CIIP OVERVIEW

# INTRODUCTION TO CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

Aaron Boyd – aboyd@welchmankeen.com

Philip Victor– vphilip@welchmankeen.com

Elvin Prasad– eprasad@welchmankeen.com

WELCHMAN KEEN

ITUEvents

CyberDrill

for the Pacific Islands

Online event:
8-10 December 2020

#Cybersecurity

ITU Pacific CyberDrill

ABOUT US

# WELCHMAN KEEN IS A STRATEGIC ADVISORY

- ✓ As a part of our focus on connectivity, we provide training on a variety of topics.
- ✓ Help to build a country’s CII strategy from the ground up through a measured approach to include what is necessary in achieving their specific objectives.
- ✓ Our key focus on critical information infrastructure (CII) represents a belief that these pillars hold the key to national, economic, public safety and social well-being.

TECHNOLOGY POLICY

TELECOMMUNICATION INVESTMENT STRATEGY

CYBER RISK AND POLICY

Wk.

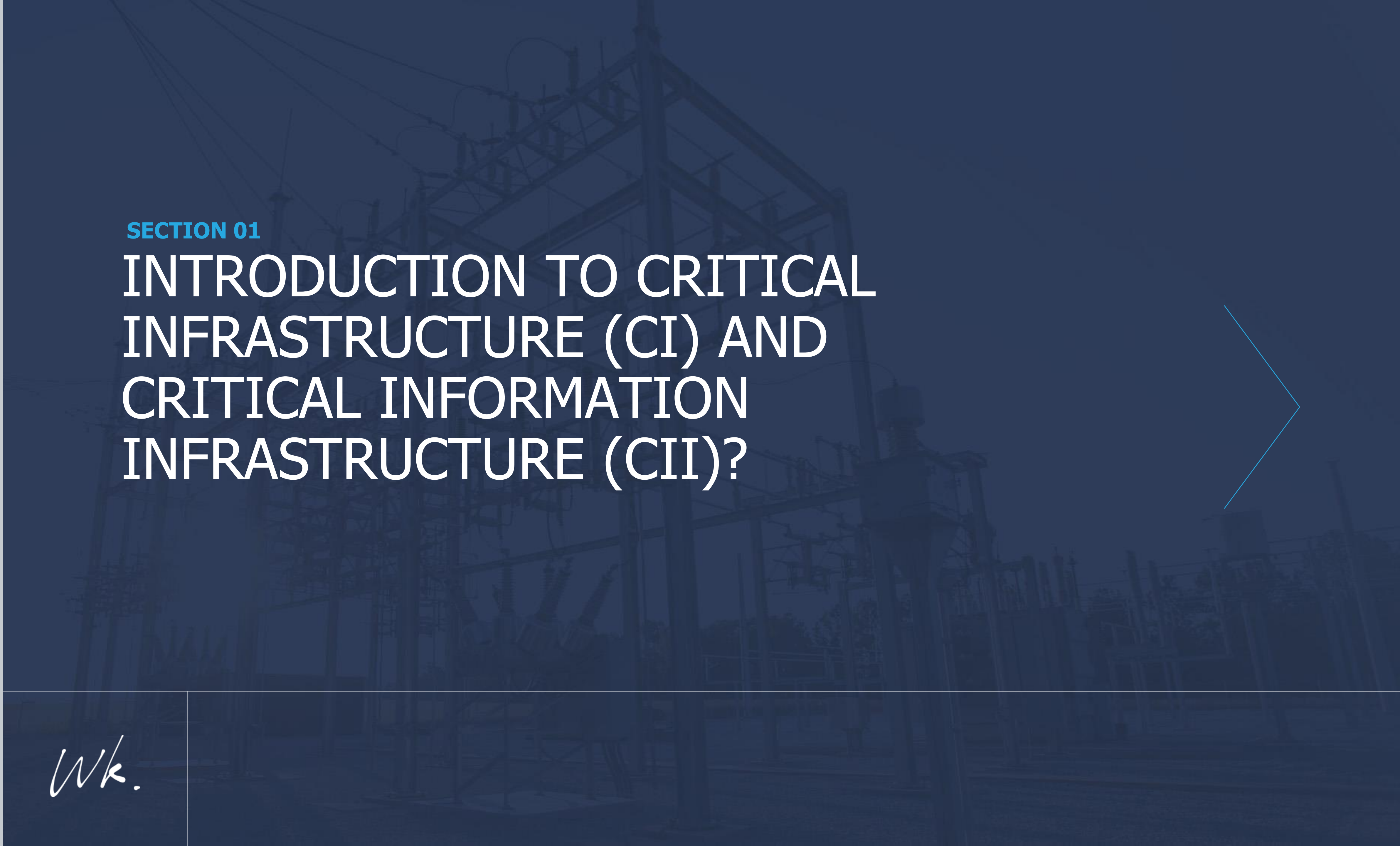
ITU SECTOR MEMBER

## AGENDA

- ✓ Introduction to critical infrastructure (CI) & Critical Information Infrastructure (CII)
- ✓ Define and describe the importance of ensuring the security and resiliency of critical information infrastructure
- ✓ Understanding and defining critical sectors in the country
- ✓ Breakout session 1 – Group discussion
  - Critical infrastructure status in Pacific Island countries
  - Critical infrastructure sectors identification
  - Niche sectors identification (during pandemic?)
  - Challenges to identify critical sectors

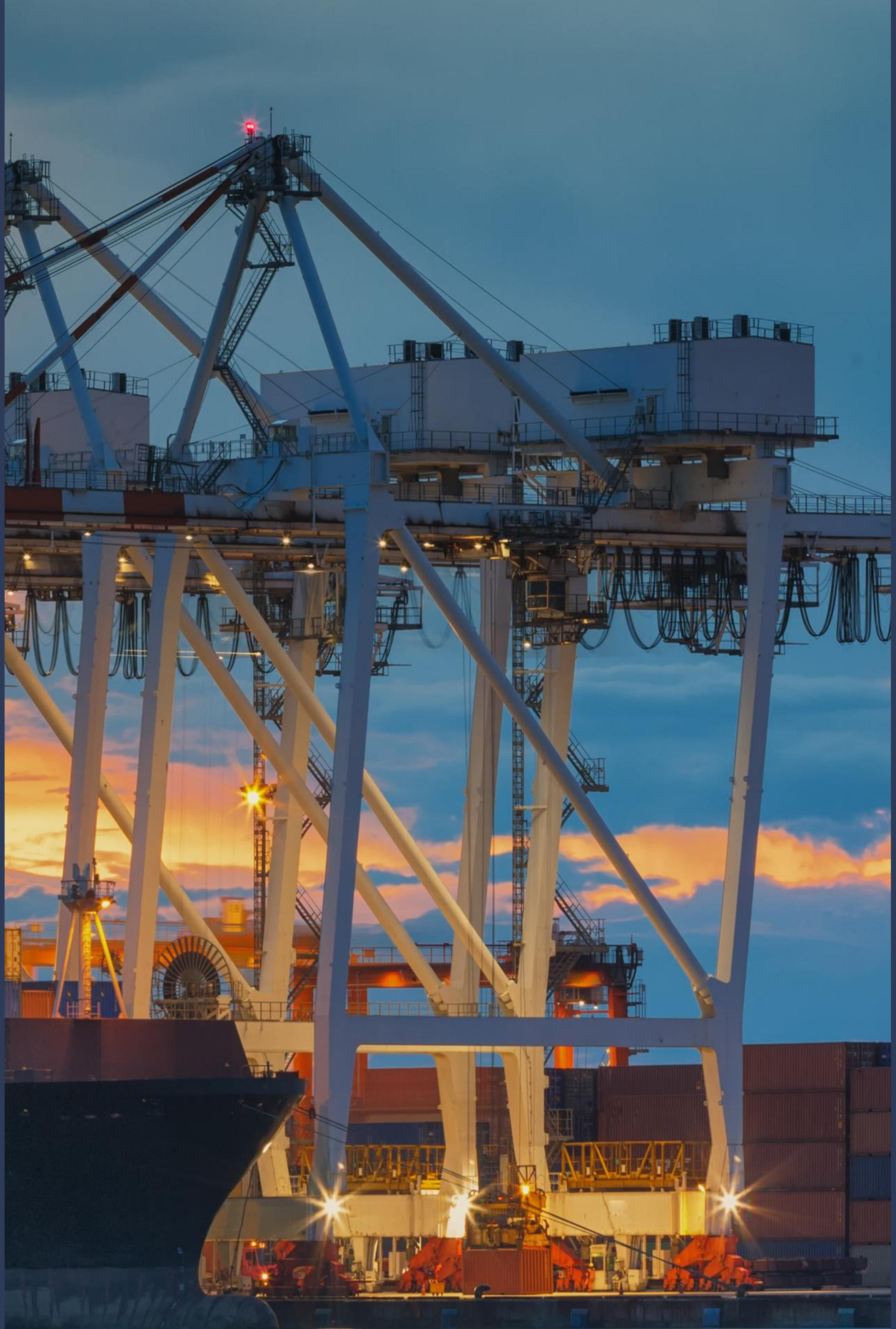
# AGENDA

- ✓ Identifying roles and responsibilities in managing the protection of critical information infrastructure within the government and sector specific agencies
- ✓ Threats and attacks on critical information infrastructure
- ✓ Breakout session 2 – Group discussion
  - Identification of roles and responsibilities – Government, industry & agencies
  - Collaboration and information sharing between government and critical infrastructure
  - Computer Emergency Response Team (CERT)
- ✓ Strategies to address cyber threats for the protection of critical information infrastructure
- ✓ Conclusion



SECTION 01

# INTRODUCTION TO CRITICAL INFRASTRUCTURE (CI) AND CRITICAL INFORMATION INFRASTRUCTURE (CII)?



## Critical Infrastructure

“Those infrastructures which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have serious consequences.”

SOURCE:

Global Forum on Cyber Expertise (GFCE)

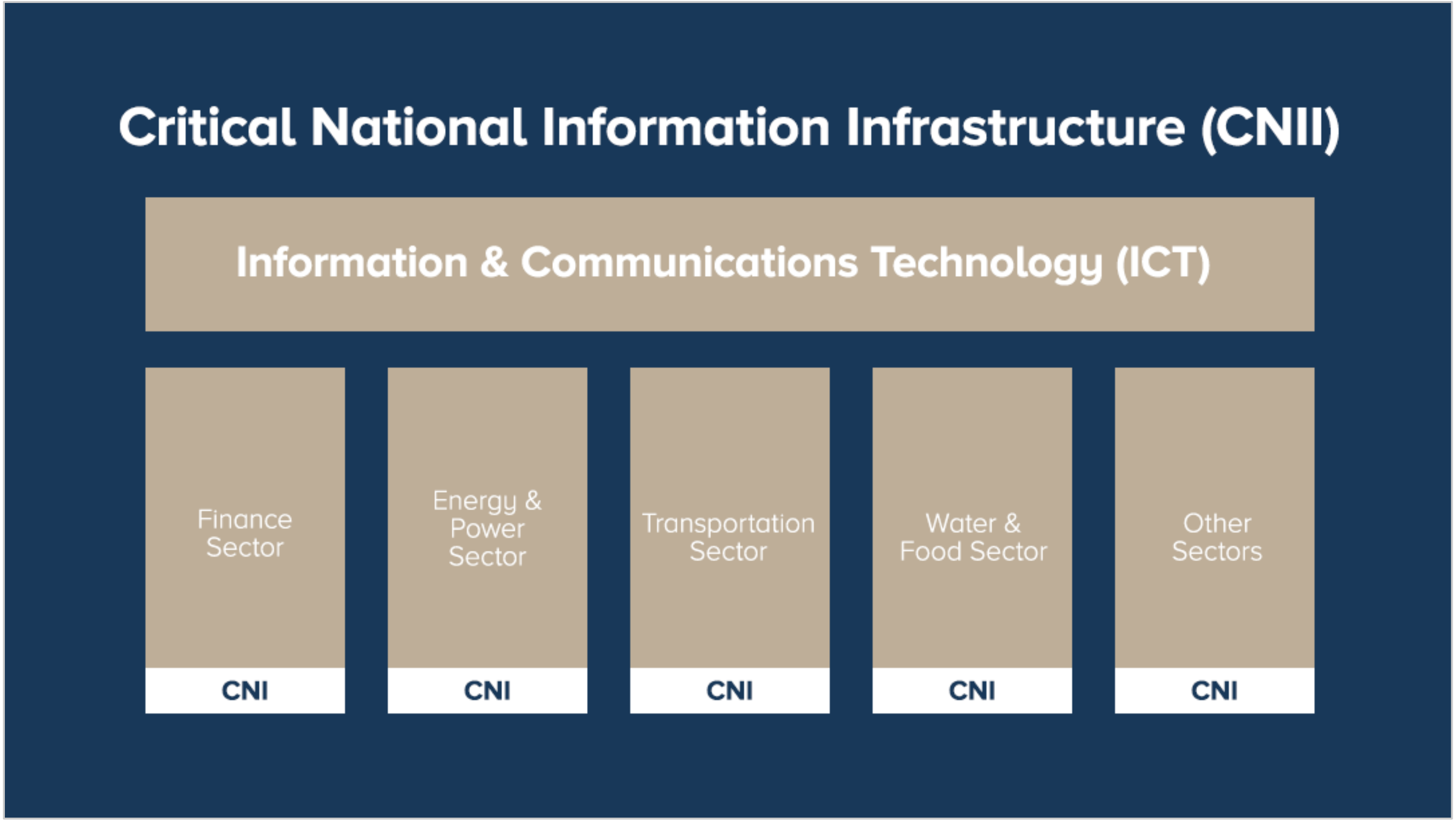
## Critical Information Infrastructure (CII)

> “Material and digital assets, networks, services, and installations that, if disrupted or destroyed, would have a serious impact on the health, security, or economic well-being of citizens and the efficient function of a country’s government.”

SOURCE:

INTERNATIONAL CIIP HANDBOOK 2008/2009

# CNI & CNII Integration



Critical National Information Infrastructure (CNII)

Information & Communications Technology (ICT)

| Finance Sector | Energy & Power Sector | Transportation Sector | Water & Food Sector | Other Sectors |
|---|---|---|---|---|
| CNI | CNI | CNI | CNI | CNI |

CNI FOCUS

# OECD 2015 Security Risk Recommendation:

✓ CNI should focus on the protection of essential services against digital security risk rather than the protection of critical information infrastructures themselves.

Wk.

SECTION 02

# SECURITY AND RESILIENCY OF CRITICAL INFORMATION INFRASTRUCTURE

# IMPORTANCE OF CII SECURITY

- ✓ Critical Information Infrastructure plays a vital role for the well-functioning of society and economy
- ✓ A cyber attack or an outage affecting these infrastructures could have cascading effects on large part of the population
- ✓ Cyberattacks on critical infrastructure have become increasingly more complex and more disruptive, causing systems to shut-down, disrupting operations, or simply enabling attackers to remotely control affected systems
- ✓ Traditionally, control systems were segregated from the open internet as they were deployed on air-gapped networks and under tight physical security
- ✓ Eliminating air-gap security in favour of improving efficiency and cutting down costs has opened critical infrastructures to threats and cyberattacks

# IMPORTANCE OF CII SECURITY

- ✓ Smart sensors and communication technologies bundled into various industrial control systems expose infrastructures and organizations to risks. (IoT)
- ✓ Cyberattacks on critical infrastructures can have a significant economic impact, especially when targeted in conflict between nations
- ✓ Securing these systems is not a matter of fully reverting to physical access, but a matter of understanding how internet-connected control systems work, how they are configured, and how they are accessed
- ✓ Visibility and management is key in beefing up security, but security and IT professionals must be aware of the risks and set-in place security controls aimed at reducing the impact of a potential cyberattack and increasing the cost of attack for threat actors

SECTION 03

# IDENTIFYING AND DEFINING CRITICAL SECTORS

# CRITICAL SECTORS DEPENDENCIES - EXAMPLES

### HYOGOKEN-NANBU EARTHQUAKE (KOBE, JAPAN)

The Hyogoken-Nanbu earthquake that struck Kobe, Japan and surrounding areas on January 17, 1995.The earthquake resulted in more than 6000 deaths and 30,000injuries, and accounted for an estimated economic loss of US$200billion. Trains were derailed and a power failure left approximately one million people without electricity

### POWER GRID FAILURES (INDIA)

In July 2012, several power grids failed in India, resulting in power blackouts in most of the northern and north-eastern states. The blackouts and their crippling effects on the other critical infrastructures affected the lives of approximately six hundred million people

### HURRICANE KATRINA (UNITED STATES)

Another example is the 2005 Hurricane Katrina in the United States, which caused severe floods and critical infrastructure collapse that completely paralyzed New Orleans, Louisiana and severely affected several Gulf Coast states

# Overarching Notion:

A disruption will have severe consequences on socio-economic well-being and public safety, including national security

# CNII SECTORS

✓ A critical sector in one country may not be critical to another, however, there are common sectors that most countries agree on to be categorised as critical and essential.

✓ Governments must prioritize these sectors when it comes to its protection as it relies on the availability of funding, technology and human capacity.

Health

ICT

Energy

Security & Defense

Water

Manufacturing

Food

Transportation

Finance

Government

SECTION 04

# BREAKOUT SESSION 1 – GROUP DISCUSSION

## QUESTIONS

- ✓ Has your country identified its critical sectors? If yes, what are these sectors and are there any niche sectors?
- ✓ Were there any new sectors identified during the recent pandemic? Discuss
- ✓ What are the challenges faced in identifying critical sectors? (especially for countries that have not identified these sectors)

SECTION 05

# IDENTIFYING ROLES AND RESPONSIBILITIES IN MANAGING CRITICAL INFORMATION INFRASTRUCTURE

# PROTECTING CII – ROLES AND RESPONSIBILITIES

- ✓ Protecting critical infrastructure against growing and evolving cyber threats requires a layered approach.
- ✓ ***Government*** must actively collaborate with the public and private sector partners to improve the security and resilience of critical infrastructure
- ✓ Information sharing and collaboration platform is vital between public-private CII
- ✓ Build and grow the cyber workforce to ensure sufficient skills and talent is available
- ✓ National Computer Emergency Response Teams (CERT) must respond to and mitigate the impacts of attempted disruptions to the nation's critical cyber and communications networks and to reduce adverse impacts on critical network systems

# PROTECTING CII – CERT/CIRT

A CERT/CIRT is an organisation or team that provides, to a well-defined constituency, services and support for both preventing and responding to computer security incidents

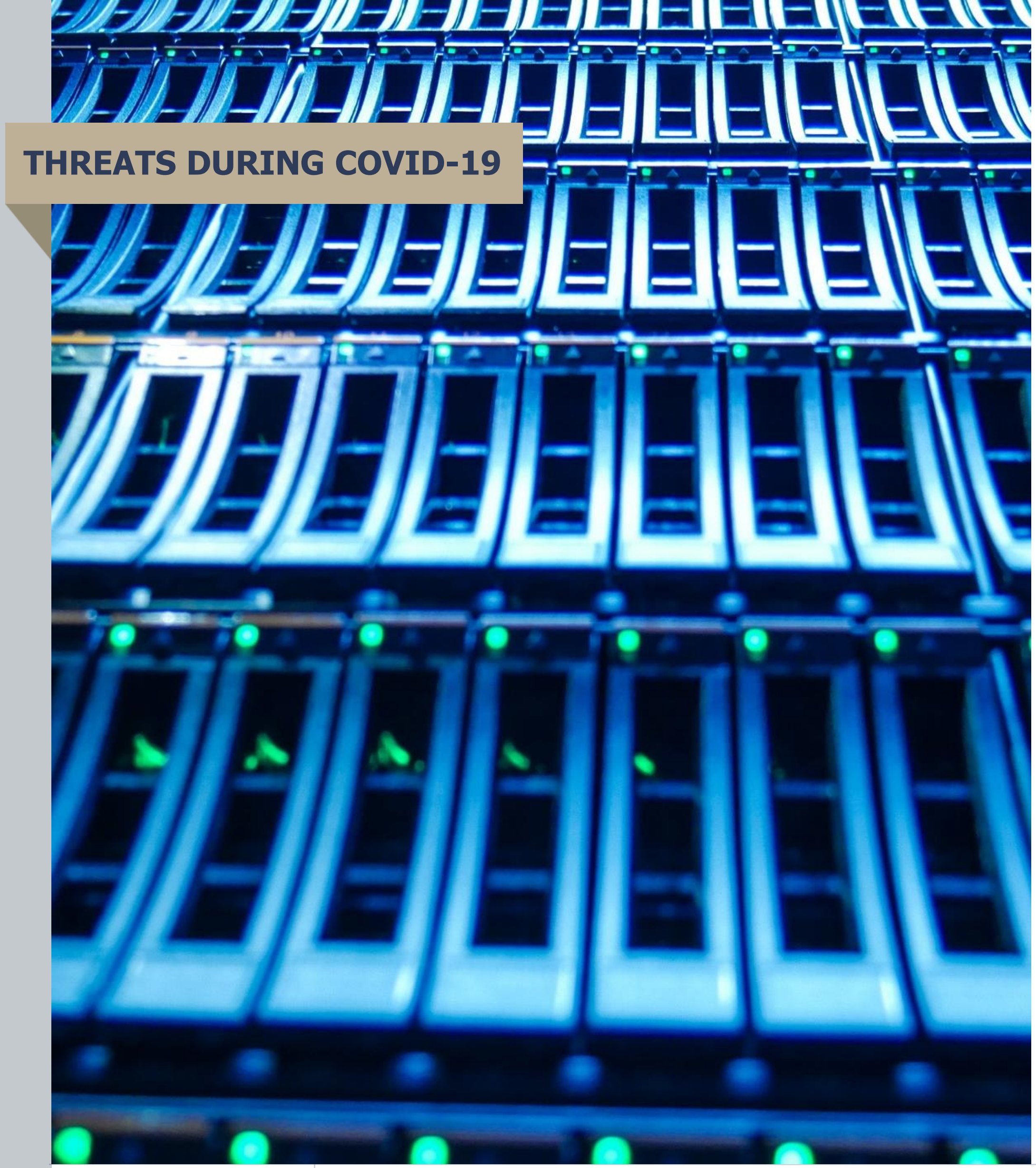
**Objectives of incident response:**

- ✓ To mitigate or reduce risks associated to an incident
- ✓ To respond to all incidents and suspected incidents based on pre-determined process
- ✓ Provide unbiased investigations on all incidents
- ✓ Establish a 24x7 hotline/contact – to enable effective reporting of incidents.
- ✓ Control and contain an incident
- ✓ Affected systems return to normal operation
- ✓ Recommend solutions – short-term and long-term solutions

SECTION 06

# THREATS AND ATTACKS ON CNII

Cybersecurity



THREATS DURING COVID-19

# INCREASED CYBER THREATS DURING COVID-19

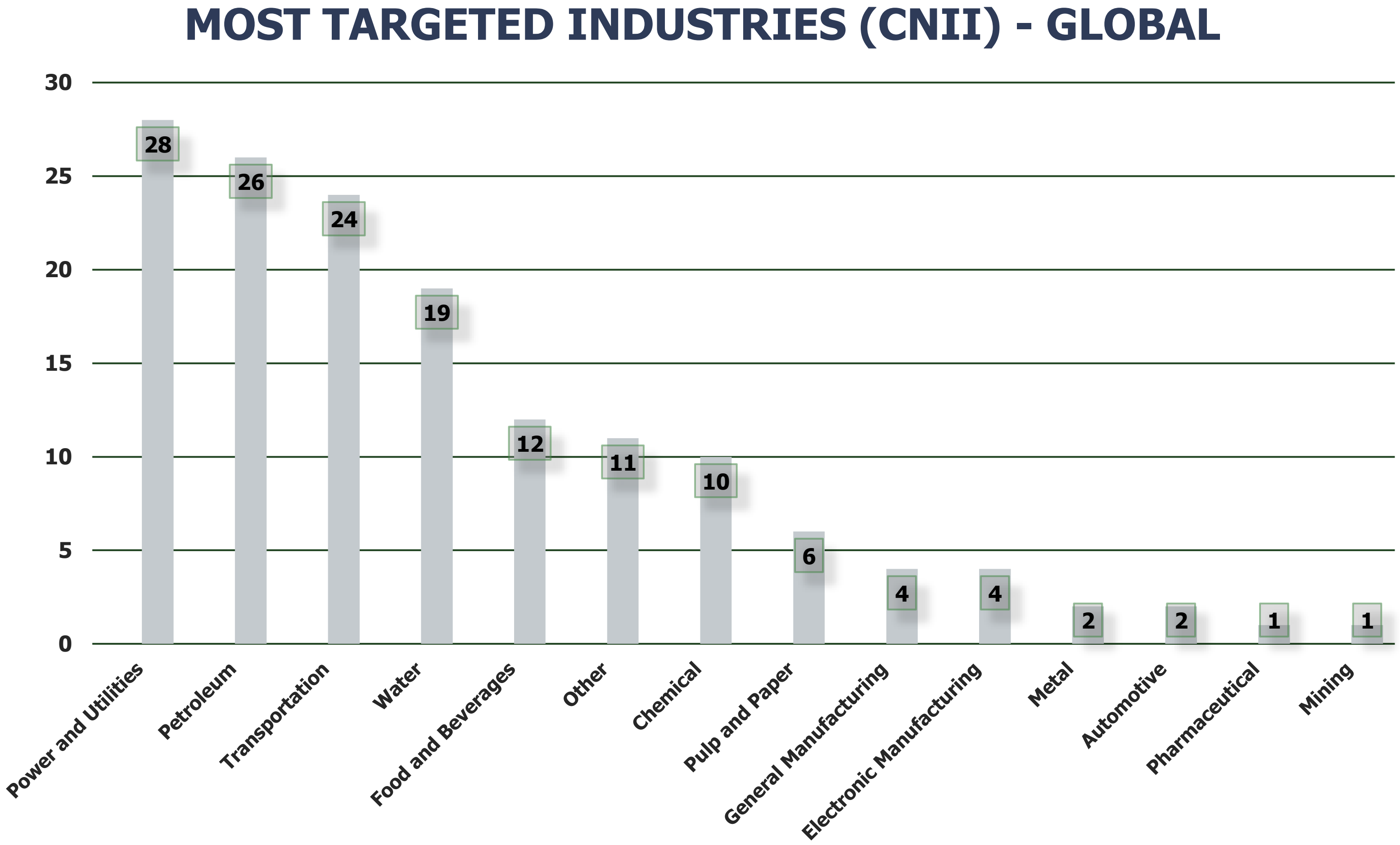
- ✓ Recent assessment conducted by INTERPOL, it was revealed that the Covid-19 pandemic has seen a shift of attacks from small businesses to critical infrastructure, government and major corporations.
- ✓ Deloitte reported that COVID-19 is seeing a "next normal" where sectors not classified as critical before are now being viewed as critical.
- ✓ Healthcare and humanitarian organisations such as WHO are being targeted and Check Point Software Technologies reported a 500% increase in attacks toward these organisations.
- ✓ Hackers targeting companies critical to the distribution of Covid-19 vaccines. "A global phishing campaign" focused on organisations associated with the Covid-19 vaccine "cold chain" – IBM, Dec 3, 2020

Wk.

THREATS AND ATTACKS

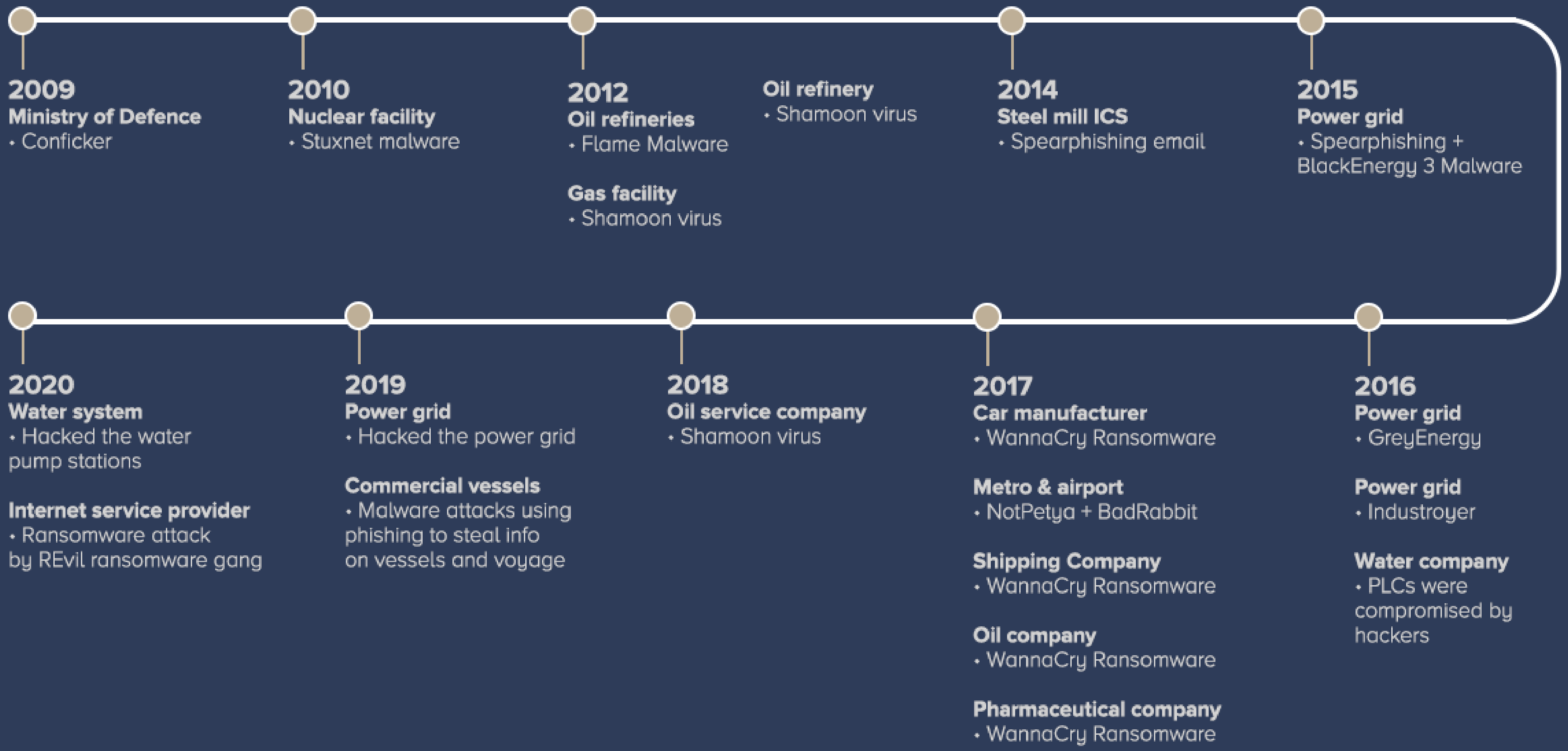
# Most Targeted Industries

Global Statistics


MOST TARGETED INDUSTRIES (CNII) - GLOBAL

# Global CNII Cyber Attacks

2009 - 2020



**2009**
**Ministry of Defence**
- Conficker

**2010**
**Nuclear facility**
- Stuxnet malware

**2012**
**Oil refineries**
- Flame Malware

**Gas facility**
- Shamoon virus

**Oil refinery**
- Shamoon virus

**2014**
**Steel mill ICS**
- Spearphishing email

**2015**
**Power grid**
- Spearphishing + BlackEnergy 3 Malware

**2016**
**Power grid**
- GreyEnergy

**Power grid**
- Industroyer

**Water company**
- PLCs were compromised by hackers

**2017**
**Car manufacturer**
- WannaCry Ransomware

**Metro & airport**
- NotPetya + BadRabbit

**Shipping Company**
- WannaCry Ransomware

**Oil company**
- WannaCry Ransomware

**Pharmaceutical company**
- WannaCry Ransomware

**2018**
**Oil service company**
- Shamoon virus

**2019**
**Power grid**
- Hacked the power grid

**Commercial vessels**
- Malware attacks using phishing to steal info on vessels and voyage

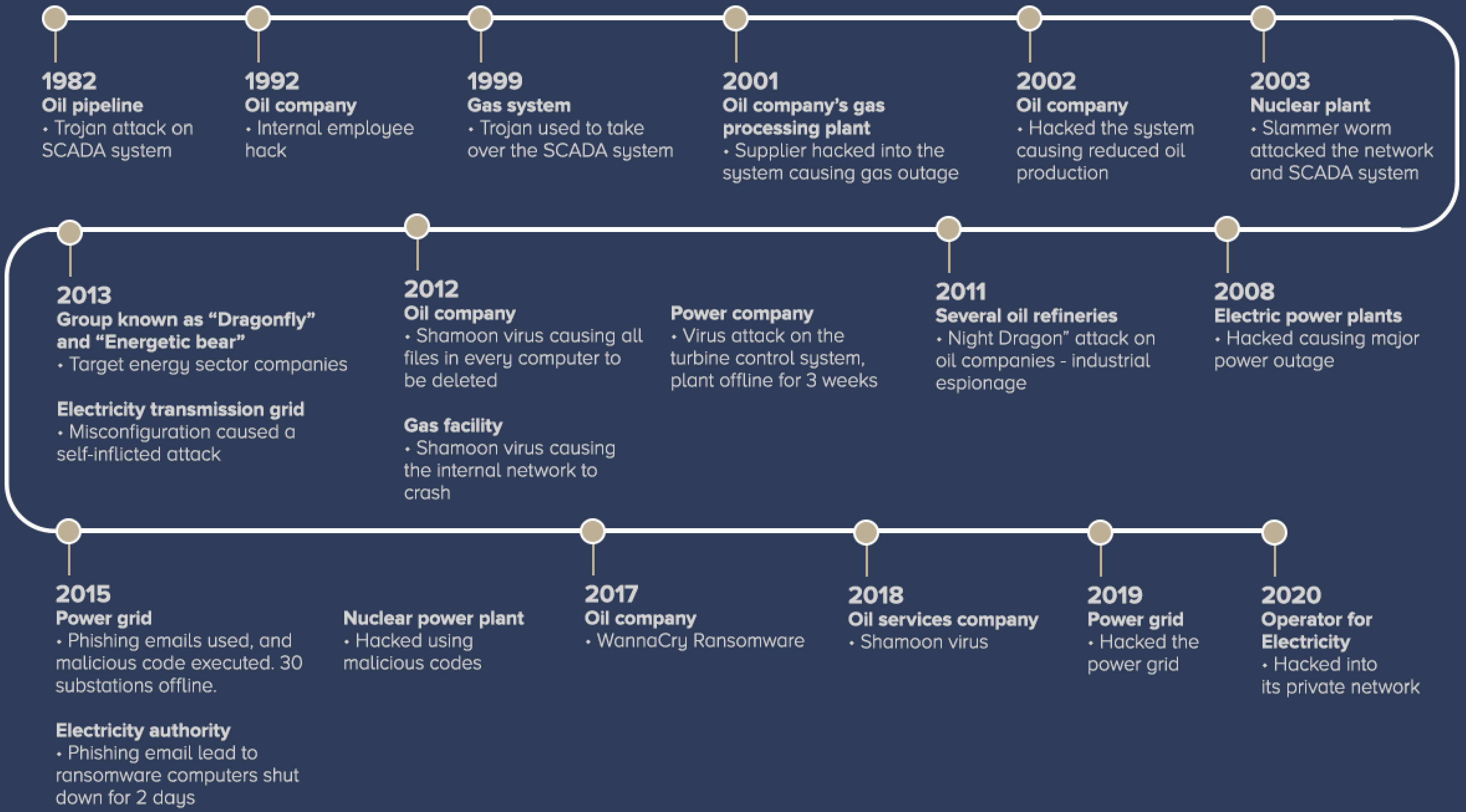
**2020**
**Water system**
- Hacked the water pump stations

**Internet service provider**
- Ransomware attack by REvil ransomware gang

# CNII Cyber Attacks

Energy & Power Grid

(1982 – 2020)



**1982**
**Oil pipeline**
- Trojan attack on SCADA system

**1992**
**Oil company**
- Internal employee hack

**1999**
**Gas system**
- Trojan used to take over the SCADA system

**2001**
**Oil company's gas processing plant**
- Supplier hacked into the system causing gas outage

**2002**
**Oil company**
- Hacked the system causing reduced oil production

**2003**
**Nuclear plant**
- Slammer worm attacked the network and SCADA system

**2008**
**Electric power plants**
- Hacked causing major power outage

**2011**
**Several oil refineries**
- Night Dragon" attack on oil companies - industrial espionage

**2012**
**Oil company**
- Shamoon virus causing all files in every computer to be deleted

**Gas facility**
- Shamoon virus causing the internal network to crash

**Power company**
- Virus attack on the turbine control system, plant offline for 3 weeks

**2013**
**Group known as "Dragonfly" and "Energetic bear"**
- Target energy sector companies

**Electricity transmission grid**
- Misconfiguration caused a self-inflicted attack

**2015**
**Power grid**
- Phishing emails used, and malicious code executed. 30 substations offline.

**Electricity authority**
- Phishing email lead to ransomware computers shut down for 2 days

**Nuclear power plant**
- Hacked using malicious codes

**2017**
**Oil company**
- WannaCry Ransomware

**2018**
**Oil services company**
- Shamoon virus

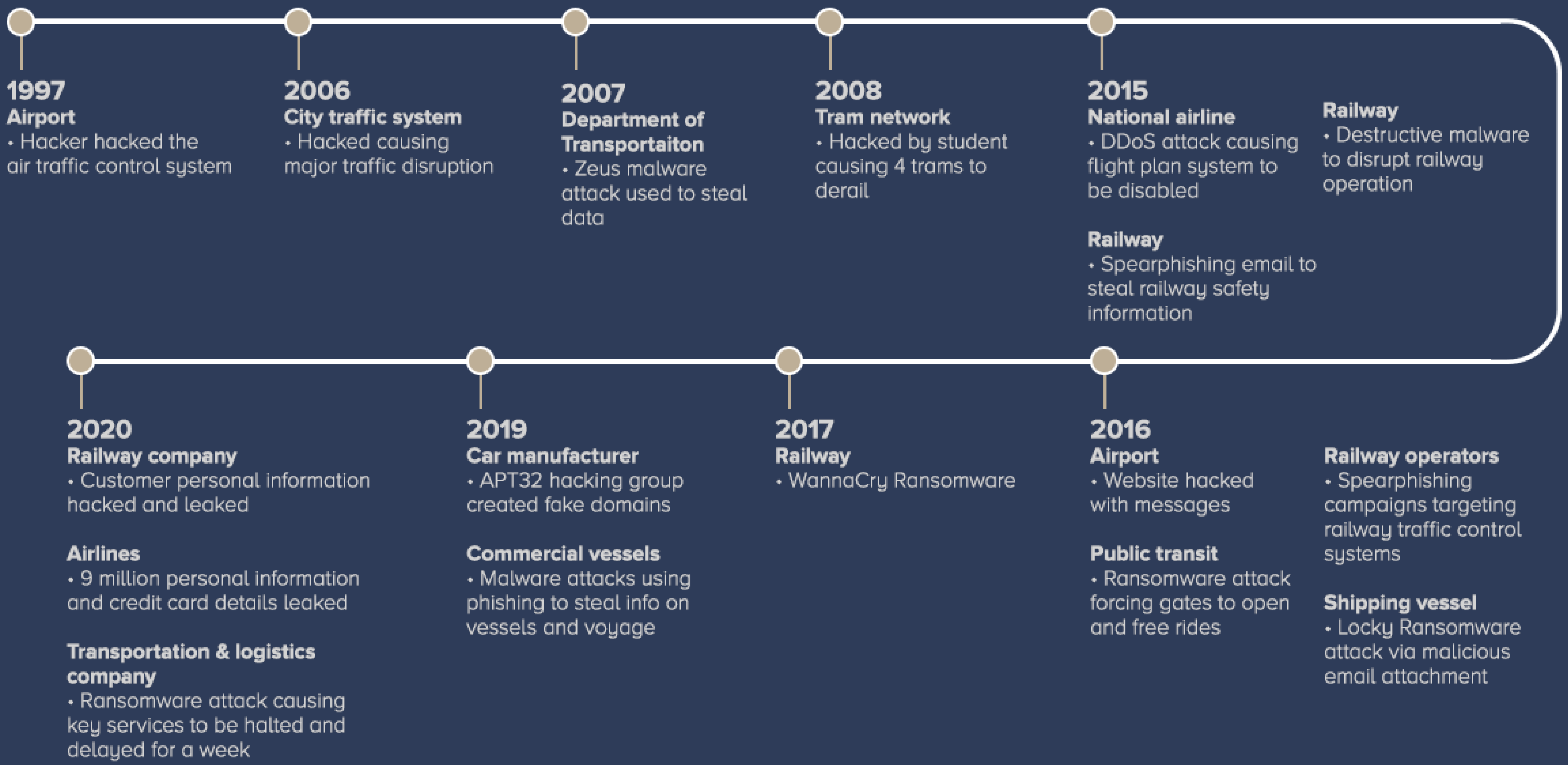
**2019**
**Power grid**
- Hacked the power grid

**2020**
**Operator for Electricity**
- Hacked into its private network

# CNII Cyber Attacks

Transportation

(1997 – 2020)



**1997**
**Airport**
- Hacker hacked the air traffic control system

**2006**
**City traffic system**
- Hacked causing major traffic disruption

**2007**
**Department of Transportaiton**
- Zeus malware attack used to steal data

**2008**
**Tram network**
- Hacked by student causing 4 trams to derail

**2015**
**National airline**
- DDoS attack causing flight plan system to be disabled

**Railway**
- Spearphishing email to steal railway safety information

**Railway**
- Destructive malware to disrupt railway operation

**2016**
**Airport**
- Website hacked with messages

**Public transit**
- Ransomware attack forcing gates to open and free rides

**Railway operators**
- Spearphishing campaigns targeting railway traffic control systems

**Shipping vessel**
- Locky Ransomware attack via malicious email attachment

**2017**
**Railway**
- WannaCry Ransomware

**2019**
**Car manufacturer**
- APT32 hacking group created fake domains

**Commercial vessels**
- Malware attacks using phishing to steal info on vessels and voyage

**2020**
**Railway company**
- Customer personal information hacked and leaked

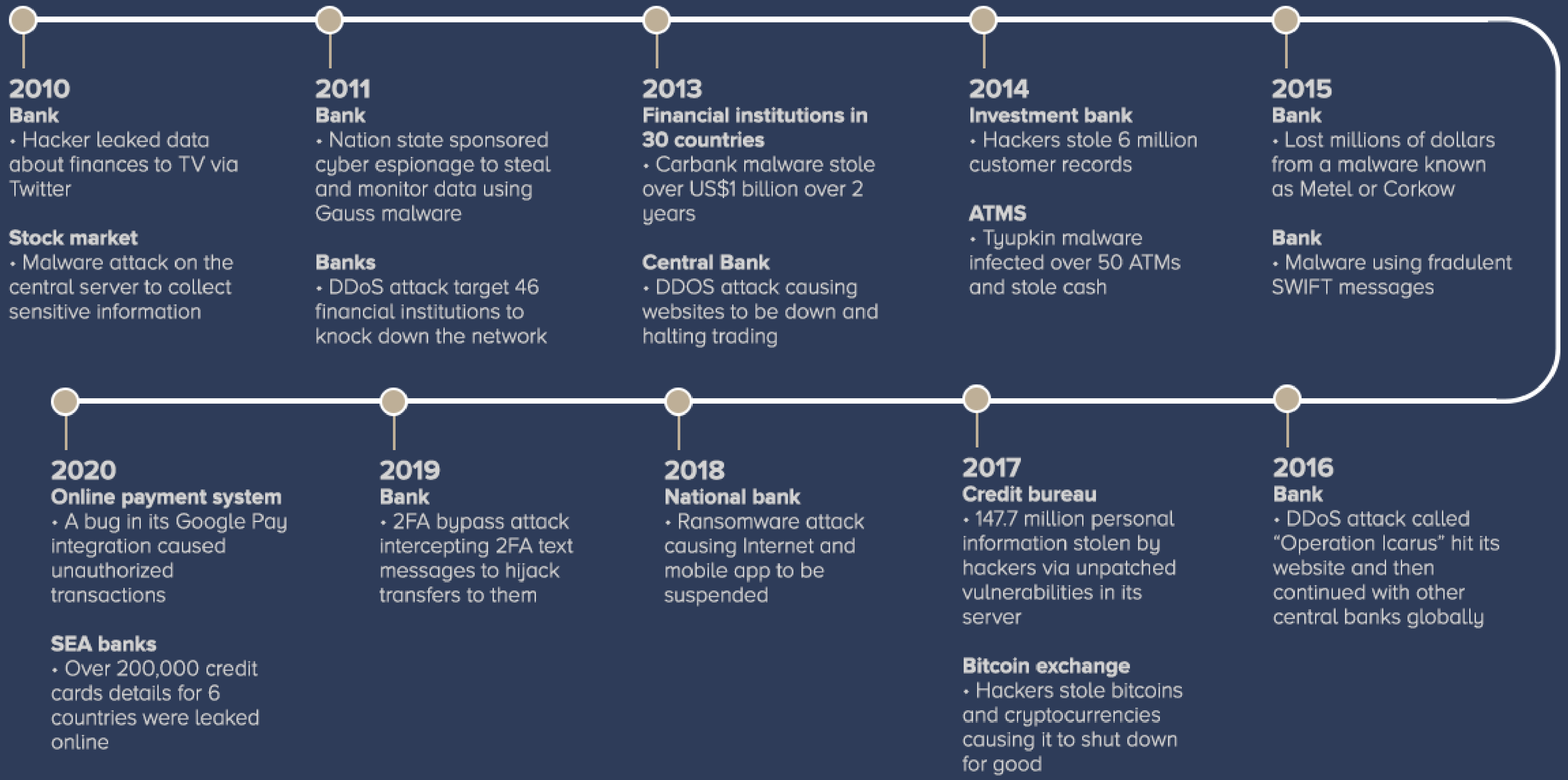
**Airlines**
- 9 million personal information and credit card details leaked

**Transportation & logistics company**
- Ransomware attack causing key services to be halted and delayed for a week

# CNII Cyber Attacks

Financial

(2010 – 2020)



**2010**
**Bank**
- Hacker leaked data about finances to TV via Twitter

**Stock market**
- Malware attack on the central server to collect sensitive information

**2011**
**Bank**
- Nation state sponsored cyber espionage to steal and monitor data using Gauss malware

**Banks**
- DDoS attack target 46 financial institutions to knock down the network

**2013**
**Financial institutions in 30 countries**
- Carbank malware stole over US$1 billion over 2 years

**Central Bank**
- DDOS attack causing websites to be down and halting trading

**2014**
**Investment bank**
- Hackers stole 6 million customer records

**ATMS**
- Tyupkin malware infected over 50 ATMs and stole cash

**2015**
**Bank**
- Lost millions of dollars from a malware known as Metel or Corkow

**Bank**
- Malware using fradulent SWIFT messages

**2016**
**Bank**
- DDoS attack called "Operation Icarus" hit its website and then continued with other central banks globally

**2017**
**Credit bureau**
- 147.7 million personal information stolen by hackers via unpatched vulnerabilities in its server

**Bitcoin exchange**
- Hackers stole bitcoins and cryptocurrencies causing it to shut down for good

**2018**
**National bank**
- Ransomware attack causing Internet and mobile app to be suspended

**2019**
**Bank**
- 2FA bypass attack intercepting 2FA text messages to hijack transfers to them

**2020**
**Online payment system**
- A bug in its Google Pay integration caused unauthorized transactions

**SEA banks**
- Over 200,000 credit cards details for 6 countries were leaked online

THREATS AND ATTACKS

# CNII CYBER ATTACK

Common attacks:

Social engineering

- ✓ Phishing: Spearphishing, Whaling, Smishing, Voice phishing
- ✓ Baiting

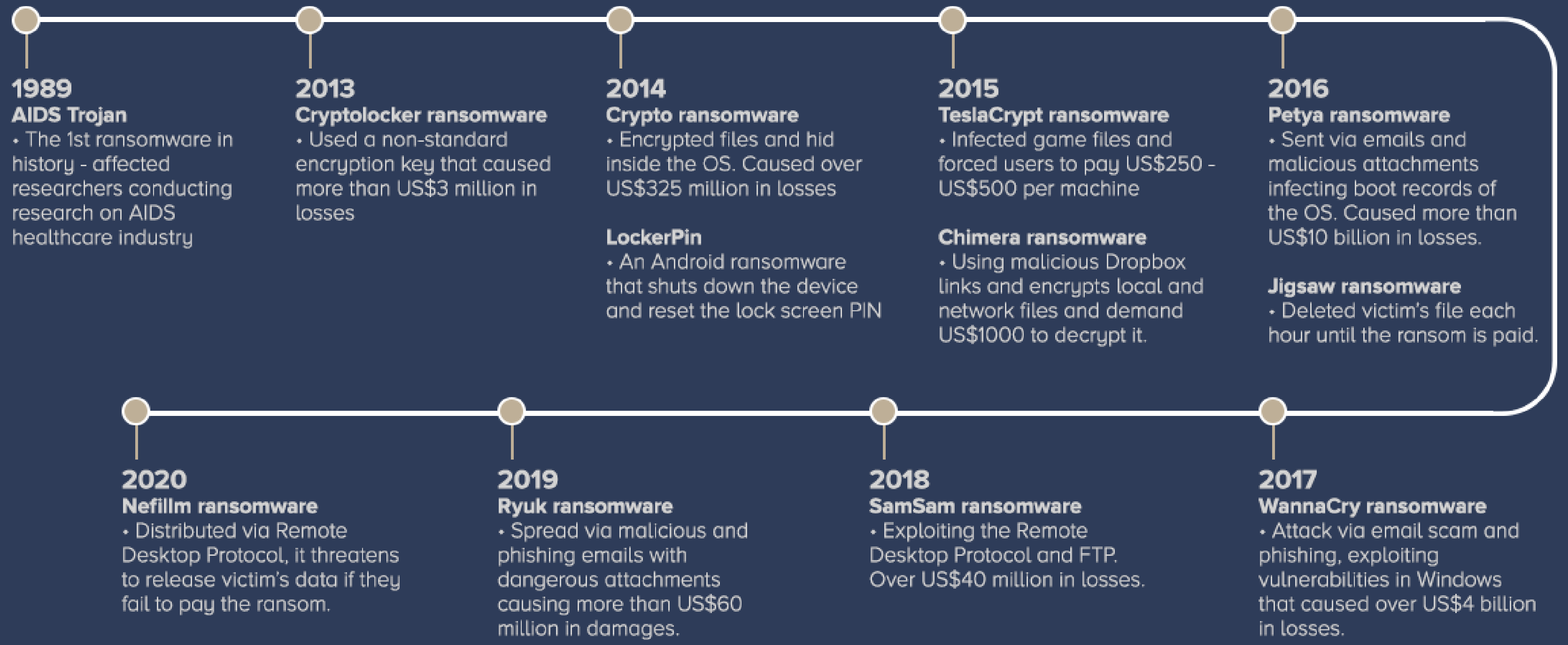
Malware

- ✓ Trojan
- ✓ Spyware
- ✓ Keylogger
- ✓ Ransomware

DDoS

# CNII CYBER ATTACKS

Ransomware
(1989 – 2020)



**1989**
**AIDS Trojan**
- The 1st ransomware in history - affected researchers conducting research on AIDS healthcare industry

**2013**
**Cryptolocker ransomware**
- Used a non-standard encryption key that caused more than US$3 million in losses

**2014**
**Crypto ransomware**
- Encrypted files and hid inside the OS. Caused over US$325 million in losses

**LockerPin**
- An Android ransomware that shuts down the device and reset the lock screen PIN

**2015**
**TeslaCrypt ransomware**
- Infected game files and forced users to pay US$250 - US$500 per machine

**Chimera ransomware**
- Using malicious Dropbox links and encrypts local and network files and demand US$1000 to decrypt it.

**2016**
**Petya ransomware**
- Sent via emails and malicious attachments infecting boot records of the OS. Caused more than US$10 billion in losses.

**Jigsaw ransomware**
- Deleted victim's file each hour until the ransom is paid.

**2017**
**WannaCry ransomware**
- Attack via email scam and phishing, exploiting vulnerabilities in Windows that caused over US$4 billion in losses.

**2018**
**SamSam ransomware**
- Exploiting the Remote Desktop Protocol and FTP. Over US$40 million in losses.

**2019**
**Ryuk ransomware**
- Spread via malicious and phishing emails with dangerous attachments causing more than US$60 million in damages.

**2020**
**Nefillm ransomware**
- Distributed via Remote Desktop Protocol, it threatens to release victim's data if they fail to pay the ransom.

SECTION 07

# BREAKOUT SESSION 2 – GROUP DISCUSSION

## QUESTIONS

✓ Who is “in charge” of critical infrastructure security and resilience nationally, regionally, locally, and across the critical sectors?

✓ How do the various government and private entities with critical infrastructure security and resilience responsibilities at different levels interact and collaborate with one another?

✓ Does your country have a National CERT/CIRT? If no, do you plan to establish one or face any challenges in establishing it?

Section 08

# STRATEGIES IN ADDRESSING THE THREATS

CIIP

CII PROTECTION

# CIIP for Operators

- ✓ Define a risk management framework
- ✓ Build and test emergency plans
- ✓ Training and education
- ✓ Supply chain security
- ✓ Information sharing and cooperation
- ✓ Legal compliance
- ✓ Continuous monitoring and assessment of cybersecurity posture

# CIIP FOR OPERATORS

**Define a risk management framework**

- ✓ Elaborates a continuous and repeatable methodology for identifying, assessing, and responding to cybersecurity risks. (e.g. NIST framework)
- ✓ Organisations can determine their risk tolerance, thus the acceptable level of risk for achieving their supply and organisational goals and are able prioritize remediations and make informed decisions about cybersecurity investments

**Build and test emergency plans**

- ✓ Plans must involve both physical and cyber-attacks to the infrastructure and include the process to defend, mitigate and respond against it.
- ✓ On the national level, the national cybersecurity agency will periodically organise a cyber exercise to simulate potential attack vectors against the CII. This allows the CII to prepare for such attacks better and design appropriate responses to protect, defend and mitigate those threats.

# CIIP FOR OPERATORS

**Training, awareness & education**

- ✓ Training is to equip individuals with the necessary skills to perform specific functions within the organisation
- ✓ Employees must be made aware of the information security policies and the importance of adhering to it. Communicating this to all employees is vital to ensure they know, understand and obey. The key outcome of security awareness programs and activities is to create a culture of security, change of behaviour and attitude.

**Supply chain security**

- ✓ Due to extensive outsourcing, today's supply chain is increasingly complex and externalized, with subsequent additional risks.
- ✓ The resilience of a supply chain depends on its weakest link and operators are secure only if their entire ecosystem of partners and vendors is secure.
- ✓ Adversaries can use poorly protected partners as attack vectors to compromise critical operators.
- ✓ An integrated and sustainable supply chain security objective must be included in business plans, contracts and operations

# CIIP FOR OPERATORS

**Information sharing & cooperation**

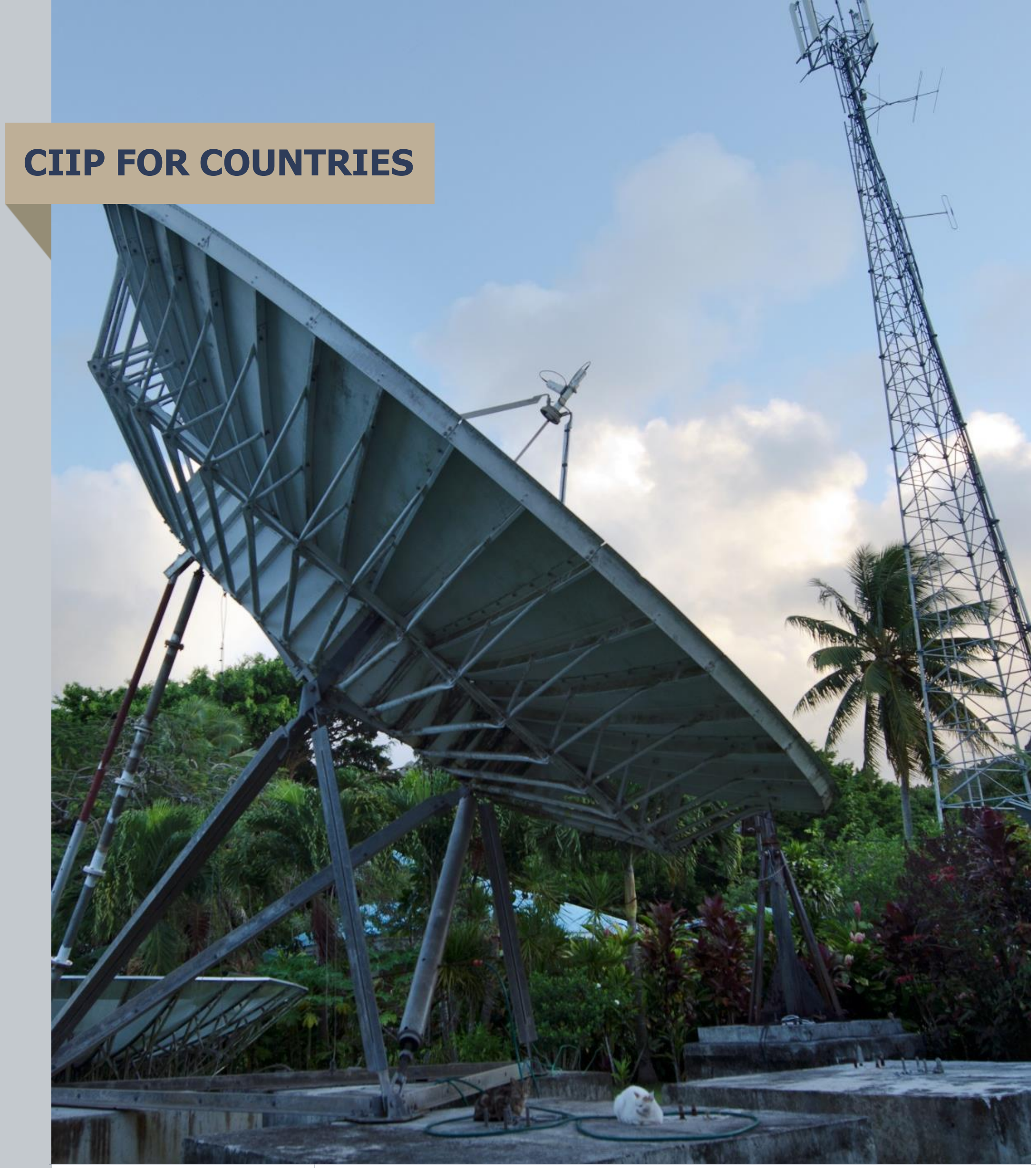
- ✓ Through information sharing, CII can reduce and prevent the spread of the attack and minimise the damage to the infrastructure and country.
- ✓ Through partnerships, sectors can share information as well as collaborate to solve issues relating to cybersecurity threats and attacks.
- ✓ Alliances also help to share skills within the sectors where some unique skills may be required from the government or private sector. (e.g. FIRST)

**Legal compliance**

- ✓ Legal compliance ensure that operators meet critical security standards identified by national decision makers.

**Continuous monitoring & assessment of cybersecurity posture**

- ✓ Digital risk landscape is in constant evolution and need to build repeatable processes to monitor and assess the cybersecurity maturity level on an ongoing basis
- ✓ Assessment should consider the risk-related adequacy of the processes, people, and technology, in order to identify cybersecurity substantial gaps and determine appropriate remedies to resolve weaknesses
- ✓ CNI must examine the general preparedness of the operator, and the ability to detect and to respond to incidents and ensure business continuity



# CIIP for Countries

- ✓ Institutional architecture
- ✓ National risk assessment
- ✓ Identification of critical information infrastructure
- ✓ Strategies, policy, regulation and standards
- ✓ Public-private cooperation
- ✓ Education and capacity building
- ✓ Development of a trusted market
- ✓ National crisis management
- ✓ Monitoring and improvement

Section 09

# CONCLUSION & MOVING FORWARD

CNII Protection

Wk.

MOVING FORWARD

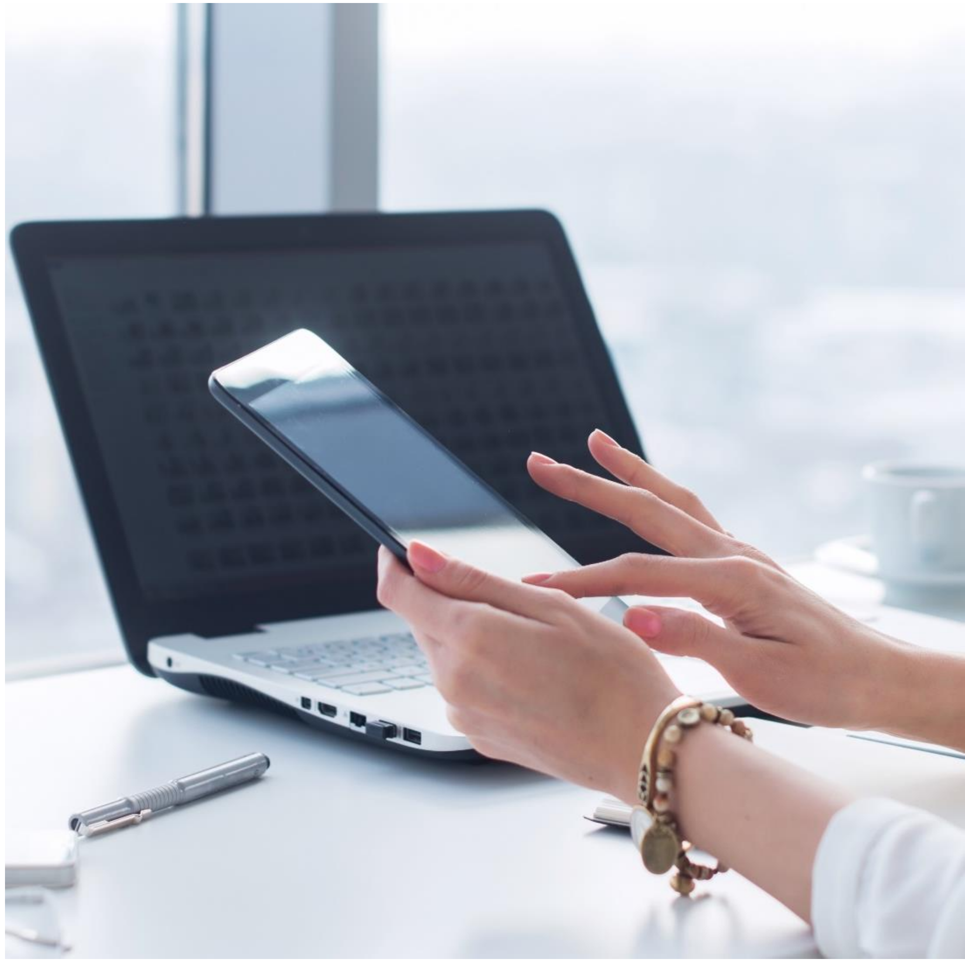
## CNII must have:

✓ A shift of mindset in the manner cybersecurity is addressed.

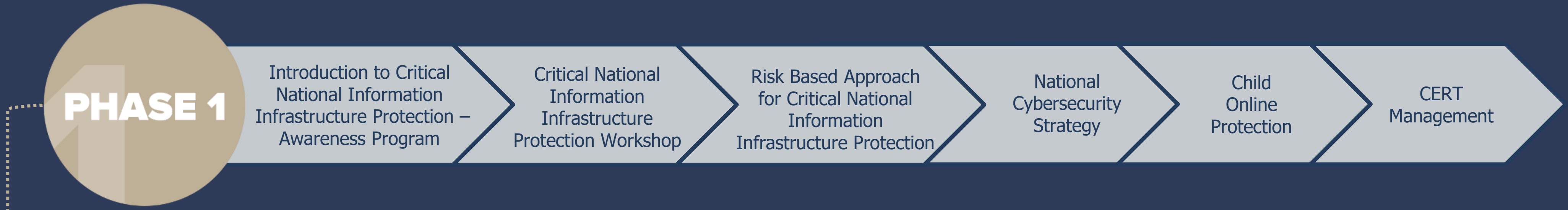
✓ Look beyond technical tools to adopt a new cyber defence strategy

# CONCLUSION

- ✓ Be prepared – training & vulnerability assessment
- ✓ Design sector specific resources & initiatives
- ✓ Cooperate with agencies on a national, regional and international level
- ✓ Expand information sharing and collaboration
- ✓ Build robust national policies & strategies



# WK Capacity Building Roadmap



PHASE 1

Introduction to Critical National Information Infrastructure Protection – Awareness Program

Critical National Information Infrastructure Protection Workshop

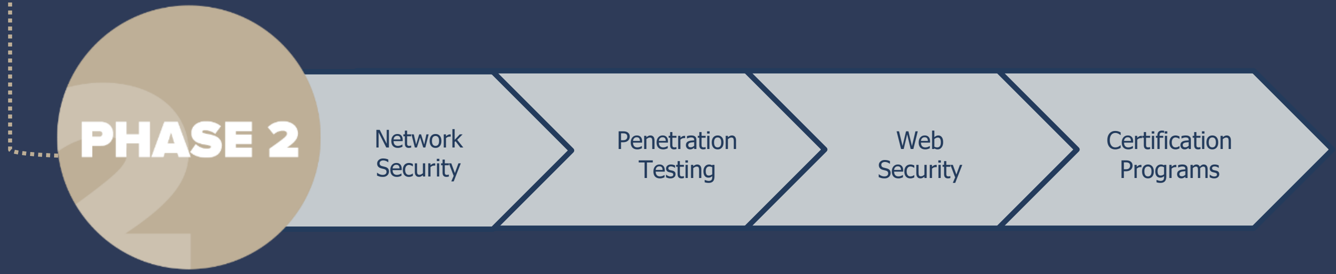
Risk Based Approach for Critical National Information Infrastructure Protection

National Cybersecurity Strategy

Child Online Protection

CERT Management

WK, as ITU’s Sector Member, will conduct trainings, webinars and workshops in the Pacific Island to enhance skills and knowledge for CII protection in 2021/2022. Current available programs are stated above



PHASE 2

Network Security

Penetration Testing

Web Security

Certification Programs

In this phase, WK will focus on building technical capabilities in the Pacific Island

THANK YOU

# INTRODUCTION TO CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

Aaron Boyd – aboyd@welchmankeen.com

Philip Victor– vphilip@welchmankeen.com

Elvin Prasad– eprasad@welchmankeen.com

WELCHMAN KEEN