Cyber Security Resilience

Tony Hill – Digicel Pacific CISO
Telstra
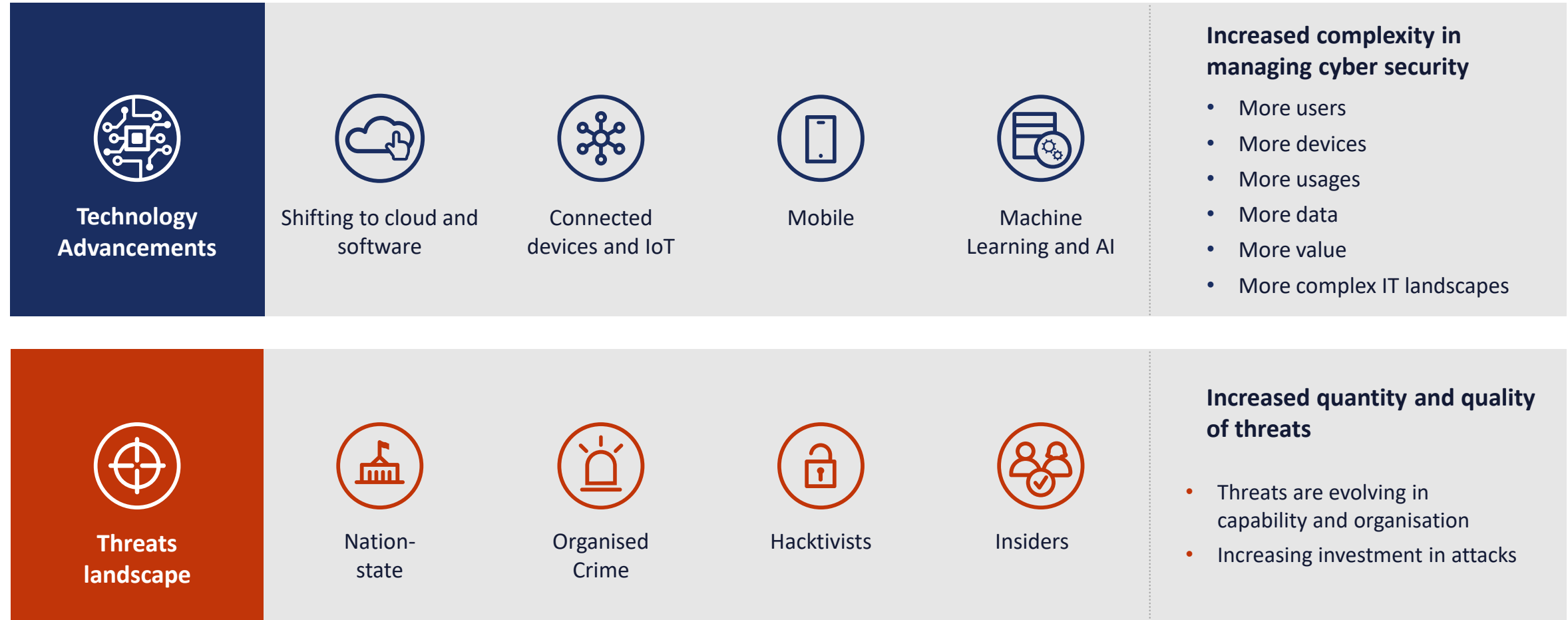
OUR WORLD IS RAPIDLY CHANGING

Cyber Security Mega Trends

Technology Advancements

Shifting to cloud and software

Connected devices and IoT

Mobile

Machine Learning and AI

Threats landscape

Nation-state

Organised Crime

Hacktivists

Insiders

Implications

Increased complexity in managing cyber security

- More users
- More devices
- More usages
- More data
- More value
- More complex IT landscapes

Increased quantity and quality of threats

- Threats are evolving in capability and organisation
- Increasing investment in attacks

General

THE CYBER SECURITY CHALLENGE

Significant **external and internal threat**

Corporate data is **valuable to many**

Growing number of vulnerabilities **with reducing time to exploit**

Increasing expectations amongst ALL stakeholders

Complex supply chain with barriers to understanding risk

Complex subject to discuss with stakeholders

PACIFIC CYBER CHALLENGES

Rapid transformation and digitisation **with exposure online**

Increasing regulatory and **corporate governance requirements**

Local skill shortages with increasing demand
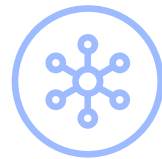
Increased (mature) telecommunications coverage across the entire nation

THE CURRENT STATE

There is an increasing internal/external threat.

Corporate data has high value – not just to nation states, but to others through online black markets.

It's not just about data breaches - integrity of data and availability of systems is increasingly important.

Cyber Security can be – or at the very least can be perceived to be – complex and not accessible to business owners or end users (low level of understanding).

But all is not lost!

THE WAY FORWARD IN THE PACIFIC

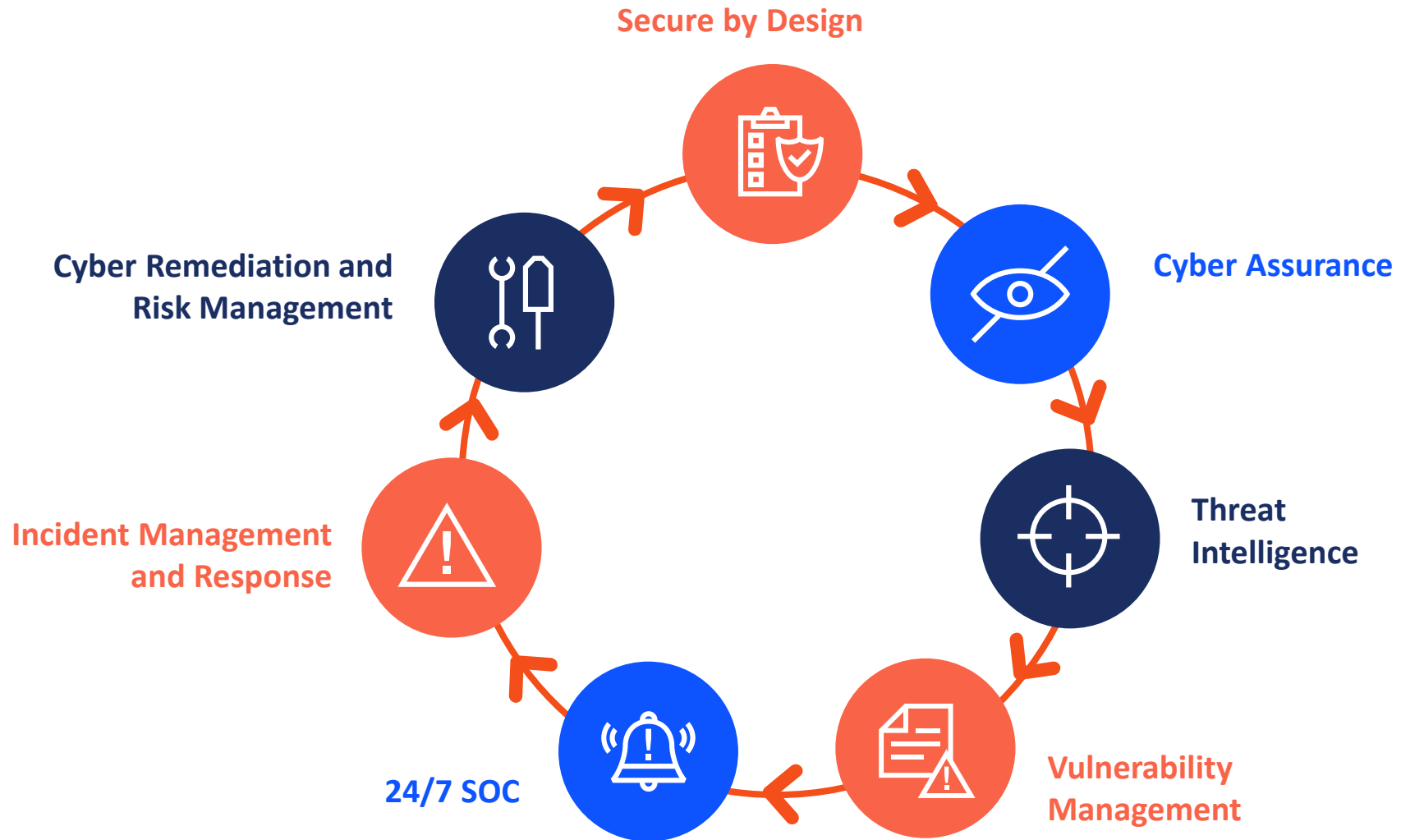The current cyber security offerings in the market are mature.

Most cloud services have built in security.

Security offerings available are global.

PNG, Fiji Government has developed guidance and policy in line with International Standards.

Opportunities exist to develop, train and build local capabilities.

General

THE CYBER SECURITY RESILIENCE MAP

Secure by Design

Cyber Assurance

Threat Intelligence

Vulnerability Management

24/7 SOC

Incident Management and Response

Cyber Remediation and Risk Management

SUMMARY

✓ Understand the **value** of your systems and data, **where** they are, **who has access** to them, and **who is protecting** them.

✓ Understand the **criticality** of your systems.

✓ Start with the '**things that matter**'.

✓ Establish robust cyber security processes including **risk management** and **incident response** processes – and **practice.**

✓ Cyber security is also about **people** (not just technology) – equip them to be a security control, not a security vulnerability.

✓ There will **never** be zero cyber security risk – but know your risk appetite, risk exposure, and manage/close the gap.

Thank you