



Gear up and Improve IT/OT Cybersecurity Maturity



Divya Dayalamurthy

Cybersecurity Lead – Arc Infrastructure

Agenda

- Introduction
- Arc Infrastructure
- Key risks in technology
- Emerging cyber threats in technology
- Deep Dive – Remediation
- Summary
- Q and A

To be the trusted manager of the State's freight rail network



SAFE, RELIABLE AND EFFICIENT

Our core business purpose is to run a safe, reliable and efficient rail network to enable growth in Western Australia

GROWTH

We are focused on our core business whilst pursuing complimentary development opportunities

RESILIENT AND SUSTAINABLE

We are investing to ensure that our business can continue to deliver into the future for our people, customers and communities

BUILD TRUST

We are seeking to build trust with every person connected to our business through our actions and behaviours

**The biggest hack in history:
Australians scramble to change
passports and driver licences after
Optus telco data debacle**

**CommonSpirit Health Ransomware
Attack Leads to \$150M in Losses To
Date**

**Latitude Financial Scrambles to Contain Large Data
Breach**

**Costa Rica State of Emergency
Declared After Ransomware
Attacks**

government to pay a \$20 million ransom.

Medibank says hacker accessed data of
9.7 million customers, refuses to pay
ransom

**Latitude Hack Worse Than First Thought, With 8
Million Driver's Licences Breached**

Triton is the world's most murderous malware, and it's spreading

Saudi petrochemical plant - Disable safety systems designed to prevent catastrophic industrial accidents

Taiwan's CPC suffers malware attack, experiences system outage

Customers asked to pay with cash or credit until Taiwan's major oil refiner resolves problem

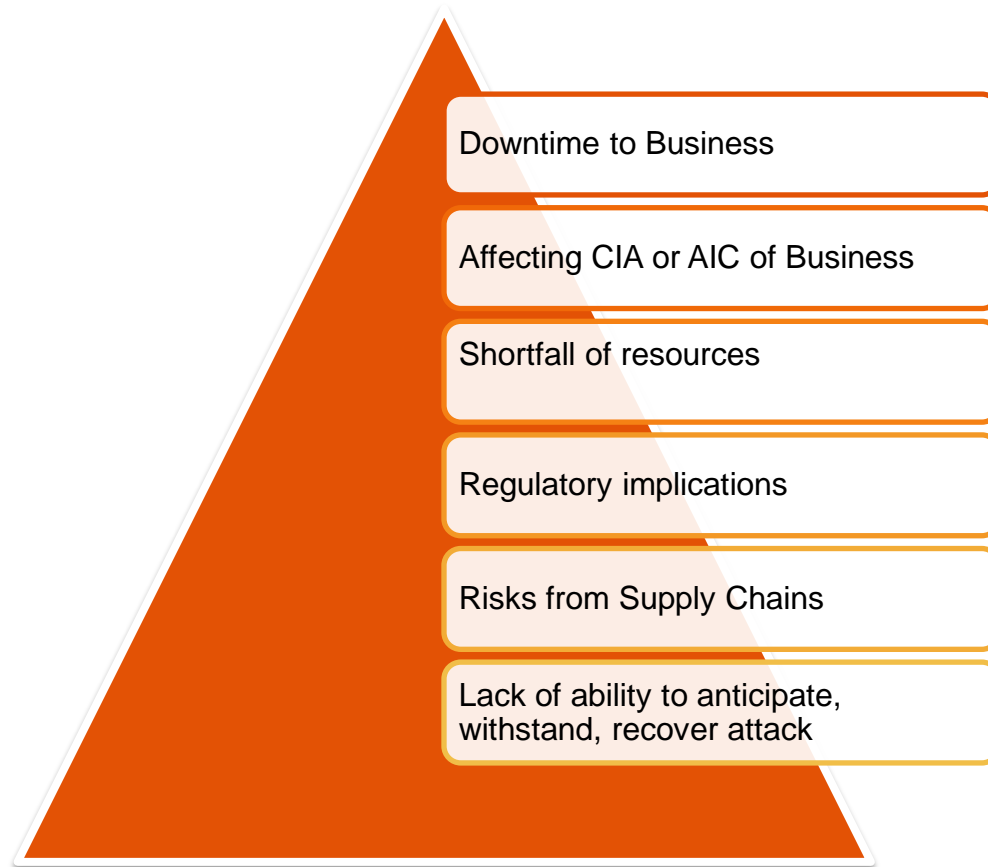
CYBERCRIME

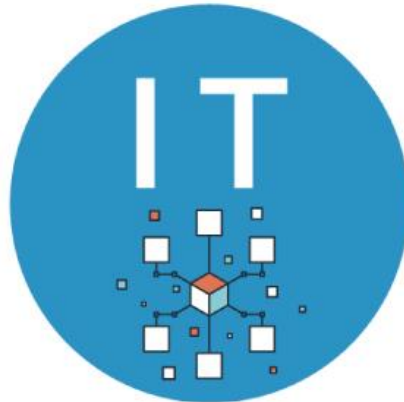
Iranian Hackers Access Unprotected ICS at Israeli Water Facility

Cyber-Attack Against Ukrainian Critical Infrastructure



The deeper impacts





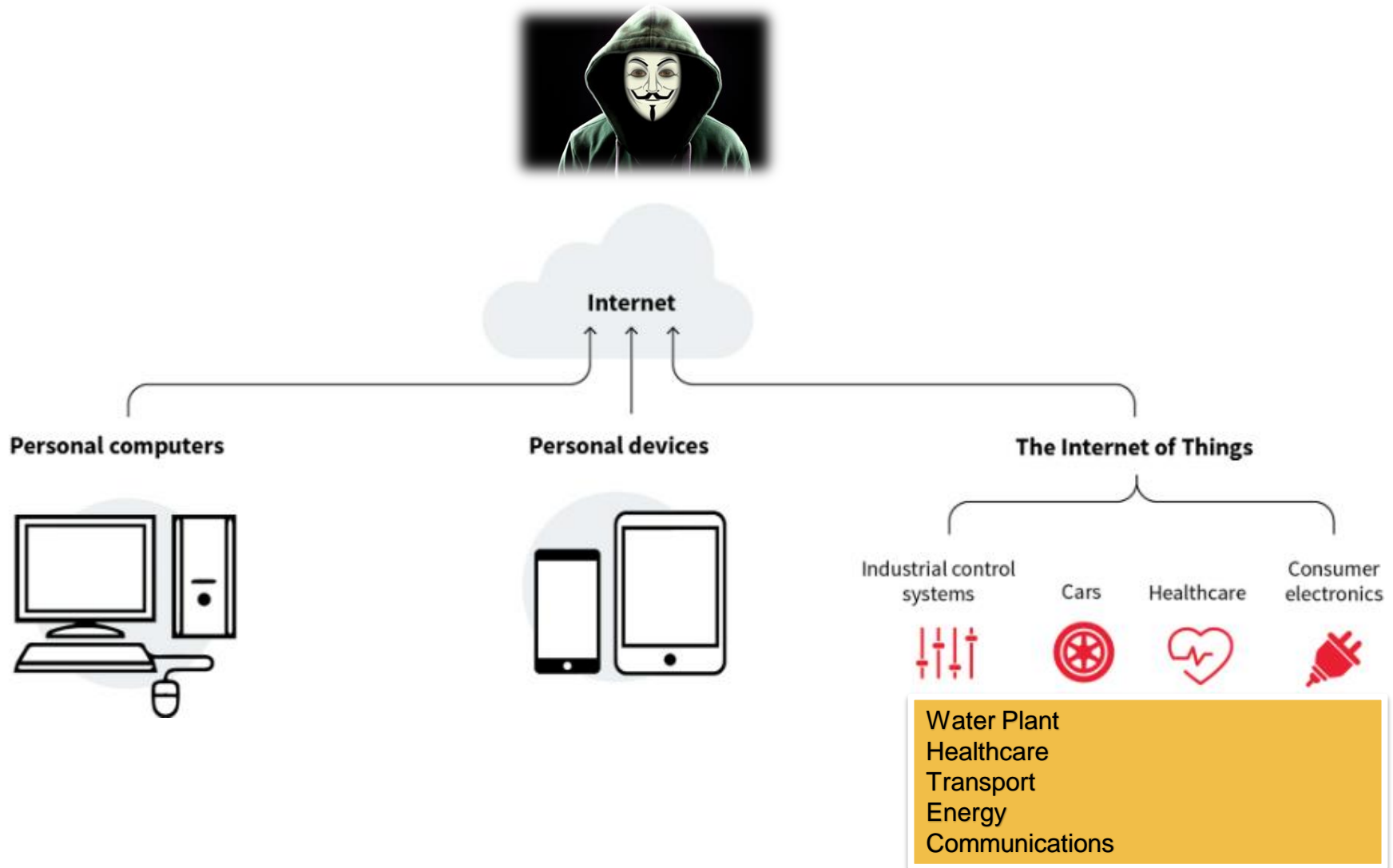
- Almost all the software and hardware have standardized.
- Allow software update.
- Being more tolerant (e.g. force-restart)

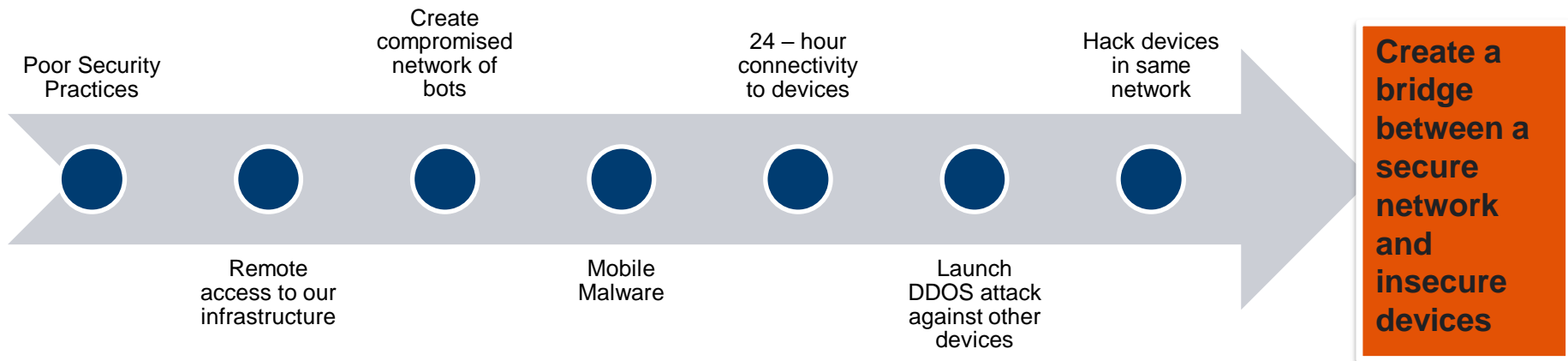


- 24-hour operating.
- Maximum production efficiency.
- Rarely updating software.

- **Critical and Zero-Day Vulnerability**
- **Lack of visibility**
- **Unknown assets are major vulnerability**
- **Any SIEM requires extra eye!**
- **Automated response is challenging**

- **Business Email Compromise**
- **Supply Chain threats**
- **Cloud based threats**
- **Ransomware**
- **IoT Hacking**
- **Insider threats**
- **State-sponsored cyber warfare**





Where to Start...!!!

- *ISA/IEC 62443 Standards for Security of Industrial Automation and Control Systems*
- *CISA Cybersecurity Best Practices for Industrial Control Systems*
- *ISO 27001 and ISO 27002*
- *NIST Cybersecurity Framework*
- *Security of Critical Infrastructure Act (SOCI)*
- *ENISA Good Practices for Security of Internet of Things in the Context of Smart Manufacturing*
- *NIST Guide to Industrial Control System (ICS) Security*
- *CIS Critical Security Controls ICS Companion Guide*
- *Australia: SLACIP Act / AS 7770*



- 01 Identify and maintain an Asset Inventory**
- 02 Risk assessment based on criticality of assets**
- 03 Understanding potential threats / vulnerabilities of assets**
- 04 Keep updating..!**
- 05 Include Supply Chain assets/ systems**



01 Segment the networks

Identify with asset owners

VLANs / Subnets


Interfaces between application and systems

02 Access Controls

03 Encryption

04 Security Awareness Training

05 Defence in depth protections

- 
- 01** Network Monitoring for abnormal activities
 - 02** Log Analysis – SIEM
 - 03** Endpoint detection and Response
 - 04** Threat Intelligence (Reports, governments, external sources)
 - 05** Test your technologies – Pen Test

- 01 Backup and recovery Plan**
- 02 Incident Response Plan**
- 03 Disaster Recovery**
- 04 Test - System and data restoration**
- 05 System and data validation**
- 06 Continuous improvement**

Cybersecurity maturity is not a destination, it is a journey.!

**Know
your
Assets**

**Segment
your
Networks**

**Invest in technology and
tools suitable for your
business**

**Cybersecurity
Training**

**Collaborate and build relationship with government agencies and
other organization to share threat intelligence and best practices**

Email Address

- Divya.Dayalamurthy@arcinfra.com

LinkedIn

- [linkedin.com/in/divyadayalamurthy/](https://www.linkedin.com/in/divyadayalamurthy/)

