6 tips for maximising success in your cybersecurity program

February 2023

pwc

As cyberattacks against Australian businesses continue to rise in scale and severity, many organisations are delivering complex programs of work to uplift their defensive capabilities. Considering a large number of these cyber initiatives fail, it raises serious questions about what must be done to increase their chances of success.

Cyber threats can be difficult for stakeholders to understand. While organisations should have well-established cyber risk management plans, many still don't have the foundational controls and processes to keep their organisations safe.

PwC's 2022 global risk survey identified cybersecurity as the biggest risk to revenue growth, with Australian respondents rating it higher than COVID-19 impacts, economic volatility or climate change.

While organisations are seeking risk buy down and efficiency gains, it can be incredibly difficult to quantify the benefits of cyber investment. This makes it difficult to develop a business case and clearly articulate the benefits of cyber uplift. It's also important to remember there is no one-size-fits-all approach to cyber programs, as every organisation has unique requirements and a different risk appetite, which impacts what should be delivered and how.

PwC supports the delivery of cybersecurity programs designed to meet compliance and risk objectives for many of Australia's leading organisations. That's why we've developed six key tips to help businesses better consider the way they deliver their cyber programs.

PwC’s six tips for boosting your cybersecurity program:

Lean into compliance, but plan for risk conversations – A compliance-led program is a useful starting point, although it can be difficult to sustain. Organisations must plan to pivot to a risk-based approach, which helps organisation remain agile and adapt to new challenges as they arise.

Seek to understand and manage your change restraints – There is a perception money can be thrown at cyber to quickly meet compliance goals, but this couldn’t be further from the truth. Organisations must make measured investments at a steady pace to ensure sustainable operations and prevent change fatigue.

Expect issues and prepare to pivot – It’s inevitable issues will be identified when rolling out cyber programs, causing delays and hampering success. It’s critical to bake agility into cyber programs so businesses can deal with surprises.

Develop realistic strategies to build cyber resources – Cyber skills are in high demand and short supply. Organisations must build succession plans for when people leave and level up their reskilling activities to ensure sustainable resourcing.

Foster a culture of agility and accountability – Cyber programs must be commensurate with the size and complexity of the business, able to operate with appropriate resourcing once developed. Build accountability into the program and give every initiative an ‘owner’ to keep things moving.

Get senior stakeholders involved – C-suite and board executives are increasingly concerned with cyber risks, so it’s imperative they’re actively engaged in the process, advocating for meaningful change.

Tip 1: Lean into compliance, but plan for risk conversations

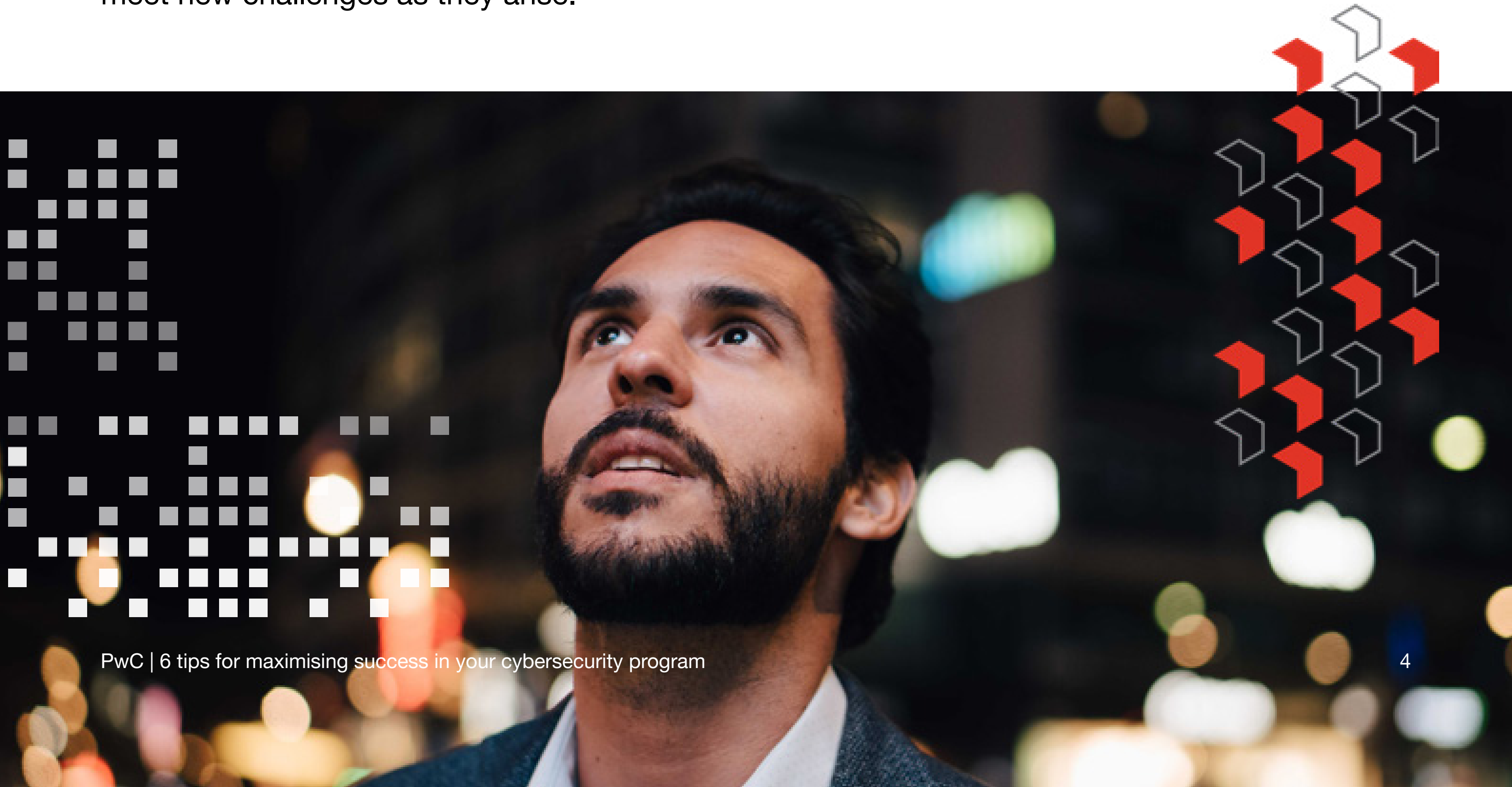
Organisations across all sectors are being pushed to implement and uplift their cybersecurity controls, ranging from critical infrastructure requirements, to Australian Energy Sector Cyber Security Framework requirements and APRA's CPS 234 and proposed CPS 230. As a result, many organisations are currently leading their cyber risk programs with compliance-oriented objectives.

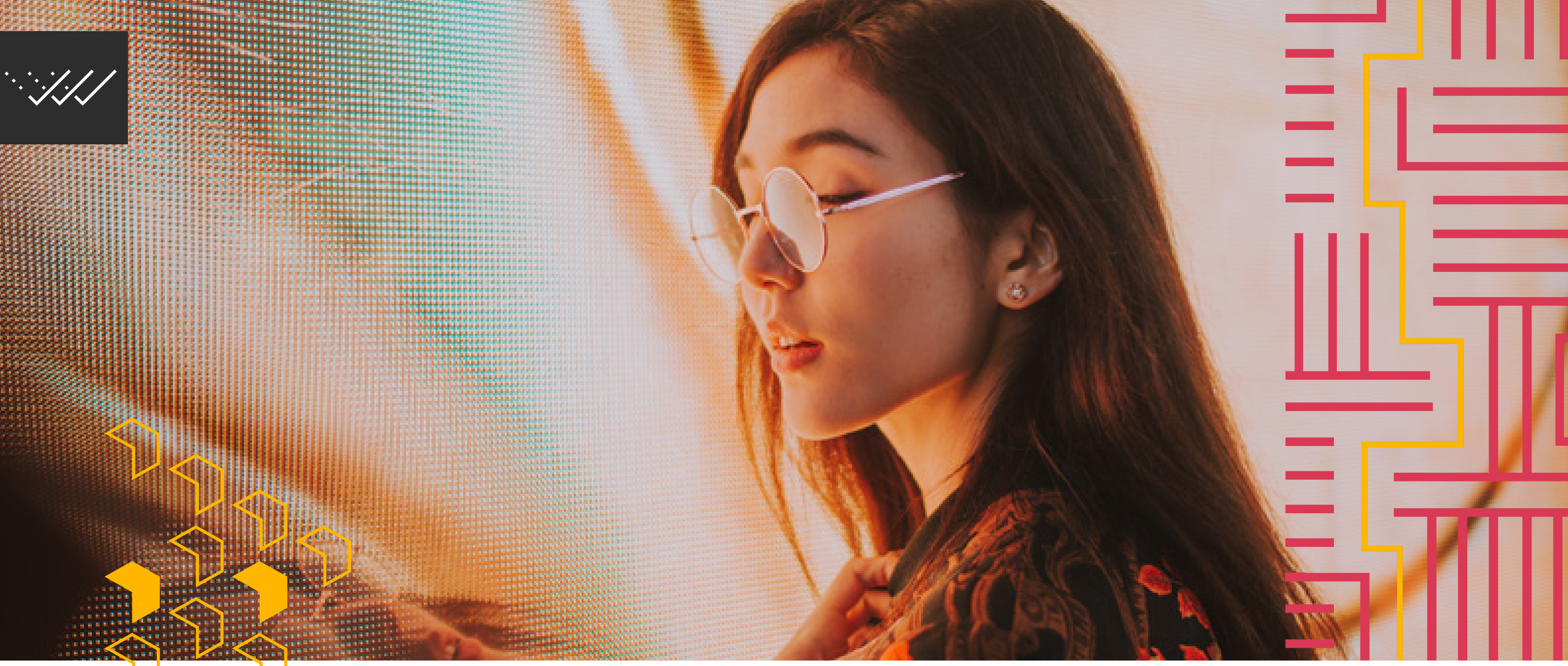
While this is a useful starting point and helps build momentum, it can be difficult to sustain a security program with compliance-led objectives. Once met, there can be a perception the work is done. This makes it harder to link activities to a corporate objective and maintain progress, as people will start to lose interest over time. Taking a risk-based approach helps organisations remain agile to change and meet new challenges as they arise.

It's critical security program teams are equipped to have meaningful and educated conversations around cyber risk with their customers and stakeholders. It can be difficult to talk about the state of cyber risk, but giving stakeholders visibility over these risks and reinforcing the need to implement controls that address them is critical in a sustainable security program.

"Create an environment where people don't feel threatened by asking a stupid question. Cyber is a complex subject, so it's really important to create an environment that is open, where anyone can ask any question. You're going to get the best type of conversation and interaction and ultimately, the best risk management for your organisation."

Jason Smart, Director
Threat Intelligence APAC at PwC





Tip 2: Seek to understand and manage your change restraints

Once an organisation understands its cyber risks, the next logical question is: “How much will it cost to reduce these risks to an acceptable level?”. There can be a perception in enterprise organisations that the more money thrown at cybersecurity, the faster objectives are met - but this couldn’t be further from the truth.

Improving cybersecurity involves a complex combination of changes that impact people, processes and technology. As much as it requires funding, your program must be able to influence its stakeholders and create change that can be positively consumed by the people impacted.

No amount of investment can make up for spending the time with impacted users to help them understand what’s changing and why. This is especially true of changes which interrupt key business processes. For example, turning on data loss prevention tools or disabling Microsoft Office macros are key controls that can seriously impact day-to-day duties within your organisation. Inspection tools and business engagement can help you understand the impact and plan for these changes.

Investments in cyber risk mitigation programs should consist of both capital and operational expenditures. Many companies are willing to invest the capital expenditure required to implement new security tools but often overlook the operational cost of managing the enhancements from both a technology and people perspective. The total cost of ownership of the enhancement should be considered alongside the risk reduction benefit proposed by the project.

Organisations should set realistic budgets and timelines to understand and communicate with stakeholders. Perform the analysis to understand which improvements can be implemented without requiring a change to user behaviour to reduce change fatigue.

It’s also important to acknowledge what is achievable in a timeframe based on the change bandwidth of your organisation. Making measured investments at a steady pace is guaranteed to result in more sustainable change rather than short-term bursts of significant investment.

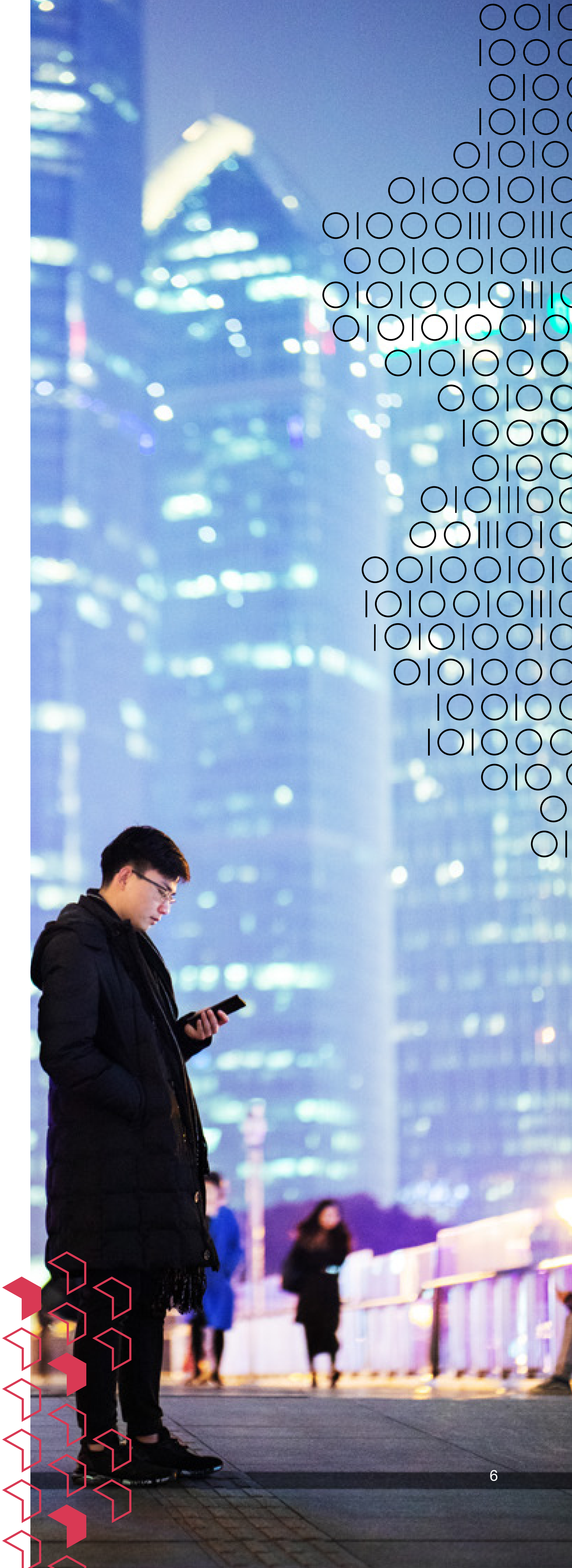
Tip 3: Expect issues and prepare to pivot

Organisations set out to deliver cyber initiatives based on a set of assumptions about the state of their environment. Significant issues are often identified that hamper success and delay deadlines.

It's important to ensure agility is baked into cyber programs so businesses can account for surprises that arise. When a significant technological barrier arises that delays your critical path, consider how resources can be redirected to issues in your backlog.

That doesn't mean organisations should employ agility at the total expense of structure, as this leads to unstable implementation and unexpected costs. Rigour and precision are still important for delivering secure technology infrastructure, so it's important to find the right balance.

Establishing flexible relationships with suppliers is critical, as they'll help execute a pivot when necessary. Partners that offer flexibility in their contracts with the ability to provide resources quickly are valuable. Depending on organisational structure, it's worth exploring flexible contractual relationships as opposed to stringent, fixed-fee arrangements.



Tip 4: Develop realistic strategies to build cyber resources

It's no secret that cyber skills are in high demand and short supply.

Research from Cybersecurity Ventures estimates 3.5 million cybersecurity jobs went unfilled in 2021, meaning the global cyber workforce needs to grow by 65 per cent to meet the dire shortage.

It's important to build succession plans for when people leave and use a blend of full-time equivalent, part-time, consultant and contracted employees.

Consider how you can partner with the right organisations, including managed security service providers, who can give additional support when needed, providing continuity amid staff turnover.

Lastly, reskill existing talent. Identify transferable skills to plug the talent gap and improve retention by providing opportunities for career development. PwC's 2021 Hopes and Fears Survey shows that 77 per cent of workers have an appetite to learn new skills or completely retrain.

As an example, an organisation might have an engineer managing Operational Technology with a keen interest in cybersecurity, who could play a key role in a cyber program with some formal learning. This sense of agility is critical in a hot talent market and will prove vital for cyber leadership.

Five key questions for leaders to consider when thinking about reskilling:

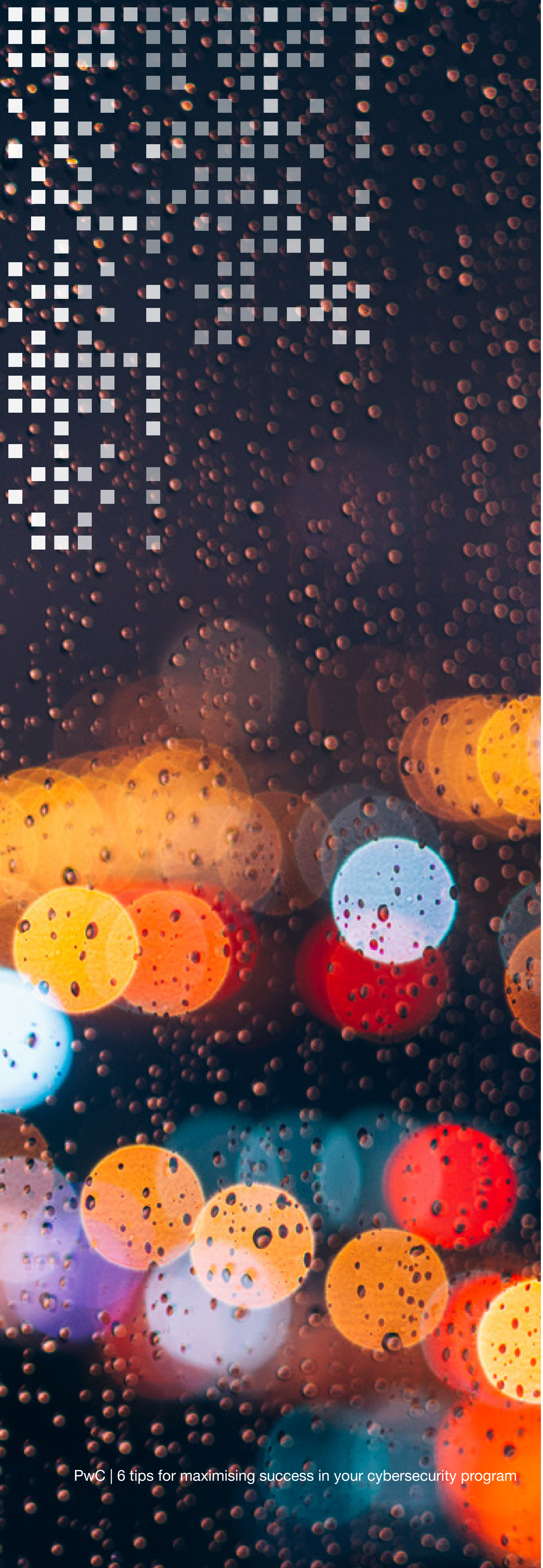
1 **What skills do you already have?** By auditing your current workforce skillset, you'll have a clear picture of the type, quantity, and location of skills. This will also give you a picture of talent pools that can be retrained.

2 **What are the required skills?** Be very clear on the skills needed to meet your organisation's cybersecurity goals. Think beyond headcount and define the nature and extent of skills required, now and into the future.

3 **What are your preconceived ideas about reskilling?** Leaders who pursue a reskilling strategy need to keep an open mind, believing in their people's learning aptitude and growth mindset.

4 **Do you have the infrastructure to reskill your people?** Reskilling is a proven strategy, but you need to have the right learning programs and support.

5 **Are you promoting a culture of learning?** People will be much more likely to embrace change and growth in an atmosphere of respect and support.



Tip 5: Foster a culture of accountability

Cyber uplift is a journey that doesn't end. As priorities shift, the manner in which you deliver uplift will change. Cyber programs must be commensurate with the size and complexity of the business, able to operate with appropriate resourcing once developed. This is especially pertinent when working with a delivery partner that won't be involved after program implementation.

A culture of accountability can be a key success factor for your cyber program. Build accountability and responsibility into the program, bring technology and business teams together to take ownership of certain controls and functions, and ensure every initiative has an owner capable of pushing it forward and communicating why it's important.

Key questions to ask:

1. What are our most important cyber priorities?
2. Is everyone brought in on those priorities?
3. Do we have the appropriate resources to operationalise the program's output?
4. Is this program sustainable and adaptable to our future needs?

Tip 6: Get your senior stakeholders involved

C-suite and boards are increasingly concerned with cyber risks, so it's imperative they're actively engaged in the process and advocating for meaningful change. This means cyber teams must clearly communicate their requirements to executives, providing accurate and thorough cyber reporting for boards and audit and risk committees.

A CEO must treat cyber as a priority without sacrificing commitment and participation. They must frame cybersecurity as important to business growth and customer trust, not just defence and controls. This will help build a security culture across the entire organisation, critical for cyber program success.

"Cyber is complex and can be difficult to understand. It is vital that the c-suite communicate clearly with boards, avoiding cyber jargon and creating an environment where directors feel empowered to ask cyber-related questions. This sort of buy-in is priceless."

Anne-Louise Brown, Senior Manager
Cybersecurity & Digital Trust at PwC

Priorities for business and security leadership

CEO	CISO/CSO	BOARDS
• Make an explicit statement establishing security and privacy and imperatives for the entire organisation. • Empower your CISO/CSO to carry out their cybersecurity mission by offering meaningful support and providing resources for secure-by-design or secure-by-default processes. • Modify elements of the company's business or operating models when security teams identify wasteful habits. For example, ditch the "innovation first, security later" mindset, when it creates unacceptable risk.	• Move out of the technology trenches and broaden your outreach to learn and support business strategies. Identify friendlies within your organisation to pilot new tools, changes and processes. • Demonstrate to your CxO peers why cyber risk should be treated the same way as other risk activities by leveraging your governance mechanisms. • Build a solid and ongoing relationship with the CEO and speak in a language that aligns with business priorities. • Become an outspoken and visible part of the business, with regular engagement with all departments and applicable business units.	• Make cybersecurity a standing item in board papers and audit and risk committee meetings - informed directors are engaged directors. • Create an open dialogue with directors - they should feel empowered to ask cyber-related questions of management and, in areas they do not understand, ask for further information. • Involve the board in cyber scenarios and exercises so they have insight into your organisation's cyber incident response planning.

Putting it all together with the right partnerships

The cyber threat landscape is rapidly evolving.

PwC data shows 95 per cent of Australian CEOs identify cyber hazards as a key threat to organisational growth, with threats like ransomware and zero-day attacks obstacles to business continuity. It's critical that business leaders work closely with security teams to develop and scale cyber programs in a way that's aligned with business strategy and available resources.

Cyber is not about buying into the 'tech glitter' or spending a lot of money. The real value lies in building an effective strategy with the right people. These six tips are designed to help organisations do that.

To assess progress against these concepts, organisations should ultimately ask three key questions:

Key questions to ask of your cyber program:

1 How are we measuring the reduction of cyber risk in addition to achieving compliance objectives?

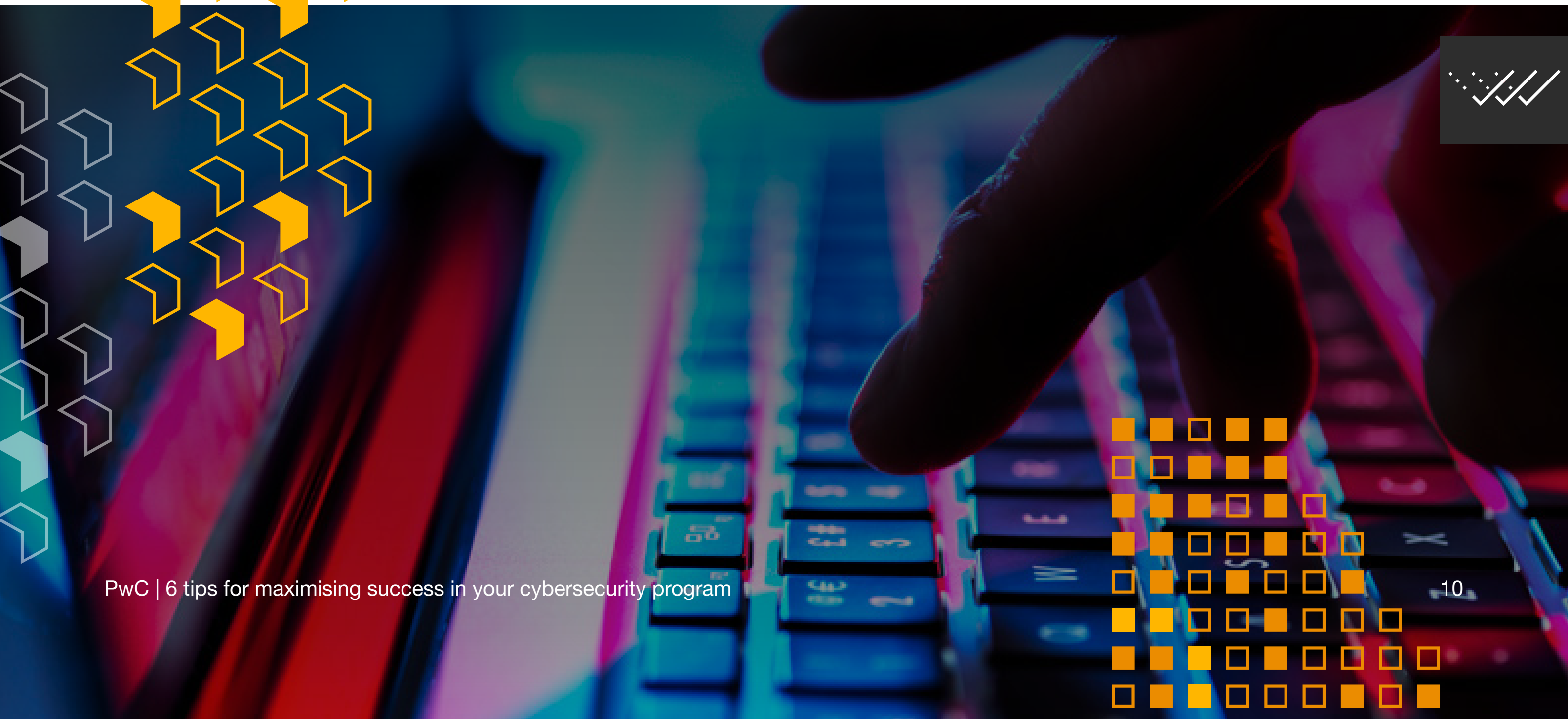
2 How are we ensuring that the outputs of our cyber program are fit-for-purpose and able to be consumed by the business?

3 What is our change management plan for the program, and how does it take everyone who's impacted into account?

Finally, solid and enduring partnerships are a key investment.

The right partner ensures organisations have the expertise necessary to safeguard their critical data and systems, allowing them to focus on what matters most to their business in the future.

Our community of problem solvers at PwC can help your organisation deliver sustained outcomes across the whole cybersecurity lifecycle, creating bespoke and practical cyber programs to fit your specific needs.



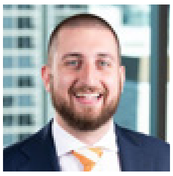
Key contacts

Mike Younger

Partner
Cybersecurity & Digital Trust
+61 490 093 981
mike.younger@pwc.com

Victoria Young

Director
Cybersecurity & Digital Trust
+61 400 215 538
victoria.young@pwc.com



Tom Huth

Senior Manager
Cybersecurity & Digital Trust
+61 405 747 957
tom.huth@pwc.com

PwC refers to the Australia member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. Liability limited by a scheme approved under Professional Standards Legislation.

At PwC Australia our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 250,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.au.

D0374163