The bridge to possible

Securing Australia's Critical Infrastructure

Foreword

“Cyber resilience has become one of Australia’s greatest challenges and is critical to the nation’s economic prosperity and security. Australia is the most attacked country in the world per capita from a cyber security perspective and needs to be particularly vigilant. This particularly applies to the nation’s critical infrastructure assets which are a target for potential attackers. These assets include utilities, healthcare systems, supply chains, defence industries and a range of other systems that are fundamental to Australia.

This white paper from Cisco is an important contribution to the national debate about how best to secure critical assets while at the same time taking advantage of the benefits afforded by digitisation. It also highlights the importance of cyber skills as part of the planning and response effort. Australia, like many countries, has forecast a significant shortage in cyber security skills, and it is critical that critical infrastructure operators, government, academia and industry collaborate on this front.

A3C has a critical role to play in terms of cyber skills and helping organisations make better decisions in relation to cyber security. Securing critical infrastructure is becoming more complex, and the stakes have never been higher. Collaborative action is required on a number of fronts, and A3C sees its role as facilitating and fostering linkages across the cyber ecosystem. A3C is proud to partner with the Cisco Networking Academy and to become home to the Secure Critical infrastructure Lab detailed in this paper that showcases world-class security technology capability and is operated by the University of Adelaide and Cisco.”

Mike Barber

Chief Executive Officer
at Australian Cyber Collaboration Centre

A3C

Executive Summary

A cybercrime was reported every eight minutes in Australia in 2020-21[1]

Australian organisations have become a global target for cyberattacks from nation-states, state-sponsored actors and transnational cybercrime syndicates. The frequency, scale and severity of attacks are intensifying, as is the sophistication and resourcing of attackers. The pandemic contributed to the 13% reported annual increase in several ways, including the high number of people working and learning from home.

Attacks

67,500
cybercrimes reported in 2020-21

13%
increase in reported cybercrimes in 2020-21

Australian Cyber Security Centre, 2021

Layers of complexity thwart cybersecurity efforts

Technical

- Proliferation of devices
- Multi-cloud environments
- Securing the entire stack

Operational

- Balancing Confidentiality, Integrity and Availability
- Ensuring availability of OT

Policy and regulatory

- Data sovereignty
- Data framework
- Privacy

Skills

1.8M
Global cyber security workforce gap by 2022

Frost & Sullivan, 2017

60%
Organisations in ANZ that find recruiting cyber talent "difficult" or "very difficult"

Hays, 2020

$33B

33B self-reported losses from cybercrime in Australia

Australian Cyber Security Centre, 2021

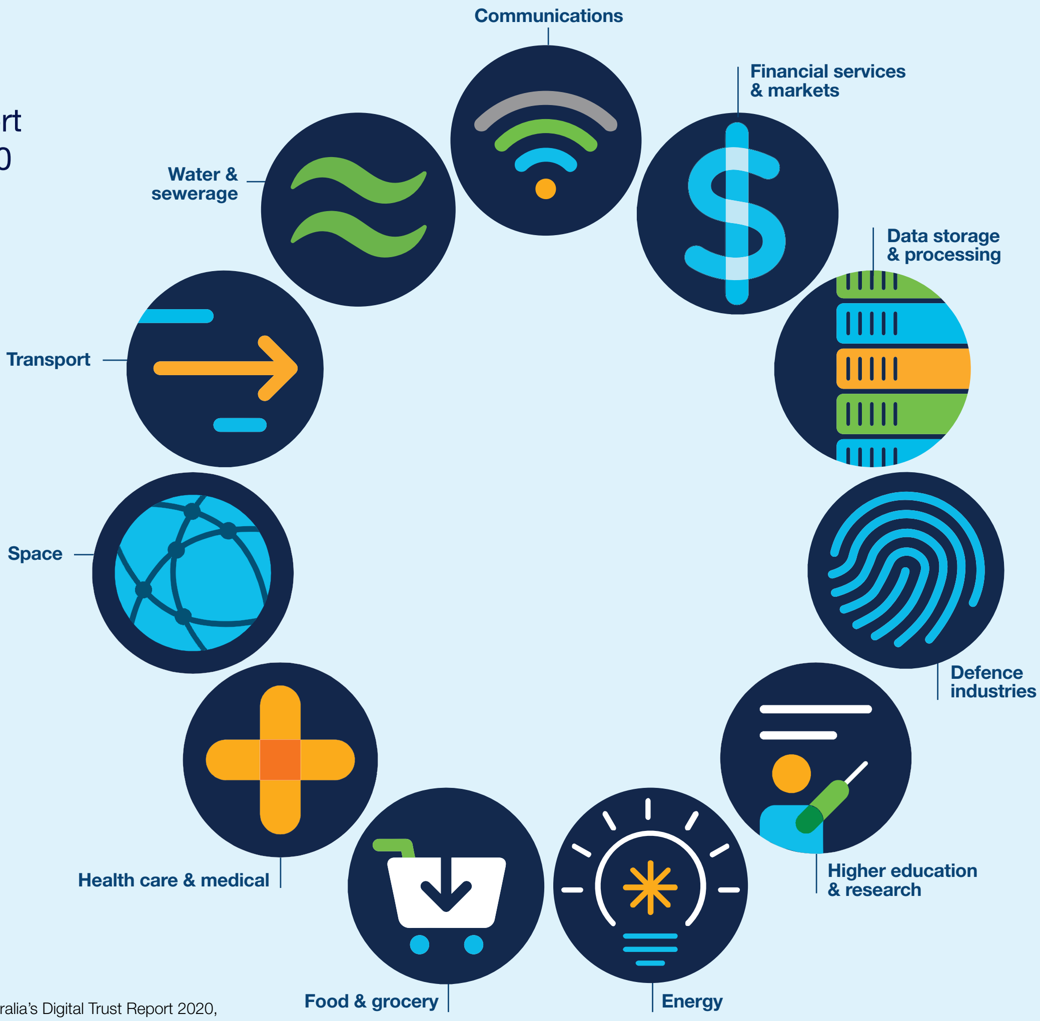
Critical infrastructure is a prime target for attackers looking to disrupt

Critical infrastructure is defined as "those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period would impact on the wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security".[2]

Approximately a quarter of all cyber incidents reported to the Australian Cyber Security Centre during the 2020-21 reporting period were associated with Australia's critical infrastructure or essential services.[3] This means an essential service or critical infrastructure was attacked every 32 minutes. Successful attacks on critical infrastructure assets likely cost the Australian economy billions of dollars, with the biggest economic costs stemming from loss of business continuity. Cyber security is one of the biggest risks facing critical infrastructure owners and operators.

The Australian Government has imposed more obligations on operators of Critical Infrastructure and Systems of National Significance (CISONS) to secure assets.

- The disruption to a a single port could cost $100 million per day.
- A national disruption could displace up to 163,000 jobs and cost $30 billion over four-weeks


Communications
Financial services & markets
Data storage & processing
Defence industries
Higher education & research
Energy
Food & grocery
Health care & medical
Space
Transport
Water & sewerage

Source: AustCyber (2020), Australia's Digital Trust Report 2020, available at https://www.austcyber.com/resource/digitaltrustreport2020

The data network is the first line of defence against cyber aggressors

Identity and networks are the foundations of digital trust and the core technology platform for sustained cyber resilience. Networks connect and manage computing devices (such as laptops, desktops, servers, smartphones and tablets) and an ever-expanding array of industrial Internet of Things devices that communicate with one another. As critical infrastructure operators digitise assets, they are simultaneously seeking to make their industrial environments more connected.

The network has three critical roles in securing critical infrastructure:

1. Securing internal IT access to provide business continuity. This is done through identity-based segmentation (which allows organisations to protect their assets by controlling what users and devices are able to communicate with), visibility tools that provide early warning systems, and high levels of automation to reduce the time taken to detect, disrupt, and recover from attacks.
2. Securing external access required by third parties that need access to systems. Critical infrastructure supply chain is not only the technology but often also the specialist technologists to support it. This includes validating and securing access in multi-cloud environments.
3. Securing the blurred boundary between IT and operational technology (OT) systems by harmonising the controls, policies and governance in both domains and unifying security visibility.

Securing operational technology is complex in an industrial Internet of Things world

In the past, critical infrastructure entities have relied on their operational technology (OT) systems being able to operate reasonably autonomously of other systems and technologies to provide maximum safety and security. As critical infrastructure entities seek to capture additional data from OT and enable automation, OT systems are being connected to IT infrastructure and indirectly often to the Internet. This creates complexities because many OT systems and protocols are not designed with security in place and may not be upgradable to fix known vulnerabilities. In this case, the network must protect OT systems. The focus has moved away from perimeter security (keeping attackers out) to dynamic threat management (detecting threats early and minimising damage) where the network plays a role in protecting OT systems that cannot protect themselves.

Encrypted data presents new challenges

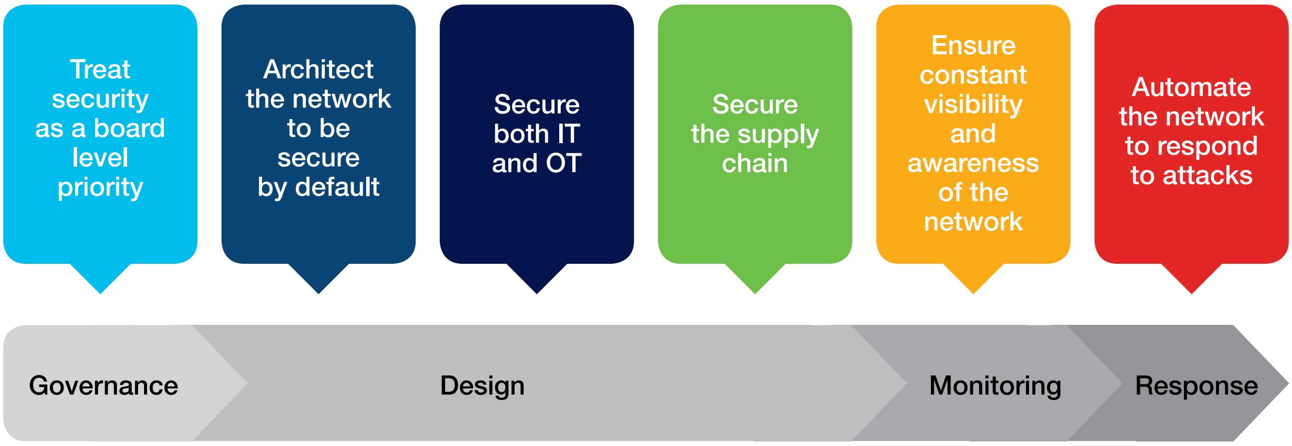
Cyber attackers are becoming increasingly sophisticated in the use of encryption to disguise or hide threats. Basic networks aren't capable of performing detailed analysis of encrypted traffic, including analysis of the origin of the traffic (where the security certificate was issued) and its likely legitimacy.

Projected skills shortages in cybersecurity create another vulnerability

Australia faces a significant cyber security skills shortage across a spectrum of cyber security roles, ranging from specialist engineers to blue tech[4] (technology-intensive jobs that do not require a degree). Industry has a vital role to play in partnership with universities and TAFEs to forecast and respond to potential shortages. The challenge is also acute in relation to digital and cyber literacy and awareness. Human factors and education are important in combatting phishing attacks.

Pre-requisites for secure critical infrastructure

Securing critical infrastructure is complex and demands action on four fronts: governance, design/policy, monitoring and response. These factors are dynamic, not static, which reflects the continual evolution of cyber security. Tactics used by critical infrastructure operators need to anticipate and respond to the tools and strategies used by cyber attackers, including the use of encryption to disguise threats. This includes being able to change policies quickly, and access controls as threats become visible. Cybersecurity needs to be treated as active combat. Organisations need to continuously monitor attackers' strategies, tools and tactics and respond accordingly. This includes dynamic updating of technology and the ability to test solutions in a simulated environment before they are fully deployed.



Treat security as a board level priority

Architect the network to be secure by default

Secure both IT and OT

Secure the supply chain

Ensure constant visibility and awareness of the network

Automate the network to respond to attacks

Governance

Design

Monitoring

Response

Recommendations for critical infrastructure entities

1 Treat the network platform as the first and most powerful line of defence

The network is the foundational platform of digital trust. The network can deliver critical ingredients for a cyber security response but it requires continuous investment. The network - like buildings and facilities - needs be managed based on its lifecycle.

2 Map and meet cyber skill demand in partnership with industry

Organisations need to map skill requirements including advanced technical skills, blue tech and general cyber awareness. Industry partners can play a role in co-creating curriculum and programs that build cyber capability.

3 Test security solutions before they are deployed

Infrastructure operators and ecosystem partners should validate solutions in controlled lab environments before deployment. Lab environments allow organisations to replicate instances of their own network environment and test potential solutions.

Australia's critical infrastructure landscape

What is critical infrastructure?

Australia's critical infrastructure includes networks of electricity, communication, transportation, gas and water assets, food and grocery networks and digital assets such as education and health data. It consists of both public and private infrastructure and extends beyond the infrastructure assets to include supply chains. Only assets essential to the functioning of society and the economy are included. For example, a telco's 5G network is critical infrastructure, but its retail stores are not.

Why critical infrastructure and why it needs to be secured

Australia is a global infrastructure leader. Australia is among the most advanced economies in terms of effective collaboration between the public and private sectors to deliver transport, energy and social infrastructure. In 2017, Australia spent A$1,777 per capita on transport infrastructure alone, ranking second among OECD countries.[5] To meet the demands of its rapid population growth in urban centres, Australia is investing in new infrastructure projects at scale, up from around AU$26 billion in 2016 to an estimated AU$75 billion in 2020.[6]

Major infrastructure projects include:

- The Western Sydney Aerotropolis, including the construction of a new airport and a major new metropolitan area with associated transport, communication and energy infrastructure
- Over $5.7 billion of health infrastructure projects across Australia, including new hospital builds, expansions and upgrades[7]
- Over $11.1 billion of education infrastructure projects across Australia, including opening of new schools and major TAFE upgrades[8]
- The Sydney Metro program, the most significant public transport project in Australia, will expand Sydney's rail network to include 46 stations and more than 113 kilometres of track
- Expanding container terminal capacity at the Port of Melbourne, Victoria's busiest port and the largest container and general cargo port in Australia
- Planned infrastructure upgrades to support Brisbane's 2032 Olympic Games
- Snowy 2.0 linking two existing dams via 27km of tunnels and construction of an underground power station.

Protection of these infrastructure assets – as well as existing infrastructure – is essential. Without proper safeguards, vulnerabilities could be deliberately or inadvertently exploited to cause cascading consequences across Australia's economy, security and sovereignty.

The impact of digital technology on critical infrastructure operators

Digital infrastructure is much broader than just telecommunications assets and connectivity. All infrastructure should now be considered digital. Technologies such as the industrial Internet of Things, Artificial Intelligence (AI) and Big Data are being embedded across all types of built infrastructure – making the infrastructure more intelligent, more integrated, connected and potentially more resilient. A prominent example is what has happened to operational technology (OT), which has traditionally been disparate (siloed) or disconnected. These OT systems encompass examples such as ticketing systems in public transport, building management systems, supervisory control and data acquisition systems that monitor plant equipment and process control systems. The rapid pace of digitisation has meant that additional sensors are being deployed and connected. Data from these sensors provides critical input into OT systems, but it also needs to be connected to the organisation's IT environment and, therefore, the network. These sensors are potentially 'hackable' without the proper protection and create a point of vulnerability for critical infrastructure. The scale of the issue becomes apparent when you consider that a single organisation – Woodside – deployed more than 200,000 sensors in six months.[9]

The question is: why would infrastructure operators open themselves up to more threats? The simple reason is the benefits of digitisation overwhelmingly outweigh the risks (assuming they can be managed). The economic returns from investing in digital infrastructure are greater than returns from traditional, non-digital infrastructure. Researchers estimate if the rest of the European Union built out its digital infrastructure to the level Norway achieved in 2011, GDP would increase by $315 billion[10] – representing 2.4% of Europe's GDP. The gains from digital infrastructure are often associated with the value that can be captured at the data layer. For example, Transport for NSW is investing in digitising major intersections (through the installation of cameras and sensors) so traffic flow can be predicted and controlled[11]. Data from those cameras and sensors will enable new analytical, optimisation and automation capabilities that unlock new efficiencies.

The threats against these environments have evolved to the point where attacks can come from anywhere in the system. In 2000, the Maroochy Water Breach[12] demonstrated that insecure systems within the ICS environments are able to be maliciously controlled to cause damage.

The pace of digitisation in built infrastructure – and the fact cyber attacks can be launched from anywhere in the world – make cyber attacks on infrastructure more likely than physical attacks. The risk is greater than compromised data. Disruption to Australia's critical infrastructure could result in a loss of operational continuity that threatens the availability and uptime of essential services. Now more than ever, owners and operators of critical infrastructure need advanced cyber security protection and capability to respond to an attack and achieve secure digitisation automatically.

Protecting Australia’s critical infrastructure

Legislation for protecting critical infrastructure

The Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 came into effect on 2 April 2022. The Act amends the Security of Critical Infrastructure Act 2018 to introduce the following key measures:

- A new obligation for responsible entities to create and maintain a critical infrastructure risk management program
- A new framework for enhanced cyber security obligations required for operators of systems of national significance (Australia’s most important critical infrastructure assets).

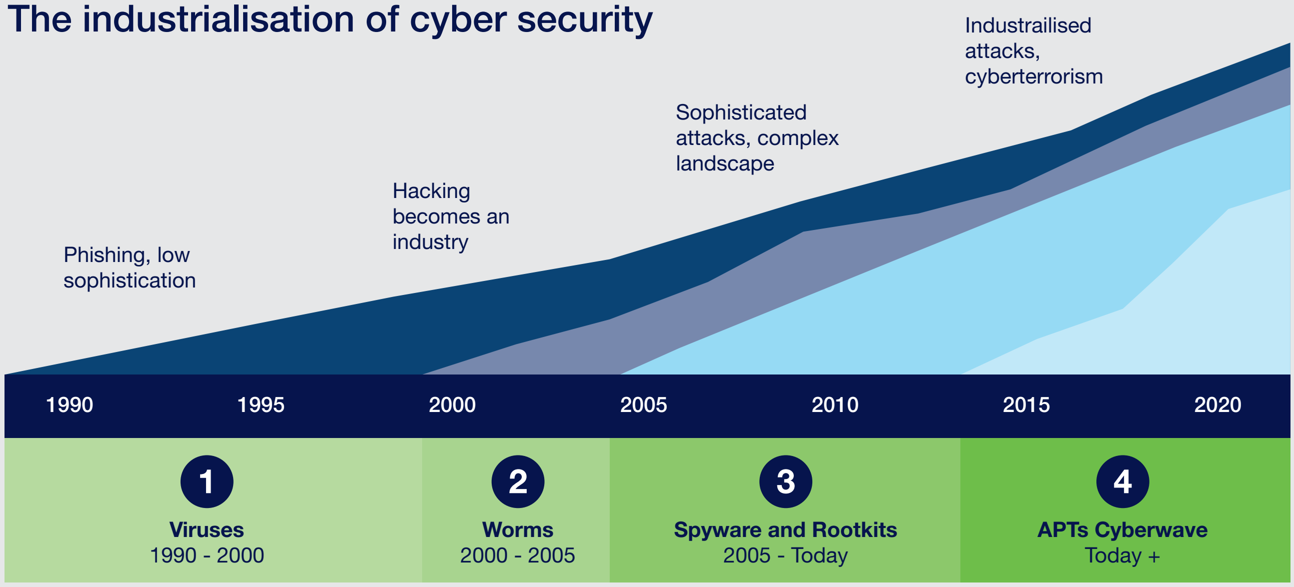
Under the new framework for enhanced cyber security obligations, systems of national significance can be required to:

- Develop cyber security incident response plans to prepare for a cyber security incident
- Undertake cyber security exercises to build cyber preparedness
- Undertake vulnerability assessments to identity vulnerabilities for remediation
- Provide system information to develop and maintain a near-real time threat picture.

Nature of cyber security threats

While the practice of malicious computer hacking may be as old as the IT industry itself, the scale and nature of hacking have changed significantly in recent years. Gone are the days when hackers were amateurs intent on creating minor disruption to business operations.

The industrialisation of cyber security



Over the 2020-21 financial year, the Australian Cyber Security Centre received over 67,500 cybercrime reports, an increase of nearly 13 per cent from the previous financial year. Approximately one-quarter of these were associated with Australia's critical infrastructure or essential services.[13] Four of the most targeted vulnerabilities affect remote work, VPNs and cloud technologies.[14]

Threat actor categories vary in their intent and sophistication and include:

- **Nation-states and state-sponsored actors:** sophisticated and well-resourced, seeking to steal sensitive data or disrupt to undermine Australia's national security and economy
- **Financially motivated criminals:** transnational cybercrime syndicates seeking to extort individuals and organisations through ransomware, phishing, and malware
- **Issue-motivated groups:** focused on disruption to draw attention to specific causes.

Cyber security incidents erode trust in Australian organisations and the Australian Government, lowering investment and business confidence. Successful attacks on critical infrastructure assets cost the Australian economy billions of dollars. The highest economic costs stem from the loss of operational continuity that renders essential services unavailable. A port could lose $100 million a day from the loss of operational continuity following a cyber-attack.[15] The costs associated with the recovery of functions and reputational damage exacerbate the direct commercial losses.

This played out in global news recently when the largest fuel pipeline in the U.S. was hacked and led to shortages across the East Coast. The attack resulted from a single compromised password that gave hackers entry into the networks of Colonial Pipeline Co. through a virtual private network. Pipeline operations were shut down for six days. During that time, the average national cost of gas rose to its highest in over six years and severe gas shortages persisted across states (80% of gas stations were without fuel in Washington; 63% of gas stations were short of supplies in North Carolina, more than 40% in Georgia and South Carolina, and 38% in Virginia). Attackers have also compromised sensors to distort the data provided to OT systems with sometimes catastrophic results. An example is compromising a temperature sensor, so it does not signal that a core system is overheating, or manipulating power output data to create an electricity blackout.

Securing critical infrastructure is complex

The IT security market has evolved significantly in just a few years. Gone are the days when security was all about protecting the hardware and software assets within the data centre. Today, much of an organisation's processing already happens outside the data centre. Perimeter security has become just a small part of the overall challenge. Smart cities, mobile devices, cloud computing and various small devices from the 'Industrial Internet of Things' have together driven security to the very edges of the network and into cyberspace.

The network is the point at which all of these technologies coalesce. The network is the foundational platform of digital trust and is the core platform upon which critical infrastructure must rely to ensure cyber resilience. It transports data between data centres, remote locations, edge devices and endpoints. This presents challenges for critical infrastructure owners and operators because, if the network is compromised, it is only a matter of time before every network system is compromised. Distributed denial-of-service attacks (DDoS) are a widespread threat vector for achieving a simple outage and can undermine the entire network – and therefore, the infrastructure asset base. As attacks become more sophisticated, infrastructure owners and operators need to keep up with new approaches to network security protection.

Many organisations are starting from a low base of cyber capability

Many Australian organisations have found it challenging to secure their assets. For example, many higher education institutions – which are particularly vulnerable given the sensitivity of data they hold and access they have to high-power computing resources – have struggled to keep pace with a changing threat landscape. An article published in early 2021 revealed almost half of Australia's top 20 universities appeared to have little or no protection in place for hackers impersonating their domains in phishing attacks.[16] Only two of the 20 universities are proactively blocking fraudulent emails from reaching students, alumni and faculty.

Cyber security demands action on multiple fronts

Layers of complexity thwart efforts to secure critical infrastructure and maintain business continuity.

Technical

- Proliferation of devices
- Multi-cloud environments
- Securing the entire stack (applications, data acquisition / transformation / delivery, connectivity, sensors & things)

Operational

- Balancing Confidentiality, Integrity and Availability (CIA)
- Ensuring availability of operational technology

Policy & regulatory

- Data sovereignty
- Data framework
- Privacy

Lack of cyber skills are a major vulnerability

Australia faces a significant cyber security skills shortage. Around 60% of organisations in Australia and New Zealand find recruiting for cyber security talent either "difficult" or "very difficult".[17] Forecasters predict a global cyber security workforce gap of 1.8 million by 2022, a 20% increase over forecasts made in 2015.[18]

Shortages are being experienced across the spectrum of cyber roles, from specialist engineers to blue tech[19] jobs that are technology-intensive but do not require a degree. Oxford Economics' Report[20] looked into the Australian jobs future and highlighted that new roles would be created, and existing roles transformed by digital technologies. Cyber security is likely to account for a major share of these new roles, and workers and businesses will need to reskill and adapt. As the report noted, workers will spend less time and effort on routine, predictable functions and more on those tasks that are less economical to automate at scale.

Cyber literacy among staff is also critical to combating more basic phishing attacks. Demand for cyber security skills is a focus for universities, TAFEs, schools and partnerships. Technology companies are also dedicating efforts to growing cyber security skills at scale. For example, Cisco's Networking Academy prepares learners for Cisco Certification and other industry-recognised certification exams in cyber security. Certified graduates are recruited from industries including healthcare, telecommunications, energy and transport.

Profiling risks and priorities across different sectors

In developing the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022, the Australian Government defined 11 critical infrastructure sectors. This section provides insights into the cyber security landscape across each of these sectors. While most risks are common to all sectors, some are more acute and difficult to manage in specific settings.

1. Communications

The reliability of communications infrastructure directly impacts the productivity of every industry and underpins Australia's liveability by interconnecting people and essential services. The importance of Australia's communications infrastructure – and the surface area for cyber-attacks – has grown during the COVID-19 pandemic as more people work remotely. Any disruption to fixed, 4G, 5G and satellite communications technologies would have profound consequences on Australia's economy, as well as citizens' health and safety.

Why this sector is a cybersecurity target

- Backbone for information sharing across business, government and the community
- Essential to emergency response
- Carrier of sensitive information linked to national security
- Stores millions of customer records that are a target for identity theft

Specific challenges

1. The integration of cloud and network technologies increases security complexity
2. Low cost infrastructure equipment, such as CPE routers, provides a major attack surface that is highly accessible to cybercriminals
3. High employee turnover is making the sector vulnerable to internal attacks
4. The rollout of 5G and IOT devices that utilise voice and data networks is intensifying the scale of the cyber security challenge operators face.

High profile attacks

2021

Verizon

State-based actors hacked into Pulse Connect Secure, which provides internet security for Verizon.

2021

Belnet

A large DDoS attack disables the ISP used by Belgium's government, causing the cancellation of Parliamentary meetings.

2. Financial services and markets

Financial services and markets play a critical role in growing the economy and providing financial stability connecting businesses to capital. Cyber threats facing the financial sector are becoming better resourced and more sophisticated. In early 2021, ANZ's head of institutional banking, Mark Whelan, said the number of attacks had escalated to 8-10 million attacks a month during the pandemic. Attacks range from banking trojans affecting individual customers to systemic threats posed by ransomware and advanced persistent threat (APT) groups.

Why this sector is a cybersecurity target

Underpins economic stability by providing a safe and secure banking and investment environment

Connects into – and has potential to impact – securities exchanges including the ASX

Responsible for managing the wealth of institutions and consumers across Australia

Stores millions of customer records that are a target for identity theft

Specific challenges

1. The increase in online commerce creates new complexity in reviewing, monitoring and safeguarding transactions
2. The shift to digital banking and opening of the financial sector to new entrants is increasing the attack surface, particularly for core banking products and services
3. Financial services infrastructure is becoming more complex as institutions attempt to embrace digital transformation, including adoption of share cloud services

High profile attacks

2021

Reserve Bank of New Zealand

Unidentified hackers breached one of the data centers of New Zealand's Reserve Bank.

2020

NZX

New Zealand's stock exchange faced several days of disruption after a severe DDoS attack from unknown actors.

2020

Shirbit

A criminal group targeted the Israeli insurance company Shirbit with ransomware, demanding $1m in bitcoin.

3. Data storage and processing

Rising demand for cloud hosting solutions and big data from corporate and government entities has fuelled the growth of the data storage and processing industry. The sector underpins Australia's economy and is responsible for massive stores of sensitive and personal data. The need for risk-based approaches to data protection and data privacy has extended the importance of Australia's data storage and processing sector. A successful attack would have a devastating impact on businesses, government, and individuals alike, potentially exposing Australia's national security.

Why this sector is a cybersecurity target

Stores and processes sensitive data at massive scale

Connected with – and integrated into – the nation's largest private sector and government institutions

Powers the day-to-day operations of businesses, both large and small

Specific challenges

1. Cybersecurity and data protection are often managed by separate teams, with different software sets
2. The shift to big data has given cybercriminals the opportunities to exploit sensitive and personal information at scale
3. Traditionally, technologies and security tools that have been used to mine data and prevent cyber attacks have been more reactive than proactive.

High profile attacks

2018

Exactis

Marketing data firm Exactis suffered a data breach exposing the political preferences of 340 million people.

2016

Australian Bureau of Statistics

On census night, the Australian National Census was hit with a number of Denial of Service Attacks which took the system offline.

4. Defence industries

Defence industries are essential to Australia's national security, playing a critical role in deterring action against Australia's interests and responding with credible military force when required. Military cyber threats are growing, with defence forces increasingly acknowledging cyber as a new battlefield. Nation-states and state-sponsored actors are becoming increasingly sophisticated and well-resourced in their attempts to steal sensitive data or damage Australia's national security and economy. The cyber threat facing Australia's defence industries covers the entire defence supply chain, including government, suppliers (such as defence manufacturers) and research institutions.

Why this sector is a cybersecurity target

Underpins the nation's security and protects Australia from foreign interference

Holds IP related to emerging and next-generation defence systems and innovations

Specific challenges

1. Nation state conflicts are increasingly shifting to low-intensity cyberwarfare
2. An increasing number of defence systems rely on edge computing and IoT, which is increasing the attack surface
3. Modern force structures are organised with mobility in mind, which increases the complexity of protecting defence systems and people.

High profile attacks

2021

NATO

Tracking data of two NATO ships was falsified, positioning two warships at the entrance of a major Russian naval base.

2021

US State Department

State-based actors stole thousands of emails after breaching the email server of the US State Department.

5. Higher education and research

Australia's universities play a critical role in the Australian economy through skills development, innovation and research. Many universities are billion-dollar-plus entities with a large attack surface. They also play a crucial role in advising Government agencies on security matters, including collaborating as partners with the Federal Government on the University Foreign Interference Taskforce and targeted responses to sectors such as defence, utilities, and industry (e.g., through the Cyber Security CRC). The Australian education and research sector suffered 122 cyberattacks in the 2020 financial year, and the education sector is ranked number three in the top five industry sectors at risk of data breaches.[21]

Why this sector is a cybersecurity target

- Holds significant high performance computing resources
- Major export industry
- Underpins the nation's innovative capacity through sovereign research capability
- A leading partner and host of international collaborative research
- Links to national security
- Ingests data from industry and government which must be protected

Specific challenges

1. Universities have large and diverse user bases including staff, students and suppliers that need access to the university network
2. Scale, complexity, capability and threat landscape are different from university to university – resulting in the absence of a consistent sectoral cyber policy and approach
3. The volume of unmanaged and personal devices connecting to university networks (both on and off the campus) is growing, increasing attack surfaces
4. Unlike staff or contractors, students accessing the network are – for all practical purposes – unable to be vetted for any nefarious intent
5. Mass connectivity and sensor-driven digital campuses – enabled by next-generation technologies such as 5G – will continually enlarge the attack surface.

High profile attacks

2020

University of California

The University of California paid US$1.14M in ransom response to an attack from a Russian cybercrime group.

2020

University of Utah

The University of Utah paid cyber criminals US$457K after university data was stolen through a ransomware attack.

2019

Australian National University

Hackers accessed 19 years' worth of Australian National University student and staff data.

6. Energy

A reliable and safe supply of energy is essential to everyday life for Australians and critical to economic growth. The energy sector is becoming increasingly digitised and now operates vast networks of operational technology, which, if compromised, can result in significant physical disruption and/or destruction. This sector is also experiencing massive disruption with Distributed Energy Resources, and the shift towards electric vehicles results in further moves towards digitalised solutions. Attacks have been reported in global news recently when a cyber-attack forced US-based Colonial Pipeline Co. to shut down pipeline operations for six days. During that time, the average national cost of fuel rose to its highest level in over six years.

Why this sector is a cybersecurity target

Underpins economic stability by powering the nations' industry and households

Critical to Australia's energy security

Possible to create significant physical disruption and/or destruction

Facing scrutiny from politically-motivated 'hacktivists'

Specific challenges

1. A complex value chain – from generation to transmission, distribution and the network – create potential for large scale attacks
2. The geographic distribution of energy companies adds additional complexity that makes them vulnerable to cyber attacks
3. Interdependencies between physical and digital infrastructure, such as wireless smart meters, increase the attack surface
4. The potential for physical disruption due to the prevalence of operational technology can create losses that often exceed the value of any ransom sought.

High profile attacks

2021

Colonial Pipeline Company

A ransomware attack forced Colonial Pipeline to shut down the US' largest fuel pipeline and pay a $5M ransom.

2021

National Atomic Energy Agency of Poland

The website of Poland's National Atomic Energy Agency was hacked to spread false alerts of a radioactive threat.

2021

LineStar

70GB of internal files were stolen from pipeline business LineStar Integrity services due to a ransomware attack.

7. Food and grocery

The security of food and grocery supply is critical. The food and grocery sector operates vast supply chains – spanning metropolitan and regional, and remote areas – for which efficiency, cost competitiveness and resilience are key priorities. These supply chains are increasingly becoming digitised, accentuating cyber security risks. Major risks include disruption to the supply of essential goods by, for example, attacks on routing systems and the destruction of perishable items through attacks on operational technology such as temperature-controlled storage.

Why this sector is a cybersecurity target

Critical to Australia's food security

Constitutes a major spending item for the nation's householders

Possible to create significant physical disruption and/or destruction

Specific challenges

1. Food supply chains are becoming increasingly digitised, including through the use of IoT networks that increase the attack surface
2. COVID-19 has put new cyber pressures on food and grocery operators as customers move to digital channels such as online ordering
3. Operational technology, such as temperature-controlled storage, creates added complexity and potential for disruption
4. Dependency on physical transportation / logistics.

High profile attacks

2021

JBS

A ransomware attack forced the shutdown of meat plants that process more than a fifth of the US' beef supply.

2020

CMA CGM

French shipping company CMA CGM was impacted by a ransomware attack that disrupted its IT networks.

2019

Plus

Netherlands-based Plus supermarkets' refrigeration system was remotely hacked and altered, damaging stock.

8. Healthcare and medical

The healthcare sector faces growing cyber security threats; the number of hacking incidents reported in healthcare climbed for the fifth straight year in 2020, rising 42%.[22] Healthcare organisations are particularly vulnerable and targeted by cyber attackers because they possess high monetary and intelligence value information. This includes patients' protected health information, financial information and intellectual property related to medical research and innovation. The ramifications go beyond financial loss and breach of privacy. The loss of hospital patient data, for example, has the potential to put lives at risk.

Why this sector is a cybersecurity target

Provides life-saving care to Australians

Stores millions of private patient health records

Holds IP that can be exploited for biomedical research

Specific challenges

1. COVID-19 has led to healthcare entities sharing data at greater scale and with a larger number of organisations, increasing the attack surface
2. The rise in telehealth and virtual care solutions (such as remote monitoring) is leading to more private patient data being shared through digital channels
3. Hospitals are increasingly becoming digitised, including through IoT and connected devices, which increases the attack surface.

High profile attacks

2021

Waikato District Health Board
A ransomware attack forced a NZ district health board to delay elective surgeries and switch to paper-based processes.

2020

Universal Health Systems
Universal Health Systems was forced to divert ambulances and reschedule surgeries due to a ransomware attack.

2021

University of Oxford
Research relating to the COVID-19 vaccine was stolen and is believed to have been sold to nation states.

9. Space

Increasingly, data is transmitted via, and stored on, orbiting satellites. Given the high value of data stored on satellites and other space systems, the space industry has the potential to become an attractive target for cyber-attacks. The scale of risk is severe. For instance, if a hacker were to penetrate earth-based systems and provide false information to a satellite, it could cause an inter-space collision and potentially take out major communications systems globally. This risk is growing as the barriers to entry for governments and private organisations to become involved in space projects are lowered.

Why this sector is a cybersecurity target

- Military and civilian capabilities increasingly rely on space assets
- Links to national security
- High-growth export sector with fierce international competition
- Supplies positioning and imagery data

Specific challenges

1. There is limited regulation providing for an internationally coherent approach to operating space systems
2. The fast growing number of satellites in orbit creates potential for large-scale attacks
3. The number of parties and systems involved in creating and operating space systems create vulnerabilities
4. Satellites are often used in mesh, which creates possibilities for an attack on one node to spread to others
5. Regional Australia may come to depend on increasing use of satcomms, especially Starlink.

High profile attacks

2008

US Geological Survey

Two satellites used by the US Geological Survey and NASA were attacked four times.

2014

National Oceanic and Atmospheric Administration

A cyberattack forced the National Oceanic and Atmospheric Administration to cut off public access to imagery data.

10. Transport

Transport networks have become increasingly digitalised, with a wide range of data flowing across systems, tracking and monitoring digital and physical networks. As more devices and control systems are connected online, more vulnerabilities will appear, increasing the potential for disruption from cyber-attacks. Past attacks have disrupted business continuity, but each progressive attack is growing more dangerous. For instance, an investigation into a 2017 ransomware attack on Sacramento Regional Transit (SacRT) found hackers could control vehicles and brakes.[23] Attacks of this nature have the potential to cause devastating impacts, including loss of life.

Why this sector is a cybersecurity target

Underpins movement of goods and access to economic opportunity

Possible to create significant supply chain disruption and/or safety issues

Stores sensitive data about the movement of people and goods

Specific challenges

1. The shift to intelligent transport systems, which rely on vast sensor networks and connected vehicles, is increasing the attack surface
2. The geographic distribution of transport networks adds additional complexity that makes them vulnerable to cyber attacks.

High profile attacks

2021

Metropolitan Transportation Authority

New York's MTA was hacked by state-based actors seeking access to user data and information systems.

2021

CERT-In

State-based actors conducted a cyber espionage campaign against the Indian transport sector.

2021

Transnet

South Africa's freight rail monopoly had its rail services disrupted after a hack by unknown hackers.

11. Water and sewerage

A safe and secure water and sewerage sector are essential to the health of Australians and the liveability of our communities. It is also critical to industry, which relies on adequate water and sewerage infrastructure for operational continuity. Water and sewerage systems are becoming increasingly connected, with vast sensor networks and operational technology increasing opportunities for cyber interference. This played out recently in Oldsmar, Florida, when a hacker tried to poison the water supply by increasing sodium hydroxide levels to extremely dangerous levels. If the attack had been successful, it could have resulted in substantial loss of life.

Why this sector is a cybersecurity target

Critical to Australia's liveability, health and safety

Possible to create significant physical disruption and/or destruction

Potential to generate health risks such as water contamination

Specific challenges

① The geographic distribution of water and waste operators adds additional complexity that makes them vulnerable to cyber attacks

② High levels of reliance on operational technology create significant vulnerabilities that can lead to major health and safety risks.

High profile attacks

2021

Volue

Water treatment facilities in 200 Norwegian municipalities were shut down following a ransomware attack.

2021

City of Oldsmar

Unknown hackers attempted to raise levels of sodium hydroxide in Oldsmar, Florida's water supply.

Conclusions

Every critical infrastructure sector faces a common set of cybersecurity challenges

While the nature of attacks and vulnerabilities vary by sector, the challenges are reasonably common. These challenges relate to the sheer scale of technology environments, difficulties managing legacy technologies and human factors. Another significant challenge is the speed of technology development which creates downstream pressures on integration. This is exacerbated by inherent software and open-source code vulnerabilities that are often layered and not always effectively maintained.

The most common cybersecurity challenges include:

1. Scale of data being generated, used and shared
2. Legacy protocols, systems and technical debt
3. Lack of cybersecurity skills and awareness
4. Accelerated adoption of new technologies, including IT and OT
5. Shifts towards mass connectivity
6. Complex value chains spanning vast geographic areas
7. Inconsistent cyber policies and approaches used within and across sectors

The network is the primary platform for cyber defence

The network is foundational to digital trust and is the core platform critical infrastructure must rely on to ensure cyber resilience. The network is responsible for securing internal IT access, securing external access required by third parties and securing the increasingly blurred boundary between IT and OT systems. Recognising the nature and scale of the cyber threat, critical infrastructure entities have to consider deterrence, resilience, mitigation and prevention at the network layer. It is often deemed good practice to strengthen protection and assume that the network is already compromised and act accordingly. In other words, network architecture and protocols need to be robust, as well as having in place a first line of defence by prevention. This may involve backup and recovery procedures, responses to intrusions, contingency plans that minimise damage, and forms of offensive cyber operations.[24]

The network is a major weakness if proper controls are not in place

As critical infrastructure operators digitise assets, they simultaneously seek to make their environments more open and improve the ease of connectivity. This makes the network a source of vulnerability. Designing networks to be secure by default is a first step to mitigating risks.

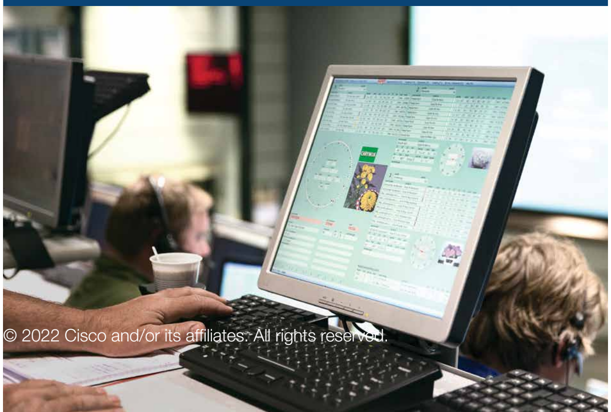
Organisations need to adjust those defaults in response to their context. This includes establishing controls so authorised users are contained within a segmented data plane. For example, most users do not need to access the control plane or management plane of networks. Each network security layer implements policies and controls, allowing authorised users to gain access to network resources and blocking malicious actors from carrying out exploits and threats. Assuring real-time network integrity is a major priority for all infrastructure entities, with telecommunications network operators the most advanced.

Anything connected to a network presents a cyber risk

While sensors and endpoints may not have high levels of capability, they can represent a way in for potential attackers. Peripheral devices such as printers and industrial Internet of Things sensors are part of the attack surface. They need to be protected through an edge architecture approach, using tools such as Extended Detection and Response (XDR) and Zero Trust Architecture (ZTA).

In addition, endpoints need to be secured at the network level. It is critical that policies can be applied to individual endpoints, which dictate their role and operation. For example, a policy can be created for a networked printer that prescribes that the device performs only the functions you would expect from a printer. If the printer is trying to communicate into a data centre, the network assumes it has been compromised and prevents it.

> “The network needs to defend the critical asset that cannot defend themselves.”



The IT and OT domains demand different security responses

There are key differences in the cyber landscape for information technology (IT) and operational technology (OT), which relates to industrial operations/systems:

- **The degree of openness**
  OT systems have tended to be locked down and operate independently of the IT network environment. IT systems are the opposite: data sharing is at the heart of IT system design, including with internal and external parties.
- **The power contained in the endpoint device**
  In an IT environment, the endpoint is usually a general-purpose device designed to do many things. In an OT environment, the endpoint is typically a sensor with a dedicated function.
- **What motivates attackers**
  With IT systems, attackers are more likely to be focused on accessing (or preventing access to) data (financial, personal, commercial and intellectual property), compared with an OT attack, which is more likely to be motivated by disrupting business continuity.
- **Security response**
  Availability is often more critical in OT environments than IT environments. In an IT environment, a device can be taken offline and quarantined in the event of an attack. In an OT environment, systems such as those required for safety must remain available and cannot be taken offline. This necessitates a different security response.

Visibility and awareness are the first steps to preventing breaches and detecting them early

If you can’t see it, you can’t measure it. Visibility is critical to understanding macro-level issues (such as insights delivered by Talos about global threat trends) through to specific tools that reveal applications running on the network such as Cyber Vision, Netflow/IPFIX and DNS. It is impossible to have absolute protection, but collecting telemetry for visibility and supporting detection and response is critical. Tools such as CX Cloud use telemetry, AI/ML-driven insights, use cases and contextual learning to help make better security decisions.

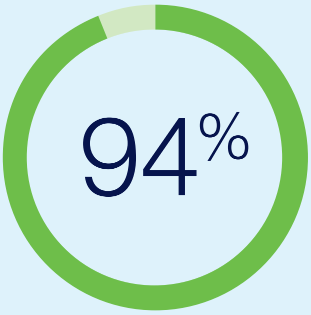
Automation of network functions provides scale, accuracy and agility

The scale and complexity of securing IT and OT systems have driven automated diagnostic tools and interventions uptake. For example, if malware is detected by end point software, then automation tools are used to send alerts, generate triage tickets, and manage the response process without human intervention. Machine learning enables automated detection and response to occur with greater precision and speed by recognising patterns and predicting threats based on massive data sets at machine speed. By automating analysis, cyber teams can rapidly detect threats and isolate situations that need deeper human analysis.

Cisco’s own cyber threat intelligence organisation, Talos, in conjunction with Cisco CSIRT and Cisco IT, blocks billions of cyber threats a day within its own network, which would not be possible without high levels of automation and machine learning. Cisco also uses AI and machine learning to analyse encrypted traffic on the network, for example by examining the country where security documents are issued and shaping how the network responds to information it collects.

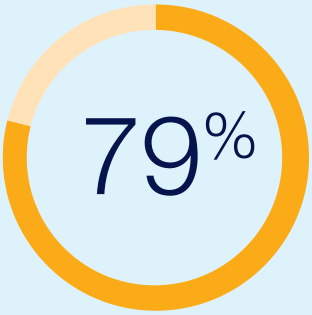
The entire supply chain needs to be secured, not just the organisation

Every part of a supply chain can have vulnerabilities, and risks can accumulate across the supply chain. There have been numerous examples of institutions being attacked through smaller suppliers, which tend to have weaker security than larger ones. Visibility and management of the entire supply chain, including third- and fourth-party risks, is critical. Organisations need to know who is in their supply chain – including cloud services providers – and how those suppliers protect themselves. Robust access and identity controls, backup, patching and vulnerability management are also critical.



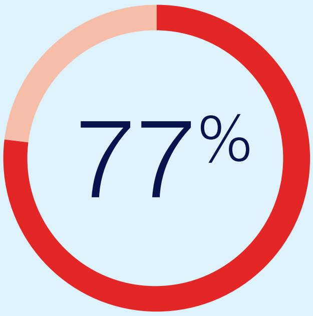
Enterprises using 3rd party cloud services

2019 RightScale State of the Cloud Report from Flex



Enterprise workloads running in cloud environments

2019 RightScale State of the Cloud Report from Flexera



Do not consider security a factor in cloud provider selection

2019 Ponemon Institute Global Cloud Data Security Study sponsored by Thales

Cisco's Value Chain Security[25] suite continually assesses, monitors and improves the security of the third parties. It validates that solutions are genuine, operating as organisations direct them to and not subject to tampering. It does this by detecting tainted solutions, counterfeit solutions, misuse of intellectual property and third-party information security breaches.

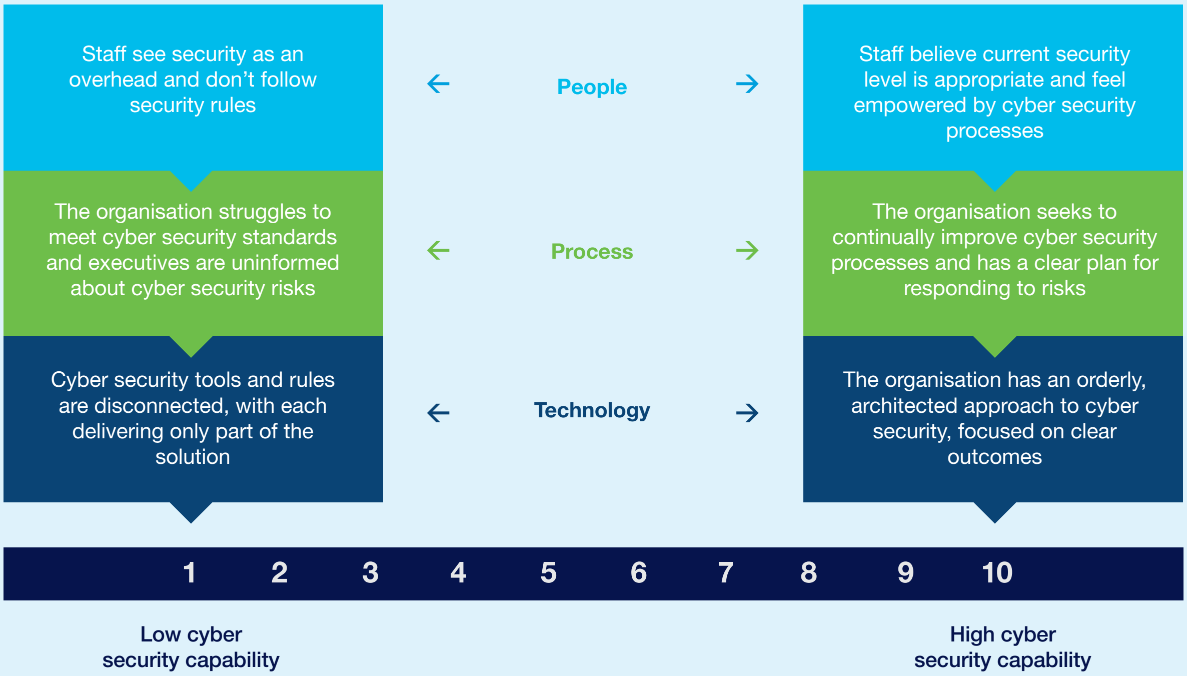
Defence industries are leading in terms of supply chain security. As part of the Australian Federal Government's agreement with the US on military capability, it must ensure defence contractors have appropriate credentials as part of the security response.

> "When it comes to cyber security, it doesn't matter if one organisation invests millions of dollars in cyber security, if there's another part of that ecosystem that's vulnerable, the attacks will find the easiest way to compromise the ecosystem as a whole."
>
> **– Ben Dawson, Vice President, Cisco ANZ**

Cyber security is a board-level priority but locking things down cannot be the default response

A primary function of boards is the identification and prevention of risk, including to the integrity, confidentiality, and assured availability of data, systems, and services. Changes are currently being considered to make board members personally liable for cyber security breaches in listed companies. Boards are applying a balanced scorecard approach that is sufficiently tight to ensure ongoing community confidence but not so restrictive that they stifle innovation or efficiency.

High-level balanced scorecard for the top leadership team



Staff see security as an overhead and don't follow security rules	← **People** →	Staff believe current security level is appropriate and feel empowered by cyber security processes
The organisation struggles to meet cyber security standards and executives are uninformed about cyber security risks	← **Process** →	The organisation seeks to continually improve cyber security processes and has a clear plan for responding to risks
Cyber security tools and rules are disconnected, with each delivering only part of the solution	← **Technology** →	The organisation has an orderly, architected approach to cyber security, focused on clear outcomes

Adapted from Cisco 'Cyber security for digital government leaders' whitepaper

Recommendations

Invest effort to map and understand your risks

Critical infrastructure entities need to always be prepared for the potential of a large-scale disruptive or destructive cyber security attack. This includes knowing that they have the capacity to both identify and respond to an attack. The essential questions for critical infrastructure entities to ask include:

1. Can we pinpoint all our digital assets and do we know their current vulnerabilities and the risk they represent?
2. Are we able to mitigate vulnerabilities/incidents anywhere and quickly produce metrics and reports?
3. Do we have the right security tools in place to be able to detect and respond to cyber incidents quickly?

In many cases, the answers to these questions and their solutions will be interconnected and integrated.

Map and meet cyber skill demand in partnership with industry and higher education

The cyber skills challenge is immense and creates vulnerability in its own right. Organisations need to map their skills requirements, including advanced technical skills, blue tech and general cyber awareness. Industry partners can play a role in co-creating curriculum and programs that build cyber skills capability. Cisco's global Networking Academy program has trained more than five million students since 1997 by partnership with training providers and institutions. The curriculum has broadened beyond networking to include cyber security, industrial Internet of Things, entrepreneurship and IT essentials. Cisco has also co-developed micro-credentials with universities, recognising that workers need flexibility in the intensity of courses and mode of delivery. Cisco and Curtin University co-designed the Internet of Things Micro Masters program and offers this through the edX platform.

Treat the network as the first and most powerful line of defence

The network can deliver essential ingredients for a cyber security response, but this requires continuous investment. The network – like buildings and facilities – needs to be managed based on its lifecycle. Upgrades and maintenance are needed to improve functionality and performance, including:

- Continuously improving visibility and early warnings/detection
- Adding/strengthening control points capable of defending assets across the organisation
- Driving operational efficiency through automation and orchestration.

Test security solutions at a critical infrastructure lab before they are deployed

The reasons security measures are not implemented include fear they will not work or that they will create unforeseen problems (particularly OT systems). With the University of Adelaide, Cisco has established a Critical Infrastructure Security Lab that allows infrastructure operators and ecosystem partners to validate solutions in a controlled environment. The lab environment allows organisations to replicate instances of their own network environment and test potential solutions. The service allows solutions to be proven before they are deployed and helps IT and OT security personnel better understand interactions between complex systems.

An opportunity for Australia to be a cyber leader

The reward for cyber leadership is measured in economic terms. The Australian Cyber Security Centre warns that a four-week interruption to digital infrastructure resulting from a significant cyber incident would cost the economy $30 billion (1.5% of gross domestic product) and about 163,000 jobs. A useful analogy in relation to cyber security is the brakes on a Formula One car. The brakes certainly do not power the car nor create velocity, but the braking performance of a vehicle is one of the primary determinants of lap times. The same is true of cyber security, where trust and confidence in cyber systems allow dynamic innovation and accelerates the pace of technology uptake. Estimates are that by 2020, 75% of businesses will be digital or preparing to become digital. Australia can be a global leader in cyber security operational excellence. Achieving this vision requires a partnership between government, public and private entities.

Acknowledgments

We would like to thank all contributors to this white paper, most notably:

- **Matt Carling,** National Cybersecurity Advisor, Cisco ANZ
- **Simon Finn,** Critical Infrastructure Cybersecurity Advisor, Cisco ANZ
- **Reg Johnson,** Director Education and Strategic Industries, Cisco ANZ
- **Professor Wei Xiang,** Cisco Chair of AI and Internet of Things and Director of Cisco-La Trobe Centre for AI and Internet of Things
- **Professor Michael Rosemann,** Director of the Centre for Future Enterprise and a Professor for Information Systems at the Business School, Queensland University of Technology
- **Gary Hale,** Chief Security Officer and Director Defence & Space, Curtin University
- **Professor Reza Nejabati,** Co-Chair for the Cisco-Curtin Centre for Networking
- **Professor Iain Murray,** Co-Chair for the Cisco-Curtin Centre for Networking
- **Professor Trish Williams,** Cisco-Flinders Digital Health Research Chair and Director of the Cisco-Flinders Digital Health Design Lab
- **Professor Aaron Quigley,** Head of School for UNSW's School of Computer Science and Engineering and advisor to Innovation Central Sydney.

References

1 https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21

2 See *Australian Government's Critical Infrastructure Resilience Strategy Plan (2015)* and https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protectioncritical-infrastructure-from-terrorism.pdf; https://www.legislation.gov.au/Details/C2018A00029

3 https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21

4 *Critical Role of Blue Tech and Digital Skills in Australia's Economic Recovery, May 2020*

5 https://www.mckinsey.com/~/media/mckinsey/featured%20insights/asia%20pacific/australias%20infrastructure%20innovation%20imperative/australias-infrastructure-innovation-imperative-final.pdf

6 Ibid

7 Based on analysis of federal, state and territory government stimulus funding

8 Based on analysis of federal, state and territory government stimulus funding

9 Based on anecdotal evidence

10 https://doi.org/10.1108/info-10-2013-0051

11 See also *Brisbane-based Advanced Mobility Analytics* which is predicting incidents at intersections

12 https://www.mitre.org/publications/technical-papers/malicious-control-system-cyber-security-attack-case-study-maroochy-water-services-australia

13 https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21

14 https://www.cyber.gov.au/acsc/view-all-content/news/joint-advisory-top-cyber-vulnerabilities

15 Figure is anecdotal

16 The Age. '*Common target': Only 10% of Australian universities automatically blocking fraudulent emails*.' January 20, 2021 https://www.theage.com.au/politics/federal/common-target-only-10-per-cent-of-australian-universities-automatically-blocking-fraudulent-emails-20210120-p56vg0.html

17 Hays

18 Frost & Sullivan, 2017

19 *Critical Role of Blue Tech and Digital Skills in Australia's Economic Recovery*, May 2020

20 https://www.cisco.com/c/dam/m/en_au/cda/cisco-future-of-australian-jobs-report2019.pdf

21 https://www.campusreview.com.au/2021/09/how-universities-can-combat-increasing-cybersecurity-threats-opinion/

22 https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=7daa8a195650

23 https://securityboulevard.com/2021/07/whats-at-stake-when-the-transportation-sector-lags-behind-in-cybersecurity/

24 Stanislav Abaimov and Paul Ingram. *'Hacking UK Trident: A Growing Threat'*. June 2017.

25 Value Chain Security - Cisco

26 https://www.asx.com.au/documents/investor-relations/ASX-100-Cyber-Health-Check-Report.pdf and https://policy.federation.edu.au/forms/AS_NZS%20ISO_IEC%2017799%202001.pdf

27 AustCyber (2020), *Australia's Digital Trust Report 2020*, available at https://www.austcyber.com/resource/digitaltrustreport2020

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/ trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)