Back to Business

Recognising and reducing cyber security risks in the hybrid workforce

Cyber Security Industry Advisory Committee

November 2021

Introduction

On 6 August 2020, the Government released ***Australia's Cyber Security Strategy 2020*** and a $1.67 billion package to help protect Australians from cyber security threats.

The perspectives and expertise of industry and academia in the delivery of Australia's Cyber Security Strategy 2020 is critical to strengthening Australia's overall cyber resilience through a trusted and secure online world.

Recognising this, in October 2020, the Cyber Security Industry Advisory Committee was established by the Government to provide independent strategic advice on Australia's cyber security challenges and opportunities to help guide the Strategy as it enters the implementation phase.

The Committee comprises the members listed below:

- Andrew Penn, Industry Advisory Committee Chair, *CEO of Telstra*
- Cathie Reid, Industry Advisory Committee Deputy Chair, *Chair of AUCloud*
- Darren Kane, *Chief Security Officer of NBN Co*
- Chris Deeble AO CSC, *Chief Executive of Northrop Grumman Australia*
- Bevan Slattery, *Chairman of FibreSense*
- Corinne Best, *Trust and Risk Business Leader of PricewaterhouseCoopers Australia*
- Patrick Wright, *Group Executive Technology and Enterprise Operations NAB*
- Rachael Falk, *Chief Executive Officer Cyber Security CRC*
- Professor Stephen Smith, *Chair of Advisory Board, University of Western Australia Public Policy Institute*
- David Tudehope, *Chief Executive Officer, Macquarie Telecom Group*

The Committee welcomes the opportunity to contribute to robust and effective cyber security outcomes for Australia and is pleased to publish this thought leadership.

Future Workforce

COVID-19 has forever changed the way Australians work. In less than two years Australia's remote workforce has grown from 8% to 40%, representing the biggest shift to working norms in our nation's history[1].

Worker sentiment is clear. A large proportion of workers no longer want to be in the office five days a week, with survey[2] results indicating:

72% **of respondents who can work remotely say they prefer a mixture of in-person and remote working.**

19% **would be happy to not return to an office at all and work entirely remotely.**

9% **of those who can work remotely want to go back to a traditional commute and work environment full time.**

And organisations are listening, with the promise of increased workforce productivity, reduced overheads and improved employee wellbeing driving forces. Many are exploring normalised hybrid working as an ongoing organisation-wide policy. At the same time, organisational focus is shifting from business continuity as a benchmark of success to effective implementation of long-term operating model changes for a post-COVID world.

This drastic change has driven unprecedented digital transformation. According to McKinsey[3], the pandemic sped up organisations' adoption of digital technologies across key business areas by three to seven years in a matter of months. Hence, the 'new normal' is not just about how we work – the very systems that underpin business functions have irrevocably altered too. Therefore, a holistic and multi-pronged approach is needed as we enter this new era of work – and cyber security must be a prime consideration.

Hybrid work increases cyber security risk for several key reasons. First, the threat surface for compromise is expanded, with the workforce more dispersed, often widely. Second, working from home can leave individuals more vulnerable to threats, often due to poor cyber hygiene and digital fatigue. And third, many organisations have not had the time to put the correct controls, policies and processes in place to effectively manage the cyber security uplift required for the hybrid workforce.

Importantly, this significant shift will require a team effort. Government, business and individuals need to work together to harden the cyber security of the hybrid workforce. While awareness and education are key, public-private partnerships, incentivisation and new ways of thinking will also be core to affecting effective change.

This paper explores what the hybrid workforce is and the cyber security challenges it presents; how operational budgets and security convergence can support organisational cyber uplift; the role education, policies and people can play; and how SMEs can be supported in the hybrid transition. Finally, the paper includes practical key principles and actions for organisations, businesses and individuals to help support a cyber secure transition to hybrid work in Australia.

What is the challenge?

Ensuring Australia's post-COVID hybrid workforce is cyber secure.

More Australians than ever before desire a shift to hybrid work, a move many organisations support. While there are financial, work satisfaction and productivity gains this shift promises, there are also risks, a key one being increased cyber security vulnerability. Therefore, Australian organisations require practical advice and assistance in making the hybrid shift, with cyber security front of mind.

What is the solution?

Organisations of all sizes seeking to implement hybrid working practices now and into the future need to have the correct processes in place to bolster the cyber security of a dispersed workforce.

While there is no one-size-fits-all model for organisational cyber security, it's even more important for organisations to have the basics right, in addition to some specific actions that can be taken to bolster cyber security for hybrid workforces. This paper provides practical information for organisations transitioning to long-term hybrid working.

[1] https://www.pc.gov.au/research/completed/working-from-home
[2] https://www.pwc.com/hopes-fears
[3] https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-foreve

The Big Picture

What is Hybrid Working?

Hybrid working provides flexibility for employees as to where, when and how they work. It affords the ability for employees to work when they are most productive and in different locations, for example, in an office at times, at home at times, or at a remote location.

A new research paper by the Productivity Commission has found hybrid work could lift Australia's productivity because workers have better control over their time; enjoy better work–life balance; are able to work longer hours and complete more work due to the lack of a commute[1].

In a hybrid working world - working anywhere, anytime - the security risk is everyone's to own and manage. The best results are when people gain an interest in security, rather than just having rules set out.

Hybrid Working and cyber security risk

Rapid transitions to remote working during the pandemic have meant many businesses have not had sufficient time and resourcing to implement critical business-as-usual IT services for the remote workforce. As a result, many business – notably small and medium enterprises (SMEs) – have been forced to quickly adopt new remote networking solutions, sometimes to the detriment of their cyber security. For many, this has resulted in the increased use of 'shadow IT', which is not monitored by organisational IT departments, and is therefore omitted from risk assessments.

Hence, hybrid working brings with it a myriad of cyber security risks, from data protection, employee and customer privacy and, of course, the risk of cybercrime victimisation. Key concerns include:

Remote access: For workers to be productive, access to an organisation's documents and systems outside the office environment is critical. Remote access carries inherent data protection and security risks, particularly for organisations who have moved quickly to a remote access environment without appropriate technical and security measures. Put simply, an organisation's attack surface gets larger. When it comes to remote access, weak username and passphrase combinations are of particular concern, as they can allow criminals access to and control an organisation's systems remotely.

Treat Work from Home like Workplace Health & Safety

Workplace health and safety (WHS) assessments for staff working from home (WFH) are undertaken by organisations to ensure their home-based work environment meets WHS compliance requirements. A similar approach could be used to ensure security (physical and cyber) requirements are met. For example, an initial self-assessment for approval to work remotely could be undertaken and assessed, with any security gaps filled. In addition, ongoing cyber training for WFH staff should be mandated to help ensure employees are as best placed as possible to mitigate cyber security risks and remain alive to the threat.

Defences not as effective: Cybercrime threats like phishing and ransomware can more easily evade organisational defences in the hybrid work environment. Staff working outside the office may feel disconnected from their organisation's purpose and values and more willing to share information more widely. Or they may simply leave data accessible - in a cafe or shared living environment - in a way that could expose it to bad actors.

People: The weakest link in the strongest cyber security program is often people – people click on dodgy links, use work devices for personal business and, in the home environment, can be more complacent about cyber security. An increased volume of digital communication results in people finding it more difficult to filter out and recognise the potential risks. Blurring lines between work, home life and other responsibilities impacts concentration and potentially the ability to make optimal decisions.

Online platforms and collaboration tools: Working requires new online collaboration tools, raising issues related to monitoring the usage of these tools to ensure only sanctioned tools are used. Furthermore, if such tools are being used, organisations must ensure platforms are licensed and secure.

[1] https://www.pc.gov.au/research/completed/working-from-home

Budgeting effectively for cyber uplift in a hybrid environment

As the risk of cyber attacks increases for organisations, budgets are under more pressure. Despite this increased risk, more than half (55%)[1] of respondents to a recent global survey lack confidence that cyber spending is aligned to the most significant risks.

55% believe that their budget is not placed to provide the best return on investment when it comes to remediation, risk mitigation and/or response technique, and if a severe cyber attack took place, over half (55%) say they wouldn't have the budget to cover this expense.

With regard to preparedness for future risks, respondents are not confident that cyber budgets provide adequate controls over emerging technologies (58%). With confidence lagging in the process used to fund cybersecurity, they say it's time for an overhaul.

Even though organisations are typically spending more on cyber security, the relative proportion of budget allocation has remained consistently low.

It is important to note that increased spending does not necessarily translate into improved cyber security for organisations – real attention needs to be paid to what the cyber security budget is spent on and how it is adopted and utilised[3].

The cornerstone of risk management for a cyber secure hybrid workforce has people at its heart, and it is essential cyber security is ingrained in organisational culture. This is particularly pertinent to organisations where increased cyber security spending is driven primarily by regulatory compliance costs, which is an increasing trend[4].

Given the challenges associated with cyber security budgets, three models have been suggested[5], taking into account the different needs of different organisations:

Reactive vs proactive approach: dealing with incidents after the fact vs investing in preventative programs/controls.

Benchmarking approach: comparing what your organisation spends vs peers in the same industry with differing levels of security maturity.

Risk-based approach: breaking down risk by category via frameworks and allocating funds to uplift areas of greatest need.

[1], [2] https://www.pwc.com.au/important-problems/cyber-security-digital-trust/digital-tru
[3] Transforming cybersecurity_March2019.ashx (mckinsey.com)
[4] Cybersecurity budgeting and spending trends 2020: How does yours compare? - Infosec Reso
[5 Three Approaches to Setting Cyber Security Budgets - Cipher
[6]Cyber Insurance History | ProWriters (prowritersins.com)
[7] Underwritten or oversold? How cyber insurance can hinder (or help) cyber security in Austra

Security convergence

Increasingly, organisations recognise the importance of managing security risks holistically across physical, cyber and personal security domains. Given these domains are intrinsically connected, an integrated approach with unified accountability is required to manage them. This is because breaches can start in one domain and compromise another – they cascade.

In line with a trend towards a converged security model, awareness and education programs that have traditionally focused on cyber threats like phishing or weak passphrases have expanded to include practical and behavioural advice around physical and personnel security. As we move towards a future of hybrid work, the shaping of security behaviours must account for a different convergence of security risks, which may be heightened. This has been starkly observed by the US National Institute of Standards and Technology (NIST), which notes "a lack of physical security controls" in the hybrid working context could elevate security risks because "devices are used in a variety of locations outside of the organisation's control, such as employees' homes, coffee shops, and other businesses".

Working from home: ASIO guide for managers

As organisations move to hybrid work models, threat actors will continue to adapt to gain access to data and systems. Hence, businesses need to consider the practicalities of how employees access online systems safely and securely. Businesses should also monitor physical security and encourage staff to conduct a self-assessment of their home residence to determine whether existing security measures are adequate to protect business assets.

It is critical to ensure staff are provided with ongoing support, guidance and security awareness training to minimise risks from malicious cyber threats when working at home. Staff should also know what devices can be used, and what can be discussed, in the presence of others.

The ASIO Security Managers Guide Working from Home is available to eligible subscribers of the ASIO Outreach website at www.outreach.asio.gov.au.

[1] Cyber Security: A roadmap to enable growth opportunities for Australia – Executive Summary, CSIRO, 2018

To this end, there are practical considerations that need to be taken into account. For example:

- Do staff require document destruction capabilities in the home environment?
- Are phone conversations secure and confidential or can they be heard by others?
- Can work devices be used in unsecure public locations, like cafes?

Simplifying secure-by-design hybrid workplaces

Security-by-design means that from the moment a new system is conceived, security is 'baked in' to its foundations. In short, it ensures new products, services, platforms and processes are designed with cyber security as a key consideration[1]. The vital thing to note is that security-by-design principles have to be in place right from the get-go, not implemented as an afterthought which adds more complexity and cost.

In our digital society, where virtually everything, including home and work, is interconnected, business processes are incredibly (and increasingly) complex, including cyber security processes. Therefore, when it comes to security-by-design, especially for a hybrid workforce, solutions must promote user intuition.

Know what you need to protect. What are the 'crown jewels' of your organisation? Understand what is critical to business continuation and focus security investment decisions in these areas. Who are the high profile users who may be subject to targeted cyber attacks?

Prioritise using data. Use trusted data to assess your risks continually and stay up-to-date with the Australian Signals Directorate's Australian Cyber Security Centre (ACSC) threat alerts. Use this information to build in security controls up front.

You can't secure what you can't see. Simplify by uncovering the blind spots first: build a reliable, accurate data platform that informs intelligence, decision-making and new data-intensive business models. Actively manage information security and know what information is held, where it is and how sensitive it is.

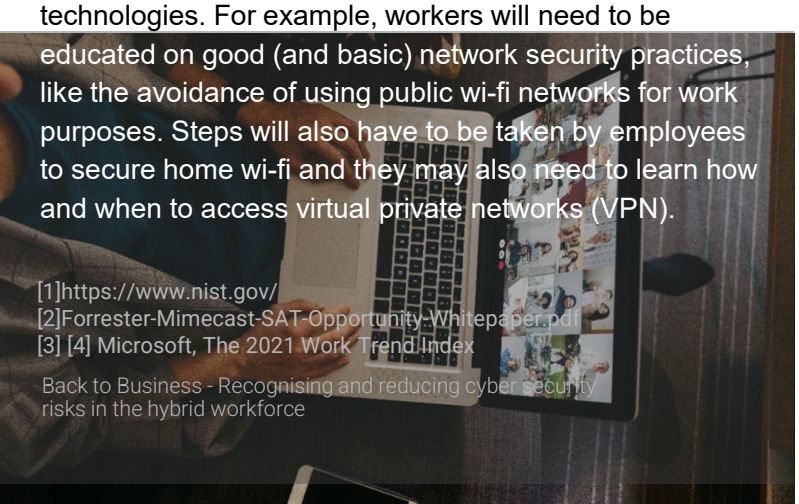
Shifting the dial on workplace cyber security education

The pervasiveness of technology in the workplace teamed with the security risks posed by hybrid working mean organisational security education programs need to be reviewed. Advocacy-based approaches are needed to influence attitudes, mindsets and behaviours in a more profound and lasting way.

Such change requires a multi-disciplinary approach. According to NIST: “Security advocacy necessitates a different set of competencies beyond the technical skills possessed by most security professionals. Non-technical competencies, such as interpersonal skills, communication skills, an appreciation of the audience, a customer-service orientation, and boundless creativity, may be essential for this role”[1]. In addition to changing skillsets, methods will also need to evolve, and increased use of marketing techniques and behavioural sciences will play a key role in achieving behavioural and cultural change[2]. The continued professionalisation and maturation of the security influence industry will also be critical, with the need to respond quickly to new challenges necessitating active sharing of best practices and new approaches to shaping behaviours.

Cyber criminals are taking advantage of hybrid working and the cognitive biases humans make in decision-making when working outside of the office. Traditional efforts to train employees against sophisticated attacks have faced an uphill battle. Awareness alone is not sufficient in creating a cyber safe culture. By understanding how people make decisions, organisations can tailor interventions. One example of this is providing 'just in time' training or 'nudges' that creating positive reinforcement.

The need to manage certain risks more closely will also require workers become more familiar with certain security technologies. For example, workers will need to be educated on good (and basic) network security practices, like the avoidance of using public wi-fi networks for work purposes. Steps will also have to be taken by employees to secure home wi-fi and they may also need to learn how and when to access virtual private networks (VPN).



[1]https://www.nist.gov/
[2]Forrester-Mimecast-SAT-Opportunity-Whitepaper.pdf
[3] [4] Microsoft, The 2021 Work Trend Index

Being outside the corporate IT environment also creates the potential for employees to adopt non-standard, and inherently riskier, practices. As well as ensuring workers can access secure and approved platforms to perform all their duties, security education should also highlight the importance of using approved services and the risks of using unsanctioned alternatives.

Culture is key

Culture is the expression of shared values and, when it comes to enshrining security, it is key. Shaping organisational culture, even beyond attitudes to security, is a more complex task in the hybrid workplace. As human resource and corporate communications teams evolve approaches to embedding organisational values in the hybrid workforce, security influence programs will need to reflect the changing nature of work to ensure security plays a central role in new strategies. Cultural leadership will play an important role in setting the appropriate tone across organisations.

More than ever, identifying ‘security champions’ will be critical to bolstering security education efforts, especially in an increasingly noisy digital environment. In addition to senior figures, champions should include a broad range of employees who continuously advocate the importance of organisational security.

Digital overload and screen fatigue

The number of emails delivered to commercial and education customers in February 2021, when compared to the same month last year, is up by **40.6 billion**[3].

The average Microsoft Teams user is sending **45%** more chats per week and **42%** more chats per person after hours[4].

Workers are facing large increases in digital content and meetings, increasing the potential for digital overload and fatigue when it comes to cybersecurity awareness.

What about Policies?

Consideration must be given to how security and other compliance behaviours will be managed when employees are out of sight. And this will likely involve an overhaul, or at least revision, of corporate policies. Traditionally, performance management regimes have been centred around 'seen' behaviours and measures of compliance. However, in the absence of specific tools to manage personnel offsite, ensuring compliance and security behaviours is difficult.

Bring Your Own Device

Of particular concern, especially for SMEs, is employees using personal devices to access corporate networks, known as 'bring your own device' (BYOD). This is a common practice – one that opens organisations up to a myriad of serious cyber risks.

It becomes more complicated when staff are using their personal device to store, process and communicate work information. Even more so when a person's hobby is being conducted on their personal device and leverages skills or knowledge related to their work role. This makes it very hard to define and enforce security policies. It can also cause legal complications should it ever get that far.

While there are no industry standards or principles for managing devices, there are guidelines and recommendations, which can be broken down into several broad categories:

Multi-factor authentication: Enforce strong multi-factor authentication (MFA) and authentication policies and processes to verify a user's identity.

Policy: Provide clear guidance and policies on how users can use personal and corporate devices in the scope of their work. BYOD policies should cover which devices can connect to corporate assets; requirements for installation of security, application management, and/or device management controls; procedures relating to device loss or theft; connections to secure networks; and acceptable use policies.

Compartmentalise and configure: Compartmentalise work and personal data through policies, processes and relevant technologies and implement a means of ensuring minimum standards of patching and security configuration appropriate to a user's level of access or role.

Encryption: Use encryption to ensure work-related communications and data are protected. In the case of BYOD and personal devices, use of a corporate VPNs should be limited to reduce risk and attack surface.

Device management: Establish a centralised repository for device management to enable appropriate and proportionate monitoring, onboarding/offboarding and configuration on any internet-accessible device. This is essential to understand risk and compliance levels.

Know your limits when it comes to monitoring hybrid workers

A global survey[1] of more than 32,000 workers found 44% of respondents would agree to let their employer use technology to monitor their performance at work, including sensors and wearable devices, with 31% against it.

Imposing policies on the hybrid workforce can have legal implications. Be aware of:

- surveillance legislation – specific surveillance legislation exists in States and Territories that regulates computer surveillance of employees.
- employee privacy – collection of personal information not relevant to an employment relationship can have Privacy Act implications.
- liability – demarcate between what is 'work' at home and what isn't to ensure coverage for liability.

[1] https://www.pwc.com/hopes-fears

Learning from one another

Case study

Security through innovation

A culture of innovation was key to ensuring a near-seamless transition to hybrid working for National Australia Bank (NAB) employees right across Australia during the COVID-19 pandemic.

And it's worked so well, the big bank will be sticking with the model.

"What we saw was a huge amount of innovation, new ways of thinking and approaching the way work was done in a very short period of time," said Steve Day, NAB's Chief Technology Officer.

"Fortuitously, a hybrid working model was something we'd been working towards for a while and planning for a good six months before the pandemic hit. The system we previously used for working remotely was unreliable and made working from home challenging. In addition, the processes of working from the office versus working for home were very different, making it difficult for our teams. Our vision was to make the working from home experience as similar as possible to working in the office.

We hit the ground running in February 2020 and then in March the pandemic hit. Virtually almost all of our entire workforce started working from home overnight."

In lockstep, a more human-centric approach was also taken to cyber security, with simple changes to multi-factor authentication using biometrics, helping streamline and simplify logging-on processes for employees.

While the transition was not without challenges – simple things like how to print and transfer documents securely suddenly became an issue – Mr Day said any emerging issues were ironed out quickly.

"The results have been startling. Productivity has increased by about 10 per cent and a culture of greater trust has been established."

"Everyone across the business has really changed and evolved in their thinking around hybrid working," Mr Day said.

"It's got us thinking about a whole list of other innovations we can make and how we can leverage this opportunity to expand our workforce and capacity, with cyber security a key priority."

Sandro Bucchianeri, NAB's Chief Security Officer, said the move to hybrid working had seen employees gain a much better understanding of cyber security than they previously had.

"Security awareness has definitely grown, and we continue to innovate our cyber security solutions to support our hybrid workforce now and into the future," Mr Bucchianeri said.

"While it's been tough, a unique and vibrant culture has flourished through NAB's shift to hybrid working and it's one we will continue to embrace."

The importance of getting the basics right

Patching

Patch management is essential for effective cyber security and ensures the security features of software on computers and devices are up to date. All software is prone to technical vulnerabilities and, when a vulnerability is exposed and shared, cybercriminals have a metaphorical front-door key.

A 2019 report by the Ponemon Institute on vulnerability responses found that, of the 48% of organisations that had experienced data breaches in the preceding year, 60% reported that the breaches resulted from failure to patch[1].

With the fast paced introduction of new technology, a theme emerges where old technology has not been decommissioned and a lack of focus on the security related to this technology makes it a prime target for cyber attackers.

Multi-factor authentication

MFA is a security measure that requires two or more proofs of identity to grant access, typically requiring a combination of something the user knows (pin, secret question), something the user has (card, token) or something the user is (fingerprint or other biometric).

The more tailored the authentication method is to the role of the individual, the more impactful the measure will be.

MFA offers significantly more powerful security and protection against cyber criminals because even if they manage to steal one proof of identity they still need to obtain and use the other proofs of identity to access an account.

[1] Ponemon Institute LLC, Costs and consequences of gaps in vulnerability response, ServiceNow

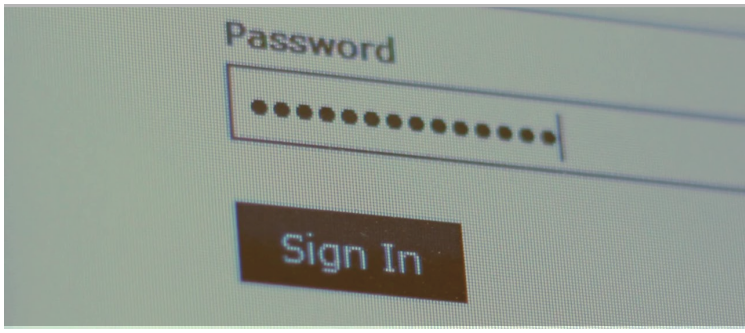
Regular staff training

Organisations should ensure ongoing cyber security awareness training is provided to all personnel in order to assist them in understanding their security responsibilities. The content of cyber security awareness training will depend on the objectives of the organisation, however, personnel with responsibilities beyond that of standard users will require tailored content.

Passphrase policy

Passphrases are the frontline of organisational system protection. Therefore, it is prudent for organisations, no matter how large or small, implement a passphrase policy.

A passphrase policy is a set of rules designed to enhance computer security by encouraging users to employ strong passphrases and use them properly. Comprising user responsibilities (not sharing passphrases etc) alongside minimum passphrase standards (e.g. 14+characters, 4 random words, unique).



Enabling “off the shelf” security settings

Business and personal use of IT is progressively shifting to managed cloud-based services which include effective built in security controls. Switching on the security features included with many ‘commercial off-the-shelf’ software packages will increase the levels of security and protection whilst reducing the related risks.

Learning from one another

Case study

Telecommunications Integration SME

After falling prey to a ransomware attack, the team at a major telecommunications integration SME knew they had to get their hybrid work environment cyber secure, and employee education has been a cornerstone of the strategy.

The company, with about 120 Australian-based employees, was forced to move its operations online as the COVID-19 pandemic hit.

But a phishing email that led to malware being deployed on the company's systems brought operations to a grinding halt, resulting in some branches being unable to trade for three months.

The company's Finance Manager said, while the effects of the attack had been remediated, the breach had been a huge wake up call.

"We thought we were protected and didn't realise how vulnerable we were," they said.

"The attackers damaged files on the server and we tried to recover what we could, but it took a lot of time and it was expensive."

Prior to the attack there were limited restrictions on how staff used work computers – they could download software, shop online and use them for personal business. The company also discovered back-ups were not being completed, making recovery more difficult.

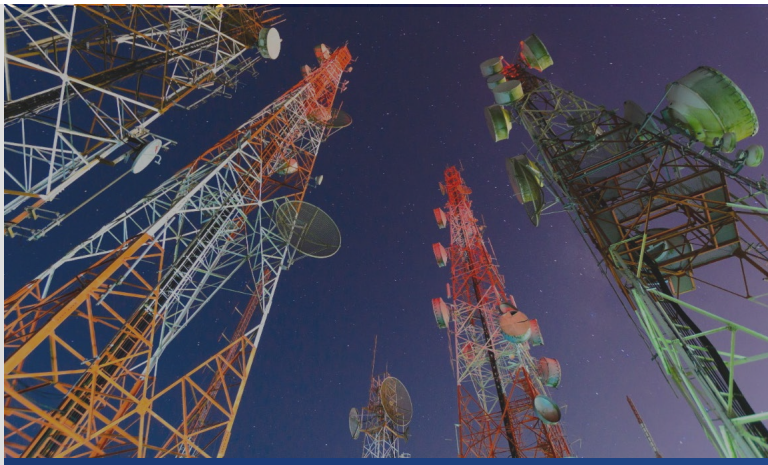
"Multi-factor authentication is now used for everything and all staff have to change passwords regularly," the Finance Manager said. "And now everything is backed up."

"While the experience was challenging, our business is now much more cyber secure. It put the microscope on our cyber security practices and showed us we needed to make improvements.

It has changed the whole way we do business and we now know how paramount cyber security has to be."

To upskill staff about cyber security best practice, the company has started running regular training sessions about phishing emails and other common threat vectors, like business email compromise. This has helped upskill and educate teams that previously did little work online.

"For us it's important employees understand cyber security isn't something done to you," the Finance Manager said. "Everyone has a part to play."



Cyber Security Cooperative Research Centre South Australia SME Pilot Project

The Cyber Security Cooperative Research Centre (CSCRC) led Australia's first 'hands on' pilot project focused on uplifting cyber security for SMEs.

The project focussed on cyber security implementation, with the purpose of understanding the best ways for SMEs to achieve realistic and sustainable cyber uplift.

The pilot involved six Adelaide-based SMEs across a broad range of critical sectors, from medical services to satellite technologies, measuring their baseline cyber security and providing practical, cost-effective uplift solutions over six months.

The pilot identified common cyber security challenges faced by SMEs, including:

- Cyber security is considered as an add-on and is not built-in to business operations
- Lack of cyber security risk assessment in supply chain management
- Physical assets are better secured than digital assets
- Incident preparedness is very poorly developed
- Bring-your-own-device (BYOD) practices pose a significant cyber security risk

The key reasons driving the desire for cyber uplift among the SMEs were improvement of service delivery for clients, upscaling of business reach to larger, potentially international clients, and to be eligible to apply for Federal Government contracts[1].

[1] Report: CSCRC SA SME Cyber Uplift Pilot Project, CSCRC, 2021

Geographically Diverse Workforce

Benefits and challenges

Australia is anticipated to have 1.1 million less people in 2031 than if COVID hadn't happened. Organisations will be in a war for talent and will need to look outside their traditional geographical/market based talent pools due to constrained skilled migration and heightened competition for talent - particularly for digital and technology skills.

This challenge is expected to increase as the demand for these skills grow. The short term gap (not including new to career students) will only be able to be met by reskilling from other professions, hiring from a broader market (domestically or internationally), outsourcing, or other partnership arrangements (e.g. shared services centres).

There are of course challenges to a geographically diverse workforce. In a remote environment, traditional modes of management won't suffice. Uplifting and adapting managers' performance measurement approaches and communication skills will be fundamental to enabling performance of dispersed teams. It's critical that organisations take steps early to ensure that certain employees do not end up 'out of sight, out of mind' while others gain prominence and favour out of proximity to those with influence.

Organisations need to have an ongoing system for reviewing control measures around risks associated with remote work to ensure they are effective and working as planned.

They should encourage their staff to determine whether existing security measures are adequate to protect business assets. This includes securing devices when not in use and considering how employees' personal circumstances may influence the safety of businesses' data, such as not having a private space to work and the overhearing of business material by other individuals within the household. To address this, businesses should provide staff with advice on what devices can be used, and what can be discussed, within the presence of other household individuals.

Organisations need to be aware of the potential risks relating to data storage and international legal requirements (e.g. GDPR) if using offshore employees.

Removal of geographic employment boundaries

Australian industry has been facing a skills shortage across many areas for a considerable period of time. The Government has sought to address this through skilling and education programs and the provision of focussed criteria for skilled migration.

Businesses in the information economy who do not require staff to be physically present in a location have proven their ability to continue to deliver using remote working options.

The ability to undertake this work through remote working options could remove some skills shortage problems by enabling businesses to access skills they would not normally be able to attract to a given location.

Further, hybrid working models combined with flexible working may enable access to skilled resources who may otherwise not be available to the workforce through inability to commit to particular hours.

The Australian Cyber Security Centre (ACSC) report on vulnerabilities and issues with patch management

In July 2021 the US Cybersecurity and Infrastructure Security Agency (CISA), the (ACSC), United Kingdom's National Cyber Security Centre (NCSC) and Federal Bureau of Investigation (FBI) released a joint cyber security advisory today, highlighting the top Common Vulnerabilities and Exposures (CVEs) routinely exploited by cyber actors in 2020 and those vulnerabilities being widely exploited thus far in 2021.

One of the key findings is that four of the most targeted vulnerabilities in 2020 involved remote work, VPNs, or cloud-based technologies. Many VPN gateway devices remained unpatched during 2020, with the growth of remote work options due to the COVID-19 pandemic challenging the ability of organisations to conduct rigorous patch management.

Malicious cyber actors monitor public reporting of vulnerabilities and scanning tools to identify unpatched software and hardware appliances for exploitations. Improving cyber hygiene and rapid patching can help protect organisations from being compromised by publicly reported security vulnerabilities.

ACSC Resources

The ACSC's Annual Cyber Threat Report for 2020-2021 found the significant increase in the number of Australians working remotely due to COVID-19 had seen malicious cyber actors take advantage of increased vulnerabilities to steal money and sensitive data and disrupt the services on which Australians rely on.

To enhance the ability of Australians to protect themselves from common cyber security threats the ACSC has published a number of guides for SMEs and business more generally:

- Small Business Cyber Security Guide
- Cyber Security Prevention, Protection and Emergency Response guide series
- Personal Cyber Security guide series
- Step-by-step guides on:
  - Turning on two-factor authentication
  - Backing up and restoring your files
  - Turning on automatic updates
  - How to check your email account security
  - Creating stronger passphrases for remote access
- COVID-19 pandemic guides, focussed on:
  - Cyber security considerations for working from home
  - Advice on multi-factor authentication

ACSC Partner Program

The ACSC Partnership Program enables Australian organisations and individuals to engage with the ACSC and fellow partners, drawing on collective understanding, experience, skills and capability to lift cyber resilience across the Australian economy.

Australian organisations including Government and those in the private sector, as well individuals are welcome to sign up.

To sign up to be an ACSC Partner go to cyber.gov.au.

ACSC's Essential Eight

The mitigation strategies that make up the Essential Eight are:

- **Application control:** Preventing non-approved applications from running on computers.
- **Patch applications:** Fixing security vulnerabilities in applications on computers.
- **Configure Microsoft Office macro settings:** Preventing Microsoft Office from being used to run malicious code using web browsers on computers.
- **User application hardening**: Restricting the use of popular ways to run malicious code using web browsers on computers.
- **Restrict administrative privileges:** Protecting special user accounts that adversaries can use to gain full access to ICT systems.
- **Patch operating systems:** Fixing security vulnerabilities in operating systems on computers.
- **Multi-factor authentication**: Implementing more robust ways to authenticate legitimate users to computers.
- **Regular backups:** Ensuring systems and important information can be accessed following a cyber security incident.

While no set of mitigation strategies is guaranteed to protect against all cyber threats, the ACSC recommends all businesses implement the Essential Eight as a baseline, choosing a maturity level that suits your risk environment. For more information on the Essential Eight and how you can implement them visit cyber.gov.au.

Bundling: From big things little things grow

When it comes to SME cyber security uplift, there is a key role for big business to play in supporting small business. This aligns with the objectives of Australia's Cyber Security Strategy 2020, with regard to SME cyber security uplift, which recognises "integrating cyber security products into other service offerings will help protect SMEs at scale and recognises that many businesses cannot employ dedicated cyber security staff"[1].

In the US, where there has been a concerted effort towards public-private partnerships to uplift cyber security, big business has taken up the challenge. For example, Amazon recently announced it would freely provide a multi-factor authentication device to Amazon Web Services account holders and make its internal security awareness training resources publicly available at no charge[2].

[1] Australia's Cyber Security Strategy 2020 (homeaffairs.gov.au)
[2] FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity | The White House

Key Principles / Actions

Everyone across our ecosystem is accountable for their cyber safety and in the context of our new hybrid working landscape, all businesses and individuals should consider:

Know what you're trying to protect across your hybrid environment

- What are the 'crown jewels' of your organisation? Understand what is critical to business continuation and focus security investment decisions in these areas.

Revise your corporate policies so they are fit for purpose in a hybrid world

- Make sure polices are clear and explicitly communicate how and where work devices can be used.

Get the basics of cyber hygiene right

- Focus on cyber hygiene basics – people, patching/updates, MFA, passphrases, back ups.
- Know what resources are available for you and where to find them - cyber.gov.au is a great place to start.
- Educate staff about cyber security, with a specific focus on the risks that increase through working hybrid. Make staff education human-centric, real-time and interactive.
- If staff have connectivity issues make sure they do not use unmandated devices or networks to connect (e.g. public wi-fi, personal dongles).

Leverage innovation and build in security up front

- Integrate cyber security uplift into hybrid workforce business innovations.
- Make the shift easier for staff my making intuitive cyber security a part of basic processes, for example, introduce biometric MFA so staff don't have to remember multiple passphrases.

Small and Medium Enterprises

- Do your research - wherever possible choose products and services that easily enable continual cyber security update.
- Optimise the benefits and incentives that may be available to you by working with your accountant or financial team e.g. if tax incentives like instant asset write-offs can be used to uplift cyber security.
- See if there are cyber uplift subsidies or grants your business may be eligible for.

Large Businesses and Corporations

- Identify staff members more likely to be targeted by cyber criminals (e.g. CEOs, executives, accounts payable) and conduct at-home cyber security assessments.
- Consider the introduction of a 'cyber allowance' for hybrid workers to support the strengthening of home networks.
- Identify and shut down legacy technology.

Individuals

- Be part of the team – attend and actively engage in cyber security training.
- Know what your employer's cyber security policies for hybrid work are – and stick to them.
- Be aware of your online activity and make sure you separate work from recreation.
- If you are a member of staff more likely to be targeted by cyber criminals always be alert - if an email or other online interaction doesn't seem quite right, refer it to your security team.