

Critical Information Infrastructure Protection

Enhancing Cybersecurity and Resilience



Presentation at the 12th International Conference
Nigeria Computer Society

Tope S. Aladenusi, CISA, CISSP, CRISC, CBCI, CEH, CIA, COBIT5(i), ISO27001LA
Cyber Risk Services Leader, Deloitte Nigeria
22 July 2015

Contents

Background

Critical Information Infrastructure

Why is Security of CII so important?

Types of Threats and Threat Vectors

What are Other Countries Doing to Protect CII?

Enhancing Cybersecurity and resiliency of CII

Way Forward

Background

President talks about cybercrime during Inaugural Speech...



“I also wish to assure the wider international community of our readiness to cooperate and help to combat threats of cross-border terrorism ... financial crime, cyber crime, ... and other challenges of the 21st century.”

Polish Airline Cyber Attack - 2015

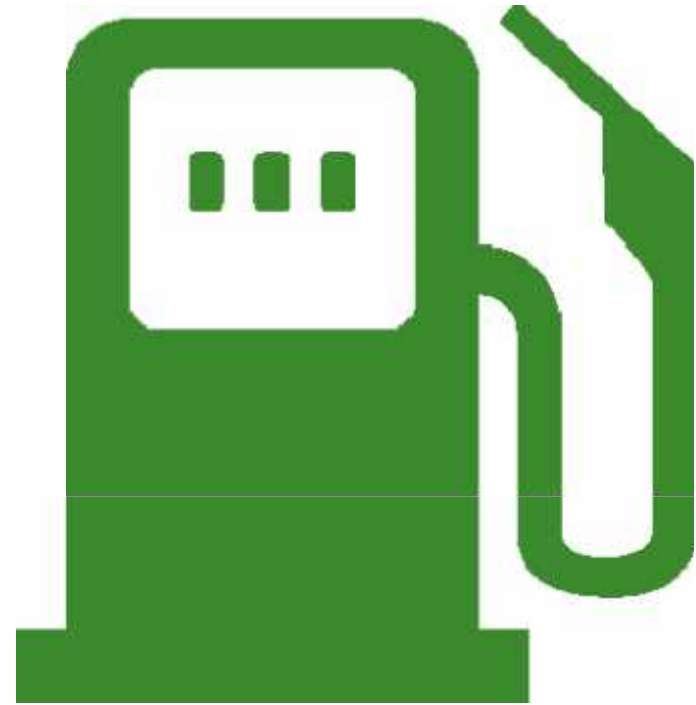
Ten planes and around 1,400 passengers of Polish airliner LOT were grounded Sunday after a major hacking attack jammed the carrier's systems, the company confirmed.

The issue, which took five hours to solve, meant that 10 flights were cancelled and around 15 were delayed at Warsaw Chopin airport.



Aramco Cyber Attack - 2012

On 15 August 2012, the computer network of **Saudi Aramco** was struck by a self-replicating virus that infected as many as 30,000 of its Windows-based machines. Despite its vast resources as Saudi Arabia's national oil and gas firm, Aramco, according to reports, took almost two weeks to recover from the damage.



The virus also spread to the networks of other oil and gas firms, including that of RasGas

Telvent - 2012

Telvent, the smart grid giant owned by Schneider Electric, reported that hackers breached its network, left behind malicious software and accessed project files for its OASyS SCADA system.

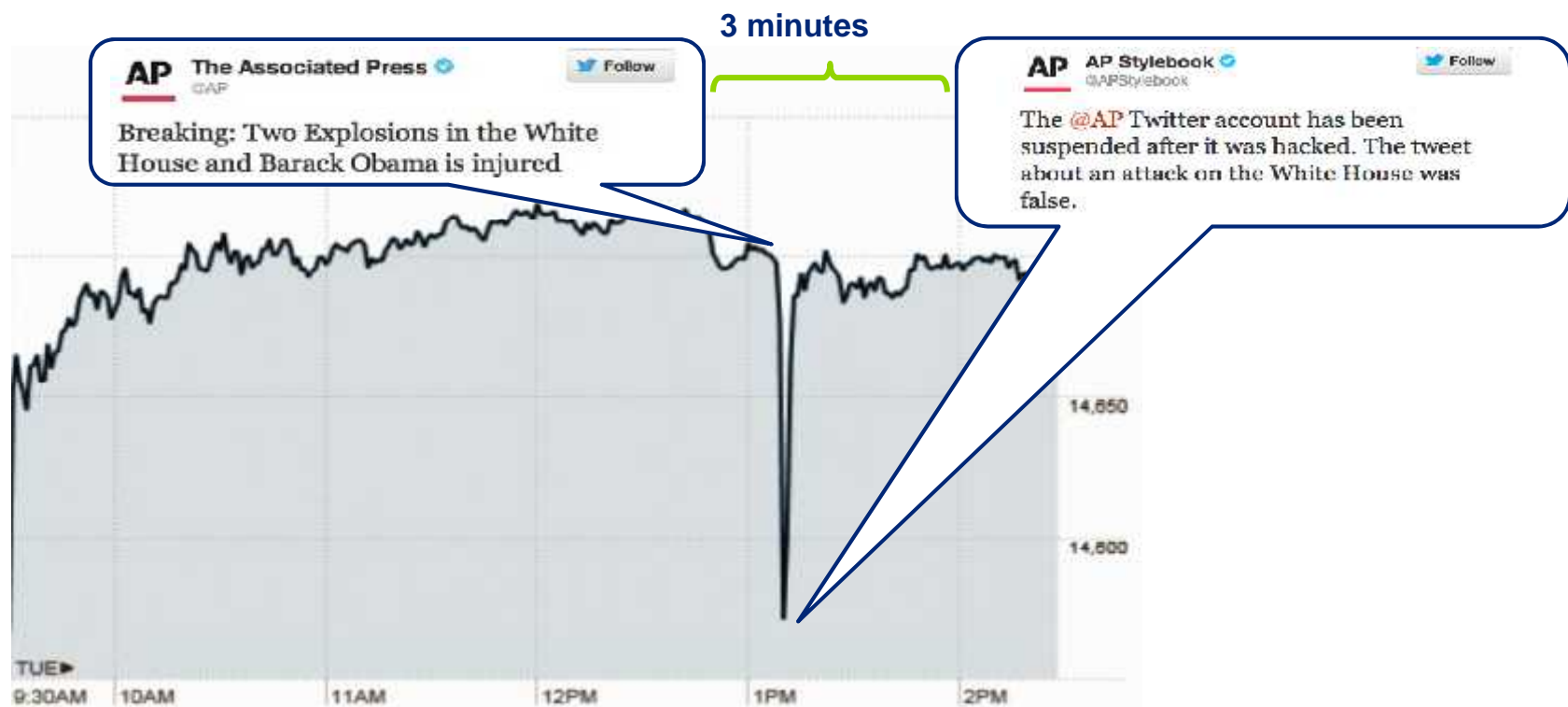
This was the same system that Telvent used to control power grid, oil and gas pipeline, and industrial controls around the world, as well as to integrate them with utility enterprise systems and new smart grid platforms.



TELVENT

Associated Press Twitter Account hacked - 2013

On April 23, 2013, hackers used the Associated Press Twitter account to report an attack at the White House. The Dow Jones Industrial Average plunged over 150 points within moments, and quickly corrected itself after the hack was discovered.



The Mask and Stuxnet

The Mask - 2014

- Researchers uncovered a sophisticated cyber spying operation that had been alive since at least 2007 and used sophisticated techniques and code.
- The attack targeted government agencies and diplomatic offices and embassies. It also targeted companies in the oil, gas and energy industries as well as research organizations and activists.
- The attackers sought to steal documents, encryption keys, etc.

Stuxnet - 2010

- Stuxnet is a computer worm that was designed to attack industrial programmable logic controllers (PLCs).
- Stuxnet reportedly compromised Iranian PLCs, collecting information on industrial systems and causing the fast-spinning centrifuges to tear themselves apart. Stuxnet reportedly ruined almost one-fifth of Iran's nuclear centrifuges.

Related Cyber Attacks in Nigeria

INEC - 2015

- The website of the Independent National Electoral Commission has been hacked. The website was hacked by a group that paraded itself as Nigerian Cyber Army. The hacking was confirmed by INEC on its Twitter handle, @inecnigeria
- “We are aware of the recent hack of our @inecnigeria website, we are currently investigating this incident #NigeriaDecides”

Nigerian Defense Website - 2015

- The Defense website was hacked 'ISIS' style (i.e. an attempt to hack into the Government platform). Spokesperson of Defense HQ, Chris Olukolade confirmed it, then later revealed that the website has been taken back from the hackers.

Critical Information Infrastructure

Critical Information Infrastructure (CII) are those ICT infrastructure upon which *core assets that are essential for the functioning of the society and economy* is dependent.
















The destruction of these assets has a catastrophic impact on national security, governance, economy and social well-being of a nation.

Critical Information Infrastructure Protection (CIIP) refers to the security and protection of these IT connections and solutions.



Currently, there are 15 industry sectors defined as critical infrastructure

According to section 7.5 of the National Cyber Security Policy (2014), the following have been defined as Critical Infrastructure sectors in Nigeria.

Critical infrastructure sectors					
	Food and Agriculture		Dams		Information Technology
	Financial Services		Defense		Public Health and Healthcare
	Chemical (Oil and gas)		Emergency Services		Transportation Systems
	Commercial Facilities		Power and Energy		Water and Wastewater Systems
	Communications		Government and Facilities		Manufacturing

Why is Security of CII so important?

Intensity and impact

- Heavy reliance on cyber
- Interdependence of industries and sectors of the economy
- Complexity and volume of threats
- Velocity of change
- Highly centralised operations
- Potential for catastrophic physical and economic damage



Types of Threats to CII

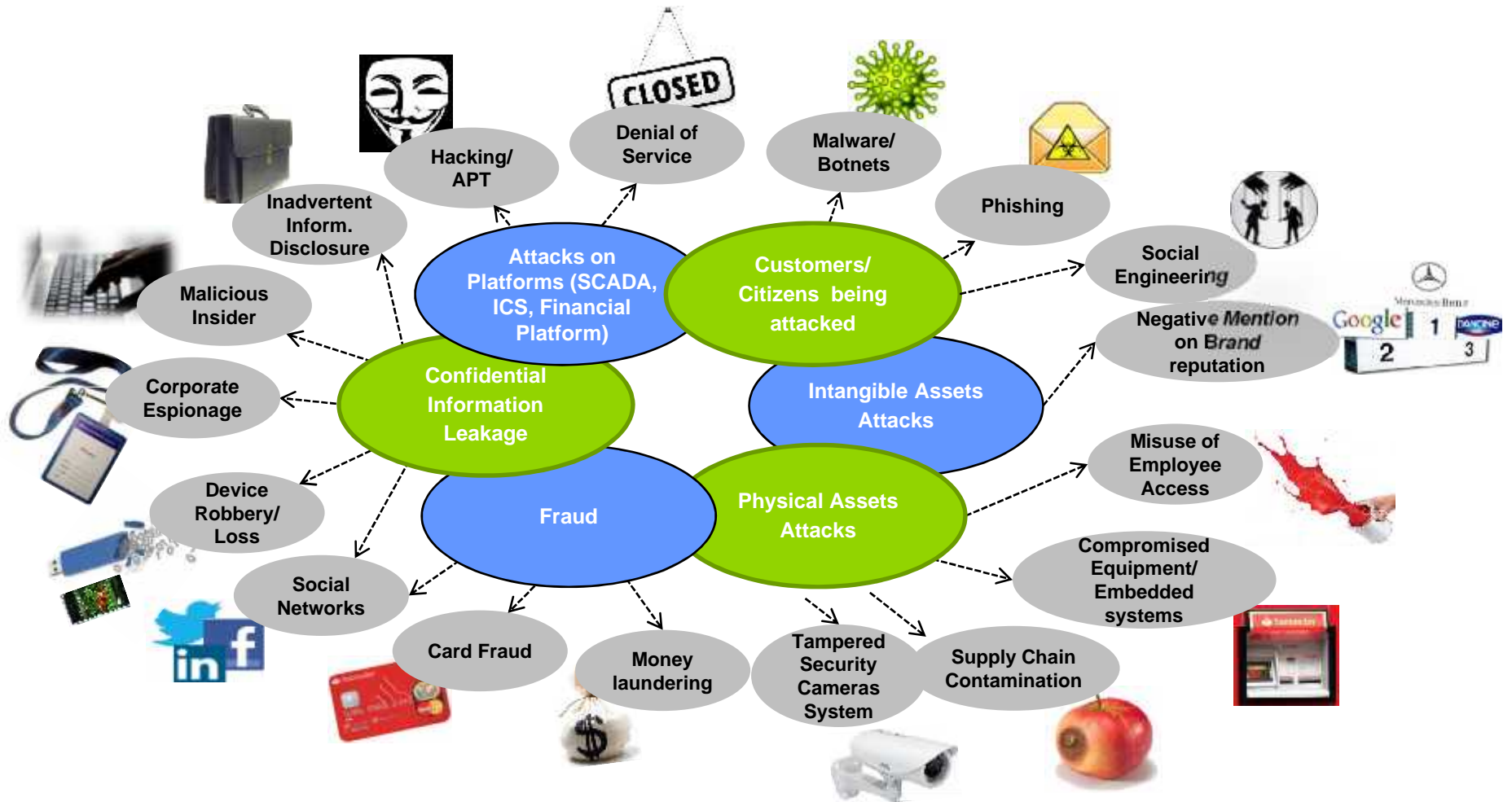
Internal Threat

- It is defined as “One or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity’s security, systems, services, products, or facilities with the intent to cause harm.”
- Insider betrayals cause losses due to IT sabotage, Fraud, and Theft of Confidential or proprietary information
- This may be intentional or due to ignorance

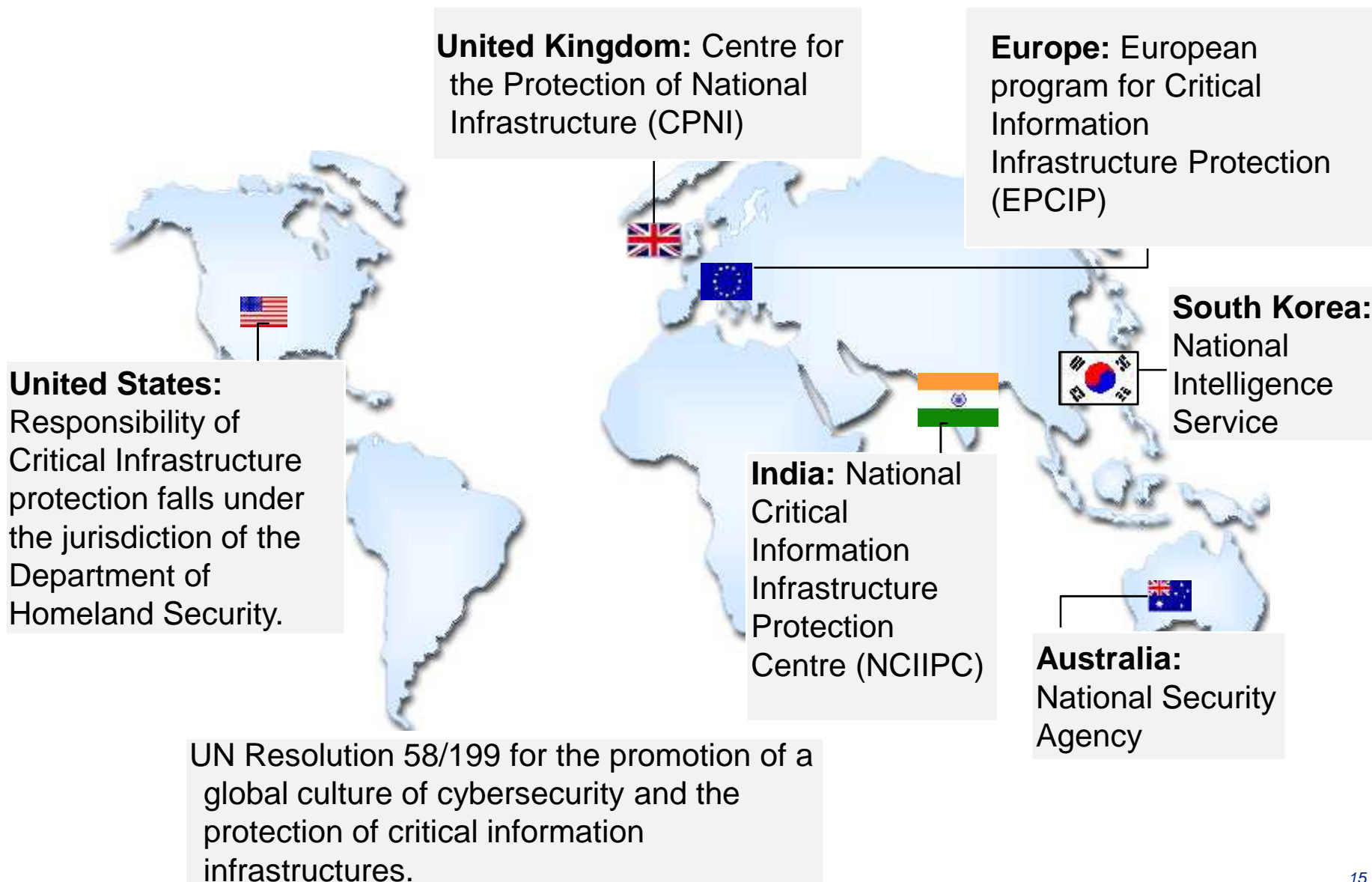
External Threat

- Arise from outside of the organization by individuals, hackers, organizations, terrorists , foreign Government agents, non state actors and pose risk like Crippling CII, Espionage, Cyber/Electronic warfare, Cyber Terrorism etc.

Threat Vectors



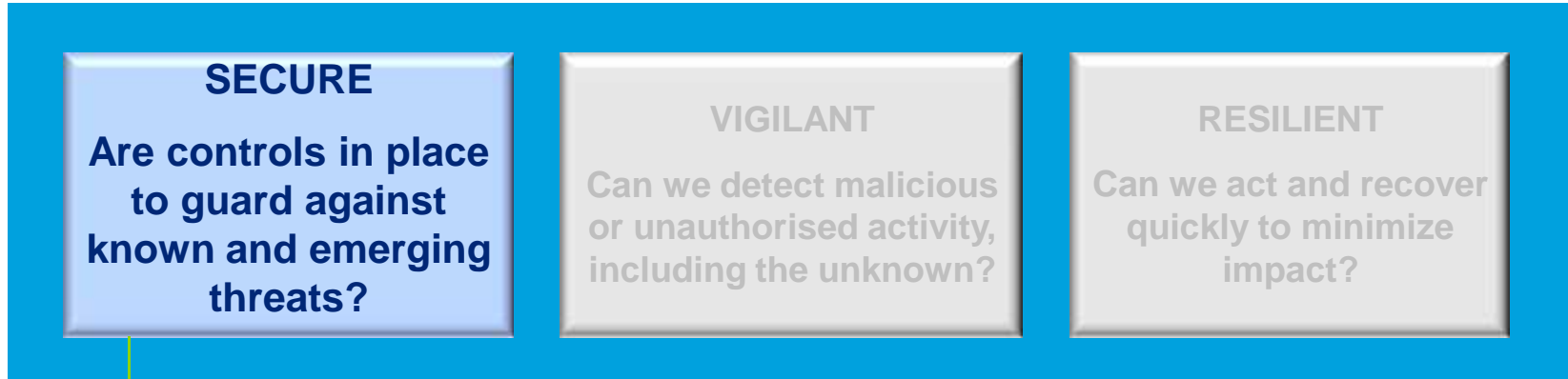
What are Other Countries Doing to Protect CII?



Enhancing Cybersecurity : - *Key Considerations*

Enhancing Cybersecurity and resiliency of CII

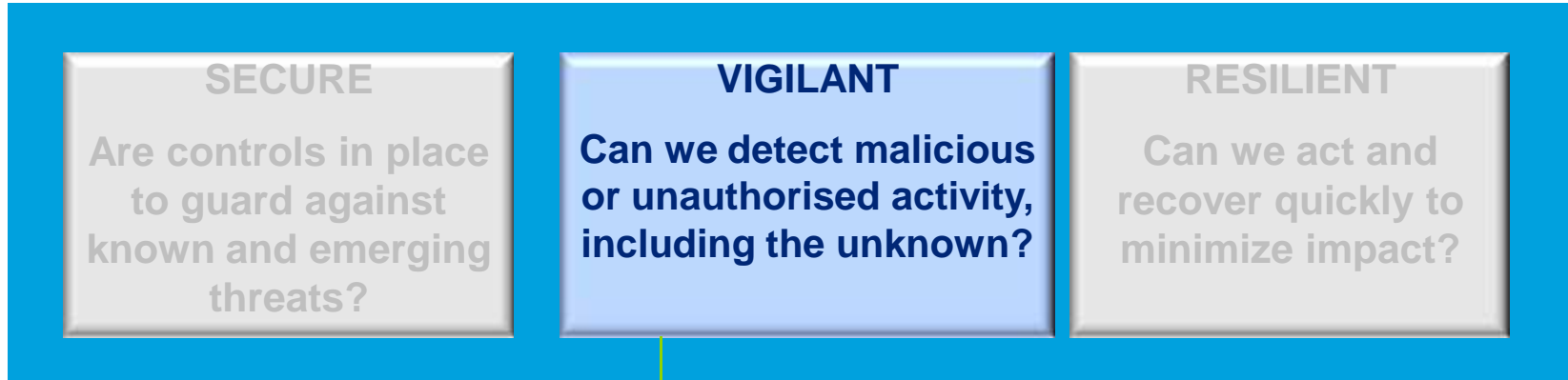
Secure – Vigilant – Resilient



- *Identify specific CII*
- *Development and enforcement of a framework/standard for protection of CII*
- *Education and Awareness*
- *Government should implement the Cybercrime Act*
- *Drive sector specific programs for cyber security*
- *Organisations in CII sectors should regularly perform self assessment*

Enhancing Cybersecurity and resiliency of CII

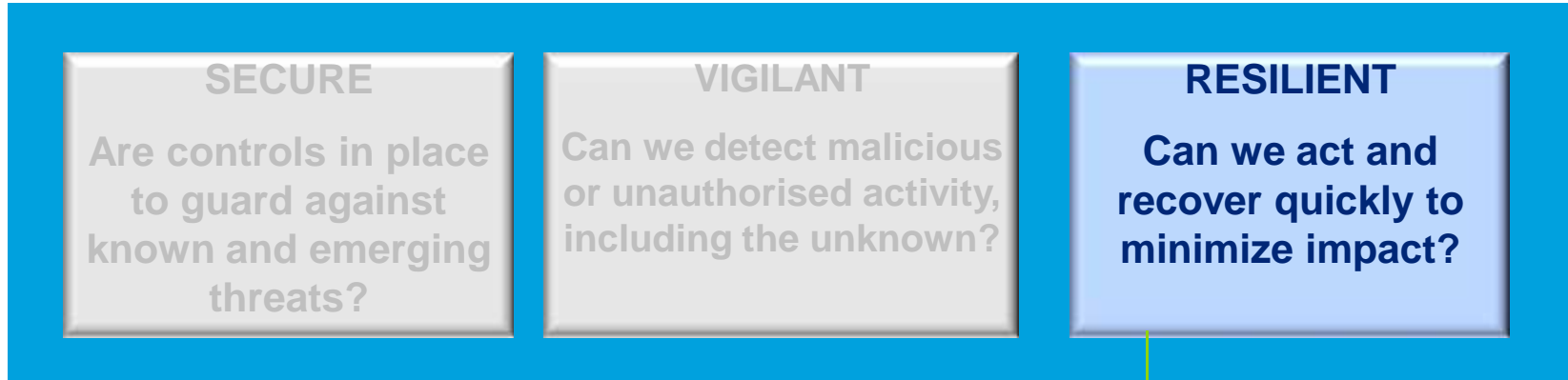
Secure – Vigilant – Resilient



- *Public Private Partnership*
- *Develop 24/7 Cyber Intelligence capabilities*
- *Cyber threat and countermeasures Clearing House*

Enhancing Cybersecurity and resiliency of CII

Secure – Vigilant – Resilient



- *ngCERT effectiveness*
- *War Gaming*
- *Integrated Crisis Response*
- *Digital Forensics*
- *Business Continuity Management*

Way Forward

Way Forward

Maintaining the Cybersecurity and Resilience of Critical Information Infrastructure (CII) is not a destination but a journey. As our interconnectedness and reliance on cyber security increases, the criticality of these systems also increase and so does our risk exposure.

Key considerations include ...



Thank You

The views and opinions expressed in this presentation are those of the author and do not in any way represent the views of the author's employer. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication. The author does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

References

All sites access 21 July 2015

<https://ccdcoe.org/sites/default/files/multimedia/pdf/2014-Technical%20Analysis%20of%20Advanced%20Threat%20Tactics%20Targeting%20Critical%20Information%20Infrastructure.pdf>

http://www.dis.uniroma1.it/~tenace/download/deliverable/Report_tenace.pdf

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF>

<http://pulse.ng/tech/cyber-attack-nigerian-defence-official-website-hacked-isis-style-id3429555.html>

<http://indiasmartgrid.org/en/Lists/Member/Attachments/19/ISGD%20Plenary%20III%20Muktesh%20Chander%20NCIIPC.pdf>
<http://usa.kaspersky.com/threats/gauss>

<http://www.vanguardngr.com/2015/03/inec-website-hacked/#sthash.gvxuVTk7.dpuf>

<http://techloy.com/2015/05/16/nigerias-president-jonathan-signs-the-cybercrime-bill-into-law/>

<http://www.cybersecuritynigeria.org.ng/ncsf/index.php/downloadable-docs?download=8:NCSP%20main%20body>

[http://www.cybersecuritynigeria.org.ng/ncsf/index.php/downloadable-docs?download=12:NCSS%20Volume%2010%20main%20body%20\(3\)](http://www.cybersecuritynigeria.org.ng/ncsf/index.php/downloadable-docs?download=12:NCSS%20Volume%2010%20main%20body%20(3))