ecosystm

fastly

CYBERSECURITY MATURITY OF ORGANISATIONS IN THE POST-PANDEMIC WORLD

How are Australian Companies Adapting to the New Threat Landscape?

AUTHORED BY

Andrew Milroy

Principal Advisor, Ecosystm

MAY 2022

Executive Summary

Despite the common perception that Australian companies are mature in terms of their cybersecurity postures a recent Ecosystm study reveals the opposite.

As companies move more resources to the cloud, increase IoT usage, and employees increasingly work remotely, a new approach to cybersecurity is required. A recent study based on 204 interviews with Australian cybersecurity decision-makers conducted by Ecosystm, in partnership with Fastly, highlights the cybersecurity challenges faced by Australian companies, the inadequacy of their current controls, and their lack of cyber maturity.

65%
of large enterprises in Australia rate nation state attacks a very high or high risk

53%
of Australian companies will place more emphasis on moving business logic from the application server to the edge, over the next 2 years

>50%
of Australian companies are challenged by the lack of appropriate skill sets in managing application security initiatives. This has led to greater automation - with 47% managing over 50 separate cybersecurity tools.

Organisations continue to consider data breaches and data loss as their biggest cyber risk followed by endpoint compromise. Larger enterprises in Australia, however, consider nation state attacks to be the biggest risk.

Despite an awareness of the external and internal risks of highly centralised architecture, organisations in Australia are struggling to adapt to new, more decentralised IT architectures. As business logic moves from back-office application servers to remote locations and devices, companies need visibility into their resources across dispersed locations and a much larger attack surface.

Cybersecurity skills shortages in Australia are forcing companies to embrace greater automation as security operations centres (SOCs) are increasingly unable to handle the number of alerts including false positives they receive that result in wasted time. This challenge is compounded by the large number of discrete cybersecurity tools used, many of which are not integrated, increasing the burden on practitioners.

Australian companies need to transform their cybersecurity postures starting with an assumption that corporate resources will be accessed from multiple locations and from multiple devices and that breaches will occur.

They need to augment existing controls with tools and processes that make it difficult to cause significant damage when systems and networks are attacked. This requires assets to be continuously monitored and cybersecurity postures to evolve with changing threat and regulatory environments – all in a largely automated fashion.

Expanding Attack Surfaces: Increased Digitalisation and Shift of Business Logic from Applications Servers to the Edge

The pandemic accelerated the adoption of digital technologies, as companies sought contactless ways to engage with stakeholders and to enable employees to work remotely.

But it has also exposed these companies to increased digital risk. Cybersecurity was not a primary consideration when companies needed to implement new tools quickly to keep their businesses running during the pandemic.

As the number of remote employees increased and business processes were rapidly digitised, corporate IT systems and data stores have grown in size and complexity almost overnight – offering fertile terrain for attackers. Companies in Australia are aware of this increase in risk and have made cybersecurity a greater priority (Figure 1). And amidst the growing risk, organisations are also challenged with a shortage of the right cyber skills. While more than 40% of organisations state that they have increased cybersecurity budget, it is important to evaluate whether investments are being made in the right areas.

FIGURE 1:

The Impact of the Pandemic on Cybersecurity Posture in Australia

55% Cybersecurity became a greater priority

51% Remote working created new vulnerabilities

48% Our cybersecurity risk increased

44% We increased our cybersecurity budget

40% Skills shortages increased

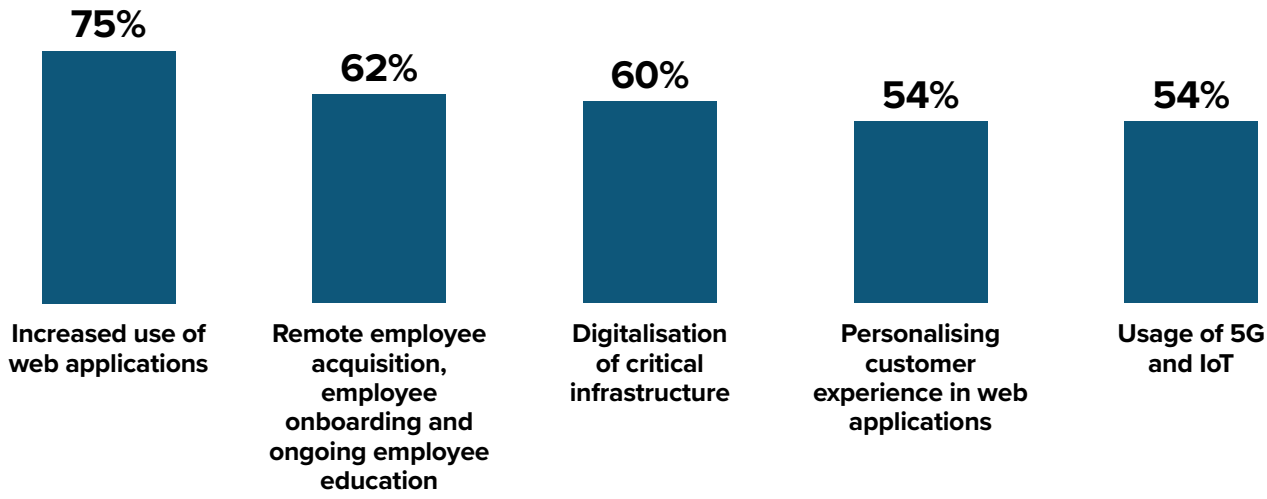
Q:Which of these statements relate to your organisation's cybersecurity posture during the pandemic?

Source: Ecosystm-Fastly Cybersecurity Maturity Study, 2022

N=204

Cybersecurity risks increased exponentially when the pandemic hit. The largest contributor to an increased attack surface was the increased use of web applications to engage with remote employees, customers, and other stakeholders (Figure 2). The workforce has become increasingly dispersed – now employees are location-agnostic. HR and talent applications have proliferated and increased risk exposure beyond the company network. The need for infrastructure modernisation and digitalisation has led to adoption of newer technologies, further expanding the risk.

FIGURE 2:
Key Contributors to an Expanded Attack Surface in Australia



Q: Which are the top 5 areas that will see increased focus in your organisation over the next 2 years?
Source: Ecosystm-Fastly Cybersecurity Maturity Study, 2022
N=204

Adoption of cloud services has become imperative for greater agility and efficiency to support increased digital engagements and remote working. But cloud resources expose organisations to new vulnerabilities and gaining full visibility of these resources remains a major challenge. 53% of Australian companies are moving business logic from the application server to the edge, where the data is being generated, increasing the urgency for greater visibility.

The expansion of networks to the edge and an increased use of remote devices will necessitate more resilient cybersecurity postures that can secure a massive and growing attack surface.

Although most companies are aware of the increased digital risk, taking the right actions to mitigate this risk is challenging, especially with a growing cybersecurity skills shortage.

Organisations' Cybersecurity Challenges

Despite the awareness of the expanding threat landscape and a greater focus on cybersecurity, organisations continue to face challenges in managing cybersecurity strategies and measures.

FIGURE 3:

Leading Cybersecurity Challenges in Australia

42%
Compliance and understanding of the relevant compliance environment

36%
Low cybersecurity awareness among staff and other stakeholders

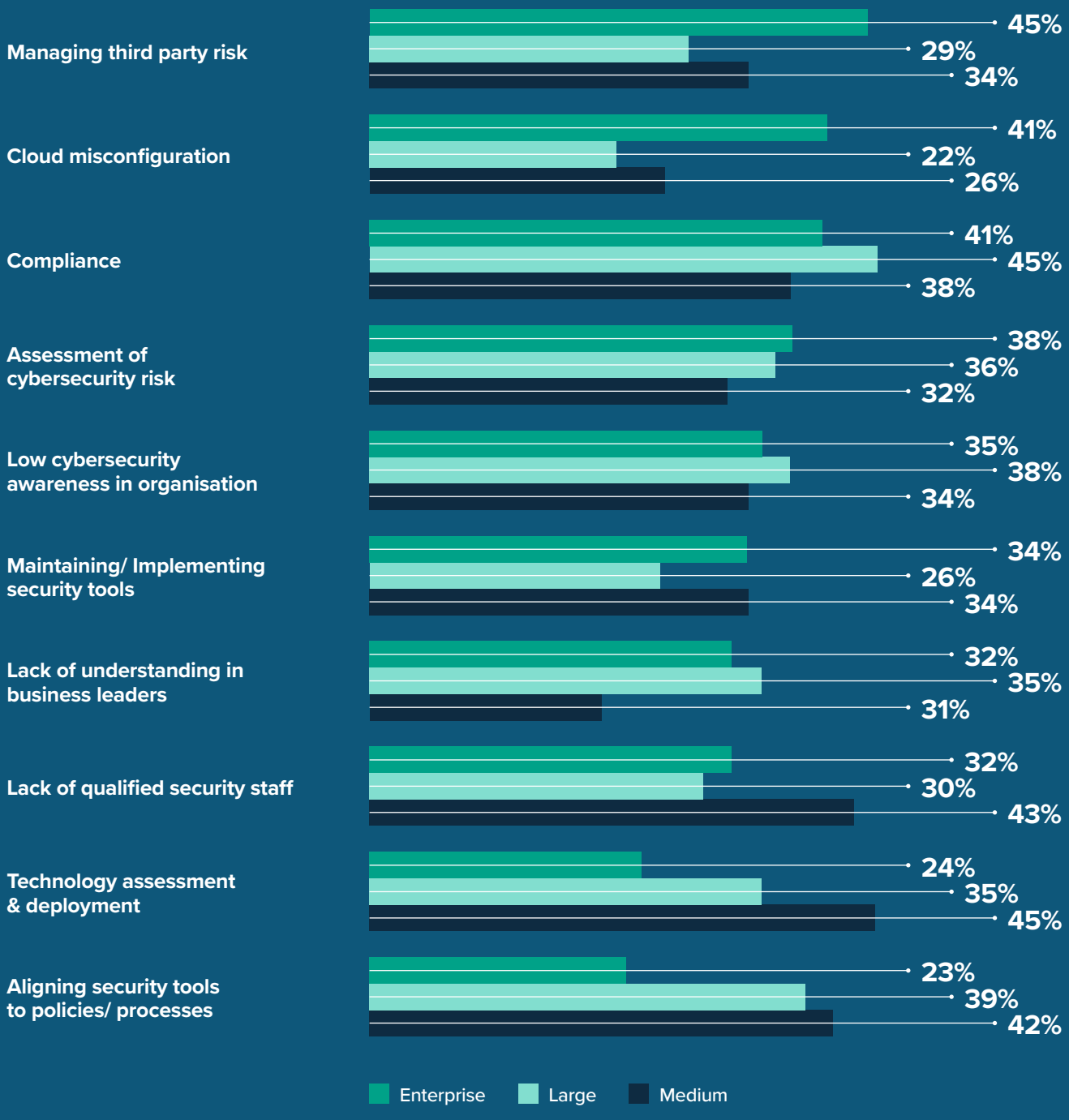
36%
Managing third party risk

There are numerous federal and industry cybersecurity guidelines that organisations have to follow in Australia. As regulators evolve their guidelines and mandates, they are placing greater accountability on companies to secure their IT environments and to protect their customers, particularly in industries such as the Financial Services and Healthcare. Companies will increasingly turn to automated cybersecurity processes to comply with the regulations, particularly given the ongoing cybersecurity skills shortages in Australia.

These challenges that organisations face are made worse by insufficient awareness on cyber risks among business leaders. For example, too often, customers, employees and third parties fall prey to phishing attacks leading to devastating breaches, or they fail to adhere to guidelines on customer personal information protection. Finding ways of improving awareness and changing behaviour is an enormous human challenge. Understanding a company's own risks, the gaps in its posture and closing those gaps is also an increasingly complex and dynamic activity – as is finding skills to minimise digital risk as much as possible.

FIGURE 4:

Cybersecurity Challenges Vary Vastly with the Size of Organisation



Q: What are your organisation's TOP 5 cybersecurity challenges?

Source: Ecosystm-Fastly Cybersecurity Maturity Study, 2022

N=204

There are clear differences in what organisations find most challenging based on their size. While smaller organisations find skills shortage; technology assessment and deployment; and aligning technology policies and processes particularly challenging, large enterprises are challenged more by third party risks, cloud misconfiguration and compliance.

Current Cybersecurity Controls are Inadequate

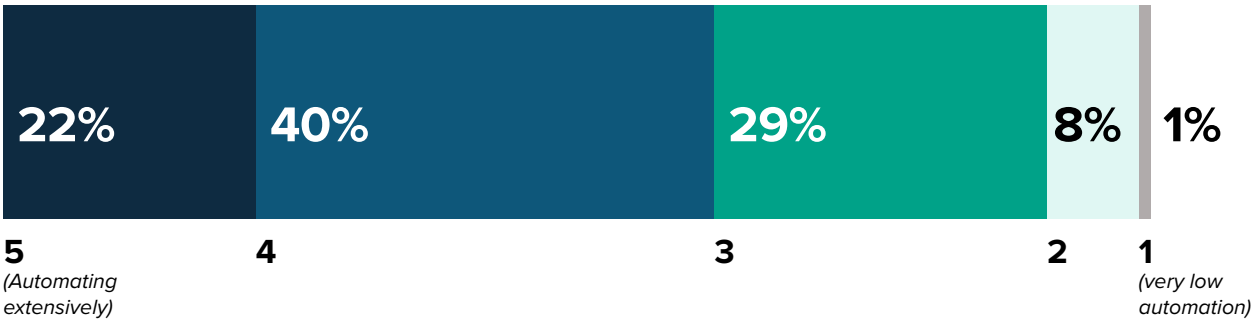
Against a backdrop of extended disruption and increased cybersecurity risks, current defences are proving to be inadequate.

The traditional network infrastructure model of centralised corporate data centres secured by on-premises network perimeters does not work today. Data that once resided in data centres is now in the cloud, on SaaS applications, and on endpoints.

Traditional security controls struggle to deploy sufficient automation to instantly detect, monitor, and secure changes within clouds. The dynamic nature of the cloud makes integration with traditional security solutions difficult, and sometimes impossible – every time there is a change in cloud service requirement, a new security gap can emerge. Bridging these gaps to reduce risk exposure requires automation. And more than 60% of organisations in Australia place a high degree of importance on automation of cybersecurity processes (Figure 5).

FIGURE 5:

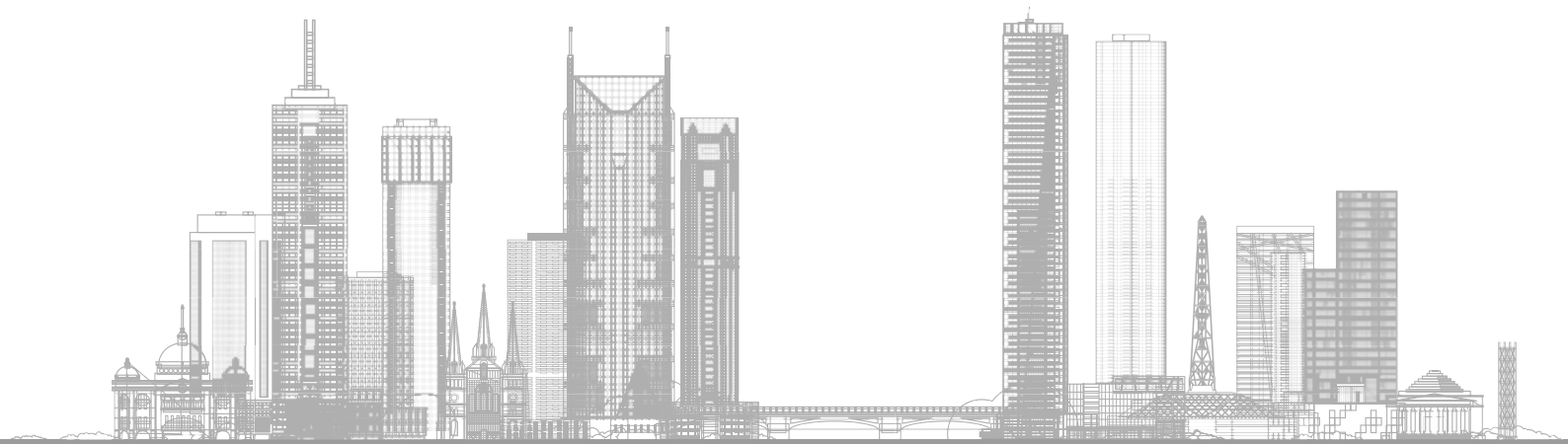
Australian Organisations Place High Importance on Cybersecurity Automation



Q: To what extent is your organisation automating cybersecurity processes?

Source: Ecosystm-Fastly Cybersecurity Maturity Study, 2022

N=204

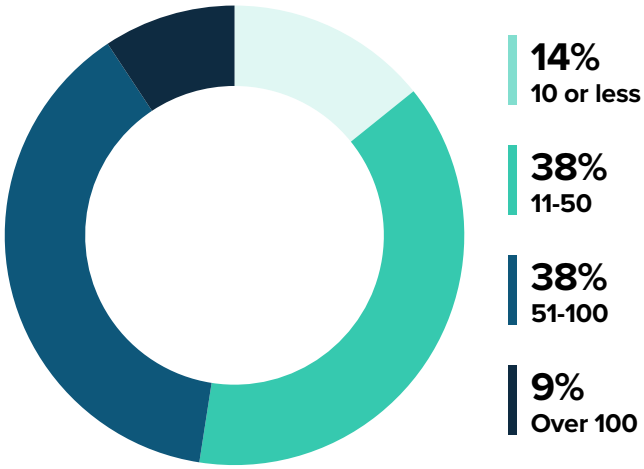


As cloud adoption increases, nearly half of Australian companies have more than 50 cybersecurity tools – which adds to the complexity of the cyber measures.

In addition to greater automation, a typical response by decision-makers to the increasing complexity of their technology environments is to deploy additional new security solutions (Figure 6) where existing tools can't always detect new and emerging threats.

FIGURE 6:

Australian Organisations Deploy a Number of Cybersecurity Tools



Q: How many security tools are in operation within your company's infrastructure to secure cloud(s)?

Source: Ecosystm-Fastly Cybersecurity Maturity Study, 2022

N=204

While on the surface an increase in automation and the number of tools being used appear as good signs, they might in fact be adding to the complexity and challenges! Having multiple, discrete tools means having to manage the high volume of alerts – and dealing with the false positives. If these tools are not integrated on one unified platform, cybersecurity teams have an estate of siloed security products, each reporting to its own dashboard. There is often no provision for the centralisation of security alerts, with cybersecurity staff facing the challenge of monitoring multiple consoles and cross-referencing between disparate screens and information formats.

How Can Today's Cybersecurity Threats be Addressed?

Adaptive Cybersecurity Posture, Combined with Continuous Monitoring to Address Threats

Risks are growing in frequency and impact which highlights the need for a more adaptive and agile approach to cybersecurity. To achieve greater cybersecurity resiliency, organisations need a concrete understanding of their current posture, which can be achieved by a compromise assessment performed by reputable third-party security consulting firms. These assessments can:

1. Determine if the organisation has already been compromised. Assessment might reveal that attackers have already successfully breached the environment. Experienced security consulting firms can devise remediation strategies and, if possible, prevent further damage.
2. Complete an analysis to prevent attackers from stealing customer data, intellectual property, or financial assets.
3. Identify existing security practices that are putting organisations at further risk, including ineffective policies or tooling.

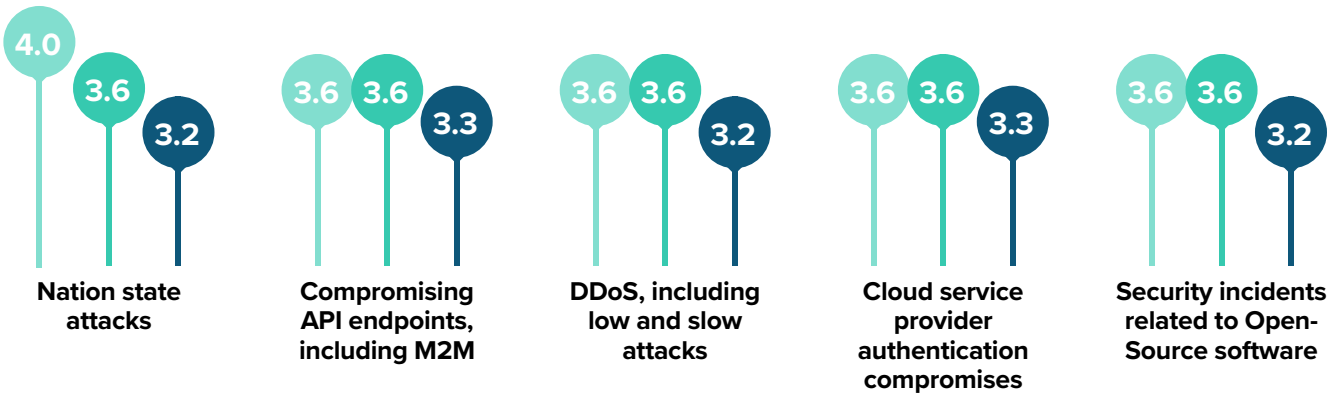
This provides an understanding of where they are in mitigating these risks and identifying gaps in their current measures.

When asked to rate what organisations consider to be their leading risks, we see differences by company size. Recent geo-political activities, including the conflict in Ukraine, have caused nation state attacks to be considered as the greatest risk by larger companies. Compromised API endpoints, DDoS attacks, cloud authentication compromises and open-source vulnerabilities are rated as leading risks by most Australian companies (Figure 7).

FIGURE 7:

How Australian Organisations Rate their Risks*

**Rated on a scale of 1-5 where 1=very low risk and 5=extremely high. Data represents average rating by all respondents.*



Q: Please indicate how high you consider the risk from the following threats to be

Source: Ecosystm-Fastly Cybersecurity Maturity Study, 2022

N=204

Malicious actors keep pounding corporate IT with credential theft, ransomware, and DDoS attacks. With all the sensitive data collected, transmitted, processed, and stored, companies need to continually evaluate their cybersecurity posture, ensure that it is adaptable and seek to make their postures more mature.

Addressing these risks will involve a variety of controls and configurations, especially as the threat landscape continues to evolve. Organisations need to find ways to:

1. Automate as many of their cybersecurity controls as possible. An example is to leverage modern web application firewalls (WAF) to automatically block abusive traffic when defined thresholds for key application functions are met.
2. Continually assess risk and adjust controls accordingly.
3. Gain visibility across all of their assets deployed and operating in their infrastructure.

Anticipating threats before they happen and responding instantly when attacks occur is critical to modern cybersecurity postures. It is equally important to be able to rapidly adapt to changing regulations. Companies need to move towards a position where monitoring is continuous, and postures can adapt, based on risks to the business and regulatory requirements. This approach requires security controls to automatically sense, detect, react, and respond to access requests, authentication needs, and outside and inside threats, and meet regulatory requirements. It needs to be enabled by detection technologies that are effective in production environments. Ideally, security tooling should integrate with DevOps tools and processes to power rapid release cycles. They should also integrate either natively or via API with security information and event management technology (SIEM) and security orchestration, automation and response (SOAR) tools so security teams can access reporting and alerts in the tools they already use.

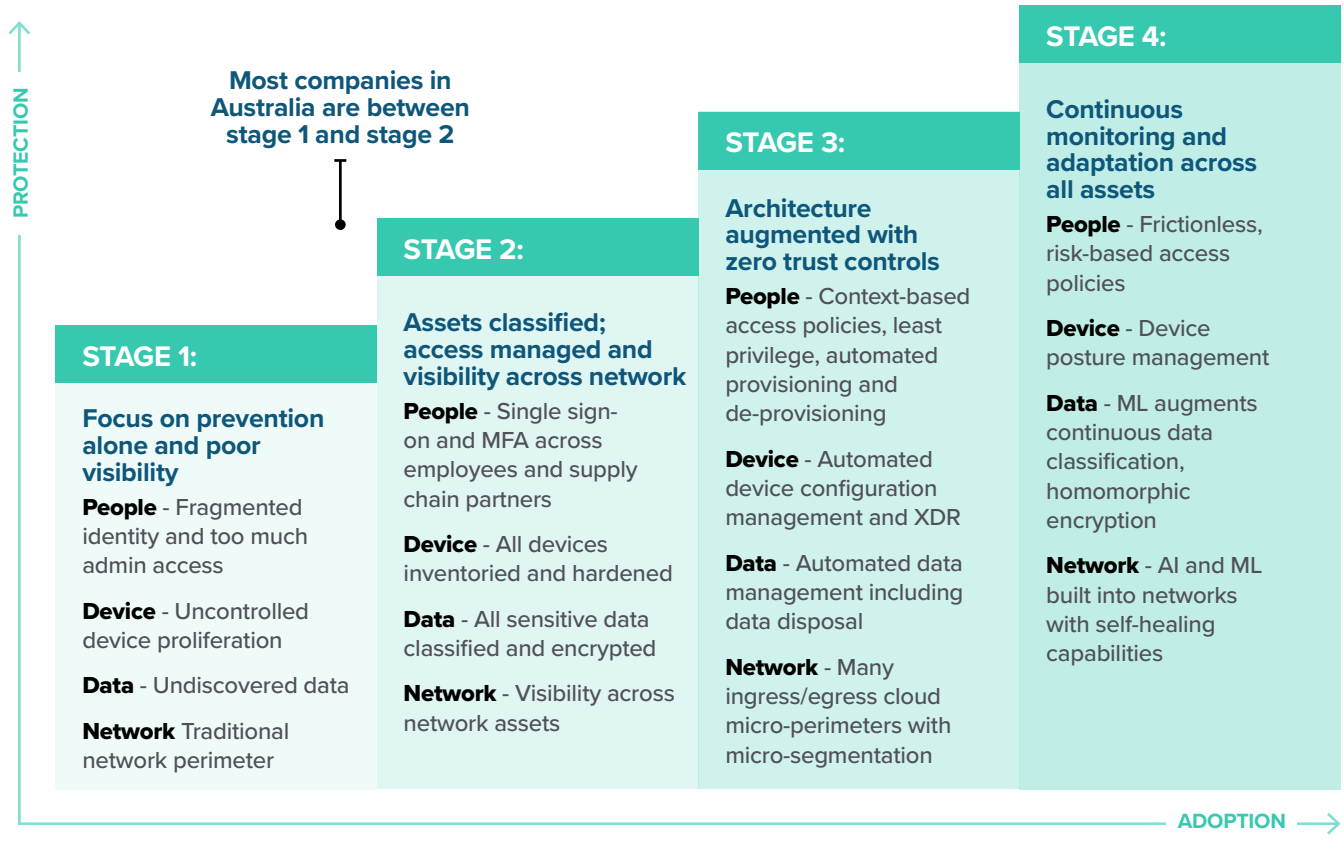
What Can Organisations do to Advance on the Journey to Cyber Maturity?

Cyber Maturity of Australian Companies is Low

Over 60% of Australian companies exhibit a low level of maturity in at least one of the 4 categories in the maturity assessment.

There is a need today to develop a cyber maturity model that is based on existing models, and yet reflects current market needs, given the rapid shifts that organisations have had to make in the last two years and the expansion of the threat landscape. As business leaders increasingly become key stakeholders in an organisation's cyber strategy, we have designed a model specifically for them. Cyber maturity can be assessed by breaking cybersecurity controls into four categories, assessing maturity for each one and then aggregating levels of maturity for these categories – People, Devices, Data and Networks (Figure 8).

FIGURE 8:
The Cyber Maturity Journey



Model based on the responses to multiple questions, ongoing Ecosystm research and the analyst's market insights

Source: Ecosystm-Fastly Cybersecurity Maturity Study, 2022

N=204

The study reveals that too high a percentage of Australian companies either fail to classify their data or have not embraced critical access controls. For this reason, the majority of Australian organisations sit between stages 1 and 2.

This makes them vulnerable to a complex and dynamic threat and regulatory environment. They need to address these gaps urgently and gain much better visibility across their systems and networks.

#1 PEOPLE
Focus on Identity and Access Management (IAM) and enforcing the principle of least privilege.

Most breaches involve the compromise of IT and business user credentials such as IDs and passwords. Attackers with possession of these credentials gain access to the systems and networks of their victims and, often move laterally. IAM is an essential way of mitigating the risk of unauthorised access.

Increased cloud integration and the proliferation of digital identities require increased focus on securing identities and making customer experience seamless. As public cloud infrastructure is more widely used, user identity management issues related to over-assignment of entitlements and a lack of visibility into those existing permissions are threats. Another major concern is the explosion in 'non-human' identities, such as applications, virtual machines, containers, serverless functions, and others. Gaining visibility across all these identities can be a major challenge.

Over one third of Australia companies have immature cybersecurity postures from a people and access perspective – they either give indiscriminate admin access or have fragmented identities.

#2 DEVICE
Focus on limiting the expanded attack surface caused by the proliferation of endpoints and reducing the likelihood of device compromise.

Remote working has enabled business operations to continue in a time of extreme disruption, but it does expose businesses to many more threats. The increased number of endpoints inevitably expands the attack surface and exposes companies to new vulnerabilities. Often companies are not aware of the status of devices accessing their resources. Companies need visibility across all corporate devices and to apply strict risk-based access controls to non-managed devices.

While Australian companies are more advanced on their device security journey than on other categories, 15% have still not identified all employee devices that access their company resources.

Policies must be triggered in real time, based on access authentication and other customisable attributes. For example, a new IoT device with outbound internet access must be identified and automatically assigned to a restricted network segment. Devices must be continually assessed while they are on the network, and each time they start and finish a session. These assessments should analyse device health and context in real time and initiate necessary actions such as re-scanning for vulnerabilities and indicators of compromise. Ideally, network traffic is isolated in the cloud where content is visible but never downloaded to endpoints.

#3 NETWORK

Focus on the segmentation and isolation of resources to limit the impact of a breach.

Network segmentation is a more common approach to security as companies assume that breaches are inevitable and seek to limit damage caused by attacks. It involves dividing a computer network into smaller physical or logical components. It is one of the best mitigations against attacks. This limits the ability of malware or attackers remotely accessing the network to move laterally.

Segmentation can also be based on device type. For example, IoT devices can be placed on their own network partition to increase security. In the healthcare sector, medical devices such as MRI machines might be separated from the rest of the network. Different approaches to segmentation can be blended, depending on requirements.

Companies are adopting other approaches like micro-segmentation. This approach decouples the enforcement of segmentation policies from the physical network, allowing more granular control and simpler, more flexible administration. The end game is to protect each workload with its own micro-perimeter making lateral movement almost impossible.

18% of Australian companies say that they still have traditional ‘castle and moat’ defences.

#4 DATA
Focus on the classification, categorisation and encryption of corporate data.

Different levels of protection are then applied to data, based on sensitivity and value. Once categorised, data can be isolated from everyone except those that need access. But, step one is to classify data. Classifying data is a necessary activity for any credible cybersecurity posture. Not classifying data not only means that organisations are unlikely to be compliant with key regulations but that they are also not in a position to know what to protect and how to protect it.

Data visibility is also essential so that anomalous patterns of data usage can be identified rapidly. Visibility of data in all business ecosystems makes it easier to quickly detect breaches and contain them. This involves building capabilities for visibility into the interaction between users, applications, and data across all policy enforcement across all of these devices.

Advancing further on the cyber maturity journey requires existing security controls to be augmented with zero trust controls. The zero trust model is location-independent security based on cryptography, authentication, and certificate management. Organisations with a strong security are more likely to be implementing these kinds of controls. Greater cyber maturity can be built by continually monitoring all data traversing all systems, networks and endpoints while continuously adapting cybersecurity postures to address changing threats, technology mixes, and regulations. In this ideal state, the damage caused by breaches is limited and incident response is automated. Importantly additional controls do not impact experience – they are invisible to users.

25% of Australian companies have not classified most of the data that they use.

Conclusion

The cyber maturity of Australian companies remains low. Given the increase in frequency and impact of attacks, Australian companies need to assess their existing controls and seek more mature postures which can offer greater risk mitigation.

Typically, Australian companies have already invested heavily in cybersecurity controls. But these investments are commonly focused only on preventing breaches; have limited access controls; and are often designed based on an assumption that sensitive data is accessed from office locations.

Increased digital engagement, widespread remote working, and greater use of IoT expand attack surfaces and expose many cybersecurity postures as inadequate. Companies are often combating threats with multiple cybersecurity tools, often with separate dashboards. Too many false positives are generated across these tools, which often require manual intervention. Greater automation and interoperability between tools are urgently required to take the pressure off SOCs and to address the burgeoning cybersecurity skills shortages.

These challenges can be addressed by gradually developing a cybersecurity posture which allows continuous monitoring of internal assets, combined with the ability to adapt to changing threat and regulatory environments.

Progressing on the cyber maturity journey is not easy. Perhaps now is the time for companies to step back, assess their risks and current controls, identify the gaps and put people and processes in place that can implement an adaptable posture that aligns with the new distributed technology environments. Cybersecurity technology investments should come after a desired set of cybersecurity policies and processes have been determined. After all, the role of technology is to implement these policies and processes. Too often, companies buy technology reactively when they encounter a threat and pay insufficient attention to policies, people and processes.

About the Study

This Ecosystm study represents the views of 204 cybersecurity decision-makers in Australia. The study was commissioned by Fastly and conducted in April-May 2022.

By organisation size

26%
Medium
(100-499) employees

38%
Large
(500-999 employees)

36%
Enterprise
(More than 1,000 employees)

By job roles

25%
CISO/CIO

15%
VP IT/ VP Security

54%
Director IT/ Security Director

6%
IT Manager

This whitepaper is sponsored by Fastly. The data presented is based on the findings of Ecosystm-Fastly State of Digital Brand Study conducted by Ecosystm on behalf of Fastly. The paper is also based on the analyst's subject matter expertise in the area of coverage in addition to specific research based on interactions with technology buyers from multiple industries and technology vendors, industry events, and secondary research.

About the Author

Andrew Milroy

PRINCIPAL ADVISOR ECOSYSTM

Andrew Milroy is a well-known and respected thought leader and speaker in the APAC region.

With more than two decades of experience in the technology sector, Andrew has worked with clients in a variety of tech domains including cybersecurity, cloud computing, IoT, blockchain, service provider strategies, and customer experience. His most recent work has been focused on the current challenges in technology markets, cybersecurity and digital transformation.

Since moving to Singapore in 2011, he has held regional leadership roles with Frost & Sullivan and Ovum (now Omdia). Prior to working in Singapore, Andrew gained invaluable technology knowledge and insights while working in Europe, the United States, and Australia.

Andrew is frequently invited to speak, chair and moderate at major technology events. He is also widely quoted on the global broadcast media, including BBC, CNBC, Bloomberg and Channel News Asia.

Andrew has a BSc from Newcastle University (UK), an MA from Middlesex University (UK) and an MBA from MGSM (Australia). Andrew is a long suffering Sheffield United supporter and enjoys hiking and running in his spare time.

About Fastly

Fastly is upgrading the internet experience to give people and organisations more control, faster content, and more dynamic applications. By combining the world's fastest global edge cloud network with powerful software, Fastly helps customers develop, deliver, and secure modern distributed applications and compelling digital experiences. Fastly's customers include many of the world's most prominent companies, including Pinterest, The New York Times, and GitHub. Australia and New Zealand customers include Freelancer, Kogan, Linktree, Nine, NRL, Radio New Zealand, Seven Network, Trademe and Vodafone. For more information on our mission and products, visit https://www.fastly.com.

About Ecosystm

Ecosystm is a Digital Research and Advisory Company with its global headquarters in Singapore. We bring together tech buyers, tech vendors and analysts onto one integrated platform to enable the best decision-making in the evolving digital economy. Ecosystm has moved away from the highly inefficient business models of traditional research firms and instead focuses on research democratisation, with an emphasis on accessibility, transparency, and autonomy.

Ecosystm's research originates from its proprietary "Peer-2-Peer" platform which allows Tech Buyers to benchmark their organisation in "real-time" against their industry or market peers. Ecosystm's broad portfolio of advisory services is provided by a team of Analysts from a variety of backgrounds that include career analysts, CIOs and business leaders, and domain experts with decades of experience in their field.