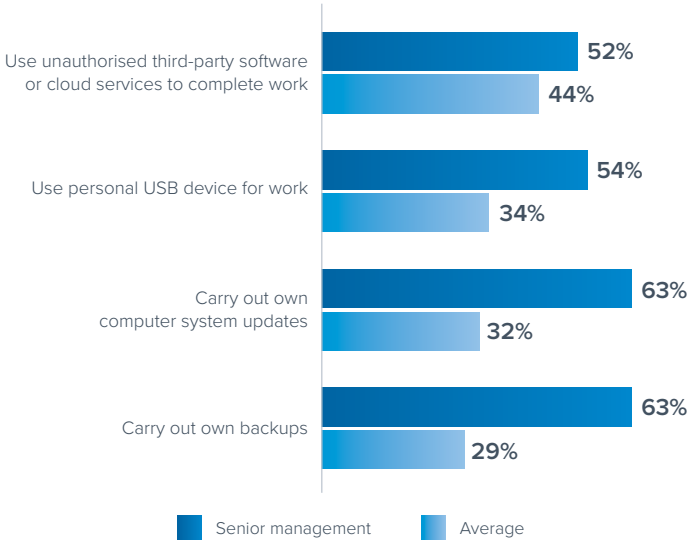
FINDING #4

Users with excessive privileges increase risk by circumventing security controls

In recent years, senior managers forwent special treatment to lead by example on cybersecurity. Top-down support of cybersecurity measures through actions, not just words, was naturally of great assistance to security teams, but is much harder to maintain if managers don't abide by the same rules they make for others.

And here lies the juxtaposition: the survey found that senior managers are far more likely to be 'extremely' aware of the importance of cybersecurity (66%) than staff at other levels of the organisation (53%) but are also far more likely to ignore or bypass security best practices themselves or left to initiate their own software updates and backups.

Senior management is more likely to circumvent security controls



Reports suggest that senior managers with excessive privileges are typically the primary targets for hackers to access to sensitive data or financial gain. Our survey found that 41% of senior managers experienced cybersecurity challenges when working from home, much higher than the average worker (27%).

The number of senior managers that need to initiate their own system updates and backups is especially concerning. 63% say they carry out their own computer system updates and make their own backups, double the average (32% and 29% respectively). Without timely or properly managed security checks, there is no assurance for the organisation's security and risk functions that these devices are being patched or backed up to corporate standards. Unpatched devices are at higher risk of exploitation and can potentially be used as a gateway into the corporate network. Local data stored on unprotected personal devices or third-party cloud storage may be difficult or impossible to recover in the event of an attack.

Executives have a low tolerance for barriers and hindrances, and this may be why they choose to override the rules. Security systems have the biggest impact on senior management: 58% say that systems prevent efficient work. One-in-five (19%) senior managers say they 'frequently' circumvent rules to deliver workplace outcomes.

There is an onus — even a responsibility — for cybersecurity teams to make layered protection as unobtrusive and frictionless to the user experience as possible. By the same token, some checks and balances are unavoidable.

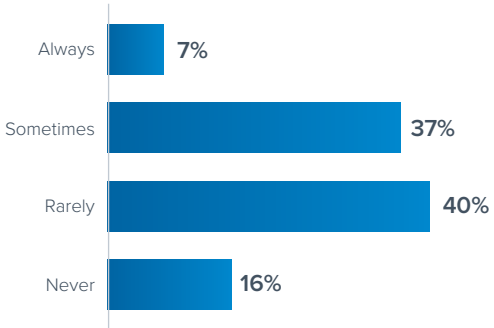
FINDING #5

Security takes a backseat to flexibility and productivity

Flexibility and agility have become business mantras, but some individuals and teams may have been allowed to flex too far in the name of continuity and productivity by bending cybersecurity rules 'to get a job done'.

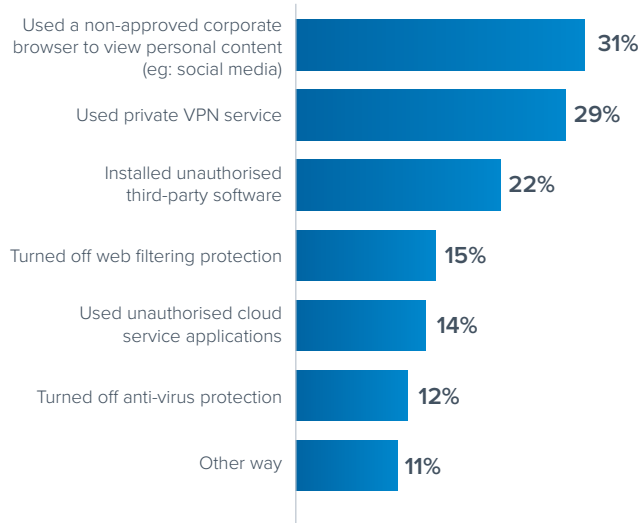
Our research shows that 44% of respondents view cybersecurity as a blockage to working efficiently. One-in-three (33%) admitted to 'always' or 'sometimes' working around the rules 'to get a job done'. Some of these were bends — using a non-approved browser (31%) or running traffic through a private VPN (29%); others were installed unauthorised third-party software (22%) or out-and-out breakages, with users administrative controls to switch off corporate web filtering or anti-virus. Another 44% admitted that they would use unauthorised third-party software or cloud services or applications to complete work.

Do security systems prevent you from working efficiently?



Base: all research participants, n=504

In which of these ways have you circumvented workplace cybersecurity?



Base: respondents who circumvented workplace cybersecurity, n=269

Organisations need to have measures in place that prevent employees from disabling critical security and protects them in the case of low-level workarounds.

Guardrails, controls and policies exist for a purpose. Structure is required for risk mitigation, auditability and peace-of-mind at an executive (or, where applicable, shareholder) level. When structure is abandoned, or flexed outside acceptable tolerances, things happen.

With new ways of work becoming far more settled now, senior managers — often rule-benders themselves — cannot continue to 'look the other way' on cybersecurity for the sake of business productivity. A balance needs to be struck, and that requires all stakeholders to recognise there is a problem, and to come to the same table to create a workable resolution.

Conclusion

Step forward to boost cyber resilience.

The survey suggests that many organisations and their employees may need a reminder about why cybersecurity exists. It exists for staff, customer, organisational and societal safety. It can't simply be bypassed or classed as a lower priority to getting work done.

To instill a cybersecurity culture and strengthen overall cyber resilience, a good place to start is to set up some refresher training on cybersecurity hygiene.

Firstly, the obvious set of cybersecurity controls for Australian organisations to implement is the Australian Cyber Security Centre's Essential Eight, which is now a mandated compliance for Australian federal government agencies and departments to improve their security posture. The obscure security framework – 88% of Australian organisations have not heard of it – provides eight essential mitigation strategies to help Australian businesses harden their defense against attacks.

Additionally, an effective protection plan should protect organisations against today's evolving email threats, application vulnerabilities and data breaches. These include:

1. Protect credentials

Implement anti-phishing capabilities by leveraging artificial intelligence to detect and block the most common 13 email threat types and social engineering attacks that bypass traditional email security, and enable proactive threat discovery with automated remediation for post-delivery threats.

2. Train users

Educate users about the types of attacks they face and the security best practices, such as password hygiene and data protection. Ensure they can recognise attacks and know how to report them. Use simulations to train users to identify attacks, test the effectiveness of your training, and evaluate the users most vulnerable to attacks.

3. Secure applications and access

Besides using MFA, implement web application security for all SaaS applications and infrastructure access points to protect against the OWASP (Open Web Application Security Project) Top 10 threats. Along with application protection, reduce the amount of access provided to external users or implement Zero Trust Access based on endpoint security postures.

4. Back up data regularly

Stay current with a secure data protection solution that can identify critical data assets and implement disaster and recovery capabilities, and help businesses meet compliance requirements. Take advantage of a cloud-native, SaaS backup solution to ensure better performance with instant scalability.

5. Set up strong internal policies

Establish security policies and regularly review existing policies to ensure personal devices and corporate data are handled properly. Create security guidelines and put procedures in place, such as regular system updates, to help employees avoid costly mistakes.

Training needs to be an ongoing effort, as attacks often become more sophisticated over time. Customised security awareness training by Barracuda Networks that is aligned with the Essential Eight can help Australian businesses to take advantage of the framework in order to protect against cyber threats and cultivate a cybersecurity culture. Organisations which comply with the Essential Eight training will be more fully prepared and able to take advantage of some additional business benefits from the investment in education and knowledge being made.

About Barracuda

At Barracuda, we strive to make the world a safer place.

We believe every business deserves access to cloud-first, enterprise grade security solutions that are easy to buy, deploy and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey.

More than 200,000 organisations worldwide trust Barracuda to protect them — in ways they may not even know they are at risk — so they can focus on taking their business to the next level.

Get more information at barracuda.com.

About StollzNow Research

StollzNow Research is a research and insights consultancy based in Sydney, Australia that operates across the world to help clients better understand business challenges and attitudes.

A focus of the business is ICT where StollzNow has helped dozens of leading organisations to understand their customers and the operating landscape for IT Decision Makers and their stakeholders.

For more information, visit https://www.stollznow.com.au/

Barracuda
Your journey, secured.