dimension data

accelerate
your ambition

2018 Global Threat Intelligence Report

Executive Guide

Australia

Cybersecurity insights for protecting your digital business

Insights
Driven by data

Contents

1. Foreword

In 2017, the World Economic Forum rated cybersecurity as one of the top risks facing the world today. Independently, business leaders reprioritised cybersecurity as a strategic initiative demanding further focus and investment. It remained top of mind and garnered significant media attention, as cybercriminals showed how easy it is to disrupt digital business while continuing to adapt their tradecraft to target specific business, industry, and geographic profiles.

Education was the most attacked sector in Australia. The technology sector moves into second position. A shift from previous years.

Attractive and lucrative in its ability to generate profits with minimal risk of attribution or interdiction, cybercrime is a pervasive threat. Diversification of illicit subscription services, automated software toolkits, and vast online criminal support forums are reducing barriers to entry. Cybercriminal ingenuity continues to mature, making the most of attack opportunities arising from new technology adoption.

The relentless evolution of the threat landscape places the onus on businesses to innovate more rapidly than their adversaries. Cyber-awareness from the top down is imperative if the business, clients, and employees are to be protected.

Also, protecting a network from compromise upfront is far less costly than dealing with post-event financial repercussions, reputational damage, legal ramifications, regulatory penalties, and breach recovery costs.

In this Executive's Guide to the 2018 NTT Security Global Threat Intelligence Report, for Australia, we highlight findings that will help you make investment decisions aligned with your industry sector, geographic profile, and risk appetite.

As part of NTT Group, we have extensive visibility into global traffic and threats faced by thousands of clients across many industries. Our security experts analyse millions of attacks each year using data gathered by our global security operations centres and research facilities.

This Guide also looks into the future, covering emerging trends such as ransomware, threat intelligence, industry targeting, and compliance regulations.

For Dimension Data, cybersecurity is at the centre of what we do, how we think, and how we accelerate our clients' ambitions. We urge you to consider security's enabling role in meeting mission-critical objectives and driving sustainable business value, providing the certainty needed in an otherwise disruptive world.

NTT Security

Mark Thomas

Group CTO Cybersecurity, Dimension Data

For the past 16 years, Mark has worked in the cybersecurity field, establishing pragmatic, business-aligned risk minimisation strategies and developing intelligence-led computer network defences. His broad knowledge and in-depth expertise result from extensive engagements in Consulting, Technical, and Managed Services with large enterprises across numerous industry sectors including finance, government, utilities, retail, and education.

2. Eight key insights into the global cybersecurity landscape

The cyberworld continues to expand, converging information and operational technology (IT and OT), industrial controls (ICS), and the Internet of Things (IoT) into an ever-evolving technology ecosystem across hybrid infrastructures: on-premise, cloud, and mobile.

1. Finance tops ‘most targeted sector’ list

Fast-paced adoption of disruptive technologies and expanding digital footprints motivate adversaries to routinely conduct automated reconnaissance to uncover potential infrastructure and application vulnerabilities. **Rising technology adoption places this sector at elevated risk**.

Adequate response demands focus **on patch and vulnerability management, advanced endpoint protection, and identity-driven controls.**

2. Supply chain risks catch digital businesses off-guard

Cybercriminals prioritise the supply chain. As business ecosystems grow, and data and applications migrate to hybrid environments, they expand adversaries’ options for compromising business through indirect means.

For this reason, the business and professional services sector is one of the top five attacked sectors globally, ranking third overall. **It’s a prime target for trade secrets and intellectual property theft, potentially exposing customer and business partner data or credentials**.

This emphasises the need for **third-party supply chain risk management, adoption of best practice standards, risk frameworks, and assurance practices.**

3. Ransomware: the cybercriminals’ weapon of choice

Globally increasing by 350% in 2017, ransomware represents 7% of total malware – up from 1% last year. Many organisations fell victim to financially motivated crime via ongoing outbreaks, attracting significant media attention. **Leaked classified government hacking tools have made ransomware even more dangerous**, enabling greater attack and tooling sophistication. The persistence and relentlessness of cyber-adversary campaigns indicate that ransomware popularity and prevalence will continue.

Rethink your approach **to backup and recovery to avoid the risks of ransomware.**

4. Ransomware morphs to become destructive

As ransomware evolves, cybercriminals use social engineering as a core technique to search for exploitable vulnerabilities, with destructive malware masquerading as ransomware. Adversary campaigns have expanded into the supply chain. **Widespread infection by the NotPetya virus was the first observed destructive malware masquerading as ransomware**.

Encourage employees to be suspicious **of received emails, particularly those asking them to open attached documents or click on weblinks.**

5. Technology sector targeted for IP

The technology sector's significant intellectual property is a prime target for competitive advantage, making the sector the second most attacked, globally. It's in the top five across all regions, signalling a shift in adversary intentions.

The sector tends to accept more risk in pursuit of greater innovation, open collaboration, and business opportunities created by being first-to-market. This inherently exposes infrastructure to vulnerability. Failure to embed cybersecurity in organisational culture and business processes will impact productivity and business profitability.

Prioritise investment in network security policies and technology controls **to support risk reductions.**

6. Manufacturing and operational technology in line of fire

Manufacturing ranks fourth for attacked sectors globally. **The line between traditional and digital forms of manufacturing has begun to blur, creating a unique landscape where high-value manufacturing and advanced technologies are key for global competitiveness**.

Once isolated systems are now converging via OT, IOT, cloud computing, and data sharing expanding into supply chains and other business ecosystems. The attack surface has widened. Smart factor cyber-physical systems are exposed to greater risk. The sector is at high risk of intellectual property and trade secrets theft, sabotage of processes and output, extortion and disruption of computing resources.

Identify threats and risks **across multifaceted, distributed architectures, including on-premise, cloud, and hybrid environments. Ensure that your detection and incident response capabilities are robust.**

7. The balance between compliance and cybersecurity remains challenging

With standards groups, industries, and governments constantly implementing new and revised policies, many organisations struggle to achieve an optimal balance between operational security and compliance.

Compliance pressure grew with the introduction in 2017 of the General Data Protection Regulation (GDPR) in Europe, Middle East & Africa and the Notifiable Data Breach (NDB) scheme In Australia in 2018. **Companies must notify individuals whose personal information is involved in a data breach that's likely to result in serious harm**.

Embrace compliance **without detriment to other security initiatives. Falling behind on patch management or regular backups can undermine compliance.**

8. Improved user awareness drives incident response maturity

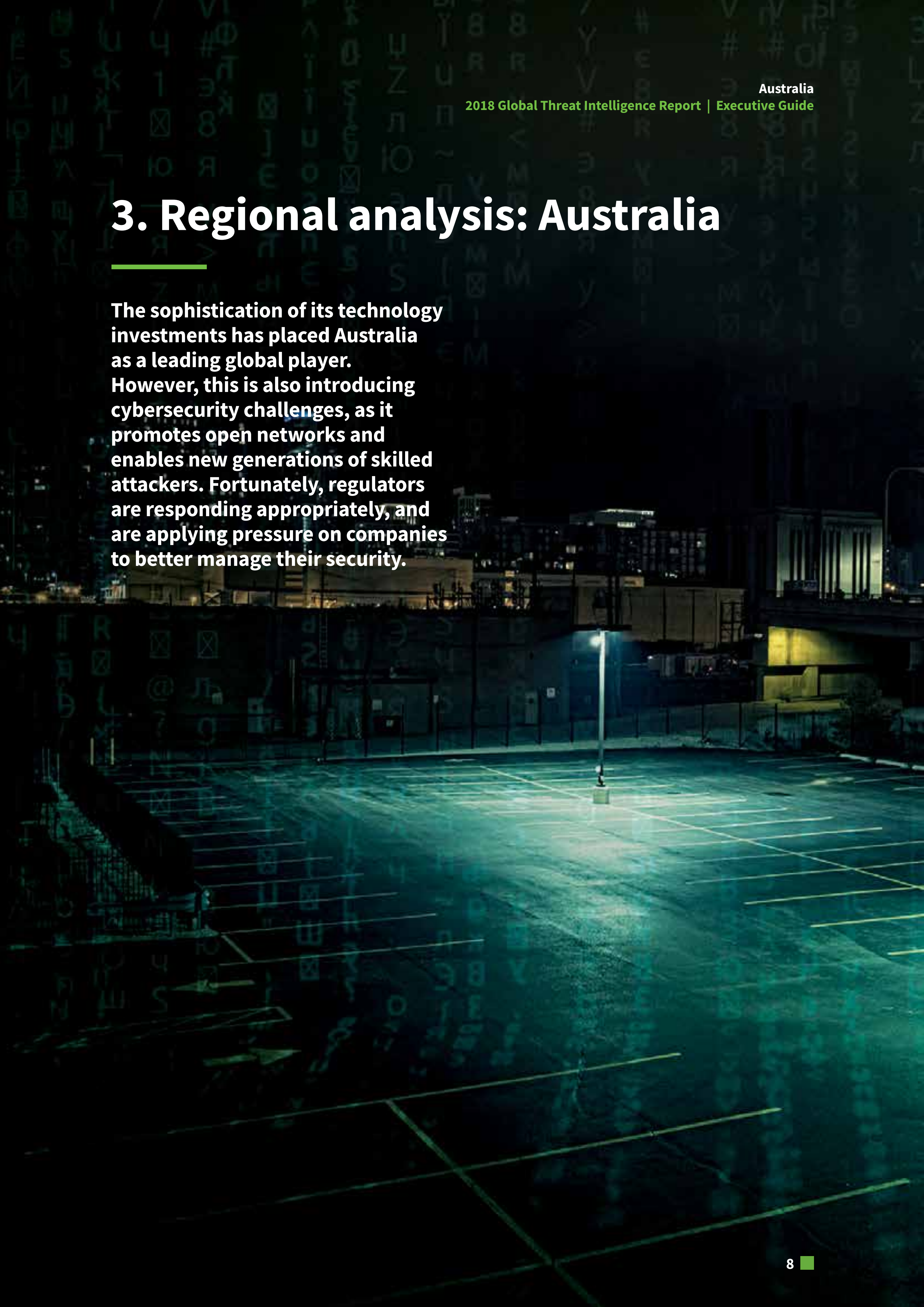
Ransomware-related incident response outsourced engagements dropped sharply from 22% in 2016 to 5% in 2017, despite accelerated ransomware infection rates globally.

Organisations have improved their in-house ability to prevent and respond to attacks through continued investments in endpoint controls, incident response playbooks, and backup and recovery plans.

Establish a predictive environment with a disaster recovery plan **that allows you to identify and isolate uncompromised critical data and ensure complete recovery.**

3. Regional analysis: Australia

The sophistication of its technology investments has placed Australia as a leading global player. However, this is also introducing cybersecurity challenges, as it promotes open networks and enables new generations of skilled attackers. Fortunately, regulators are responding appropriately, and are applying pressure on companies to better manage their security.



Favoured target for cybercriminals

Australia is a financial and geo-political giant, closely aligned to several Western nations, including the US, Canada, New Zealand and the UK (Five Eyes). As a result, it's a favoured target for cyber criminals.

Increases of breaches of businesses and state entities led to the passing of the Australian Privacy Amendment (Notifiable Data Breaches or NDB) Act in February 2017, and its enactment a year later. This Act carries stiff penalties for companies and even individuals within a business that fail to disclose a breach of their systems.

The prospect of hefty fines is one deterrent, while the public embarrassment and brand damage when a breach is revealed is another. Forcing companies to disclose if they've been successfully attacked by cybercriminals is elevating the cybersecurity conversation to the board level. The NDB Act will also spur more investment into security technology adoption, ensure the right balance and risk assurance, and re-instil customers' faith. If your company isn't yet dealing with security as part of its high-level strategy, we recommend making it an immediate priority.

Education a prime target

In the last year, the **education sector topped the list of attacked industries in Australia (26%)**.

Figure 1: Top industries attacked in Australia

Top industries attack - Australia	Percentage
Education sector	26%
Technology sector	17%
Finance sector	13%
Government sector	13%
Manufacturing sector	12%

Educational institutions should be on particularly high alert in this region. Increased levels of attacks are likely due to the move towards more collaborative environments inside and among facilities such as universities, colleges, and schools.

Open networks have become commonplace on Australian campuses, but that ubiquity makes them alluring targets for cybercriminals – especially since higher learning institutions often possess sensitive company and state information. When networks are open, security tends to be quite lax, which provides an ideal environment for low-risk-high-reward cyberattacks.

Australia as an attack source

While Australia is a frequent target, it's also a major source of attacks. In the last year, 57% of cyberattacks in the Asia Pacific (APAC) region originated from Australia, the USA, and China. A staggering 66% of attacks on the financial sector in APAC originate from Australia.

These attacks are generally sophisticated and target services, applications, and web applications.

The table below illustrates the types of attacks most commonly perpetrated in this region:

Figure 2: Types of attacks most commonly perpetrated in Australia

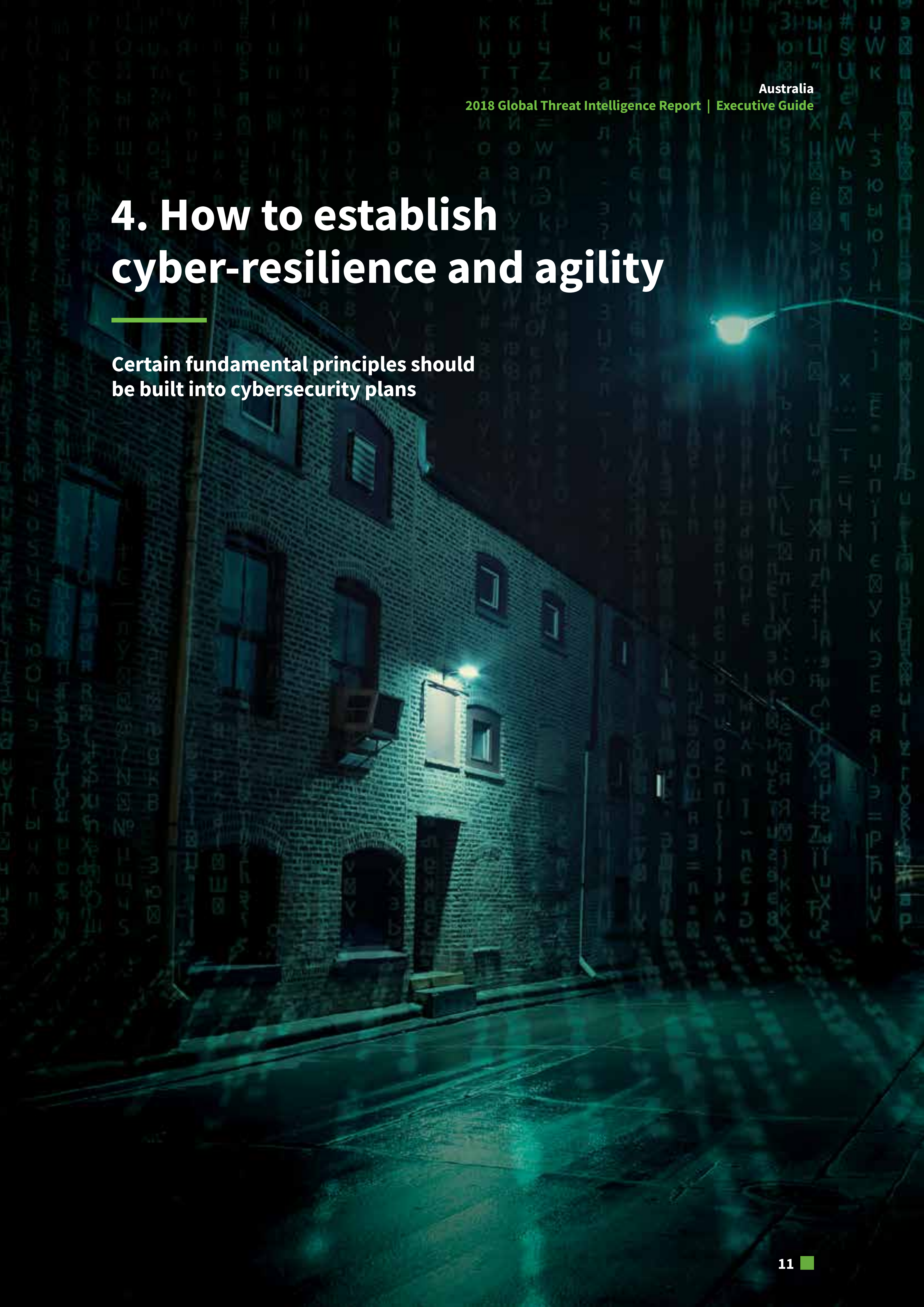
Australia	Percentage
Service-specific attack	28%
Brute forcing	25%
Application-specific attack	14%
Network manipulation	8%
Reconnaissance	5%
DoS / DDoS	4%
OS specific exploit	2%
Known bad source	0%
Evasion attempts	0%
Baiting / social engineering	0%

This isn't surprising, given Australia's advanced adoption of technology. It has many skilled technology professionals and countless budding ones. This assures that the country will remain a massive target – and continued haven – for cyberattacks.

In conclusion

To raise their defences, we recommend that organisations:

- understand the NDB scheme and its implications for your business and customers
- realise that they're now one of the most attractive targets for cybercriminals
- make cybersecurity part of the company's high-level business strategy, if they've not done so already
- embed cybersecurity culture across the organisation to improve employees' situational awareness
- reduce the attack surface by investing in improved vulnerability management practices



4. How to establish cyber-resilience and agility

Certain fundamental principles should be built into cybersecurity plans

Embed cybersecurity into the core business strategy

Cybersecurity must be core to and aligned with business strategy. It needs to be enabled by default and embedded across technology stacks by design. It must begin from a project's inception and be continuously validated across its lifecycle, thereby reducing risk potential and maximising delivery assurance. Organisations inherently gain greater understanding of the risks they face, embrace the innovation needed to counter identified risks, and have the resilience to restore operations in the event of a breach.

Drive security from the top-down and encourage bottom-up reporting

Security is everyone's responsibility. The Board and Executives must demonstrate accountability and support for security across the organisation. Recognise and empower employee vigilance and engagement as an extension of the cybersecurity programme with the power to drive cultural change. Create cybersecurity consciousness. It's far more cost-effective to investigate suspicious or fraudulent activity observed by an employee early on in the attack cycle than to respond after it has occurred.

Mitigate the impact of ransomware

Remain risk-focused. Minimise exposure of data by enforcing 'need to know' policies and implementing data and network segmentation. Prioritise and enforce endpoint hygiene, including acceptable usage policies and end-user training to reduce the likelihood of users running malicious files. Boost monitoring to identify ransomware infections early. Enforce backup strategies and store backups offline. Maintain focus on foundational practices such as patch and vulnerability management, data encryption, and identity and access controls.

Leverage multisourced intelligence

Use threat intelligence to prioritise resources effectively and mitigate threats before they impact your business. Incorporate it into attack and breach simulations to improve cyberdefences and incident management processes.

Outpace adversary sophistication through cybersecurity agility

Cybersecurity must move at the speed of digital business. The attack surface is fed by continuous releases by DevOps of features and application components that expose new vulnerabilities daily, rather than over the much longer release cycles of pre-digital development. Be agile and responsive. Shift resources based on the changing risk landscape and short development cycles.

5. Final word: scaling at pace

The threat landscape is dominated by email phishing threats, exploitable vulnerabilities, and insider actions. Attackers are using macros, scripts, and social engineering methods, finding unpatched vulnerabilities, and compromising access credentials.

They're also using newer methods, such as compromising trusted supply chains, shared infrastructure, source code, and applications, thereby increasing the need for software component validation. Although their methods continue to evolve, attackers still favour the path of least resistance.

Risks are less predictable than before, and attackers are developing more sophisticated ways of breaching defences. This calls for a mature and comprehensive approach to cybersecurity, understanding the risks while gaining buy-in from organisational leaders.

Over the last decade, one observation has remained constant: our adversaries operate on a global level, and we must counter this by investing in the right capabilities across people, process, and technologies to scale at the pace at which cybercriminals operate. With this approach in mind, and considering increasing demands by customers, industry, regulators, and governments, organisations must establish cybersecurity agility to seek competitive advantage.

Global data analysis methodology

Research referenced in the Executive Guide is sourced from The NTT Security 2018 Global Threat Intelligence Report. It contains global attack and incident response data gathered from NTT Security and supported NTT operating companies from 1 October 2016 to 30 September 2017.

The analysis is based on log, event, attack, incident, and vulnerability data from clients. It also includes details from NTT Security research sources, including global honeypots and sandboxes located in over 100 different countries in environments independent from institutional infrastructures.

With visibility into 40 percent of the world's internet traffic, NTT Security summarises data from over 6.1 trillion logs and 150 million attacks for the 2018 GTIR. NTT Security gathers security log, alert, event and attack information, enriches it to provide context, and analyses the contextualised data.

Global Threat Intelligence Center

The NTT Security Global Threat Intelligence Center (GTIC) protects, informs, and educates NTT Security clients through the following activities:

- threat research
- vulnerability research
- detective technologies development
- threat intelligence management
- communication to NTT Group clients

The GTIC combines its threat and vulnerability research with its detective technologies development to produce applied threat intelligence. Its mission is to protect and provide NTT Security clients with the services and tools to prevent and provide early warning notifications of risks and threats 24/7.

Threat intelligence management is where these efforts all come together. The GTIC continuously monitors the global threat landscape for new and emerging threats using NTT's global Internet infrastructure, clouds, and data centres along with third-party intelligence feeds. NTT Security works to understand, analyse, curate, and enrich threat data using advanced analysis techniques and proprietary tools; and publishes and curates them using the Global Threat Intelligence Platform (GTIP), for the benefit of NTT Security clients.

About Dimension Data security

Dimension Data's security business supports organisations in creating an adaptable and predictive security posture across their network, data assets, cloud, applications, and end-user environments. With our wide range of security capabilities, including consulting, and a suite of technical, support, and managed security services, we assist clients through the full security lifecycle.

Founded in 1983, Dimension Data is a USD 8 billion global leader in designing, optimising, and managing today's evolving technology environments. This enables its clients to leverage data in a digital age, turn it into information, and extract insights.

Headquartered in Johannesburg, Dimension Data employs 28,000 people across 47 countries. The company brings together the world's best technology provided by market leaders and niche innovators with the service support that clients need for their businesses – from consulting, technical, and support services to a fully managed service.

Dimension Data is a proud member of the NTT Group.

NTT Group Resources

NTT Security
www.nttsecurity.com

Dimension Data
www.dimensiondata.com

NTT Data
www.nttdataservices.com

NTT Communications
www.ntt.com

NTT-CERT
www.ntt-cert.org.

NTT Innovation Institute
www.ntti3.com

Meeting the challenges of an evolving cybersecurity landscape

With Dimension Data's cybersecurity expertise, you're better prepared to detect and respond to cyberthreats while supporting business innovation and managing risk. We help you to avoid downtime and build an agile and predictive security ecosystem across your users, applications and infrastructure.

Research shows that:

Incident response is 69% faster and repair time 32% faster on networks monitored by Dimension Data. (2016 Network Barometer Report)

Cybersecurity skills are scarce. With NTT Security, we have more than 2,000 cybersecurity specialists supporting clients around the world. Our Managed Security Services leverage our 10 Security Operation Centres and our threat intelligence and analytics to monitor, optimise, operate, and manage your security.

Our solutions span:

- securing your digital workplace
- protecting against ransomware
- securing your hybrid infrastructure
- securing your enterprise applications

Don't know where to start? With our Cybersecurity Advisory, we assess your security posture, identify gaps, and deliver recommendations for improvement.

To learn more about how we can help to protect your digital business, visit our **cybersecurity expertise page**