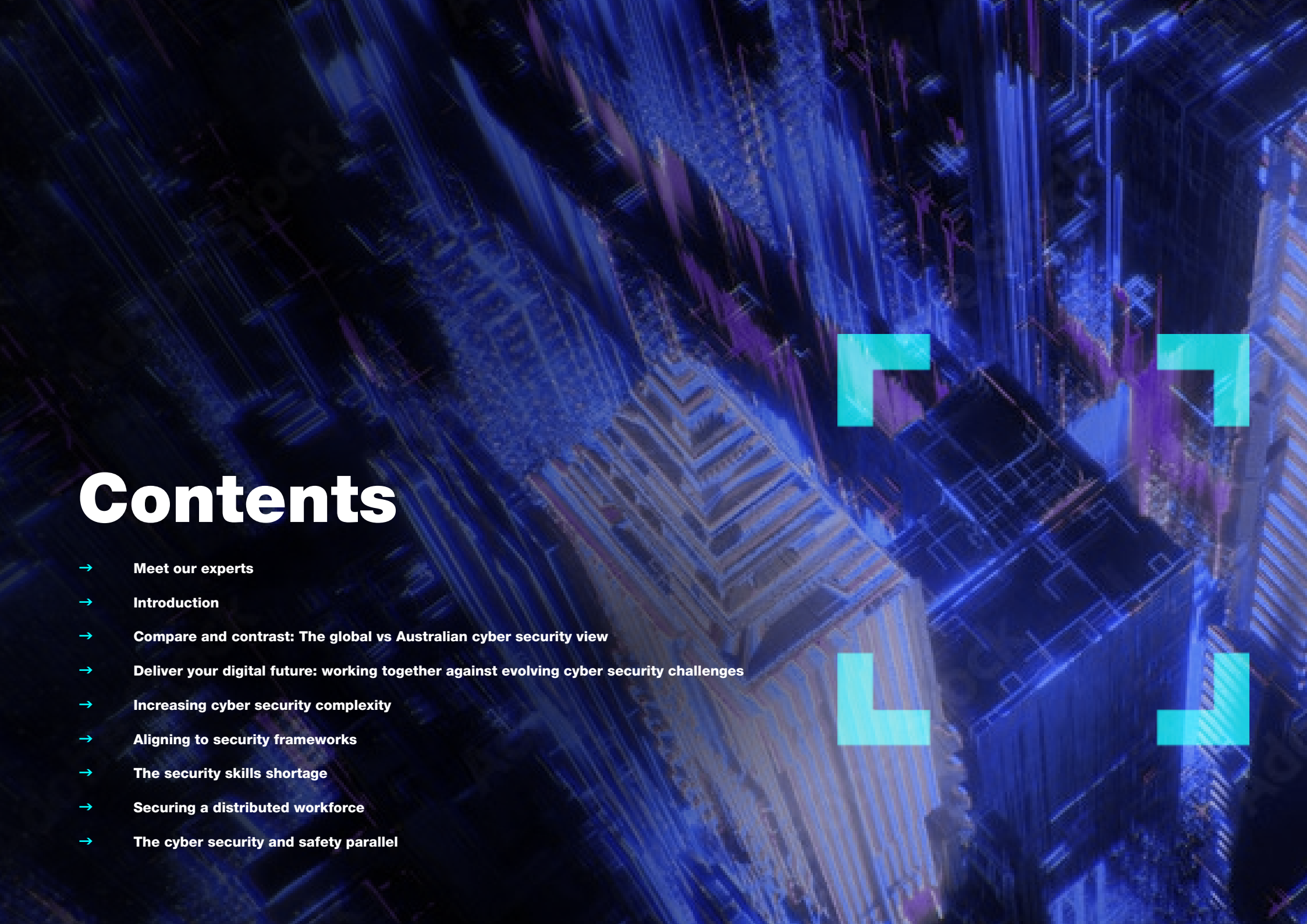
Data#3

Delivering the Digital Future, Securely.

Reframing how cyber security is considered to create a platform for growth, differentiation, and competitive advantage.



Contents

Meet our experts

Nicole Bakewell
Security Specialist, Data#3

Stan Bakulin
Solutions Architect, Data#3

Laurence Baynham
Chief Executive Officer and Managing Director, Data#3

Richard Dornhart
National Practice Manager for Security, Data#3

Paul Green
Principal Information Security Consultant, Business Aspect

Hayley Harpham
Senior Legal Council, Data#3

Chris Harvey
Principal Security Architect, Data#3

Bruce Irwin
Principal Consultant for Cyber Security & Risk, Business Aspect

Janelle Phillips
General Manager for People Solutions, Data#3

Dave Summers
Microsoft Azure Lead, Data#3

Bruce Waldron
National Manager for IPT, Data#3

Introduction

Australian businesses come up against cyber security threats daily. They must be well positioned to detect and respond to threats to avoid business interruption, reputational damage and potential regulatory enforcement actions that can result from a cyber incident. Combined with increasing security-related challenges – such as demand outpacing supply for skilled security resources, increasing supply chain attacks, and adapting security approaches to hybrid workforces – this can pose a challenge to digital transformation, and leave businesses unsure how best to progress.

What if we could change the narrative and reframe how we think of, and approach, cyber security?

At Data#3 we think of cyber security as more than an organisational obligation, we see it as a strategic enabler. Cyber security management shouldn't exist within a vacuum. Rather it requires a coordinated, multi-layered and holistic discipline with elements of organisational safety and responsibility shared throughout the organisation, not just tied to IT.

CYBERCRIME AND DATA SECURITY ARE THE NUMBER ONE ISSUE KEEPING DIRECTORS AWAKE AT NIGHT[10]

"When security is discussed or a threat is encountered, often the immediate response from senior executives is to look to the technical department for a fix to get things back on track. That needs to change."

Laurence Baynham, Chief Executive Officer and Managing Director, Data#3

We take this approach because we know that cyber security is far more effective when it is deeply embedded into an organisation's culture. Not just in company-wide procedures either. It's fundamentally about people — creating an environment where everyone understands their role in keeping the organisation safe and secure. From employees identifying phishing emails, right up to the board and management aligning cyber security to the strategic outcomes of the organisation. Stepping away from the perspective that cyber security is solely the domain of IT can encourage the organisation, from the top down, to prioritise cohesive and effective defences.

When organisations can successfully spread the load across the business and reduce the cyber security burden on IT teams, they are better positioned to innovate and give the organisation the confidence needed to tackle new markets, develop new products, securely accommodate hybrid workers, and gain a reputation as a safe company for their customers.

Hear from our team of experts as we help you on your journey to delivering the digital future, securely.

Compare and contrast:

The global vs Australian cyber security view

Compare and contrast:

The global vs Australian cyber security view

The global snapshot

In a recent webinar with Interpol — the International Criminal Police Organisation — they discussed the tsunami of cyber security activity they've seen take place over the last two years.

Ransomware continued to be a huge focus globally with attacks on healthcare providers and hospitals, as well as research centres and cross-industry supply chains already coping with border lockdowns and shortages. Scams and phishing attempts ballooned, along with a surge in IoT exploits and attacks targeted against people setting up remote work environments with minimal controls.

Interpol also saw more and more security exploits and malicious service capabilities available for purchase on the dark web, effectively lowering the bar for entry into a world of cybercrime. This resulted in a new wave of inexperienced people looking to take advantage of this ease of entry to make their own impact.

Detection rates of cybercrime continue to be low, and it has proven difficult to attribute attacks to particular sources or malicious actors. One positive outcome of this, though, is the global drive towards new public/private partnerships between law enforcement agencies, like Interpol, and security vendors, like Cisco and Microsoft, to share information and work closely together. It is making a difference.

VS

The Australian experience

In Australia, the threat vectors closely align with this global view, with one standout exception — business email compromise (BEC).

While BEC continues to be the number one attack vector for cybercrime worldwide, Australia is overrepresented, with just over 20% of worldwide BEC attacks occurring in Australia in 2020/21.[1]

We also see Australian businesses generally experience a higher number of attacks with a higher success rate than their overseas equivalents:

- **80% of Australian organisations experienced a ransomware attack in 2021 compared to the global average of 68%[1].**
- **92% of Australian organisations have experienced a successful phishing attack – the highest of any surveyed country. This represents a 53% year-on-year increase[1].**

While organisations are willing to provide information to surveying organisations for them to derive stats such as these, a general lack of formal reporting from Australian organisations and individuals is having a dampening effect on the efforts of enforcement agencies, like Interpol, to solve the crimes. Interpol indicated that despite knowing of approximately 11,000 victims of cybercrime in Australia during one particular reporting period, only 1 report was made to Police.[2]

Finding the positives

Australia is also not immune to the challenges of finding and retaining security staff, but we seem to be doing slightly better than the global average with:

- **51% struggling to recruit cyber security talent** vs 60% globally[3], and
- **34% struggling to retain that talent** vs 52% globally[3].

We're also taking the cyber security challenge seriously and there has been some progress. A global study[8] comparing cyber security defences ranked Australia as the world's 15th most secure country. According to security research firm Comparitech, Australia climbed 12 positions in a 2020 cyber security ranking report.[9] The study evaluated 76 countries' exposure to security vulnerabilities to find which countries are well prepared for cyberattacks.

As we discussed in the introduction, it feels like we've become conditioned to view cyber security with frustration, and despite major investments over many years, organisations still find it hard to deal with evolving threats. Core challenges remain such as:

- HR teams trying to fill specialist security roles
- Legal teams navigating complex regulatory and compliance requirements
- Executive teams and boards trying to justify increasingly complex investments in cyber security solutions whilst managing financial and reputational risk
- Staff adjusting to a new hybrid workforce model and understanding their role in staying safe and secure
- IT teams dealing with an overload of information and logs, making it difficult to know what incidents to focus on as a priority
- Increasingly complex threats
- Making the right choice when faced with a vast array of security products

As a result, we've seen an increase in the complexity of cyber security environments as organisations layer multiple solutions in an attempt to close identified security gaps. However, complexity is the enemy of security, so organisations following this approach make their environments harder to manage and protect, inadvertently creating new security gaps that they're often unaware of.

To provide a framework for this discussion, the following sections will consolidate the above challenges into four broad themes. We'll then discuss them in more detail to help you to deliver a sound security strategy that can be used as a springboard for change and an enabler of business growth.

IN THE PAST YEAR, THERE HAS BEEN A 26% GROWTH IN DEMAND FOR CYBER SECURITY PROFESSIONALS IN AUSTRALIA[15]

COMPLEXITY IS THE ENEMY OF SECURITY

Deliver your digital future:

Working together against evolving cyber security challenges

Deliver your digital future:

Working together against evolving cyber security challenges

As challenges and threats continue to evolve, it's imperative that we work together to stay one step ahead of cybercriminals. Hacking groups, like Nobelium, Electrum and Vanadinite, are run like well-funded enterprises, and their business models have improved over time, which means they can dedicate more time and resources to achieving their malicious goals.

So, how can businesses stay one step ahead with limited budgets, complex security environments, a shortage of skilled staff, and confusing security frameworks that are all putting more pressure on senior management and boards?

"Ensuring that security is embedded in all the changing elements of a business, as well as managing business as usual, is a huge challenge."

Bruce Waldron, National Manager for IPT, Data#3

In this section, we delve deeper into the four areas we that we see as the core challenges facing Australian businesses when it comes to cyber security:

- The increasing complexity of cyber security environments and attack vectors
- Numerous and sometimes confusing security frameworks
- The shortage of skilled staff to address all these challenges
- The need to secure an increasingly distributed workforce

We also want to change the narrative from negative to positive, developing a determined "not on my watch" mindset, not only in the IT department but throughout entire organisations. **We're presenting this approach because, with our many years of experience, we can see that different thinking is needed when it comes to cyber security.** Not to finally "win", but to help organisations deliver a safer environment today, versus last month or last year, and where your staff, customers and suppliers have the confidence to develop and deliver new services and innovations.


Increasing
cyber security
complexity

Increasing cyber security complexity

The increasing complexity of attacks

Everyone loves nostalgia in some form. In the cyber security world, long-time IT professionals look back fondly at the "good old days" when security meant a firewall and anti-virus, and the aim of hackers was more about bragging rights than the espionage, financial gain and malice we see today. The modern hacker is a completely different beast.

Today, we see the rise of nation-state attackers treating hacking like a business, launching highly complex attacks that are hard to detect and harder to recover from. These hacking groups - such as the infamous Nobelium, responsible for the Solar Winds attack and Xenotime, known for targeting oil and gas companies - appear to be well-funded and incredibly persistent. A series of articles by Microsoft[17] that uncover the depths of that attack, point to an organisation that is "persistent and determined to achieve their objectives".

"These aren't random 'script kiddies', graffitiing websites and taking out servers, they're sophisticated professionals, with clear targets, and advanced capabilities, carrying out well-planned attacks that cause as much disruption as possible."

Paul Green, Principal Information Security Consultant, Business Aspect

It's easy to dismiss these stories as media sensationalism, but the fact is, nation-state attackers are increasingly targeting enterprises for their intellectual property, as well as for potential backdoors through their trading relationships with more traditional targets, such as government infrastructure, or to launch lucrative attacks on major corporations.

COVID-19 also gave a lot of groups the opportunity to weaponise their existing toolkits and target the huge number of new weak points made available by people working remotely with consumer-grade routers, printers, IoT (such as cameras) and internet connections.

"If you're thinking *"we're not an enterprise and don't have anything of value"*, then you're missing the bigger picture."

Nicole Bakewell, Security Specialist, Data#3

Size is irrelevant. Every business has information and data that it can't afford to lose, and also has relationships that can be exploited. It could be the supply chains you're connected to, or the customers you're serving, so you become a stepping-stone to a bigger pot of gold.

If we look at the ways these threats are becoming more sophisticated, then an interesting example is Borat RAT – a Remote Access Trojan that goes beyond typical remote access capabilities, adding spyware and ransomware. The tool may have a funny name, but it shows an increasingly sophisticated combination of capabilities. The worst part, though, is that anyone can buy access to the services on underground forums or the dark web and deploy it themselves with a little self-directed learning. They even go so far as to customise these attack tools to target specific organisations and then develop ways to better cover their tracks as they infiltrate to avoid detection. We talk a lot about the democratisation of software happening with the low-code and no-code movement, but when this is also happening to malicious tools, it presents an incredibly sobering viewpoint on just how threats keep growing while also getting more and more sophisticated.

The idea of protection and staying one step ahead

With the increasing complexity of threats, the questions of how to stay one step ahead continue to mount. This has resulted in an arms race between vendors eager to solve every challenge with a new tool. Multiple vendors with multiple solutions all designed to solve a specific challenge or threat have led to cyber security environments that have become almost too complex to manage. Solutions are layered on top of each other, seemingly providing overlapping coverage. However, with often limited integration between solutions there are still plenty of gaps. Each solution also generates alerts that vary in their urgency for attention (or validity), overwhelming IT teams that lack the bandwidth to manage them all.

While it may seem a counter-intuitive idea, perhaps we need fewer layers, fewer vendors and fewer solutions. Instead of buying the comprehensive protection of multiple products from many vendors and acting as the integrator ourselves, we buy fewer, but choose those that are already tightly integrated, share information, and are better able to act as a defensive shield. This is obviously a simplified view, but the idea is sound, and we're now seeing vendors reorganise their cyber security portfolios in this way.

Cisco is just one example of a vendor modelling this thinking, and we've recently spoken about their approach, but fundamentally, our attention must shift towards people being the new network perimeter - and putting the right controls on the devices and tools they use as well as the business data they access. That includes conditional access policies, multi-factor authentication, user entity behavioural analytics (UEBA), robust malware detection, and data loss prevention (DLP). These are controls and mechanisms to detect anomalous behaviour and generate an alert, but more importantly, they can also do something about the situation without requiring user intervention.

"Treat your humans as the new perimeter."

Dave Summers, Microsoft Azure Lead, Data#3

This shift towards the network edge for security control has been underway for a while with approaches like secure access service edge (SASE), but really embedding the idea of the human perimeter takes it a step further beyond tools and devices. It encompasses an organisation's culture and attitude towards cyber security awareness. The notion that everyone is responsible for cyber security, not just the IT team, to eliminate or greatly reduce the human errors that can result in breaches – visiting fake websites, clicking links in emails, installing unapproved apps, reusing passwords etc.

"Too often cyber security is solely the responsibility of the IT team when, in fact, it's everyone's responsibility. If everybody understands the implications of an attack and takes ownership, vigilance becomes ingrained. That has to become the new normal for organisations."

Richard Dornhart, National Practice Manager for Security, Data#3

Zero trust is another long-held approach that has transformed the way we think about cyber security in general. As Microsoft CEO, Satya Nadella, said at the recent Microsoft Security Summit, *"We've spent years building our zero trust approach internally at Microsoft. We've proven its effectiveness against real-world attacks. We are committed to sharing what we have learned to help every organisation accelerate their progress."*[4]

Palo Alto Networks is also pursuing a tighter integration of zero trust principles throughout their portfolio, championing the idea that *"we all deserve the right to work and live without the fear of cyber threats."*[5]

This again supports the idea of ensuring the tight integration of security principles with organisational culture applied to the tools and systems we use every day in our work.

We've also seen the Australian Cyber Security Centre (ACSC) talk more about their REDSPICE initiative that signals the start of the most significant transformation in ACSC's history, investing in new intelligence and cyber capabilities while working with people and businesses around Australia to improve everyone's security posture.[6]

The ACSC's initiative is a timely reminder that spending time and money developing a response plan has become critically important. How are you going to identify a breach, then respond, manage, and recover? Are you perfecting the emergency drill so that teams know what to do ahead of time, quickly, before hackers and damage go too far?

“Another controversial angle towards dealing with this complexity is for organisations to get comfortable with the notion that they will get breached at some point.”

Nicole Bakewell, Security Specialist, Data#3

Managing risk

Organisations have long been accustomed to identifying and managing risk, and cyber security should be regarded in much the same way as other risk mitigation strategies, such as workplace health and safety. No matter how well an organisation instils policies and a culture of safety in the workplace, human error and freak accidents occasionally occur, but these risks should be minimised. Accepting that you can’t eliminate every single cyber security risk shifts the discussions toward risk management — a topic that every board is very familiar with.

“Cyber security prioritisation does not stop at the CEO. It is equally important for the board to be informed and involved in understanding their organisation’s risk profile.”

Laurence Baynham, Chief Executive Officer and Managing Director, Data#3

It is necessary to map and rank the risks specifically for your organisation and build a cyber security plan that prioritises those risks according to the biggest potential impact on your operations while accepting that lower-ranked risks might not be addressed to the same level.

Your cyber security plan can include a mix of cyber security tools, user awareness, and third party support – effectively building an integrated ecosystem of protections that don’t just rely on layers of technology to provide protection and don’t add to the complexity of your environment.

“We need to look at the threat landscape holistically, but also understand that there are specific risks associated with each solution. This is where cyber security is a unique skill set - the threat or breach enabler for each particular technology solution may be very different to the next. To ensure that there isn’t a pinhole gap in a particular security control, or element that lets the rest of the technology environment down, you must assess the risks across all of the individual security components in the ecosystem.”

Bruce Irwin, Principal Consultant for Cyber Security & Risk, Business Aspect

This idea of risk management also extends to productivity and user requirements. Too often, security seems to be at odds with productivity with tighter controls getting in the way of people doing their jobs. As frustrations develop, people look for workarounds that can negate the protections originally put in place, but it shouldn’t have to be this way. This reflects the role that culture plays in an organisation and a 2009 quote from Vivek Kindra - the first White House CIO – still seems relevant today; “The more a CIO says ‘no’ the less secure their organisation becomes.”[7] Adapting technology and security around user requirements is important to your overall security posture, especially with this idea of the human perimeter in mind.

“Embedding security as part of an organisation’s culture means making sure that everybody understands their role to play in securing the organisation, from the executive down to frontline staff. It’s more than just embedding it into workplace procedures. It’s about really understanding the contribution that each individual can make in terms of keeping the organisation safe and delivering the outcomes to the organisation and to the stakeholders, such as customers.”

Bruce Irwin, Principal Consultant for Cyber Security & Risk, Business Aspect

Aligning to security frameworks

Aligning to security frameworks

When it comes to cyber security, there are numerous frameworks that can go a long way to helping organisations meet their security requirements. While these guidelines are extremely helpful, businesses often struggle with how to approach the implementation of those controls.

The Commonwealth Government, through the ACSC, developed the Essential Eight framework, which features eight cyber security controls and three levels of maturity. There are also international standards like the NIST Cyber Security Framework, and ISO 27001.

"There is a trap to avoid here – treating these controls as a checklist and addressing them with the lowest cost solution possible."

Chris Harvey, Principal Security Architect, Data#3

While the ACSC Essential Eight is the minimum standard that organisations should be considering to mitigate cyber security incidents, it still covers a lot of ground in a digestible format that nearly every business could draw expertise from. The current model prioritises implementing all eight as a package because of their complementary attributes and broader focus on the evolving threat landscape. ISO 27001 and NIST offer a more comprehensive set of controls though, and organisations should think about how to include this in their planning.

"The value in any framework is in living it by implementing and embedding it in your culture. If you don't, then it's not really worth the paper it's written on."

Hayley Harpham, Senior Legal Counsel, Data#3

This comes back again to the culture of the company and the degree of importance placed on cyber security. Even armed with all the information on the costs of a breach, some organisations view cyber security as a "tick the box" exercise, rather than using it to properly improve the overall security posture.

"It's like buying a fire extinguisher and putting it in a garage to tick a fire safety requirement in fire-prone areas, without also thinking about clearing areas around your house and making sure water tanks are full."

Stan Bakulin, Security Solutions Architect, Data#3

You need to be proactive and address the reason for the requirements, not just the visuals. This approach applies equally to the executive team.

"Regular and consistent reporting is important for any organisation. Executives must understand the priorities and threat levels, but more importantly, the impact on the business. Only then can you start prioritising spend and decisions. For me, that is the critical factor."

Laurence Baynham, Chief Executive Officer and Managing Director, Data#3

The benefit of frameworks

We often see the tendency of organisations to treat compliance as just another cost to the business that needs to be done. However, with the right frameworks in place, you develop a common language, allowing you to demonstrate to customers, partners and suppliers how seriously you take cyber security.

"From a compliance perspective, standards and frameworks help tremendously because they enable us to demonstrate to our partners that we are aligning with best practice. It gives us something to point to and say this is what the industry considers we should be doing in terms of managing information security."

Hayley Harpham, Senior Legal Counsel, Data#3

Insurance companies won't give you cyber security insurance unless you have certain controls in place. Some customers won't sign agreements with you unless you can demonstrate how you're able to protect their data and their business reputation.

"You wouldn't deal with a bank that doesn't comply with banking compliance regulations, and this idea is taking hold quickly with regards to cyber security."

Richard Dornhart, National Practice Manager for Security, Data#3

We are now more often seeing organisations actively promoting their cyber security readiness as a business differentiator and a driver for change. When there is a consistent approach from the executive management group that covers all layers from regulatory compliance to technical teams and security controls, all the way down to staff awareness and training, that gives enormous confidence to develop new capabilities and ways of serving your customers. We need to change the mindset from cyber security investment being seen as a tax to a revenue and profit-generating enabler.

This is obviously not something that changes overnight, but it is worth seeking trusted advice on how to sort through all the noise and develop a plan to align to the principles discussed. The danger is underestimating the challenge, and not prioritising or resourcing the changes required. In the absence of executive support, any recommendations tend to get filed, a KPI box might get ticked - but without new investments an organisation will be no more secure 12 months later.

The reasons for this are many and varied, but a common one is a lack of skilled resources to implement these changes.

The security skills shortage

The security skills shortage

This is a challenge that really needs no introduction and the imbalance between supply and demand is affecting businesses across the board.

"I recently looked at the number of cyber security jobs being advertised on a major job platform in Australia and there were 5,568."

Janelle Phillips, General Manager for People Solutions, Data#3

Everything we've discussed so far, ultimately puts pressure on an organisation to have the right people with the right skills to respond. The increasing complexity and sophistication of threats along with compliance and regulatory requirements are moving faster than skills are being developed, resulting in a growing deficit.

"Since the pandemic, there's been a change around the availability of skilled candidates. With a limited pool of candidates if you're not putting forward a good case to attract those people you will struggle to fill cyber security roles."

Janelle Phillips, General Manager for People Solutions, Data#3

We've also arguably created more of a problem with the sheer wealth of solutions, each promising much, yet often causing new issues in the form of complexity. We feel like the job is done and we're protected when a new solution is deployed and we move on to the next thing, but the operational aspects of constantly managing alerts and tuning responses require more knowledge – knowledge that hasn't been developed.

"We're often dealing with environments that have been built and developed over many years, but the stakes today are higher than five, ten or twenty years ago. A shortage of skilled resources can mean that the depth of knowledge and experience, especially in securing complex IT ecosystems, is limited. Then, when complex problems do arise, the expertise isn't there."

Dave Summers, Microsoft Azure Lead, Data#3

This is another simplistic example to highlight the pace and depth of change, but it is symptomatic of the difference today between deploying and operationalising new security solutions.

When it comes to solving this challenge, there are a few levels to consider.

If we start at the organisational level, we've already discussed the counter-intuitive idea of fewer solutions and vendors, simplifying overly complex environments to reduce the likelihood of blind spots and gaps. However, the secondary benefit of this simplification lies in reducing the breadth of skills required to manage an environment, giving your team a chance to "catch up".

There's also a discussion to be had around what core skills should exist within the business and how many people can be feasibly employed. That obviously changes depending on the size and nature of the business, but no organisation has the luxury of employing people whenever they want – they have to work within constraints, which leads us down to the next level – partnerships.

At the partnership level, you're looking to leverage someone else's skills and resources to supplement your own. Outsourcing security is nothing new, but it also shouldn't be an all-or-nothing approach.

IN 2021, THE WORLD'S OPEN CYBER SECURITY POSITIONS WERE ENOUGH TO FILL 50 SPORT STADIUMS[14]

“We often explain it using a conductor metaphor where you maintain the overall conducting role – setting the tempo, the direction and the focus, while you outsource the musicians.”

Chris Harvey, Principal Security Architect, Data#3

If you think about all the security-related roles within your organisation, what would you classify as more of the conducting vs the musicianship? Operational tasks like monitoring, classifying and responding to alerts fall into the latter category, but liaising with users and setting strategy all require people close to the business so that would be internal. Outsourcing in this way eliminates single points of failure in your organisation based on individuals, while also scaling to 24x7 if your business requires it.

The final level we look at is the staffing level, and this is not one that is quickly solved. Upskilling internal candidates, and starting mentoring or cadetship programs are useful, but all take time. We also see anecdotal situations where smaller businesses invest in staff upskilling only to have them leave and take advantage of exorbitant salaries on offer by larger organisations – a situation distorted by this imbalance between supply and demand.

Despite this, there is still an altruistic view to consider. By investing in training, you’re contributing to the overall number of skilled staff in the market. You also do get the benefit of their growing skillsets for as long as you can keep them interested. The trick is to operationalise the training so that it’s easily repeated as new employees start and move through. Like a lot of the areas we’ve discussed, this has links to the company culture and overall level of importance put on cyber security. Whatever the choice, it must make sense for the size of the business and the relative risks identified – not every business can afford (or needs to) develop internal training programs for cybersecurity staff.

“From a macro point of view, demand is outpacing supply in terms of cyber security resources. We, as an industry, need to do more to get more people into the IT industry, specifically cyber security.”

Laurence Baynham, Chief Executive Officer and Managing Director, Data#3

THE GLOBAL CYBER SECURITY WORKFORCE NEEDS TO GROW 65% TO EFFECTIVELY DEFEND ORGANISATIONS’ CRITICAL ASSETS[13]

Securing a distributed workforce

Securing a distributed workforce

The new normal of the hybrid workforce has disrupted corporate security controls like no other event before it. We've already touched on the concept of the human perimeter and as everyone stayed home, organisations had to play catch up to move from a centralised, easily controlled environment to a distributed person-centric environment.

"Where before an organisation used to have one head office, they now effectively have hundreds with just one person working in each of them."

Richard Dornhart, National Practice Manager for Security, Data#3

To say that approaches to this challenge were delivered in a rush is an understatement (Microsoft Teams and OneDrive anyone?), but by and large, they've been working. However, those approaches weren't developed with long-term needs in mind – they were often a quick fix that got the job done and they're still in place. However, are they fit for purpose?

Now that the hybrid workforce model is here to stay, it's an opportunity for organisations to revisit those systems and ask:

- Is your data protected everywhere?
- Are your user identities and personas in place with the right level of controls and governance over data?
- Are those controls just another bolted-on solution adding to the complexity, or are they integrated with existing platforms?

Managing the user experience

Anything that makes work harder for staff than they feel it should be, becomes a target for a workaround such as using unsanctioned cloud applications for sharing sensitive documents.

This is where deliberate planning and thought around the user experience becomes vitally important. When the rush was on to support remote workers, the user experience was almost ignored. The mantra "security should be largely invisible to users" was forgotten as VPNs, multi-factor authentication tokens and multiple sign-ins for different parts of the organisation and different apps took precedent. This was in sharp contrast to the in-office experience where security remained largely hidden. Bringing those two worlds closer in terms of experience without compromising effectiveness is now the focus. When users are educated about the threats, and the implications of getting it wrong, we have observed a marked change in behaviour, with fewer trying to find workarounds. Where security cannot be invisible, users need to understand the importance of any measures in place.

This doesn't mean adopting a whole new suite of security tools for remote users, but instead building on the idea of "humans as the new perimeter". How can you adapt your security approach to a more decentralised architecture where the same underlying toolset caters for both in-office and remote work environments with a consistent user experience? Reduce complexity, consolidate vendors, and tighten integration between solutions.

The accompanying idea to managing the user security experience is ensuring users understand their responsibility when it comes to security.

"We not only ensure everyone is responsible for security, we also help them understand as individuals what that actually means for them in their role - that's a big focus for us."

Bruce Waldron, National Manager for IPT, Data#3

This brings the conversation back to culture again and the role it plays in keeping your organisation safe.

OF THE EMPLOYEES CAUGHT BY A PHISHING SCAM WHEN WORKING FROM HOME, 47% CITED DISTRACTION AS THE REASON[11]

Innovation and the challenge of legacy apps

“It’s very easy to talk about a cyber business case in the context that if you don’t do this, then this will happen. However, when you start looking at it as a business enabler, it opens up new opportunities. For example, how can we share more information with our customers and partners? How can we use our data in new ways? How, with the move to hybrid work, can we better interact with third parties and employees?”

Richard Dornhart, National Practice Manager for Security, Data#3

One positive aspect of this change was the amount of innovation that did take place with new apps being developed, along with better ways of serving and interacting with customers remotely.

REMOTE WORKERS CAUSED A SECURITY BREACH IN 20% OF ORGANISATIONS SURVEYED[12]

“There’s an element of trust that needs to be established between organisations and third parties when data is being shared between the two. Aligning to a common security framework creates that trust because it shows you have done your due diligence.”

Richard Dornhart, National Practice Manager for Security, Data#3

However, there are still a lot of legacy apps out there that are hard to replace and are holding some organisations back. They are typically harder to manage, costly and time-consuming to maintain, and require greater skill and effort to secure.

These legacy apps present additional security risks when you consider they were designed in an era with centralised security controls. They’re not easily adapted to this human perimeter concept, relying on middleware like Java and other libraries (such as the infamous Log4j2), requiring specific versions to run. Perhaps they can’t make use of MFA, relying on usernames and passwords that aren’t integrated with enterprise identity services - so again missing vital controls over password management etc. This adds, yet again, a lot of overhead and complexity that isn’t helping your overall security posture - and they’re not easy or cheap to decommission and replace.

At some point, though, the vulnerability, risk and maintenance costs tip the scales in favour of redevelopment using modern technologies into something more advanced that drives innovation forward.

The cyber security and safety parallel

The cyber security and safety parallel

Despite the negative messages the media perpetuate, we see the cyber security future as a positive one. In our dedicated security practice, our reframing of the cyber security challenge from negative to positive is resonating with our customers. As we mentioned at the start, we're not talking about a head-in the-sand, she'll-be-right type of positivity, but one based on a deep understanding of the underlying challenges, the knowledge of how to navigate a path forward and a partnership model that stands beside you every step of the way.

We also see value in using a corporate safety metaphor to help organisations reframe their own cyber security challenges and get buy-in from the top to the bottom of the organisation.

"To keep cyber security high on the priority list, it needs to be removed and extracted away from other risks — such as floods or vendor and supply chain issues — and become a risk register in its own right."

Laurence Baynham, Chief Executive Officer and Managing Director, Data#3.

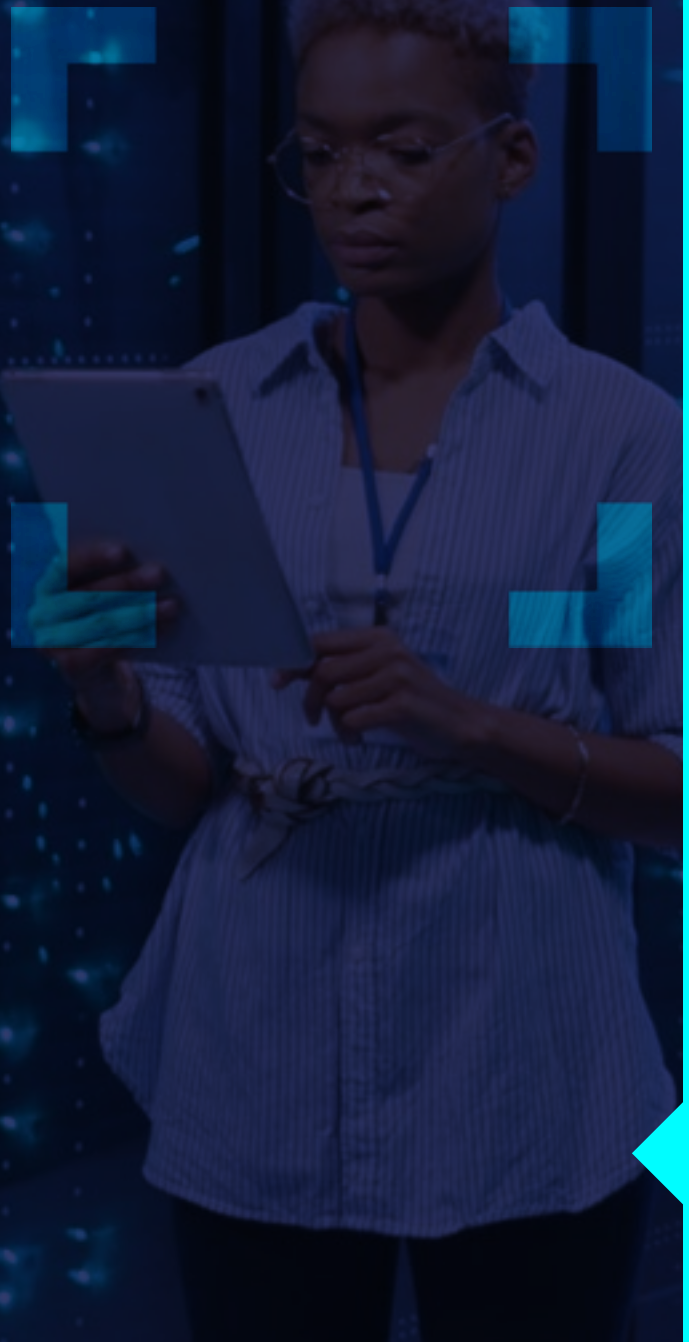
No reputable business questions the need for workplace safety. Whether that's clothing, fencing or protective guards on machines. In transport, the need for checklists, explicit processes, regular maintenance and training, lifeboats, life jackets, and escape slides is accepted. Clear lines of responsibility, approvals and escalation is commonplace.

Safety is also multi-disciplinary, with the need to consult with experts with overlapping skill sets. It's the responsibility of the entire organisation, not just the WH&S team.

However, no safety system is perfect and just like cyber security, complexity is the enemy. Accidents can happen, but with the right safety mechanisms, they don't always have disastrous outcomes.

You don't think of safety as something you attain, then forget. It requires constant work, reviews and listening to the advice of someone you trust. You're still responsible for the decisions day-to-day, but it's essential you have someone you can check in with and measure progress with - bounce ideas off. Someone to help you develop and implement a plan for success for the next six months before you check in again. It's not about giving up control, but it's not something you only do by yourself.

We must start thinking about cyber security in a similar way — a proactive, always-on discipline or ritual with safety at the core and responsibility shared throughout the organisation, not just tied to IT.



“There tends to be two ways of looking at cyber security. One is to look at it as a strategic enabler and the other is to look at it as the tax that you pay for being in business. The first one’s far more exciting. When you build a culture that views cyber security as a business enabler, the executive and management can align the program to the strategic outcomes of the organisation. By removing those risks, you become more agile and are better able to tackle new markets, bring out new products and bring new services to your customers.”

Bruce Irwin, Principal Consultant for Cyber Security & Risk, Business Aspect

The cyber security reality is this:

- Another point solution won’t help you – an architecture with all parts integrated and working together will.
- There is no endpoint, so stop thinking like there is one.
- It’s not measured in absolutes, but in relativity. Are we safer this quarter than last quarter? This year vs last year? Not about “the best” but “what’s best for us”. How do we define “good” or “secure” given our unique business?

Ultimately, when you can demonstrate clearly to customers, suppliers and staff the safety of your organisation, it becomes a platform for growth and differentiation, and completing that shift from negativity to positivity brings competitive advantage. That’s the world that we’re bringing to our customers.

Data#3 — Delivering the Digital Future, Securely.

Combining the experience of Data#3 company, Business Aspect, a dedicated strategic consulting team, as well as hands-on cyber security specialists, Data#3 has one of the most mature and highly accredited security teams in Australia. Leveraging a breadth of security solutions and a strong vendor portfolio, Data#3 can help you design, implement and maintain superior security measures, tailored to protect your business.

Learn more at **data3.com/security**

- 1300 23 28 23
- www.data3.com.au
- facebook.com/data3limited
- twitter.com/data3limited
- linkedin.com/company/data3
- youtube.com/user/data3limited

Data#3

References

1 Proofpoint (2022). Email cyber attacks on businesses soar. [ONLINE] Available at: https://www.mybusiness.com.au/resources/news/email-cyber-attacks-on-businesses-soar

2 Data#3 webinar (2022). Cybercrime Trends with Interpol. [ONLINE] Available at: https://www.data3.com/knowledge-centre/webinar/cybercrime-trends-with-interpol/

3 Fortinet (2022). 2022 Cybersecurity Skills Gap. [ONLINE] Available at: https://mysecuritymarketplace.com/reports/2022-cybersecurity-skills-gap/

4 The Channel Co CRN (2022). Microsoft CEO Nadella: 'Zero Trust Is At The Foundation Of Security Transformation'. [ONLINE] Available at: https://www.crn.com/news/security/microsoft-ceo-nadella-zero-trust-is-at-the-foundation-of-security-transformation-

5 Palo Alto Networks (2022). Palo Alto Networks Reinforces the Need for a New Zero Trust Approach Through Latest Campaign. [ONLINE] Available at: https://www.paloaltonetworks.com/company/press/2022/palo-alto-networks-reinforces-the-need-for-a-new-zero-trust-approach-through-latest-campaign

6 Australian Signals Directorate (2022). REDSPICE. [ONLINE] Available at: https://www.asd.gov.au/about/redspice

7 Forbes (2011). How Cloud Computing Is Reshaping The Role Of The CIO. [ONLINE] Available at: https://www.forbes.com/sites/ciocentral/2011/08/03/how-cloud-computing-is-reshaping-the-role-of-the-cio/?sh=36b811df165f

8 Comparitech (2022). Which countries have the worst (and best) cybersecurity? [ONLINE] Available at: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/

9 CISO Mag (2021). Australia climbs 12 positions high in cybersecurity rankings. [ONLINE] Available at: https://cisomag.eccouncil.org/australia-climbs-12-positions-high-in-cybersecurity-rankings/

10 AICD (2022). Director sentiment falls amid global economic uncertainty | Director Sentiment Index 1H22 [ONLINE]. Available at: https://www.aicd.com.au/economic-news/australian/outlook/director-sentiment-falls-amid-global-economic-uncertainty.html#:~:text=The%20first%20Director%20Sentiment%20Index,are%20anxious%20about%20global%20uncertainty.

11 Tessian (2022). Understand the mistakes that compromise your company's cybersecurity. [ONLINE] Available at: https://f.hubspotusercontent20.net/hubfs/1670277/%5BTessian%20Research%5D%20The%20Psychology%20of%20Human%20Error.pdf

12 Malwarebytes (2020). Enduring from home COVID-19's impact on business security. [ONLINE] Available at: https://www.malwarebytes.com/resources/files/2020/08/malwarebytes_enduringfromhome_report_final.pdf

13 World Economic Forum (2021). Cybersecurity training can close skills gap for a safer digital world. [ONLINE]. Available at:
https://www.weforum.org/agenda/2021/05/cybersecurity-training-skills-gap-digital/

14 Cybersecurity Ventures (2021). Cybersecurity Jobs Report: 3.5 Million Openings In 2025. [ONLINE] Available at: https://cybersecurityventures.com/jobs/

15 Microsoft (2022). Closing the cybersecurity skills gap – Microsoft expands efforts to 23 countries. [ONLINE] Available at: https://blogs.microsoft.com/blog/2022/03/23/closing-the-cybersecurity-skills-gap-microsoft-expands-efforts-to-23-countries/

16 Microsoft (2021). How nation-state attackers like NOBELIUM are changing cybersecurity. [ONLINE] Available at: https://www.microsoft.com/security/blog/2021/09/28/how-nation-state-attackers-like-nobelium-are-changing-cybersecurity/