Forrester Consulting Thought Leadership Spotlight
Commissioned By Telstra

July 2020

Act Now: Your Five Immediate Priorities To Secure A Hybrid Workforce

In just a few months, the COVID-19 pandemic has rapidly changed the way we work and live. Few companies were prepared to shift to remote work as the government imposed stay-at-home measures. In the rush to support remote working arrangements, Australian businesses had to innovate or relax policies at a much faster rate than usual. These quick fixes might have been sufficient to support remote workers as a temporary measure for a couple of weeks, but as months have gone by, it has become evident that pandemic recovery requires a long-term response.

With COVID-19 restrictions easing in some parts of Australia and retightening in others, businesses must navigate the technology implications for the phased approach to office-returning staff while balancing the needs of remote and hybrid employees. In this "new normal," cybersecurity remains more important than ever. This study highlights the key priorities and steps businesses should take to support and secure an emerging hybrid workforce.

KEY FINDINGS

Forrester's study yielded the following key findings:

- **A scramble to support a dominant remote workforce has led to security and risk exposure.** Many Australian businesses were unprepared for the rapid shift to remote working and did not have essential security practices in place to safeguard an increased remote workforce.
- **Hybrid working is here to stay; a temporary approach won't cut it in the new norm.** Australian businesses are anticipating a higher rate of remote workers post COVID-19. Forty-two percent of business decision makers expect that their organisations will permanently maintain an increased remote workforce. Quick fixes that may have been sufficient for a few weeks are not viable for a permanent hybrid workforce.
- **Businesses must ensure they take the right steps to secure a hybrid workforce.** As COVID-19 restrictions adjust in Australia, businesses must take several immediate steps to secure hybrid workers. These include streamlining security investments, training employees to be cybersafe, deploying virtual private networks (VPNs) or Zero Trust network access, and building a reliable security foundation for personal devices.

Telstra commissioned Forrester Consulting to leverage Forrester research and Business Technographics® data to explore the implications of remote working on cybersecurity and the steps businesses need to take to secure a hybrid workforce.

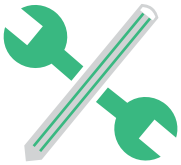
The data and insights in this study are based on existing research findings from Forrester's research on business and security decision makers in the Australian market and Forrester's Q2 2020 Australian PandemicEX Survey (May 1, 2020), which includes 262 Australian adults who work part-time or full-time.

FORRESTER®

The Rapid Shift To Remote Working Has Left Many Australian Businesses Exposed To A Rising Threat Landscape

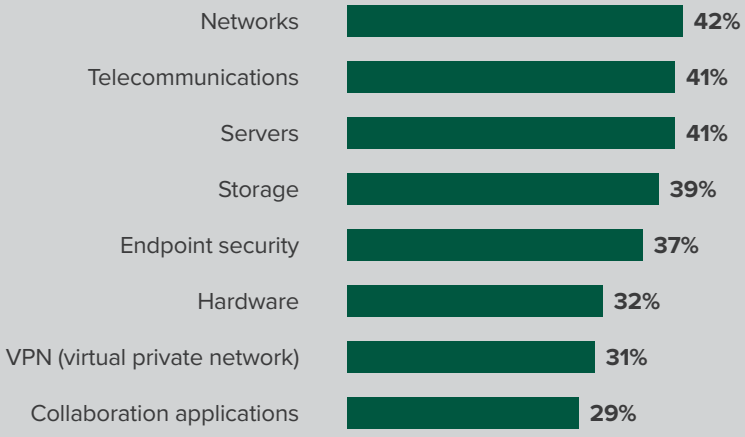
As a result of COVID-19, the percentage of employees working from home in Australia has increased exponentially — from an estimated 16% pre-pandemic to 68% at the peak of the pandemic.[1] However, many businesses were unprepared for this rapid shift to remote working and did not have essential security practices in place to safeguard an increased remote workforce.

- **Even before the pandemic, security practices were far from perfect.** Before COVID-19, 46% of security decision makers stated that they did not have sufficient tools in place to support employee use of mobile devices. A further 79% reported not having security analytics — security information management (SIM), managed security service provider (MSSP), or cloud-native — in place to protect "as-a-service" environments that are offered via cloud deployment.[2]
- **Unsurprisingly, Australian businesses do not feel prepared for cyberattacks.** As the number of employees working from home in Australia has increased exponentially, organisations have realised that they are not ready — not just from a tech, but also from a security perspective. Today, just 52% believe that their organisations' business continuity plans are equipped to address cyberattacks and/or other security incidents.[3]
- **IT decision makers had to scramble to support a remote workforce.** Even before the pandemic, 66% of IT decision makers did not feel that their organisations' IT infrastructure was prepared to handle a heavy remote employee base. With the pandemic, they've had to scramble. Now, around two in five IT decision makers report that their IT departments have adapted networks, telecommunications, servers, and storage to meet the needs of an increased remote workforce (see Figure 1). In addition, more than 30% have considered changes to endpoint security and VPNs to meet increased security demands.



Before COVID-19, 46% of security decision makers stated that they did not have sufficient tools in place to support employee use of mobile devices.

Figure 1: IT Provisioning Changes To Meet The Needs Of An Increased Work-From-Home Environment



Base: 59 Australian purchase influencers who answered during COVID-19 and who are technology decision makers
Source: Forrester Analytics' Business Technographics Priorities And Journey Survey COVID-19 Recontact, 2020

FORRESTER®

Five Immediate Priorities To Secure A Hybrid Workforce

Australians are bracing for further disruption to their work lives and don't expect to return to the office anytime soon. Sixty-seven percent of Australian workers expect that their work lives will be disrupted by coronavirus-related circumstances. Even when the crisis is over, they have mixed views on whether they want to return to the office. While 40% "cannot wait to get back to the office," 54% hope that they can work from home more often after the pandemic. At the same time, Australian businesses are anticipating a higher rate of remote workers, with 42% of decision makers expecting to permanently maintain an increased remote workforce (see Figure 2).

As COVID-19 restrictions ease in Australia, businesses must be prepared to transition to a permanent hybrid working arrangement. This study outlines five priorities with key steps Australian businesses should take to secure an emerging remote and hybrid workforce:

1. Streamline your security investments. Security remains a top priority for Australian businesses. Around one in three of Australian IT decision makers indicated that increasing security and privacy capabilities is a critical IT priority over the next 12 months. According to Forrester, in the most likely scenario, Australia's tech spending will contract by 2.7%.[4] With these imminent budget cuts and an economic downturn on the horizon, business leaders must be prepared to address security as a priority with potentially less funding.

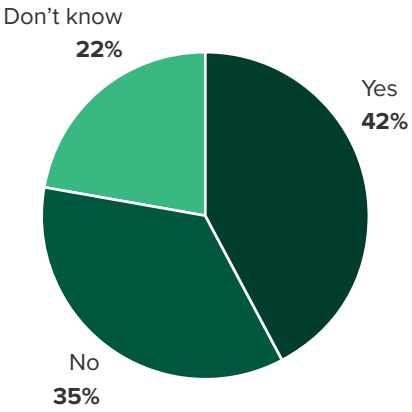
- **Concentrate spending with your most strategic partners.** Trim down your vendor list by thinking about which vendors provide the solutions that are critical to future growth and deepen your relationship with them. For those you keep, renegotiate contracts to reduce current costs in return for longer contracts.
- **Utilise a managed security service provider to help manage your capex and extend your resources.** Use a MSSP to rapidly uplift your security operations. With potential staffing cuts looming, a MSSP can augment your existing team with a deeper and wider skill set and improve the diversity of your team members' backgrounds and perspectives.

2. Train your employees to be cybersafe at home, at work, and on the move. With employees working remotely, the lines between home and work have become increasingly blurred. Cybercriminals are taking full advantage of this situation by targeting personal accounts to access sensitive corporate information through home networks. During the pandemic, there has been a 600% increase in phishing and malware attacks, including fake alerts on coronavirus cases.[5] Closer to home, the Australian Cyber Security Centre (ACSC) has received over 45 cybercrime and cyber security incident reports from individuals and businesses, all related to COVID-19-themed scam and phishing activity.[6] In their rush to be more productive and collaborative, businesses and users alike have indulged in unsafe behaviour by signing up for free tools and online applications, which expose businesses to greater vulnerability and risk.

- **Build a security awareness program, focusing on your biggest threats.** With the increase of opportunistic attacks targeting users specifically, you need to build your human firewall and help your employees with their remote working cybersafety. Your program needs to educate employees on cybersecurity threats for all online activity, regardless of whether it is personal or work-related.

Figure 2: Remote Working Outlook

"Do you anticipate that your organisation will permanently maintain a higher rate of full-time remote employees?"



Base: 113 Australian purchase influencers who answered during COVID-19 and whose organization had transitions to full-time remote work as a result of the pandemic
Note: Percentages do not total 100 because of rounding.
Source: Forrester Analytics Business Technographics Priorities And Journey Survey COVID-19 Recontact, 2020

FORRESTER®

- **Select and utilise security awareness and training tools to support your program.** Even the most sophisticated technologies and well-crafted policies can be rendered useless when employees simply decide to — or unknowingly — break the rules. Because of this, and because many cybersecurity attacks are personally tailored to mimic daily, routine actions, it is more difficult than ever to protect your workforce against today's threats. Security awareness and training can support your program and encourage the right behaviour.
- **Run phishing simulations.** Antiphishing best practices include a mix of technical controls, employee education, and incident response. Implement technical controls such as email content filtering and security awareness training. Educate your workforce to recognise and report phishing attempts. Finally, prepare for technical and human failure by having an incident response plan in place.

3. In the immediate term, keep your VPNs running and as secure as possible. As employees connect from home with company and personal devices, it is crucial to keep their connection secure. An increasing number of phishing attacks are targeting employees — and attackers are increasingly targeting employee personal accounts to compromise home networks. As an immediate step, deploy VPN access solutions to ensure security controls are enabled for all user devices.

- **Stock up on VPN licences to support a surge in remote working.** Businesses are reaching the limits of their current VPN infrastructure and licences. Take advantage of free trials and discounted VPN licences that providers are now offering to support businesses' interim surges in usage.

4. For the long term, invest in Zero Trust network access to replace aging VPNs. Prior to the pandemic, nearly two in five security decision makers in Australia considered implementing a Zero Trust security strategy as their top security priority over the next 12 months.[7] Although the current COVID-19 situation may have halted these plans, there has never been a more crucial time to invest in a robust and secure technical approach for continued remote access. Zero Trust network access (ZTNA) solutions reduce the network threat surface and have features that are more secure than VPNs, such as least-privilege application access, biometrics, and passwordless experiences.

- **Shift resources from VPNs to Zero Trust network access.** As temporary pandemic VPN licence programs sunset, consider allocating whatever resources you were planning to commit to VPN technology to ZTNA instead.
- **Gather requirements, shortlist vendors, and accelerate proofs of concept (PoCs).** Start by prioritising critical applications with the aim of maximising the number of "internal" applications that you can map to ZTNA to minimise the number of user VPNs required. If you already have Zero Trust initiatives underway, focus on accelerating — or, at the very least, not postponing — PoCs.

32% of Australian security decision makers believe employee-provisioned devices for business use (BYOD) pose the greatest risk to their firm.

5. Build a reliable security foundation for personal devices. With employees moving to work-from-home arrangements, they are likely to be remoting with their own devices and operating outside protected infrastructure, leaving many business networks exposed. Thirty-two percent of security decision makers in Australia believe employee-provisioned devices (laptops, smartphones and tablets) for business use (BYOD) pose the greatest risk to their firm.[7] Personal devices are not part of an organisation's IT infrastructure — so they're likely not protected by company firewalls and security systems.

- **Don't allow unmanaged devices onto your network.** Turn on device health checks before letting employees access your network with personal devices. And use app security to reduce your reliance on device-level security.
- **Enhance your security posture with multifactor authentication.** As passwords become easier to undermine, security teams increasingly depend on multifactor authentication. Bolster password-based authentication with a second factor to reduce the risk of data breaches on remote devices.
- **Revisit security threats in the business continuity plan.** With the emergence of a significant volume of new and sophisticated threats, you must review and stress-test current business continuity plans to assess how well the business is equipped to address cyberattacks and security incidents.

Australian businesses have been forced into an unprecedented situation, and working from home is a new experience for many. To help your hybrid workforce thrive, you must look to scale solutions that not only maximise the productivity of your workers but also maintain security wherever they choose to work — at home, in the office, or on the move.

Today's investments in securing a hybrid workforce will not only safeguard your business in the near term but will help to build resilience against any disruptions in the future.

Appendix A: Supplemental Material

RELATED FORRESTER RESEARCH

"Security Will Fall Out Of Growth Mode Due To COVID-19," Forrester Research, Inc, April 21, 2020

"Nurse Your Limping VPN Infrastructure Through This Crisis, But Embrace Zero Trust Network Access For The Long Term," Forrester Research, Inc., May 11th, 2020

"Returning To Work: How To Avoid The 15 Most Critical Risks," Forrester Research, Inc., June 10, 2020

"Center Your COVID-19 Business Recovery Planning Around Employee Understanding," Forrester Research, Inc., June 17, 2020

"The Top Security Technology Trends To Watch, 2020," Forrester Research, Inc., June 30, 2020

Appendix B: Endnotes

[1] Sources: Forrester Analytics Business Technographics Global Workforce Benchmark Survey, 2019, and Forrester's Q2 2020 Australia PandemicEX Survey.

[2] Source: Forrester Business Technographics Global Security Survey, 2019.

[3] Source: Forrester's Business Technographics Priorities And Journey Survey COVID-19 Recontact, 2020

[4] Source: "Australia Tech Market Outlook, 2020 To 2021," Forrester Research, Inc. June 22, 2020.

[5] Source: Stu Sjouwerman, "Q1 2020 Coronavirus-Related Phishing Email Attacks Are Up 600%," KnowB4, April 9, 2020 (https://blog.knowbe4.com/q1-2020-coronavirus-related-phishing-email-attacks-are-up-600).

[6] Source: "Threat update: COVID-19 malicious cyber activity 27 May 2020," ACSC, May 27, 2020 (https://www.cyber.gov.au/acsc/view-all-content/advisories/threat-update-covid-19-malicious-cyber-activity-27-may-2020).

[7] Source: Forrester Business Technographics Global Security Survey, 2019.

Project Director:
Alisha Coates,
Senior Consultant

Contributing Research:
Forrester's Security & Risk research group