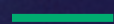




business nbn[®]

Enterprise cyber security

From business barrier
to enabler



There is no silver bullet for enterprise security.
It takes leadership, culture and people.

Contents

Contents

Click on the
image to jump
content

4.
Background



8.
A challenge for business leaders



12.
People are the missing link, not the weakest link



14.
Building a security culture



16.
Assessing security maturity



19.
Security is a shared journey



Our experts

Who are these people and why we are talking about them

Click to our experts key insights



Darren Kane
Chief Security Officer
nbn



Rachael Falk
Chief Executive Officer
Cyber Security CRC



Phil Rodrigues
Head of Security,
APJ Commercial, Amazon
Web Services



Nigel Phair
Director, Enterprise,
University of New South
Wales Institute for
Cybersecurity

[Contents](#)

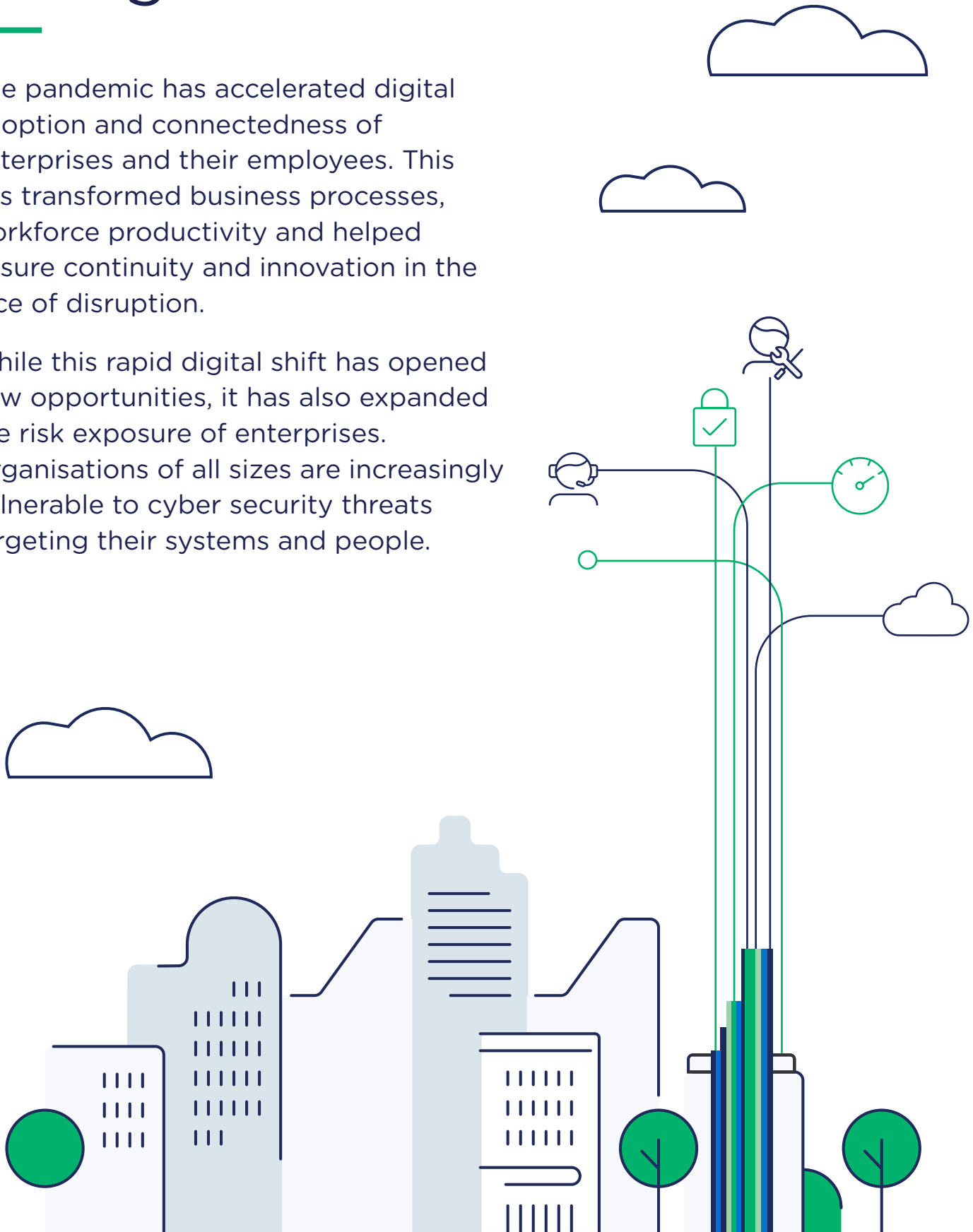
[Next section](#)

[Key takeaways](#)

Background

The pandemic has accelerated digital adoption and connectedness of enterprises and their employees. This has transformed business processes, workforce productivity and helped ensure continuity and innovation in the face of disruption.

While this rapid digital shift has opened new opportunities, it has also expanded the risk exposure of enterprises. Organisations of all sizes are increasingly vulnerable to cyber security threats targeting their systems and people.



[Contents](#)

[Next section](#)

[Key takeaways](#)

The World Economic Forum¹ has classified cyber security failure as a “top global risk” facing businesses. The growth of cybercrime is also being felt locally. According to Nigel Phair, Director of Enterprise at the UNSW Institute for Cyber Security, cybercrime costs the Australian economy an estimated \$42 billion a year².

Key cyber security trends



25%



Of cyber attacks occurred on healthcare, food distribution and energy sectors



15%



Annual increase in ransomware cybercrime reports in FY21



A rise in COVID-themed spear phishing emails



Supply chain software is increasingly targeted

Source: ACSC Annual Cyber Threat Report 1 July 2020 to 30 June 2021³

Over the 2020–21 financial year, the Australian Cyber Security Centre (ACSC)³ reported a 13 per cent increase in cybercrime reports compared to the previous financial year, with a cyber attack now being reported once every 8 minutes. Cyber criminals increasingly targeted organisations in all sectors – government agencies, large enterprises, critical infrastructure providers, and small and medium enterprises, the ACSC reported. Even hospitals, schools and charitable organisations have been attacked.

The rapid digitalisation of almost every aspect of business in the last two years has increased the vulnerability of enterprises to cyber attacks. In February 2022, the ACSC recommended Australian organisations urgently adopt an enhanced cybersecurity posture⁴.

Avoiding 'decision freeze'

According to Darren Kane, Chief Security Officer, **nbn**, while leaders need to be well-informed about security challenges, constant reports of new threats can become overwhelming, creating a risk of 'decision freeze' that prevents them taking action.

In contrast, with a sound assessment of risk and a strong enterprise security culture, directors, executives and other business leaders can stop security being an obstacle to business growth and use it as an enabler. Kane describes good enterprise security as being like brakes on a car – they give the driver the confidence to move quickly, knowing the car can be safely brought to a stop when required.

“If we haven’t changed yet, we’ll definitely change in the future to seeing security as an enabler of high performance, rather than a group of people who are living in the basement, constantly saying no,” Kane said.

How can businesses build security culture?

In a [business nbn® webinar titled ‘Enterprise Security - what is your weakest link?’](#), an expert panel examined the Australian cyber risk landscape and the security challenges faced by enterprises. This white paper presents their insights and recommendations to help business leaders strengthen their security posture while continuing to focus on innovation and growth.



Click to watch the
full discussion

[Contents](#)

[Next section](#)

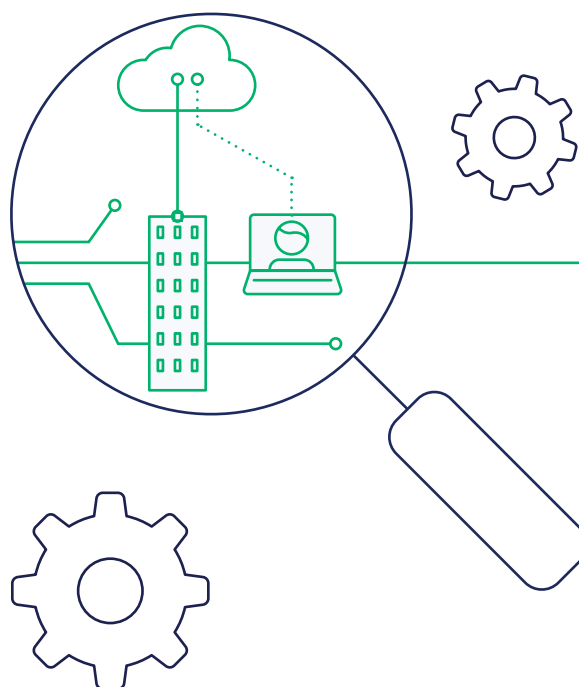
[Key takeaways](#)

A challenge for business leaders

Security risk is one of the more serious business operational risks that enterprises now face, ranking alongside finance risk, health and safety risk, and customer risks. Building a security culture must start at the top.

At a board level, many Australian business leaders appear to be aware of the scope of the challenge. According to the [Director Sentiment Index report published by the Australian Institute of Company Directors \(AICD\) published in December 2021](#), “the big issue keeping executives from getting a good night’s rest is cyber security”.

The research found cybercrime and data security were “front of mind in the small hours of the morning” for the 41 per cent of company directors that were surveyed. But at the same time, only just more than half [53 per cent] of directors surveyed said their board had sufficient oversight of cyber security threats facing their organisation⁵.



Only **53%**



of directors surveyed said their board had sufficient oversight of cyber security threats

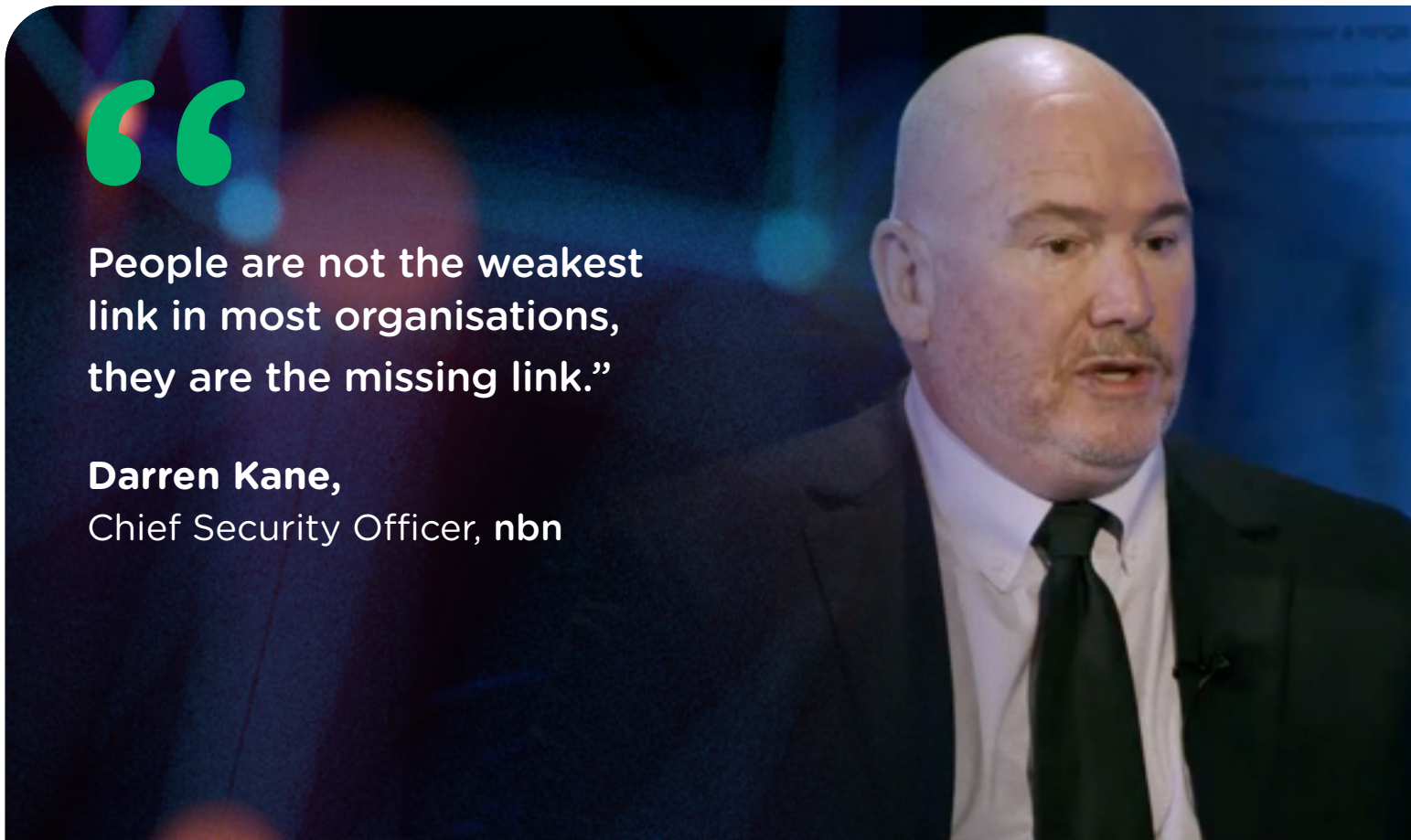
In some enterprises, there appears to be a gap between business leaders' awareness of the threats and the way their organisations are structured to deal with them.

A change in mindset about who 'owns' security in the business, and what are the roles appropriate to manage it, may be required. Traditional frameworks may need to change and enterprise security can no longer be left to the technology side of the business to run.



People are not the weakest link in most organisations, they are the missing link.”

Darren Kane,
Chief Security Officer, nbn



Executive roles may need to change. While a chief security officer can oversee enterprise security, another senior executive may need to take the lead in working with the C-suite and board members on strengthening the organisation's security posture.

“Information needs to be delivered up through the business to decision makers in a way that makes it understandable and actionable,” Kane said. “To deliver the right information to the board, you need a senior business executive that uses the language of the executive team so they can appreciate and understand it.”

Who owns enterprise security?





With senior leaders properly informed, organisations can set an enterprise security posture within the overall risk appetite of the organisation, which will also cover areas including financial and investment risk, occupational health and safety risks and regulatory requirements. This sets the framework within which an enterprise security culture can develop.

But an understanding of risk and security must extend well beyond an organisation's boardroom and executive offices.

People are the missing link

People are the missing link

Not everyone is a security expert, so it is important to bring people along on an organisation's security journey. By building awareness, employees can be empowered to help the organisation and act as the first line of defence.

"One third of all the data breaches are from an internal person. We don't know whether it's a malicious or a silly person, but we need to start being really careful with how we portray that person, and how we can help them, and how they can help us," Phair said.

"It's true that if folks can make it, folks can break it. But people are not the weakest link in most organisations, they are the missing link. We're not spending enough time educating and getting them to buy into the problem," Kane said.

In short, enterprises need to build a strong organisational culture around security.



[Contents](#)

[Next section](#)

[Key takeaways](#)

In an ISACA (Information Systems Audit and Control Association) article titled ‘Why build a cybersecurity culture?’⁵, senior enterprise architect Paul Frenken explained how building a culture of cyber security is one of the best ways an organisation can reduce cyber risk:

“Enterprises spend millions of dollars on hardware and software but neglect the simple act of properly training their employees on security practices. Teaching employees to recognise threats, curb poor behaviour and follow basic security habits can be the best return on investment. In many cases, management does not believe that just training their employees can reduce their exposure to cyber losses.”

While technology can be implemented to combat cyber threats, it cannot be the single solution to an organisation’s security challenges.

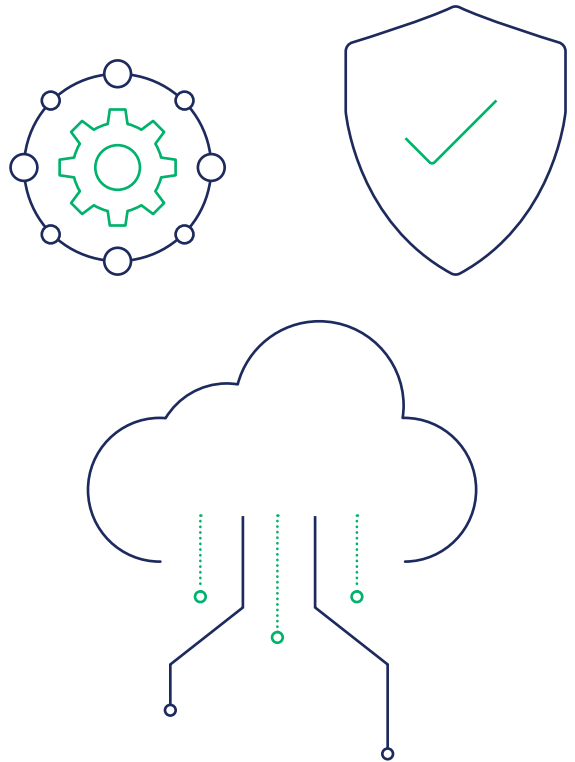
“Technology, machine-based learning, new capabilities, they will all be incredibly valuable to helping keep the risk within the appetite. But ultimately, it will be the people that ensure that that’s done,” Kane said.



Building a security culture

To build a culture of security across an entire organisation, business leaders must make security a highly visible priority for the business.

“When we look at organisations, we see some are quite secure and others not so much. So, what’s the difference between them? If it’s not technology, it’s culture,” said Phil Rodrigues, Head of Security, Asia Pacific and Japan Commercial, at Amazon Web Services.





If you're leading an organisation, get up there and help to transmit that culture - and start by talking about security."

Phil Rodrigues,
Head of Security, APJ
Commercial, Amazon
Web Services



Raising awareness on the technical aspects of cyber security in simple and accessible language helps bring everyone in the organisation along on the shared security journey. This must include regular internal communications with updates on the latest threats and clear messaging on the steps to ensure security hygiene.

Security leaders need to create stronger partnerships with other leaders and show how they can positively impact the business. Being proactive, rather than reactive, is an essential component of this strategy.



Talk about
security
in clear
accessible
language

[Contents](#)

[Next section](#)

[Key takeaways](#)

Assessing security maturity

In addition to building security culture, enterprises need to identify how mature their security measures and processes are, and where they can be improved.

Using a protocol such as the ACSC's 'Essential Eight', which rates enterprise security across eight key measures, businesses can determine their own KPIs, starting with their most vital assets. Ensuring that this process is understood at the board level will facilitate buy-in from the leadership team.

Consulting internal and external stakeholders to determine security controls and measurements can help leaders understand the organisation's risk appetite to help frame the response.





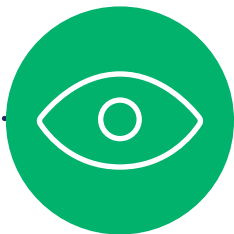
Think of everything on a maturity scale - look at advice from the government in the Essential Eight, there are three steps in maturity. Work your way through the steps. There is a lot of guidance out there.”

Nigel Phair,
Director, Enterprise,
University of New South Wales
Institute for Cybersecurity



Businesses need to spend enough to get the right controls in place that are effective for their operations and knowing the business risk helps determine the spend.

It is also important to have visibility on the security implemented by suppliers and vendors in their platforms and operations.

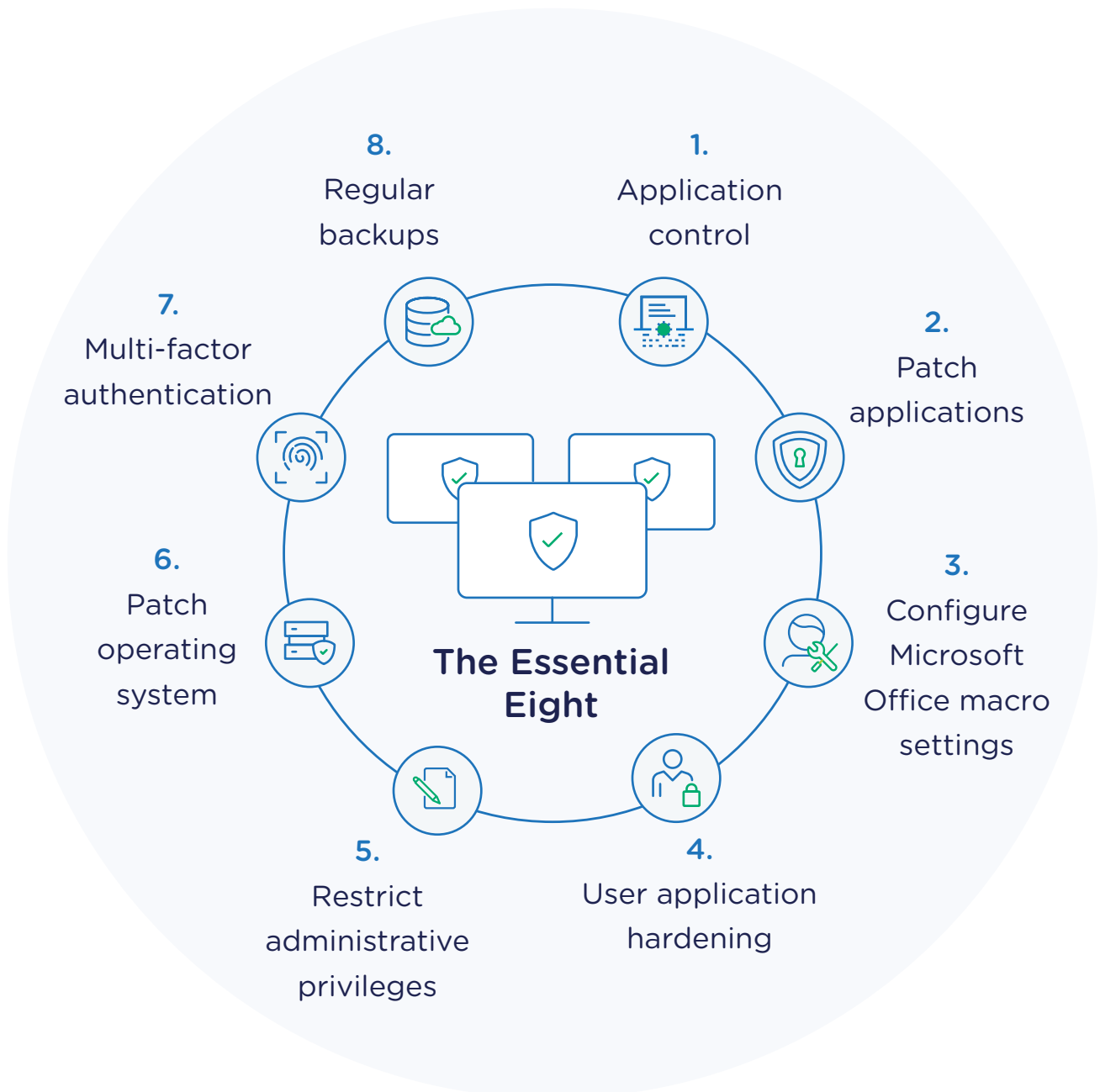


[Contents](#)

[Next section](#)

[Key takeaways](#)

The Australian Cyber Security Centre and the Cyber Security Cooperative Research Centre have valuable updates and resources to help businesses build awareness and preparedness to face cyber security challenges.



Source: ACSC

Security is a shared journey

Security is a shared journey

Enterprise security is a shared responsibility across the organisation. A CISO and security team can set the strategy and direction for enterprise security, but everybody has a role to play in ensuring a culture of security - from executives, developers and administrators down to end users.



“

If you're involved in or responsible for a company that's got systems connected to the internet, you are a security officer for those purposes.”

Rachael Falk,
CEO, Cyber Security
Cooperative Research Centre

[Contents](#)

[Next section](#)

[Key takeaways](#)

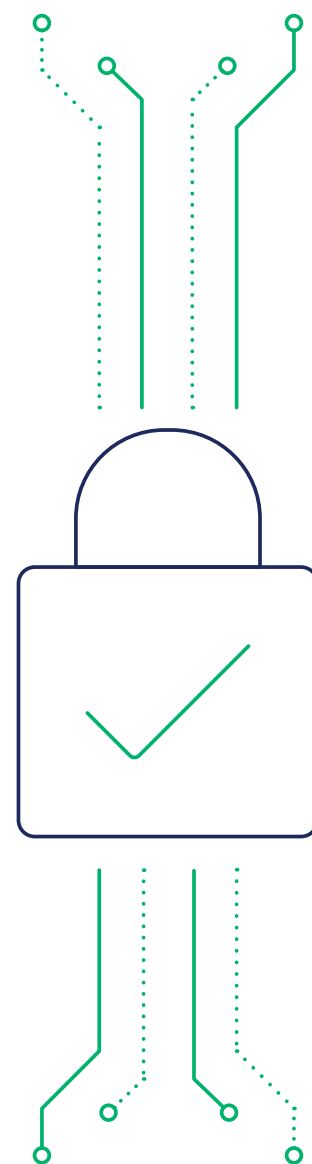
Just as technology is no panacea, it is not possible for an organisation to ‘buy its way’ out of security challenges. Cyber security budgets are only effective when they also help build a strong organisation-wide security awareness culture.

Building and maintaining a security culture has been described as an ongoing journey - “a process that is fuelled by a relentless - and consistent - drumbeat to help employees understand exactly how their daily behaviours have the potential to protect or threaten corporate data”.⁷

Businesses require leadership to maintain that drumbeat. Senior executives and board members must be given the information they need to make decisions, but also to help them start talking about security to prioritise it as a key issue for the business.

By communicating to employees that security risk is real and ensuring that they are fully aware of their role in an organisation’s security, leaders can ensure cyber security is treated as a priority by all.

With the right security culture in place, businesses can then view security as an enabler, supporting business growth.



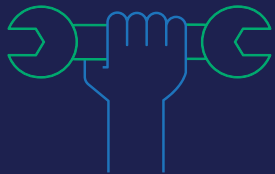
Key takeaways:



View **security** is a **business enabler**, not a barrier



Leaders must inspire a culture of security




Empower people with the right knowledge and security tools



Work to improve your **security maturity level**



From the boardroom to the mailroom, **security is everyone's responsibility**

[Last page](#)

Enterprise cyber security: From business barrier to enabler

[Click to watch the full discussion](#)

References:

1. <https://www.weforum.org/agenda/2021/01/building-resilience-in-the-face-of-dynamic-disruption/>
2. <https://www.unsw.adfa.edu.au/newsroom/news/cybercrime-estimated-42-billion-cost-australian-economy>
3. <https://www.cyber.gov.au/sites/default/files/2021-09/ACSC%20Annual%20Cyber%20Threat%20Report%20-%202020-2021.pdf>
4. <https://www.cyber.gov.au/acsc/view-all-content/alerts/australian-organisations-encouraged-urgently-adopt-enhanced-cyber-security-posture>
5. <https://aicd.companydirectors.com.au/advocacy/research/director-sentiment-buoyant-despite-post-pandemic-challenges>
6. <https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/why-build-a-cybersecurity-culture>
7. <https://www.forbes.com/sites/forbesbusinesscouncil/2021/05/27/the-importance-of-a-strong-security-culture-and-how-to-build-one/>
8. <https://cybersecuritycrc.org.au/>