



IoT, Digital Infrastructure and Cybersecurity

Mohan Baruwal Chhetri, CSIRO's Data61





Escalating cyber threats in the Pacific region

*“The activity of **cybercriminals** and **state-sponsored threat actors** has increased globally, and the direct and indirect targeting of Pacific **individuals**, **businesses**, ..., and **government systems** remains a threat”*

- The Pacific Security Outlook Report 2023-2024, Pacific Islands Forum

*“Government’s critical infrastructure, businesses and households continue to be targeted by **malicious state** and **non-state actors**”*

- The Cyber Threat Report 2022-2023, Australian Signals Directorate

*51% of the reported cybersecurity incidents in New Zealand in FY 2022-2023 are linked to **state-sponsored actors** and **financially-motivated criminals***

- Cyber Threat Report 2022-2023, National Cybersecurity Centre, New Zealand



Some recent cybersecurity incidents

Optus Data Breach (Sep 2022)

- Impact: 9.8 million customers

Medibank Data Breach (Dec 2022)

- Impact: 9.7 million customers

DP World Australia (Nov 2023)

- Impact: Disruption to 40% of Australia's maritime operation

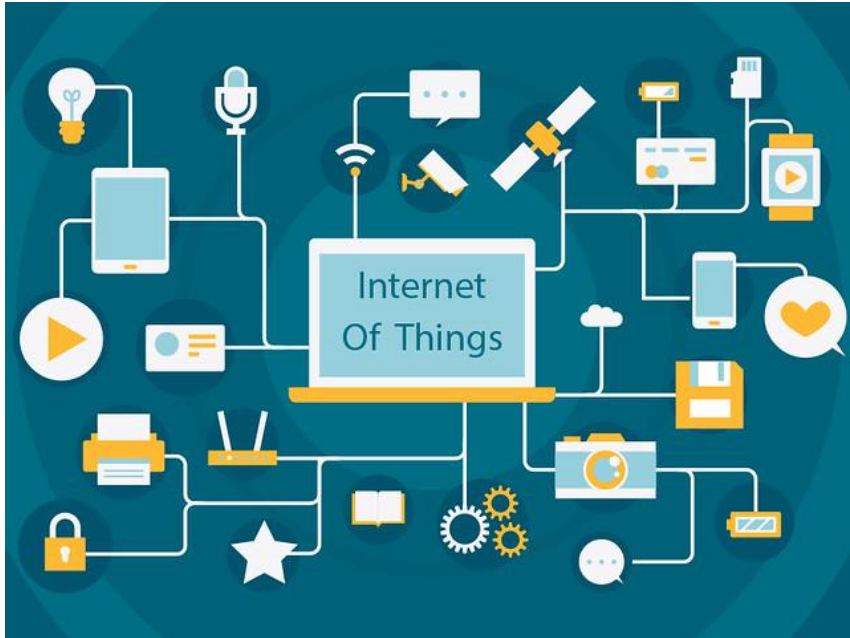
Mirai Botnet (2016-present)

- Impact: Numerous

Verkada Hack (2021)

- Breach of privacy and security (access to live video feeds)

Global IoT landscape



- 18.8 billion connected IoT devices by the end of 2024 (13%↑)
- Projected to exceed 40 billion connected IoT devices by 2030
- Common Types of IoT
- Key IoT Trends



Key IoT cybersecurity challenges

Inadequate
Authentication

Insufficient
Encryption

Firmware and
Software
Vulnerabilities

Insecure
Protocols

Supply Chain
Vulnerabilities

Maintenance
and Update
Challenges

Physical
Security Risks

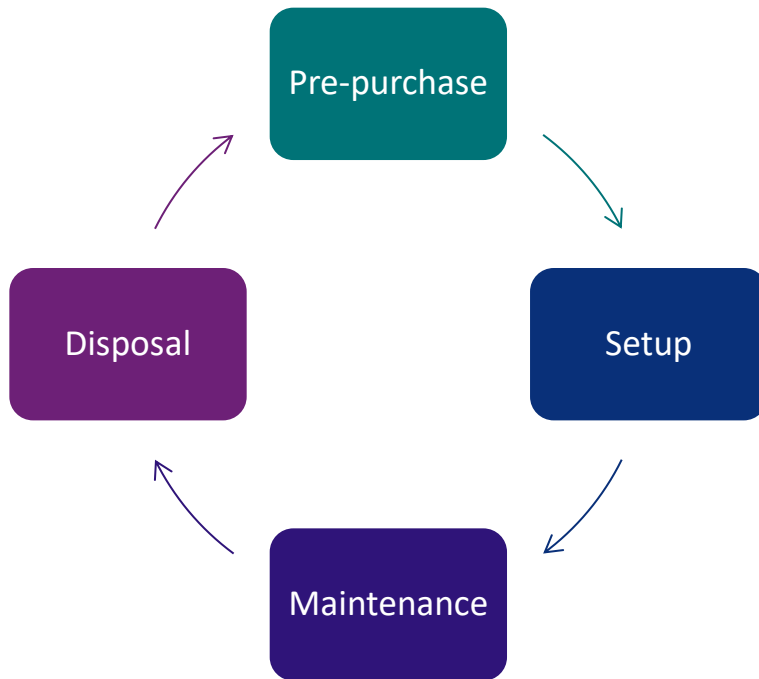
Insufficient
Privacy
Protection

Shadow IoT



- No duplicated default or weak passwords
- Vulnerability Disclosure Policy
- Secure Software Updates
- Secure Storage of Credentials
- Protect Personal Data
- Minimise Exposed Attack Surfaces
- Ensure Communication Security
- Ensure Software Integrity
- Make Systems Resilient to Outages
- Monitor System Telemetry Data
- Support Easy Deletion of Personal Data
- Make Installation/Maintenance of Devices Easy
- Validate Input Data

Guidance for individuals and businesses



Tips to secure your Internet of Things device

The infographic features a blue background with white line-art icons of various IoT devices (refrigerator, printer, house, camera, router, etc.) connected by a cloud network. A padlock icon is also present, symbolizing security.

The Australian Cyber Security Centre has developed this information to help the community buy and use Internet of Things (IoT) devices securely. An IoT device is an everyday item that has had internet connectivity added to it. Examples of IoT devices include baby monitors, drones, security cameras, smart televisions and solar inverters. IoT devices within homes and businesses generally use Wi-Fi or cellular networks, such as 4G or 5G, to connect to the internet.

Many IoT devices commonly found in Australian homes and businesses have not been designed with security in mind. This has resulted in devices being vulnerable to compromise via the internet. Such incidents can allow cybercriminals unsolicited access to your device and personal data for malicious purposes.

ACSC
Australian Cyber Security Centre

Australian Government
Australia's Smartest Resource



Guidance for individuals and businesses

Before purchasing an IoT device

- Is the device made by a well-known reputable company and sold by a well-known reputable store?
- Is it possible to change the password?
- Does the manufacturer provide updates?
- What data will the device collect and who will the data be shared with?
- Does the device do only what you want it to do?

Setting up an IoT device

- Does the device need to be connected to the internet?
- Is the device in a secure location?
- Do I change the default username and password?
- Is my Wi-Fi network set up securely and does it have a secure password?
- Are unnecessary device features turned off?



Guidance for individuals and businesses

Maintaining an IoT device

- Reboot your devices regularly
- Apply regular updates
- Turn off your device when not in use
- Watch for a significant increase in your monthly internet usage or bill

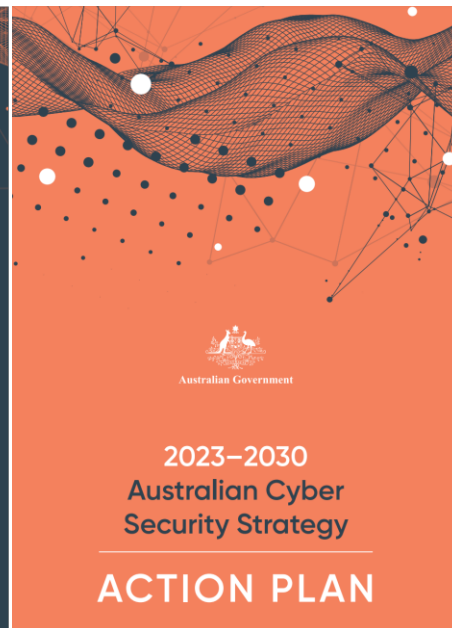
Disposing an IoT device

- Erase all data and personal information
- Perform a factory reset of the device
- Disassociate the device from mobile phones and other devices
- Remove any removable media (e.g., USB flash drives, memory cards etc.) attached to the device

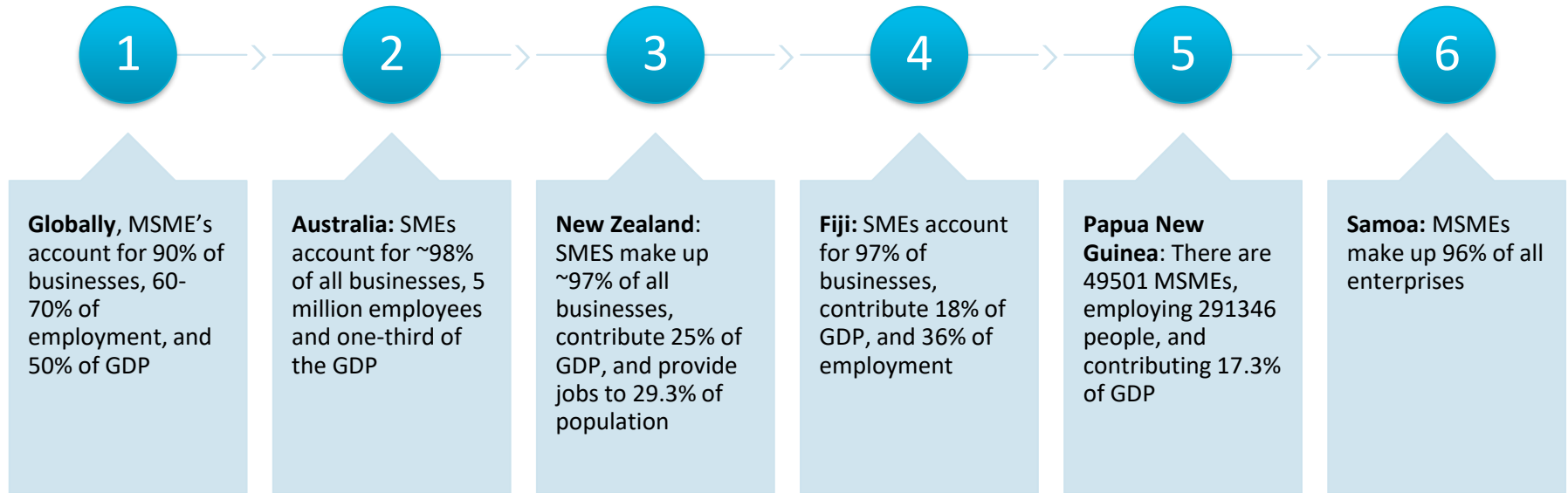
Shield 1: Strong businesses and citizens



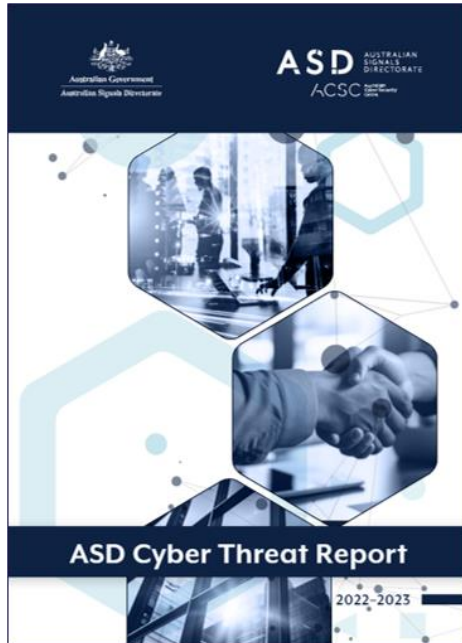
Uplifting Cyber Maturity at all levels



MSMEs: Backbone of the global economy



Small businesses make big targets



- In Australia, ~94,000 cybercrimes reported in FY 2022-23 (~23%↑)
- Average cost of cybercrime was \$46,000 for small businesses and \$97,200 for medium businesses (~14%↑)
- 60% of Australian businesses have an annual turnover < \$200,000
- 60% of small businesses experiencing a cyberattack shut down their business within six months

MSME's cybersecurity challenges and barriers



Limited Budget

~60% of Australian businesses have a turnover < \$200,000
~50% of businesses spend less than \$500 annually on cybersecurity



Lack of Awareness, Knowledge and Skills

~88% of small businesses have less than five employees
~50% of small business owners are over 50



Complacency

Cybersecurity is not a key aspect of digital strategy
SMEs underestimate cybersecurity threats



Lack of Support

One-size-fits-all approach
Overly technical
Challenges keeping up-to-date



Some initiatives to support Australian businesses

Australian Cyber Security Centre

- Resources for individuals, SMEs, large organisations, critical infrastructure, and government

Small Business Cyber Resilience Grant

- Free, tailored, person-to-person cybersecurity support for small businesses (to develop a tailored cybersecurity plan for small businesses)

Cyber Wardens

- Government-supported initiative to train 60,000 cyber wardens
- Businesses should have a cyber warden similar to a fire warden or a first aid officer

CyberBuddy

- **CSIRO-led initiative through Cyber Security CRC**
- “Do something” approach to cyber upliftment using state-of-the-art learning, gamification and nudging

Shield 2: Safe technology

- Mandating minimum cyber security standard for IoT devices
→ Cybersecurity Bill 2024
- Voluntary labelling scheme for consumer-grade smart devices
- Consistent with recommendation by CSIRO/CS CRC in 2020-21



Shield 4: Protected critical infrastructure



Shield 4: Protected critical infrastructure

Ensure the right entities are being protected

Ensure the right assets are being protected

Enhance cybersecurity obligations for Systems of National Significance

Ensure critical infrastructure is compliant with cybersecurity obligations

Help critical infrastructure manage the consequence of cyber incidents

Strengthen the cyber maturity of government departments and agencies

Identify and protect critical systems across government

Uplift the cyber skills of the Australian Public Service (APS)



AUSTRALIA'S NATIONAL SCIENCE AGENCY

[ABOUT](#) ▾

[RESEARCH](#) ▾

[WORK WITH US](#) ▾

[CAREERS](#) ▾

[EDUCATION](#) ▾

[NEWS](#) ▾

[EVENTS](#)



[HOME](#) / [ABOUT](#) / [MISSIONS](#) /

Critical Infrastructure Protection and Resilience

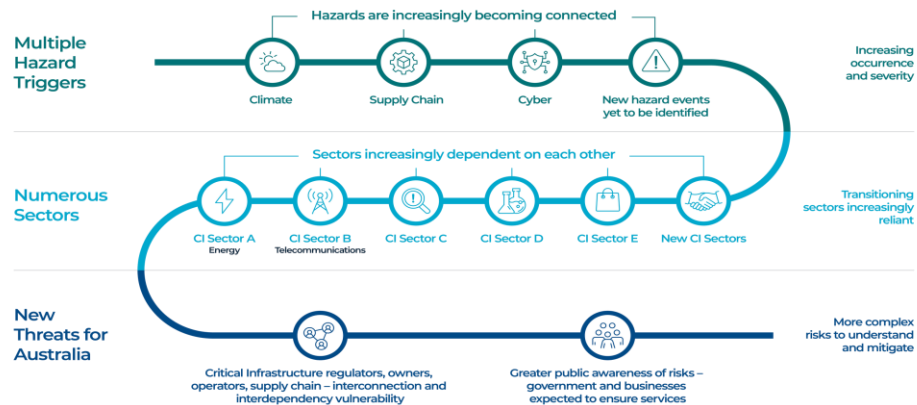
We are working with collaborators from across industry, research and government to co-design this mission. This summary reflects the mission in development and will continue to evolve.

[CONTACT](#)

[SHARE](#)



Australia's CI Challenges



Enabling Convergence

Digital Infrastructure

The foundation of an organisations IT and operation including physical and virtual technologies such as connectivity, cloud, computer, storage, network, applications and Everything as a Service (XaaS) platforms. Provides a basis for data consumption, sharing and other digital tasks.

Physical Infrastructure

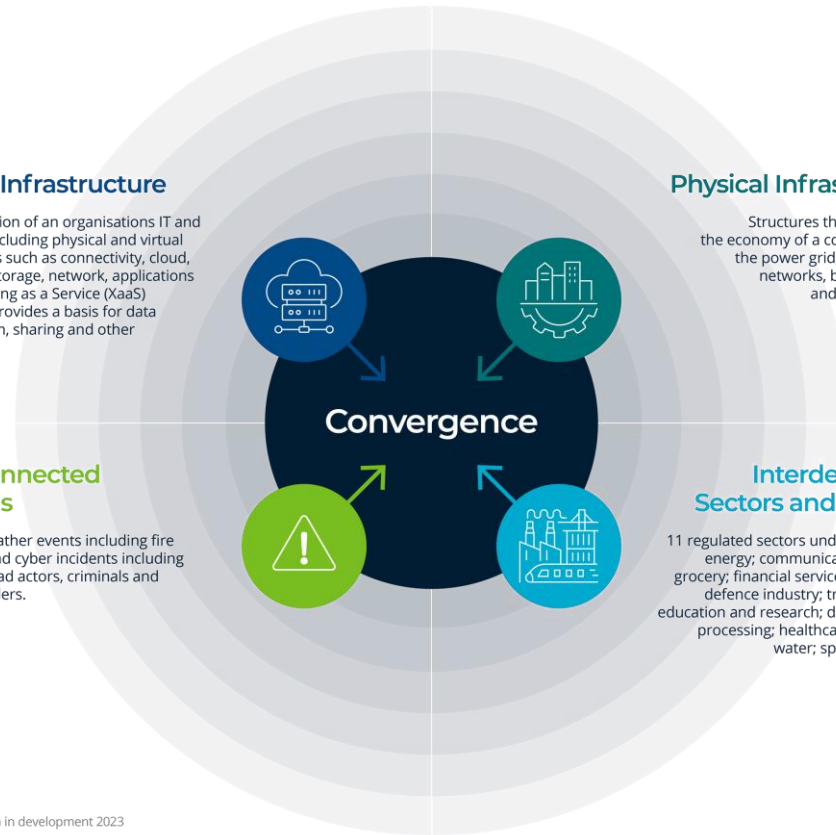
Structures that directly drive the economy of a country including the power grid, transportation networks, banks, highways and mobile towers.

Interconnected Hazards

Extreme weather events including fire and flood and cyber incidents including attacks by bad actors, criminals and trusted insiders.

Interdependent Sectors and Systems

11 regulated sectors under the SOCI Act: energy; communications; food and grocery; financial services and markets; defence industry; transport; higher education and research; data storage and processing; healthcare and medical; water; space technology.





Key Takeaways

- Develop National Cybersecurity Strategy that covers IoT-related risks, and digital transformation challenges
- Implement IoT-specific cybersecurity regulations and standards
- Launch cybersecurity awareness campaigns covering IoT and digital transformation
- Provide cybersecurity guidance for MSMEs in IoT adoption.
- Develop a national framework for resilience and disaster recovery

Thank you

Mohan Baruwal Chhetri, CSIRO's Data61

Australia's National Science Agency

