

# Theme of Cyber Strategy PoC (19-28 July)

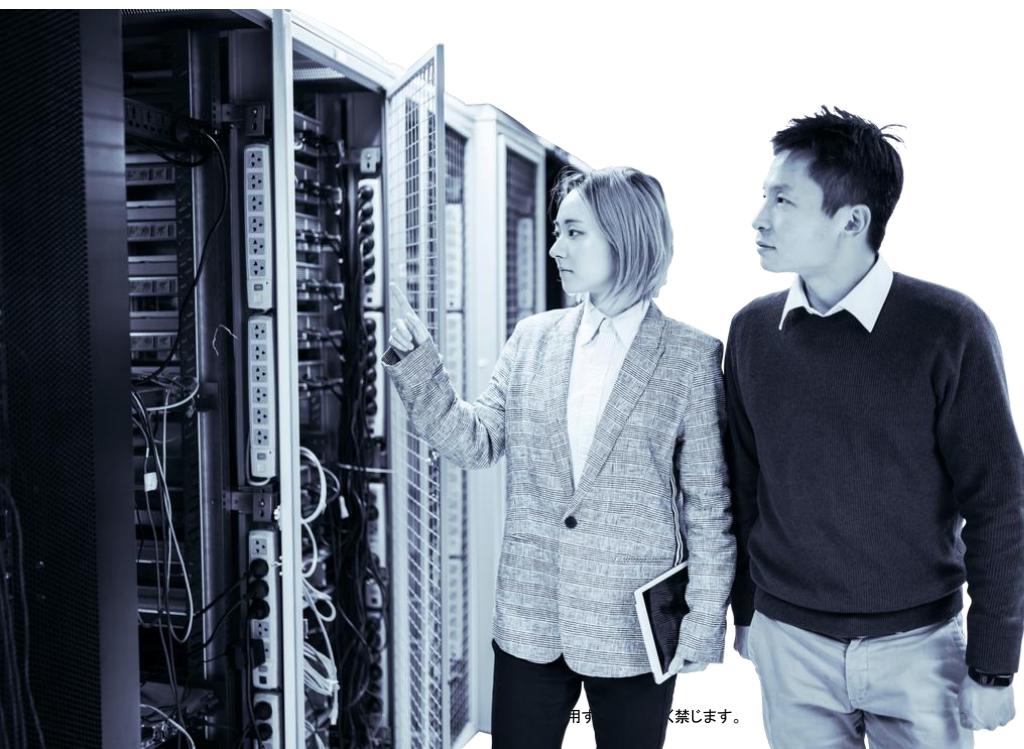
Session by Kirirom institute of technology (KIT)

Session by FPT Software

<b>Day</b>	<b>KHM</b>	<b>JST</b>	<b>Theme</b>
<b>19-Jul</b>	9:00-11:00	11:00-13:00	1. Overview of Cyber Security Trend
	13:00-15:00	15:00-17:00	2. Definition of Cyber threat and national Incident response framework
<b>20-Jul</b>	9:00-11:00	11:00-13:00	3. Cyber Security Regulation framework
	13:00-15:00	15:00-17:00	4. Partnership(Public, Private, Academia, International)
<b>21-Jul</b>	9:00-11:00	11:00-13:00	5. Professional training and certification
	13:00-15:00	15:00-17:00	6. Public awareness and alerts
<b>26-Jul</b>	9:00-11:00	11:00-13:00	7. Cyber Security for SME
	13:00-15:00	15:00-17:00	8. Critical Infrastructure Industry protection
<b>28-Jul</b>	9:00-11:00	11:00-13:00	9. CERT/ Resilience
	13:00-15:00	15:00-17:00	10. Wrap up/Discussion/FAQ -

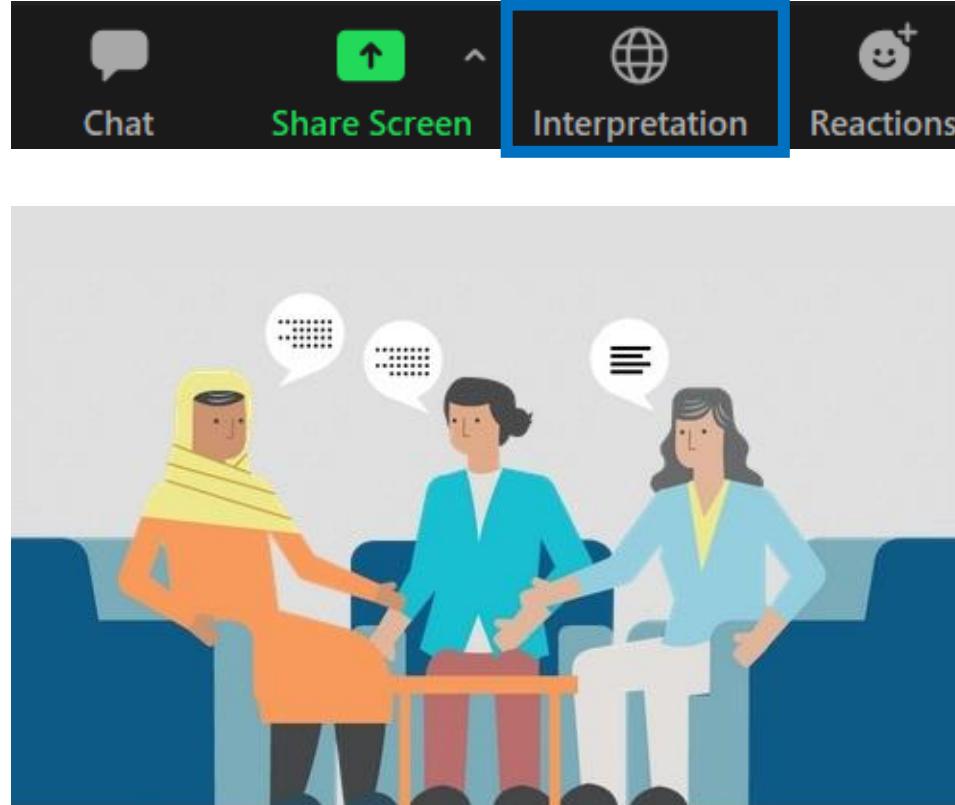
## 1. Overview of Cyber Security Trend

2. Definition of Cyber threat and national Incident response framework
3. Cyber Security Regulation framework
4. Partnership(Public, Private, Academia, International)
5. Professional training and certification
6. Public awareness and alerts
7. Cyber Security for SME
8. Critical Infrastructure Industry protection
9. CERT/ Resilience
10. Wrap up / Cyber security assessment

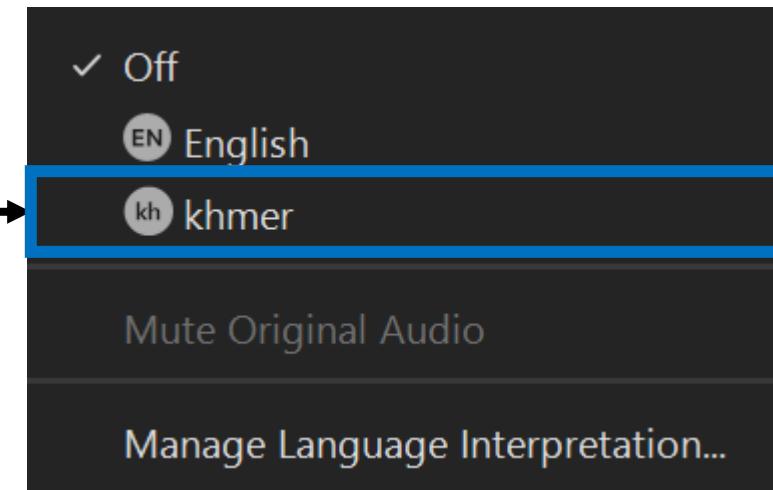


# Khmer simultaneous Interpretation available

Select “Interpretation” on the bottom



Select “Khmer”



- Presentation is simultaneously translated into Khmer
- You can post question in Khmer

# Speakers and Faculty



**Patrick M. Nagel**  
Expert Associate Partner  
– Cyber security



**Takuya Matsumoto**  
Partner, Tokyo office  
– Digital



**Tony Nakamura**  
Senior Associate, Tokyo office  
– Digital



**Yuji Hori**  
Business Analyst, Tokyo office  
– Digital



## Timeline

## Overview

100 minuets

## Workshop & QA

20 minuets

# Cybersecurity is a major issue and threat are constantly growing

---

## What everybody knows

Relentless and sophisticated attackers

More assets becoming digital

Increasing regulatory and customer scrutiny

**\$150 Mn**

2020 cost of data breach

**36%**

ransomware attacks increase  
in 2017

**175+**

confirmed breaches per day



**101**

average days between  
breach and discovery

**50%**

percent of sites with web app  
vulnerabilities

**\$3 trillion**

2019 cybercrime costs

## What not everyone realizes

Attackers have institutional cybercrime and turned it into a successful business

As nation states militarize cyberspace, private companies become collateral damage (e.g., NotPetya)

Customers placing pressures on vendors and SIs to demonstrate cyber capabilities, slowing contracting

Digital business strategies vastly increasing risk (e.g., IoT1, agile, cloud, RPA2)

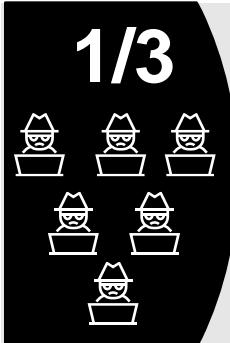
Clear winners and losers following cyberattacks – winner add ~20% in shareholder value and losers sustain ~25% loss

Cyber is a risk issue, not an IT issue and winners have learned to manage it this way

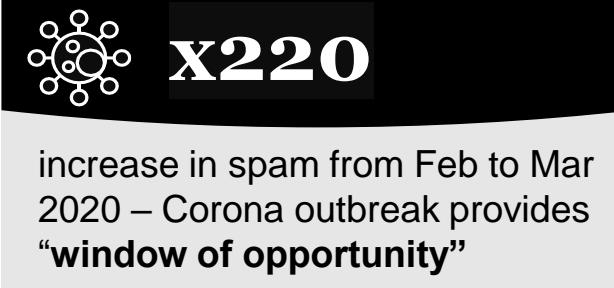
1. Internet of Things  
2. Robotic Process Automation

# Increasing threat in cyber space force both private and public sector to prepare in urgent for potential cyber risks

Cyber attacks are increasing in size and complexity...



of global organizations have experienced a cyberattack in 2019 (+36% compared to prior year)



**8 out of 12** large **cyber insurers** have started to build service offerings around core insurance products

.. and private company spending on cybersecurity increase as well...

**\$10bn**

Combined European SME spend on cyber in 2019



Strong growth outlook for global cyber security services market

**11% CAGR**

**CII Industries:**

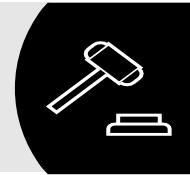
Highest spent in Finance, Manufacturing, Public Sector, Retail, Healthcare; Industry also exhibit high cyber risk exposure and regulatory requirements

**5**

... Government also put effort to protect its nation by several initiatives

**+31**

New national cyber policies implemented in the last 5 years



More than **567 CERT** teams in **97** different countries joined Global CERT's community "FIRST" to strengthen Cyber global network



**USA & Europe**



US is most mature market with ~80% of global investments in cyber companies (\$216bn since 2014); **Europe catching up**

# Cybersecurity has existed since the early days of computing and continues to the present but has grown in sophistication and impact



**Enigma:** Alan Turing cracked the Enigma Code and the Enigma machine; 211 Bombe machines<sup>1</sup> were built and ran around the clock which helped significantly to reduce the work of the code breaker



**Target:** Financial data breach of 40 million customers of Target lead to an estimated lost of \$300 million<sup>2</sup>



**OPM breach 2015:** Hackers were on the Office of Personnel Management (OPM) network for close to a year<sup>3</sup>; the impact on US Government is about US \$1bn<sup>4</sup>



**Maersk cyberattack 2017:** NotPetya cyber attack cost Maersk up to \$300mn in losses<sup>5</sup>



**"Blue box":** One of the first hacking techniques that came to limelight in 1960-1970. Blue boxes were used to crack the phone network<sup>6</sup>



**Stuxnet 2010:** Malware used to bring down nuclear centrifuges in Iran<sup>7</sup>



**Sony Pictures 2014:** Sony<sup>8</sup> was targeted by a state sponsored attack in retaliation against the release of a movie by a private company in the United States



**Bank of Bangladesh theft 2016:** Hackers were able to steal US \$81mn from the Bank of Bangladesh<sup>9</sup>



**Marriot:** Hacking exposed data of up to 500 million guests<sup>10</sup>



# What are the typical types of cyber attack?

	<b>Attack type</b>	<b>Description</b>	<b>Example</b>
<b>Un-targeted</b>	<b>Phishing</b>	Sending emails to large numbers of people asking for sensitive information or encouraging them to visit a fake website	N/A
	<b>Ransom-ware</b>	Disseminating disk encrypting extortion malware (i.e., malware that can deny the rightful user access to their computer unless a ransom is paid)	N/A
	<b>Denial of service</b>	Deploying a collection of computers compromised by malicious code and controlled across a network to deliver a distributed denial of service attack	2007 cyberattacks in Estonia that crippled government and corporate sites
<b>Targeted</b>	<b>Spear-phishing</b>	Sending emails to targeted individuals that could contain an attachment with malicious software	Target breach and Sony Pictures hack both relied on spear-phishing as the infection method
	<b>Zero day</b>	Exploiting of previously unknown security vulnerabilities to gain access to a target computer network	Stuxnet attacks on Iranian centrifuges
	<b>Subverting the supply chain</b>	Attacking equipment or software being delivered to an organization	Pre-installed Superfish adware on Lenovo note-books allowed attackers to masquerade as secure internet destinations

# Attackers are becoming more sophisticated and are often backed by sponsors with significant financial means

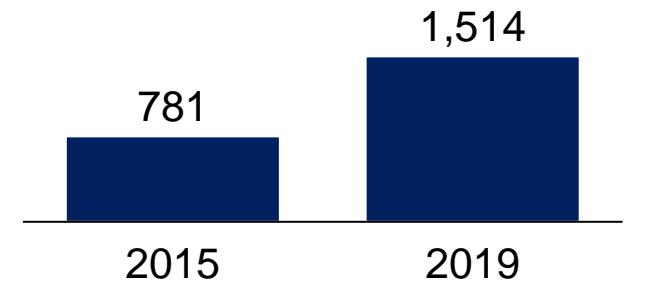
## Cyberattack typology by capability level and typical motivation

Capability	Potential adversary	Typical motivation
High	State or business-sponsored entity	<ul style="list-style-type: none"> <li>• Political - Advance a nation's posture, generate influence</li> <li>• Economic – Improve competitiveness</li> <li>• Financial – Gain financial advantage for state-owned assets</li> </ul>
	Organized crime	<ul style="list-style-type: none"> <li>• Financial – Data that can be sold or used for fraud and extortion</li> <li>• Political / Economic – acting for hire for non-state actors</li> </ul>
Med.	Hacktivist groups	<p>Political</p> <ul style="list-style-type: none"> <li>• Disrupt productivity</li> <li>• Inflict reputational damage on organization to make political statement</li> <li>• Deface website to make a statement about victim or its objectives</li> </ul>
	Corporate competitors	<p>Financial</p> <ul style="list-style-type: none"> <li>• Theft of communications to understand inner workings of organization</li> <li>• Theft of IP or information that gives attacker unfair advantage</li> </ul>
Low	Advocacy groups	<ul style="list-style-type: none"> <li>• Political – Advance specific causes through information gathering</li> </ul>
	Insiders	<ul style="list-style-type: none"> <li>• Retribution against organization for perceived transgression</li> <li>• Financial (ransom) – Get paid for information</li> </ul>
	Opportunists	<ul style="list-style-type: none"> <li>• Bragging Rights – Ability to hack celebrated by attackers circle of friends</li> <li>• Financial – Potential gain of information could be of value to sell or use</li> </ul>

# As cybersecurity becomes a bigger issue we hear the following questions from executives in private sector

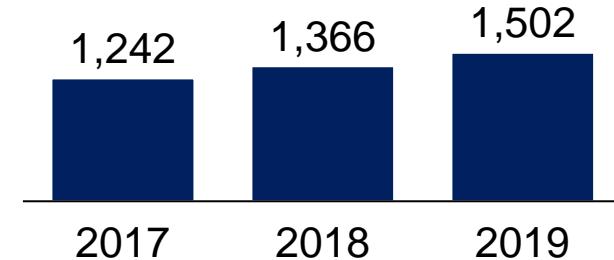
\$ Bn

**Number of reported data breaches<sup>1</sup>**



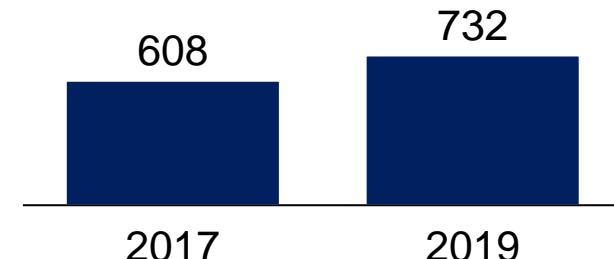
+13% p.a.

**Average global ransomware detections per day<sup>2</sup>**

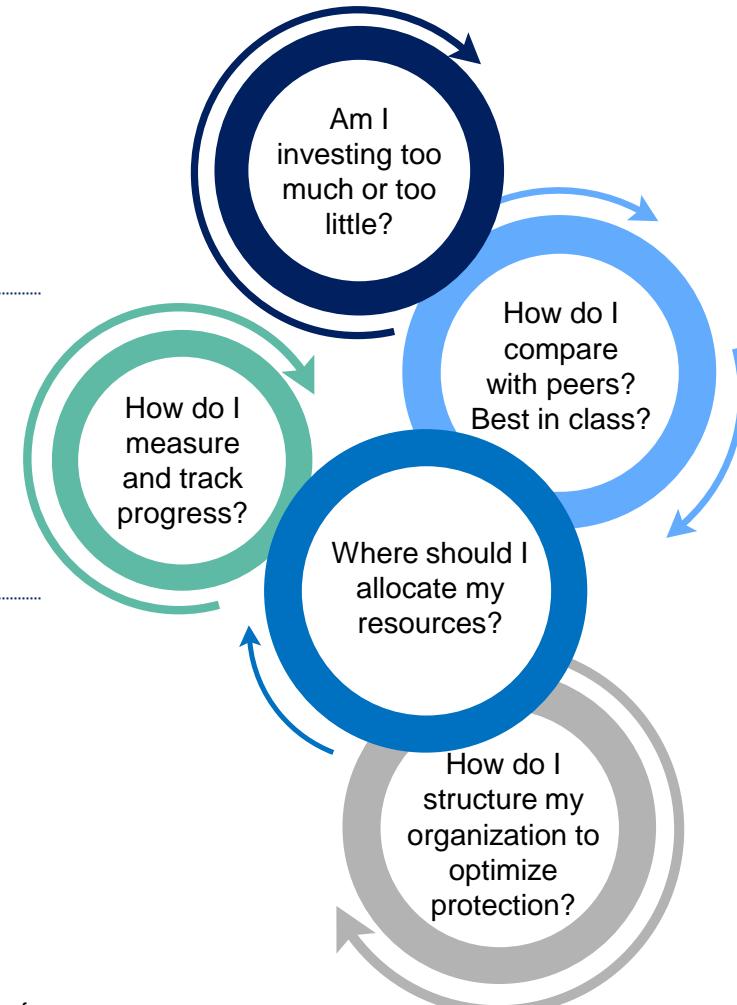


+10% p.a.

**Annual cost of cybercrime to the global economy<sup>2</sup>**



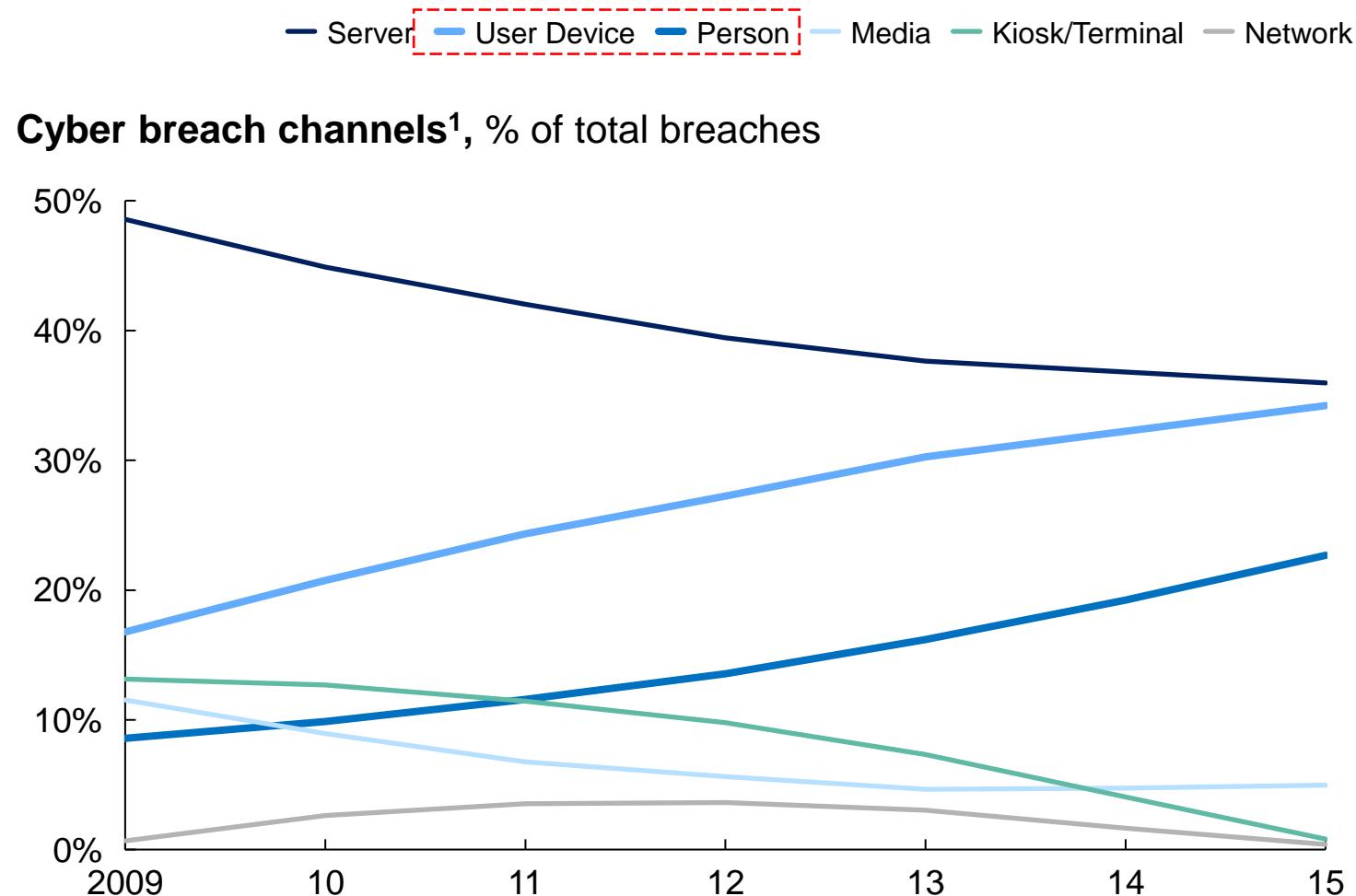
+10% p.a.



<sup>1</sup> Defined by ITRC as an incident in which Personally Identifiable Information (PII), usernames, passwords, or email addresses are potentially put at risk because of exposure

<sup>2</sup> Based on a combination of high-level estimates done by Allianz, Accenture, Cybersecurity Ventures, Herjavec Group, and Juniper Research for 2019

# Good security awareness is vital to ensure consistent protection from common cyber breach channels...



1. Verizon 2016 Data Breach Investigations Report;

2. Wombat Security: New Research Confirms Security Awareness, Training Measurably Reduces Cyber Security Risk;

3. CSO Online: "Does security awareness training even work?"



17% of cyber breaches occur through employee error<sup>1</sup>



Changing employee behaviors through training can **reduce threat exposure by 70%**<sup>2</sup>



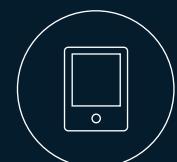
Anti-phishing training provides a **37x return on investment**<sup>3</sup>

# In the COVID-19 environment, security teams are facing a rise in both external and internal attacks

NOT EXHAUSTIVE



Working from home has opened multiple vectors for cyberattacks



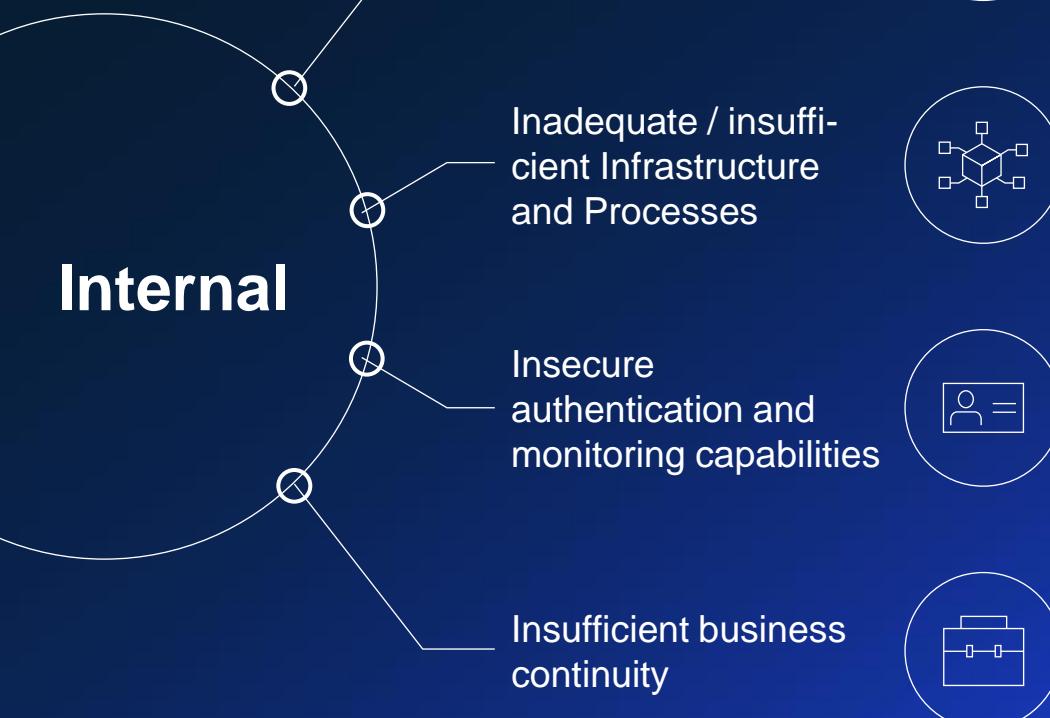
Social-engineering ploys are on the rise



Websites with weak security are being used to deliver malware.



Public-sector organizations experience acute pressure.



Use of personal devices, infrastructure and services

Inadequate / insufficient Infrastructure and Processes

Insecure authentication and monitoring capabilities

Insufficient business continuity

**Given the shift,  
criminals and nation-  
state threat actors  
using known  
techniques but  
exploiting Covid-19  
themes and remote  
work environment**

COVID-19-themed attack  
statistics

18M

85%

3.5x

12+

**COVID-19 phishing emails** blocked by Google in 1 day  
(April '20)

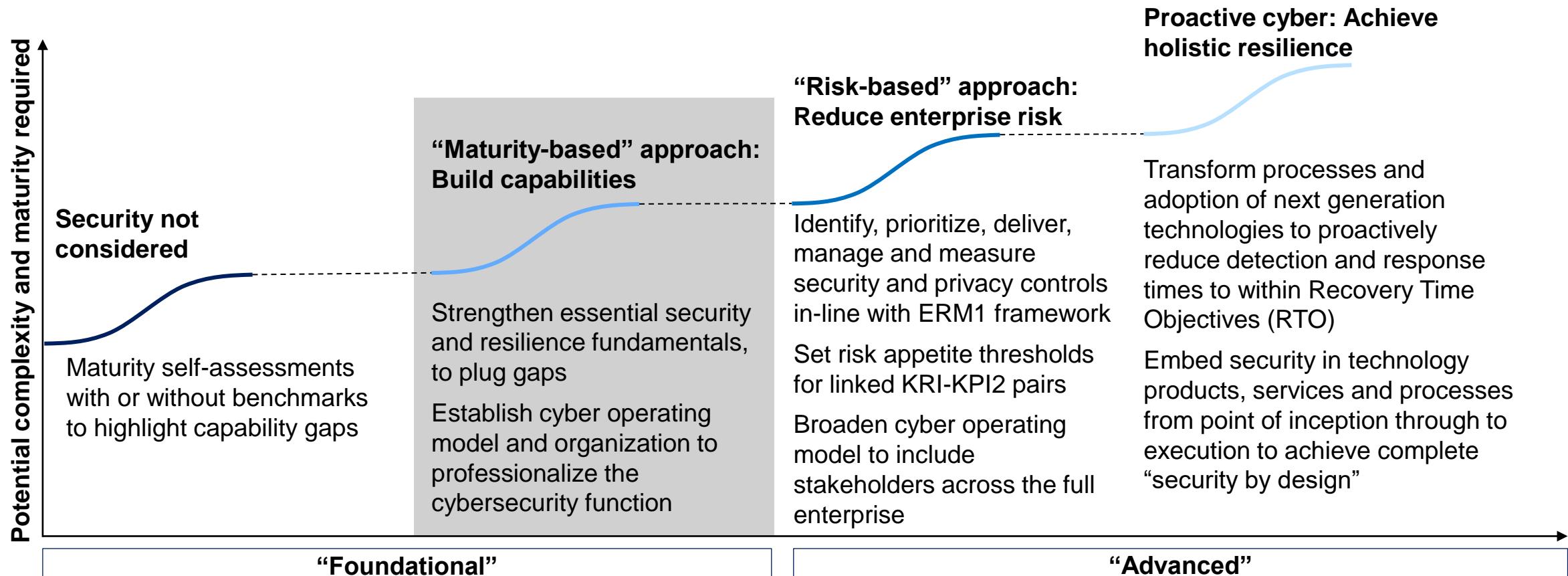
**Increase in malicious websites and malware files** blocked (Jan'20 - March'20)

More likely to contain at least one **malware family on home networks** than enterprise networks

**Nation-state backed threat actors** using the pandemic as cover for **digital reconnaissance and espionage**

# It is no longer sufficient to simply **as it is**, cyber programs must demonstrate real value

For most companies, a risk-based approach represents the next “S-curve” of cyber maturity. In today’s cyber environment, it is no longer sufficient to simply build capabilities; **cyber capabilities must demonstrate quantifiable reduction of enterprise risk.**

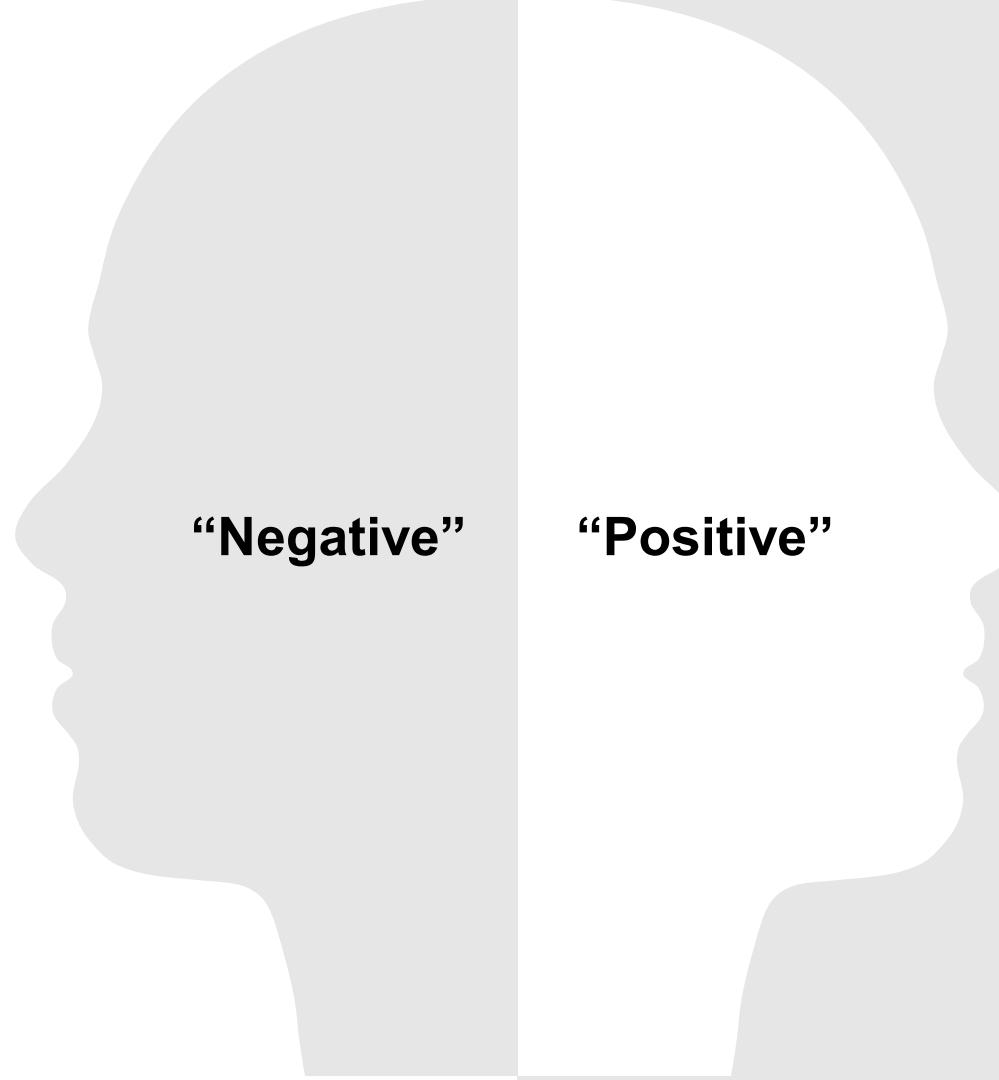


1 Enterprise Risk Management

2 Key Risk Indicator; Key Performance Indicator

Source: McKinsey Cybersecurity Practice

# But...there are always two sides to a coin



Increasing cyber incidents and crimes threaten Cambodia to negatively impact GDP

**“Negative”**

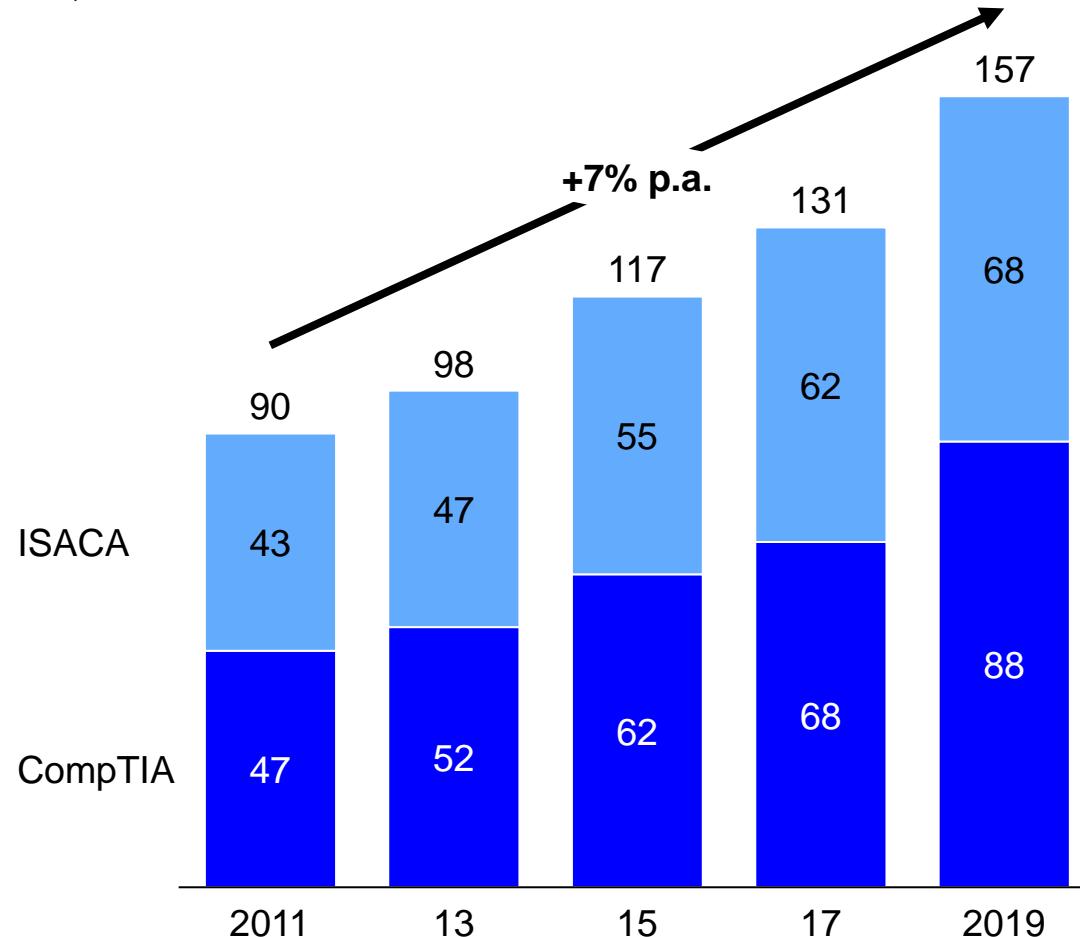
**“Positive”**

Increasing demand for cybersecurity services, products and talent provide new opportunities for both business and academia

# Huge demand for cyber skill development has driven profit surge for private professional certifiers and brought change in education

## Profit of Private Cyber security certifier

;Million USD



## Changes in Global Education

**80%**

of schools offer cybersecurity education at school in U.S.A.

**45%**

of K-12 students(age of 5-18) receive regular cybersecurity education in U.S.A

**36%**

American graduated IT professionals earn 36% higher salary than other graduates

**4.1 mil**

Cyber Security professionals demand worldwide in 2021

对外厳秘

# Reflecting demand from industry, American university progressively setup degree/master course for Cyber security (1/2)

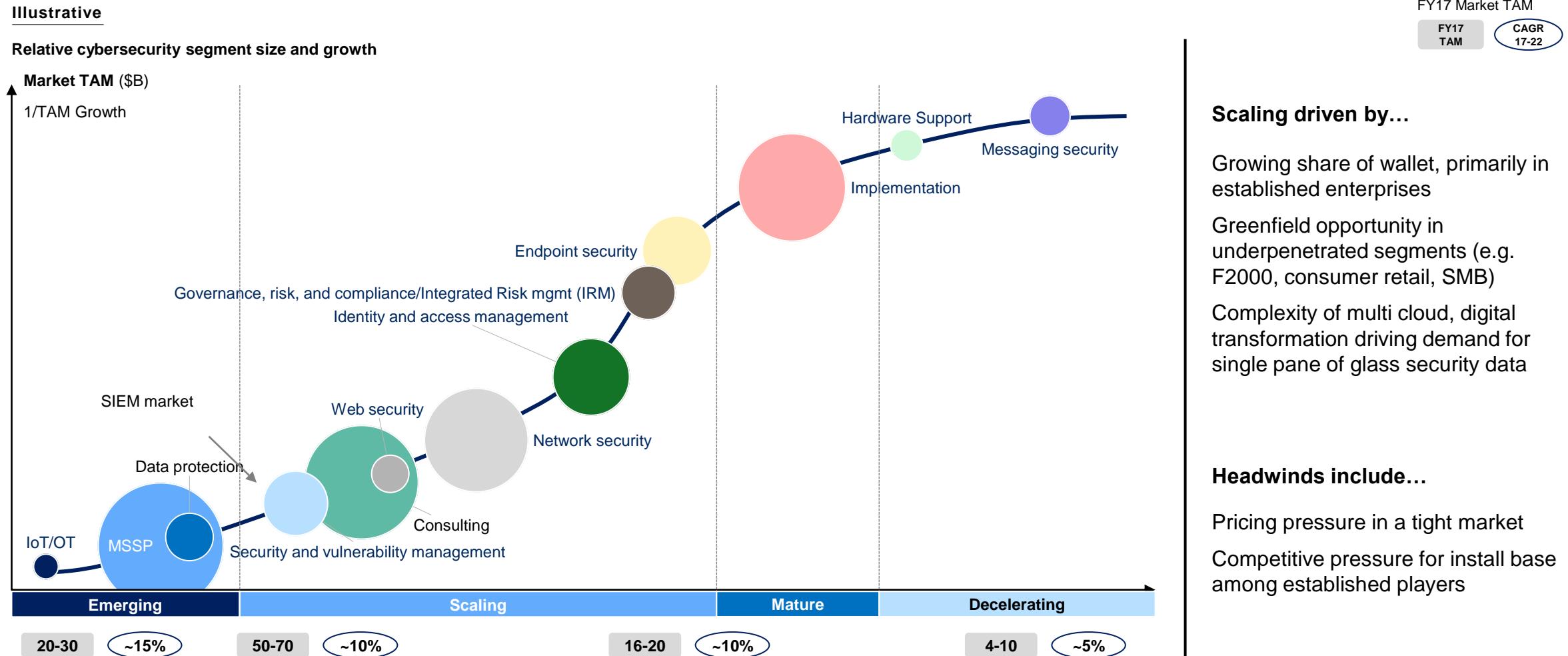
CS

Ranking	Name of university	Program name	Ranking	Name of university	Program name
1	 California State University, San Bernardino	<ul style="list-style-type: none"> <li>Cybersecurity certificate</li> <li>Cyber Security Professional (Certificate)</li> <li>National Cyber Security Studies, MS</li> </ul>	6	 Kennesaw State University, Georgia	<ul style="list-style-type: none"> <li>Master of Science in Cybersecurity</li> <li>BA in Science in Cybersecurity</li> </ul>
2	 Carnegie Mellon University, Pittsburgh	<ul style="list-style-type: none"> <li>Cyber Ops certificate.</li> <li>Cybersecurity Engineering and Software Assurance Professional Certificate</li> </ul>	7	 Naval Postgraduate School, Monterey	<ul style="list-style-type: none"> <li>Cyber Security Fundamentals</li> <li>Cyber Security Defense</li> <li>Cyber Security Adversarial Techniques</li> </ul>
3	 George Washington University, Washington DC	<ul style="list-style-type: none"> <li>GW CyberCorps: Cybersecurity</li> <li>Master of Science in Cybersecurity in Computer Science</li> </ul>	8	 Pennsylvania State University, Pennsylvania	<ul style="list-style-type: none"> <li>S. in Cybersecurity Analytics and Operations</li> <li>S. in Cybersecurity Analytics and Operations</li> </ul>
4	 Indiana University, Bloomington	<ul style="list-style-type: none"> <li>S. in cybersecurity and global policy</li> <li>S. in secure computing</li> </ul>	9	 Rochester Institute of Technology, Rochester	<ul style="list-style-type: none"> <li>Cyber Security Advanced Certificate.</li> </ul>
5	 Kansas State University, Manhattan	<ul style="list-style-type: none"> <li>BS Cybersecurity option</li> </ul>	10	 University of Maryland University College, Adelphi	<ul style="list-style-type: none"> <li>Computer Networks and Cybersecurity</li> <li>Cybersecurity Management and Policy</li> <li>Cyber Operations</li> <li>Cybersecurity Management and Policy</li> <li>Cybersecurity Technology</li> </ul>

# Reflecting demand from industry, American university progressively setup degree/master course for Cyber security (2/2) 对外厳密

CS			
Ranking	Name of university	Program name	CS
Ranking	Name of university	Program name	Ranking
11	 The University of Texas at San Antonio, Texas	<ul style="list-style-type: none"> <li>UTSA's Cyber Security Program</li> <li>Cyber Security – Online Degree Program</li> </ul>	 New York University
12	 Worcester Polytechnic Institute, Worcester	<ul style="list-style-type: none"> <li>Masters in Cybersecurity.</li> <li>BS cybersecurity concentration</li> </ul>	 Drexel University, Philadelphia
13	 University Of Southern California	<ul style="list-style-type: none"> <li>Privacy Law and Cybersecurity</li> </ul>	 Georgetown University, Washington
14	 Johns Hopkins University	<ul style="list-style-type: none"> <li>ISI Cyber security Programs.</li> </ul>	 Maryville University, Saint Louis
15	 Messiah University, Mechanicsburg, PA	<ul style="list-style-type: none"> <li>S Cybersecurity</li> </ul>	 University of Virginia-Main Campus
16			
17			
18			
19			
20			

# And..The overall cyber security market is growing at ~10%



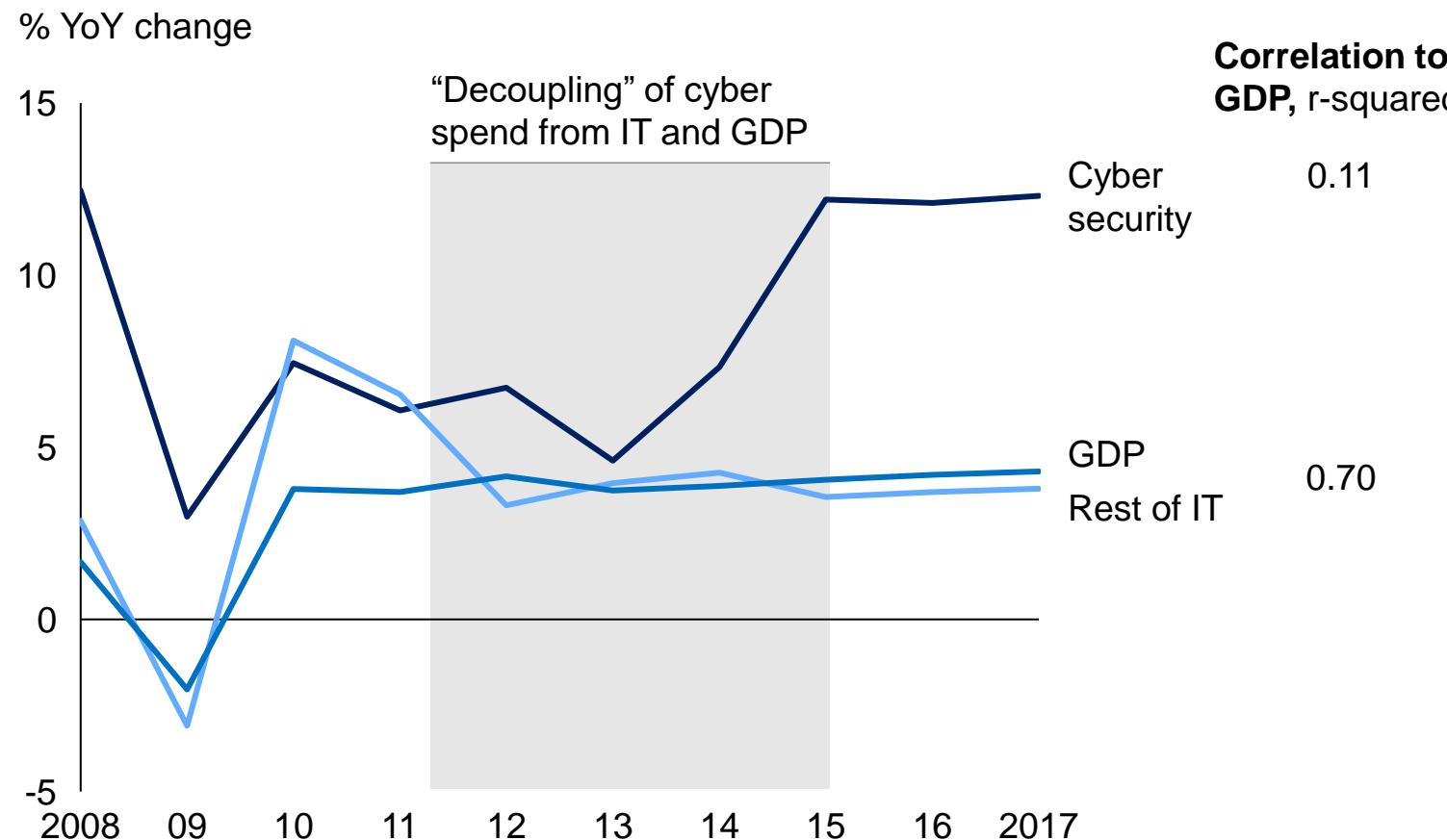
NOTE: "Emerging" is >13%, "Scaling" is 8-13%, "Mature" is 6-8%, "Decelerating" is <6%

Source: McKinsey Cyber Market Map

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# To manage increased cyber risk companies historically spent more money on cyber

## Change in cyber security/IT spend vs. change in GDP



“” Cyber security spending is largely driven by non-optional compliance needs. Unlike spending on for example, new product, marketing and sales, and business development, cyber spending has proven to be fairly immune from ups and downs.



**Industry expert**

“” Our first priority from an IT perspective is meeting the compliance requirements and fundamental security needs of the business, regardless of the economy's performance.



**Bank CIO**

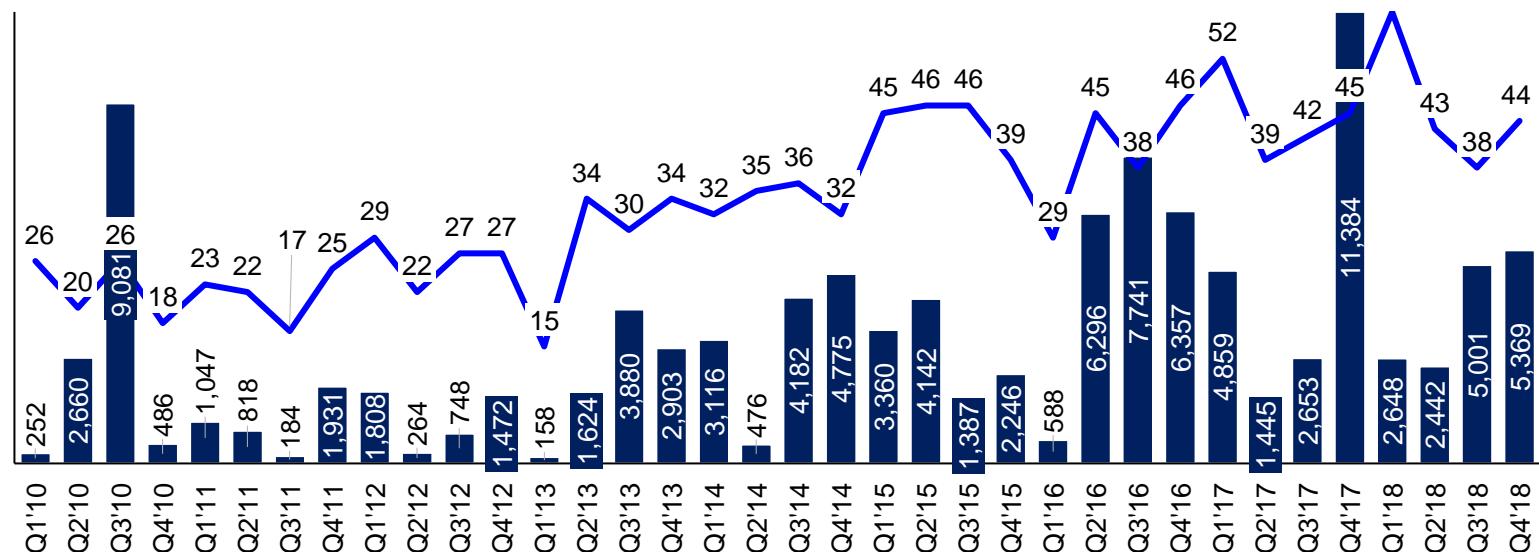
# Cybersecurity M&A totaled \$110B across 1,225 deals since 2010

■ Private Co. Volume (\$B)    ● Number of Deals  
 ■ Public Co. Volume (\$B)

Annual M&A deals and volume,  
(\$B) (2010 – 2018)



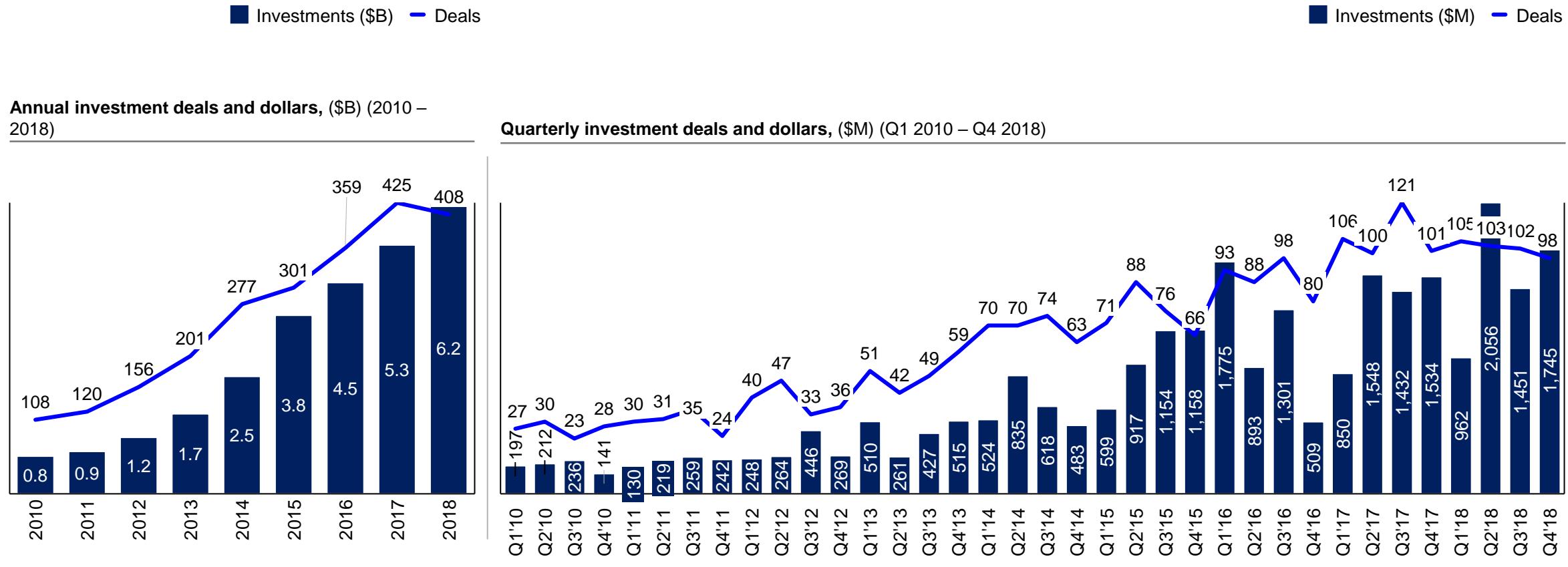
Quarterly M&A deals and volume, (\$M) (Q1 2010 – Q4 2018)



- Cybersecurity deal volume of **183** transactions sets new record; previous high of **178** set in 2017
- **96%** of deals in 2018 involved targets that were private companies or assets

- Over the last eight quarters financial and strategic buyers have completed **\$36.0B** in M&A transactions
- Q4'18 M&A activity has remained relatively constant over the two prior years, with **44** M&A transactions, but M&A transaction volume was down compared to the two prior years at **\$5.4B**
- Thoma Bravo / Imperva, BlackBerry / Cylance, and Thoma Bravo / Veracode accounted for **78%** of total Q4'18 disclosed deal value, with a total of **\$4.2B**

# Cybersecurity startups have raised \$26.9 billion across 2,358 deals since 2010



- **\$6.2B** was raised across **408** transactions in 2018
- 2018 outpaced 2017 by **\$850M** in funding volume while 2017 still holds the record by number of deals funded

- Over the last eight quarters investors have poured **\$11.6B** into Cybersecurity
- There was once again over **\$1B** invested in Q4 2018 (**\$1.7B**), making it 6 of the past 7 quarters with over **\$1B** invested; **\$504M** raised in December (26 deals), **\$557M** raised in November (37 deals), and **\$683M** raised in October (35 deals)
- 2018 had the **2** of the **3** largest funding quarters over the past 8 years by funding volume

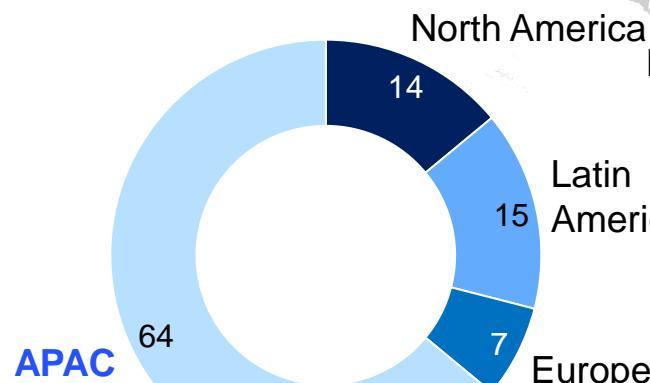
# Need for cybersecurity talent is growing globally and government must find ways to attract, develop, and retain Cyber professionals

対外厳密

## The cybersecurity workforce gap by region

Millions

Global  
~4.07



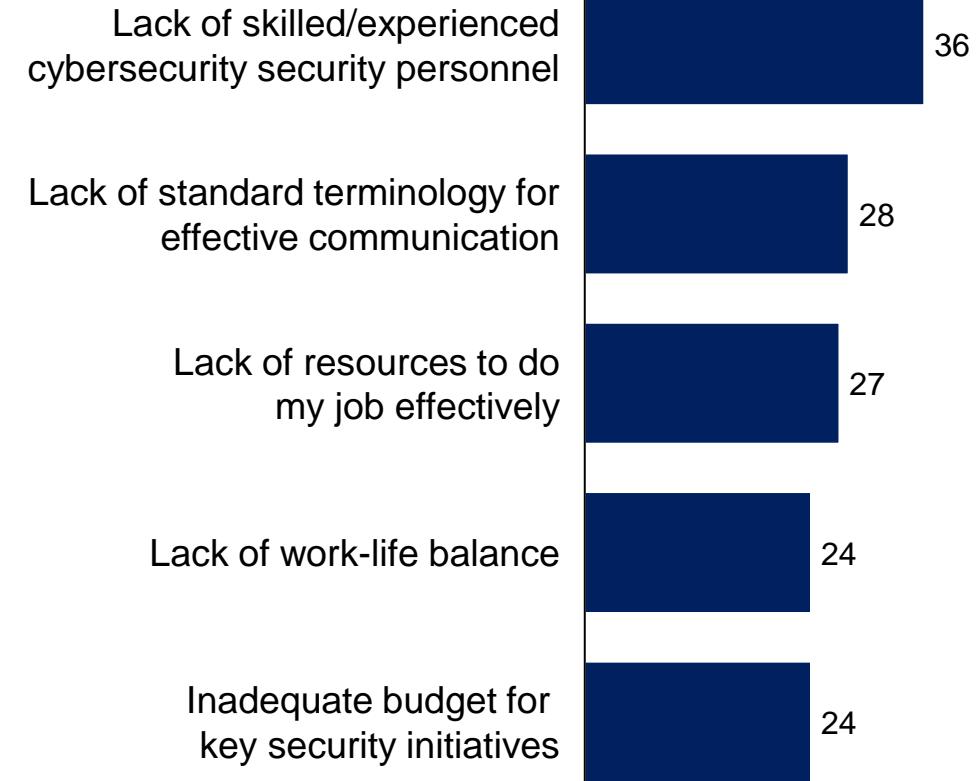
Unit;%

Source: (ISC)2 cybersecurity workforce study 2019

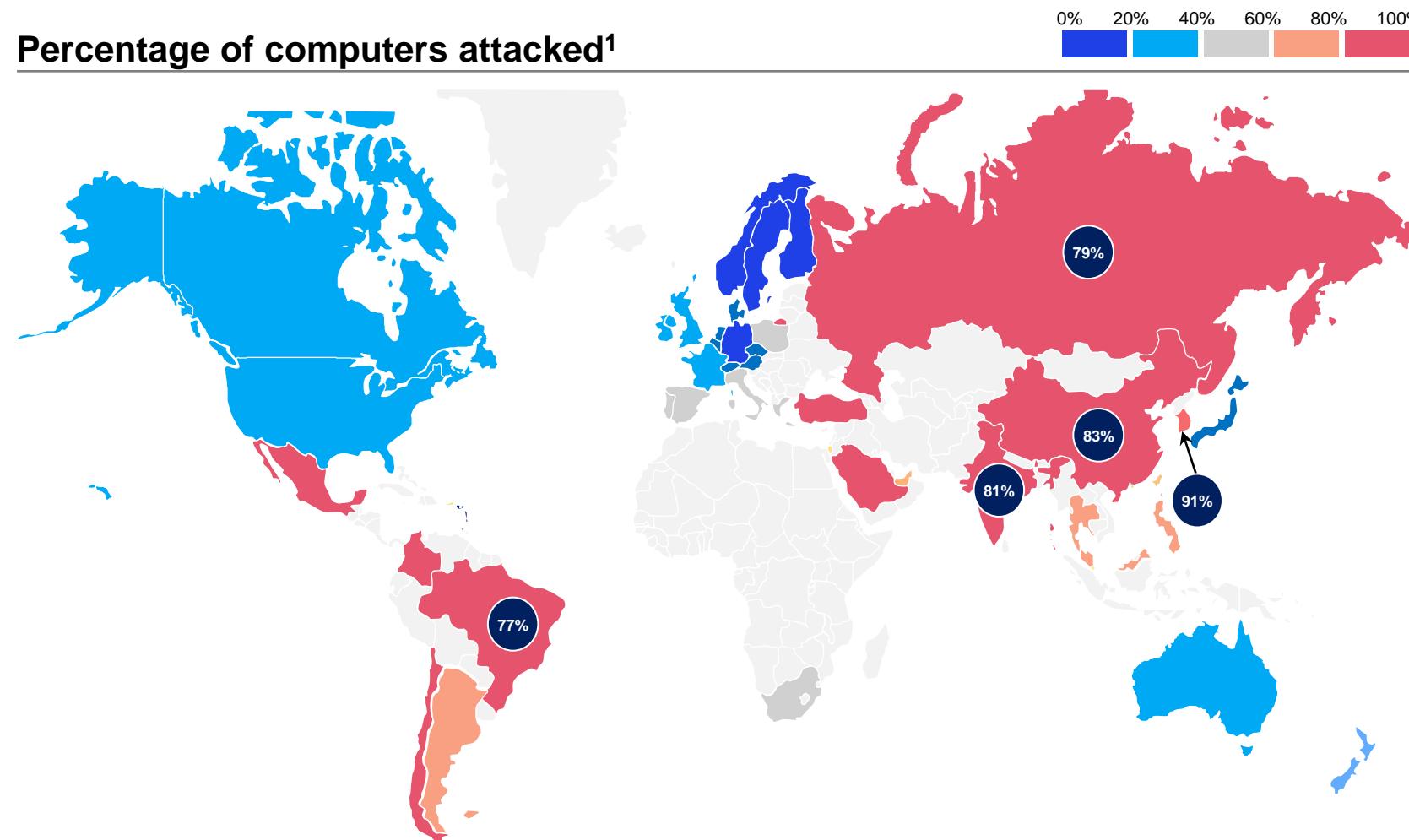
機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

## Top job concerns among cybersecurity professionals

Percent



# People across the world are impacted by attacks on their computers



1. "Computers" includes all desktop, laptop, and server hardware. Does not include mobile devices. Data from 2012

Cyber crime is a **global phenomenon** – with many markets being highly exposed to computer attacks

Approximately,

**1.0-1.6% of global GDP lost annually due to cyber crime**

# In 2017, Ukrainian companies and government institutions were targeted by NotPetya, but even unrelated internationals like Maersk were caught in the crossfire



## Target



- Ukrainian organizations, such as banks, ministries, and electricity firms virus also affected computer systems in Denmark, India and the United States, but more than half of those victimized were in Ukraine

## Tactics



- Ransomware inserted into tax accounting software
- Reused exploits developed leaked by NSA to spread
- Timed for a national holiday when offices empty
- Microsoft issued patches, but often not applied

## Damages



- More than USD \$100 Bn, with companies like Merck (\$870 Mn) and Maersk (\$300 Mn)<sup>1</sup>

Microsoft issued patches to prevent exploit from functioning in Mar 2017



Ransomware spread through Ukraine in Jun 2017, affecting more than 1 Mn computers



Ransomware spread globally to companies in North America, Europe, India, and Australia

Major MNCs (e.g., MSD, DLA Piper, FedEx, Merck, Cadbury, JNPT) caught in the crossfire

<sup>1</sup> Tom Bossert, Homeland Security Advisor to the U.S. President

# North Korea-based Lazarus Group is active to target several developing countries in Asia



2013 South Korea  
Cyberattack "Ten Days of Rain" three South Korean television stations and a bank suffered from frozen computer terminals in a suspected act of cyberwarfare.



2017 WannaCry Attack.  
300,000 computers worldwide are likely authored by hackers

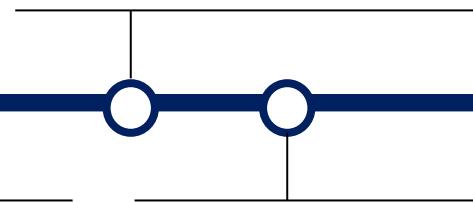


2018 Taiwan Bank. steal roughly \$60 million from Far Eastern International Bank



Late 2020: pharmaceutical company attacks, including AstraZeneca

- Stealing sensitive information to be sold for profit
- Extortion schemes
- Giving foreign regimes access to proprietary COVID-19 research



2016 Bangladesh Bank cyber heist. security hackers via the SWIFT network to illegally transfer close to US\$1 billion



2017: cryptocurrency attacks. attacks on cryptocurrency Bitcoin and Monero users mostly in South Korea



2019: new version of malware dubbed ELECTRICFISH. \$49 million theft from an institution in Kuwait

# Any nation and government owned organization can become a target of Cyber attacks(1/2)

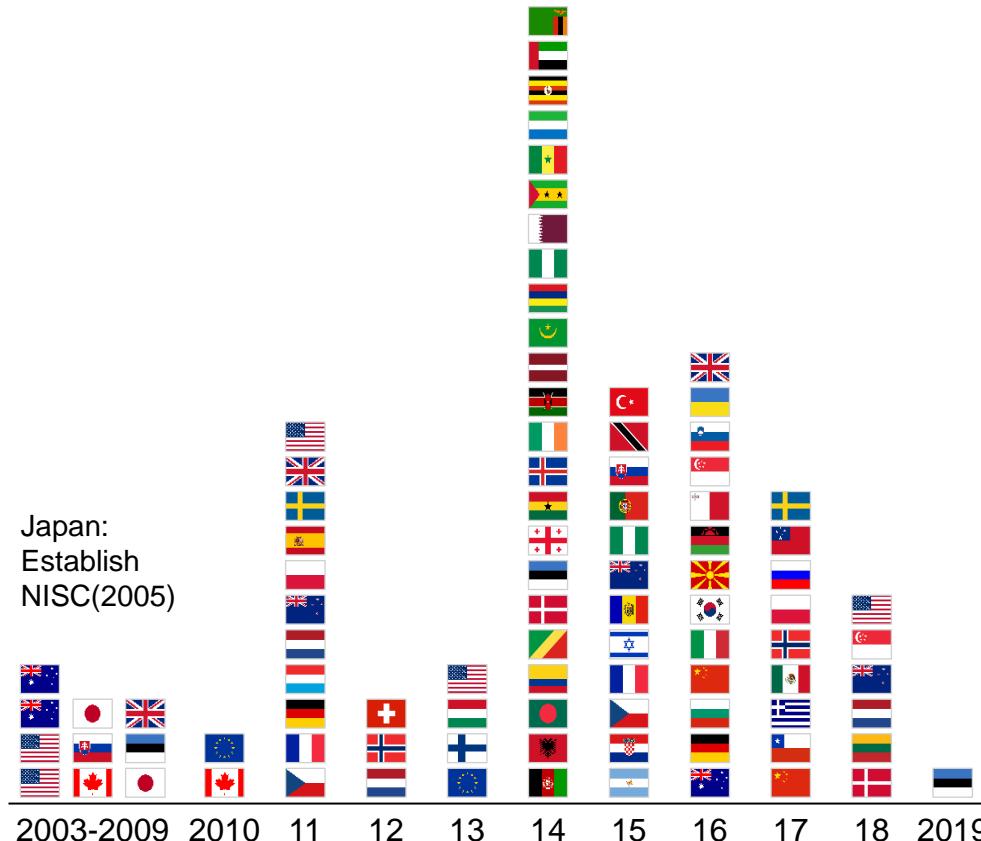
Data	Detail	Targeted Countries
March 2021	The head of U.S. Cyber Command testified that the organization had conducted more than two dozen operations to confront foreign threats ahead of the <b>2020 U.S. elections</b> , including eleven forward hunt operations in nine different countries.	USA 
	A group of Chinese hackers <b>used Facebook to send malicious links to Uyghur</b> activists, journalists, and dissidents located abroad.	Uyghur 
	The Indian Computer Emergency Response Team found evidence of Chinese hackers <b>conducting a cyber espionage campaign against the Indian transportation sector</b>	India 
	Polish security services announced that suspected Russian hackers briefly took over the websites of <b>Poland's National Atomic Energy Agency and Health Ministry</b> to spread false alerts of a nonexistent radioactive threat.	Poland's 
	Both Russian and Chinese intelligence services <b>targeted the European Medicines Agency</b> in 2020 in unrelated campaigns, stealing documents relating to COVID-19 vaccines and medicines.	European 
	<b>Ukraine's State Security Service</b> announced it had prevented a <b>large-scale attack by Russian FSB hackers</b> attempting to gain access to classified government data.	Ukraine 
	Lithuania's State Security Department declared that <b>Russian hackers had targeted top Lithuanian officials</b> in 2020 and used the country's IT infrastructure to carry out attacks against organizations involved in developing a COVID-19 vaccine.	Lithuania 
	Suspected Iranian hackers targeted <b>government agencies, academia, and the tourism industry</b> in Azerbaijan, Bahrain, Israel, Saudi Arabia, and the UAE as part of a cyber espionage campaign.	Azerbaijan, Others 
	Chinese government hackers <b>targeted Microsoft's enterprise email software</b> to steal data from over 30,000 organizations around the world, including government agencies, legislative bodies, law firms, defense contractors, infectious disease researchers, and policy think tanks.	All 
	Suspected Chinese hackers <b>targeted electricity grid operators in India</b> in an apparent attempt to lay the groundwork for possible future attacks.	India 

# Any nation and government owned organization can become a target of Cyber attacks(2/2)

Data	Detail	Targeted Countries
Feb 2021	A Portuguese-speaking cyber criminal group <b>accessed computer systems at a division of Oxford University</b> researching COVID-19 vaccines, and are suspected to be selling the data they collected to nation states.	USA 
	North Korean hackers targeted <b>defense firms in more than a dozen countries</b> in an espionage campaign starting in early 2020.	All 
	Hackers associated with the Chinese military <b>conducted a surveillance campaign against Tibetans</b> both in China and abroad.	Tibet 
	Russian hackers <b>compromised a Ukrainian government file-sharing system and attempted to disseminate malicious documents</b> that would install malware on computers that downloaded the planted files.	Ukraine 
	Hackers linked to the Vietnamese government <b>conducted a nearly three-year cyber espionage campaign</b> against human rights advocates in the country by using spyware to infiltrate individuals' systems, spy on their activity, and exfiltrate data.	Vietnam 
	Ukrainian officials reported that <b>a multi-day distributed denial-of-service attack</b> against the website of the Security Service of Ukraine was part of Russia's hybrid warfare operations in the country.	Ukraine 
	The US Department of Justice indicted three <b>North Korean hackers for conspiring to steal and extort more than \$1.3 billion</b> in cash and cryptocurrencies.	U.S.A 
	Iranian hackers <b>took control of a server in Amsterdam</b> and used it as a command and control center for attacks against political opponents in the Netherlands, Germany, Sweden, and India.	Netherlands 
	North Korean hackers <b>attempted to break into the computer systems of pharmaceutical company Pfizer</b> to gain information about vaccines and treatments for the COVID-19.	U.S.A 
	Suspected Iranian hackers targeted government agencies in the UAE <b>as part of a cyber espionage campaign</b> related to the normalizations of relations with Israel.	UAE 
	The French national cybersecurity agency announced that <b>a four-year campaign against French IT providers</b> was the work of a Russian hacking group.	Russia 

# To address national cyber threat, a rapid surge in national cybersecurity strategies since the cyber-attack on Estonia in 2007

## Issuance of national cybersecurity strategies 2003-2019



The **United States** has focused on cybersecurity since the 1990s, and has published a number of cybersecurity documents, but no overarching strategy

Victim of a cyber-attack in 2007, **Estonia** has one of the most digitally dependent societies. Cybersecurity strategy today is integrated to the national defense strategy process

**UK** has developed a cybersecurity strategy with a focus on creating a safe environment for businesses, and cross sector information sharing (Fusion Cell)

**France** and **Germany** national cybersecurity strategies involve a relatively active role of the government

**Netherlands** cybersecurity strategy is based on “Strength through cooperation”, while the Finnish strategy also emphasizes public-private partnerships as the forte of the cyber-security community

**EU** outlined a Digital Agenda (2010) prior to publishing the EU Cybersecurity Strategy (2013) – discussion today is centered around potential impact of upcoming regulation

# Current state analysis – Cambodia is facing an increased threat from cybersecurity that has the potential to impact its business

Cambodia is getting hit by an increasing number of cyber attacks

**Index**

**15.58**

at **National Cyber Security Index (NCSI)**, which is the **second lowest** among ten ASEAN Member States. **NCSI measures countries' cyber security capacity**



**Internet Penetration Rate**

**52.6%**

with **8.86 million internet users** in Cambodia in January 2021

**Over**

**21,962,421**

attacks was detected in **2018**. **21,962,421** from **26,329,551** in **2017**

**Ranked**

**7<sup>th</sup>**

among top markets in Asia under malware threats, according to **Microsoft Asia's Malware Infection Index 2016 (MII2016)**

**The organization's overall digital resilience is below the global average**

**Illustrative drivers**

**The list of information assets and risk** can be expanded to allow the organization to prioritize protection of its most critical information assets

While IT reviews systems for cybersecurity prior to release, **security can be further integrated into development and business processes** to increase cyber maturity

**The organization is building an incident response capability** that will enable it to more effectively respond to cyber-attacks

**Security controls are fragmented across systems**, which if standardized will facilitate effective system hardening

**Employees are aware of the importance of different types of information**; and use of formal risk-based controls will enable effective and efficient security

**Defense capabilities primarily focus on network activity monitoring** and formal security monitoring and threat intelligence capabilities will enable more effective security defenses

**Employees are aware of the importance of cyber; however, gaps can be closed** including risk-based protection and a defined cyber organization

# What are the typical types of cyber attack?

	<b>Attack type</b>	<b>Description</b>	<b>Example</b>
<b>Un-targeted</b>	<b>Phishing</b>	Sending emails to large numbers of people asking for sensitive information or encouraging them to visit a fake website	N/A
	<b>Ransom-ware</b>	Disseminating disk encrypting extortion malware (i.e., malware that can deny the rightful user access to their computer unless a ransom is paid)	N/A
	<b>Denial of service</b>	Deploying a collection of computers compromised by malicious code and controlled across a network to deliver a distributed denial of service attack	2007 cyberattacks in Estonia that crippled government and corporate sites
<b>Targeted</b>	<b>Spear-phishing</b>	Sending emails to targeted individuals that could contain an attachment with malicious software	Target breach and Sony Pictures hack both relied on spear-phishing as the infection method
	<b>Zero day</b>	Exploiting of previously unknown security vulnerabilities to gain access to a target computer network	Stuxnet attacks on Iranian centrifuges
	<b>Subverting the supply chain</b>	Attacking equipment or software being delivered to an organization	Pre-installed Superfish adware on Lenovo note-books allowed attackers to masquerade as secure internet destinations

# Cambodia need to design Cyber security strategy with suggested strategy element

Cybersecurity strategy element	Insights from benchmarking cybersecurity strategy	Workshop #
A Governance 	<ul style="list-style-type: none"> <li>Top-performing nations are moving towards <b>centralized governance bodies</b> reporting directly to executive branches of government and serving as <b>E2E owners of cybersecurity strategy implementation</b></li> </ul>	• #2
B Legal and regulations 	<ul style="list-style-type: none"> <li><b>Comprehensive legislative frameworks</b> cover mandatory IT security standards, regulations, and best practices, and are enforced through audits and law enforcement</li> <li><b>Specific legislations to address emerging technologies</b> are evolving at fast pace in countries with advanced cybersecurity legislations</li> </ul>	• #3
E Partnerships 	<ul style="list-style-type: none"> <li><b>Regional and international partnerships</b> are actively used to foster sharing of best practices and enhancing operational and technical capabilities through joint drills &amp; audits</li> </ul>	• #4
C Talent and people 	<ul style="list-style-type: none"> <li><b>Public awareness and training</b> programs, which draw on <b>international standards and offerings</b>, form the basis for cybersecurity talent development</li> </ul>	• #5~7
F Critical infrastructure 	<ul style="list-style-type: none"> <li>CII protection programs, executed by national cybersecurity agencies, focus <b>selectively on critical assets</b> in critical sectors with timely involvement of relevant authorities</li> </ul>	• #8
D Incident response 	<ul style="list-style-type: none"> <li>National cybersecurity agencies, through <b>specialized incident response teams</b>, lead integrated response efforts with close coordination with impacted assets</li> </ul>	• #9

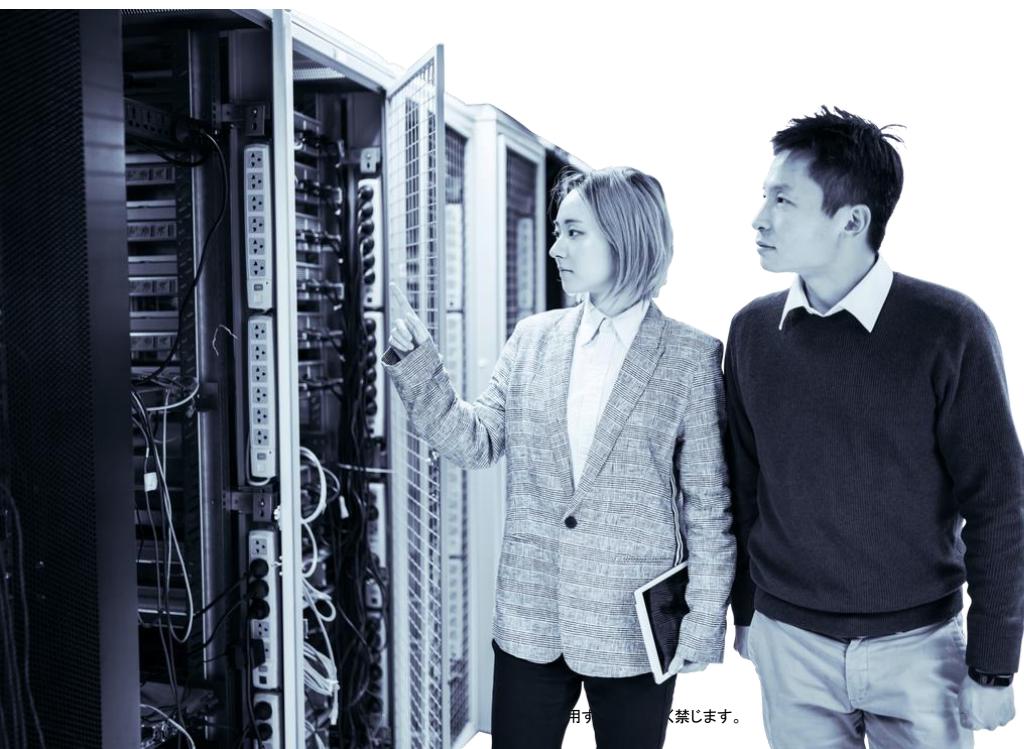
---

# Questions?

---

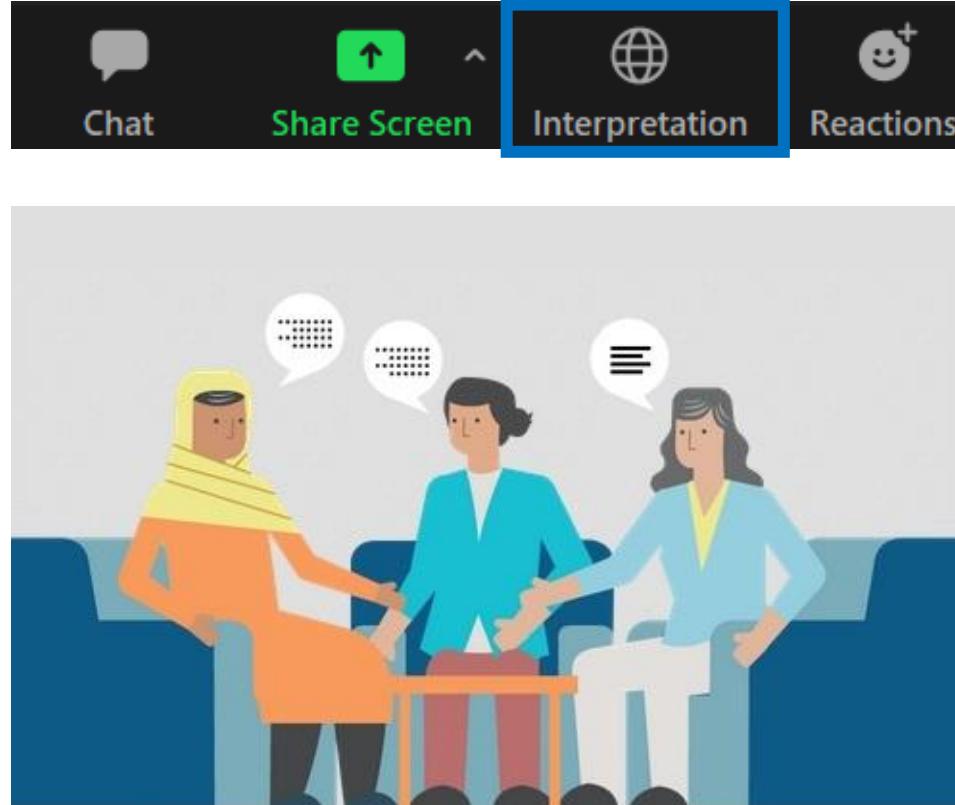


1. Overview of Cyber Security Trend
- 2. Definition of Cyber threat and national Incident response framework**
3. Cyber Security Regulation framework
4. Partnership(Public, Private, Academia, International)
5. Professional training and certification
6. Public awareness and alerts
7. Cyber Security for SME
8. Critical Infrastructure Industry protection
9. CERT/ Resilience
10. Wrap up / Cyber security assessment

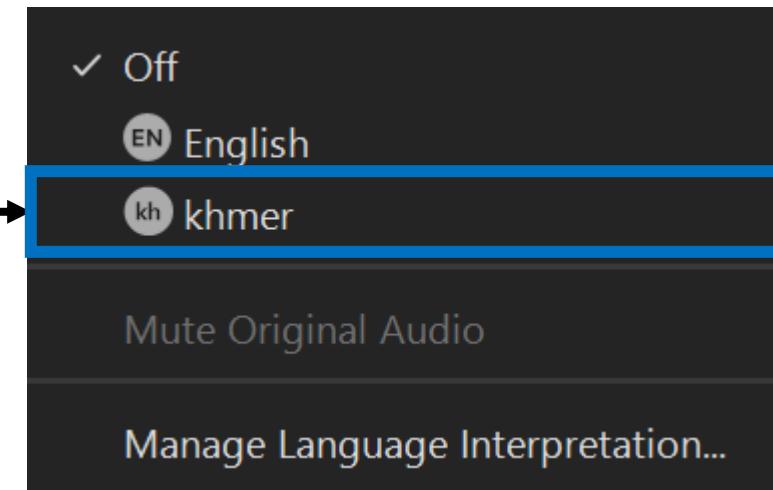


# Khmer simultaneous Interpretation available

Select “Interpretation” on the bottom



Select “Khmer”



- Presentation is simultaneously translated into Khmer
- You can post question in Khmer



## Timeline

## Overview

100 minuets

## Workshop & QA

20 minuets

# Cambodia need to design Cyber security strategy with suggested strategy element

## Cybersecurity strategy element

A Governance	
B Legal and regulations	
E Partnerships	
C Talent and people	
F Critical infrastructure	
D Incident response	

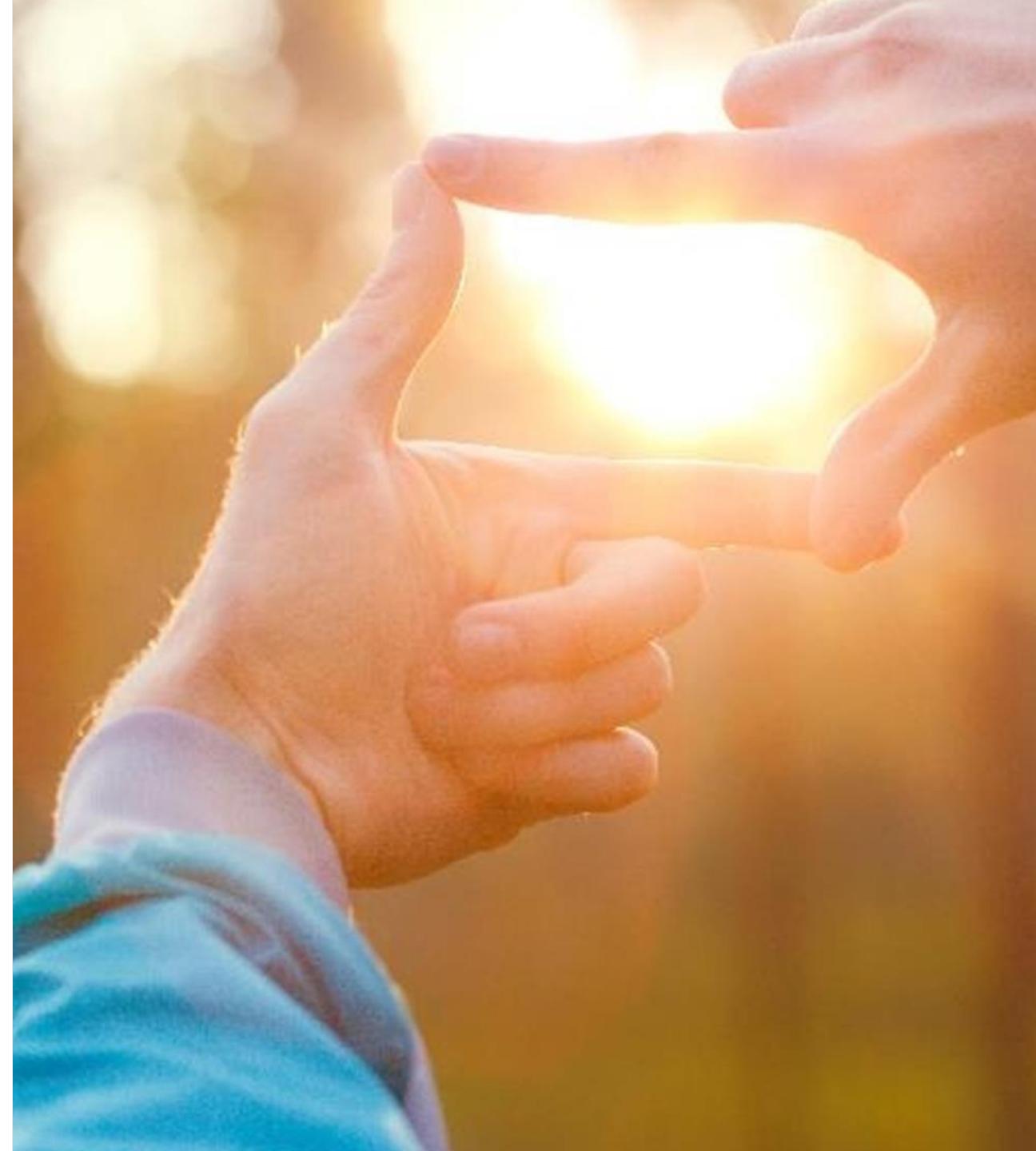
## Insights from benchmarking cybersecurity strategy

#	
• #2	<ul style="list-style-type: none"> <li>Top-performing nations are moving towards <b>centralized governance bodies</b> reporting directly to executive branches of government and serving as <b>E2E owners of cybersecurity strategy implementation</b></li> </ul>
• #3	<ul style="list-style-type: none"> <li><b>Comprehensive legislative frameworks</b> cover mandatory IT security standards, regulations, and best practices, and are enforced through audits and law enforcement</li> <li><b>Specific legislations to address emerging technologies</b> are evolving at fast pace in countries with advanced cybersecurity legislations</li> </ul>
• #4	<ul style="list-style-type: none"> <li><b>Regional and international partnerships</b> are actively used to foster sharing of best practices and enhancing operational and technical capabilities through joint drills &amp; audits</li> </ul>
• #5~7	<ul style="list-style-type: none"> <li><b>Public awareness and training</b> programs, which draw on <b>international standards and offerings</b>, form the basis for cybersecurity talent development</li> </ul>
• #8	<ul style="list-style-type: none"> <li>CII protection programs, executed by national cybersecurity agencies, focus <b>selectively on critical assets</b> in critical sectors with timely involvement of relevant authorities</li> </ul>
• #9	<ul style="list-style-type: none"> <li>National cybersecurity agencies, through <b>specialized incident response teams</b>, lead integrated response efforts with close coordination with impacted assets</li> </ul>

# Proposed definition of a national cyber incident

“ ”

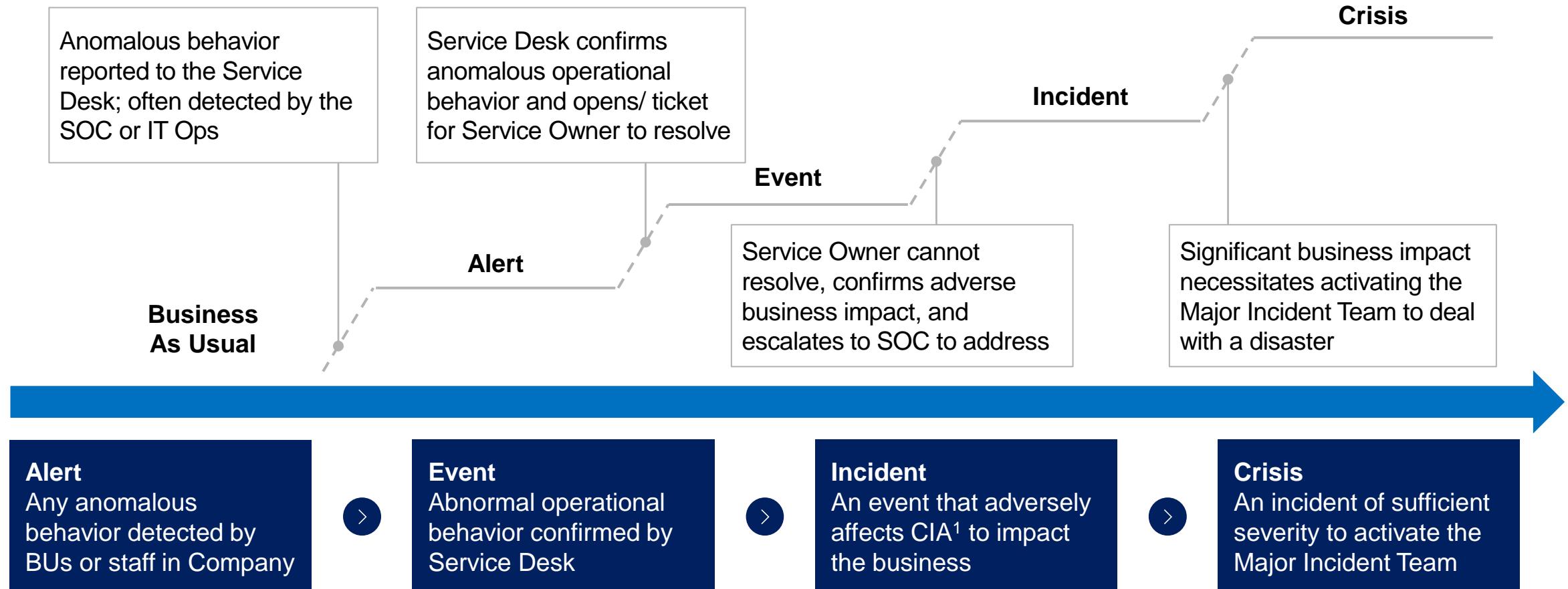
...a cyber incident is a **single or series of unwanted or unexpected events** that threaten to or actually compromise the **security, confidentiality, integrity, or availability** of an information technology (IT) system, network, or data...



# To escalate incidents, follow a path, elevating from BAU2 to crisis depending on the severity of the incident

对外厳密

The SOC must **collaborate with Service Owners** in IT Operations to investigate, triage, and resolve cyber-related events and incidents



1 Confidentiality, Integrity, and Availability

2 Business As Usual

# A national incident response and recovery plan requires a clear definition of a cyber incident

At a national level, the government will receive requests to deal with a whole range of cyber-related matters...

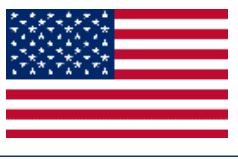
NOT EXHAUSTIVE

Type of issue	Potential cyber-related issue description
Computer Misuse	<ul style="list-style-type: none"> <li>Companies might report that their computers and servers have been used to mine BitCoin without their explicit knowledge</li> </ul>
Cyber bullying	<ul style="list-style-type: none"> <li>Adolescents and teenagers might report instances of getting bullied on social media</li> </ul>
Spam email	<ul style="list-style-type: none"> <li>Citizens might fall victim to or report suspicious email (e.g. Lottery scams)</li> </ul>
Data loss	<ul style="list-style-type: none"> <li>Companies might report that their confidential proprietary data have been hacked and posted on the Internet</li> </ul>
System shutdown	<ul style="list-style-type: none"> <li>Manufacturing plants might report an error with their IT systems causing machines to behave differently than usual</li> </ul>
Social media lockout	<ul style="list-style-type: none"> <li>Private citizens might forget their passwords and request of help recovering their accounts</li> </ul>

SOURCE: Client interview, Press search

**Having a consistent definition of a cybersecurity incident at a national level will aid agencies in deciding the types of incidents that will require a response**

# Benchmark countries typically define information assets is the Data, which consist of Confidentiality, Integrity, and Availability (C-I-A) of information

Country	Definitions
	<ul style="list-style-type: none"><li>“A cybersecurity incident is a past, ongoing, or threatened intrusion, disruption, or other event that impairs or is likely to impair the <b>confidentiality, integrity, or availability</b> of electronic information, information systems, services, or networks.”</li></ul>
	<ul style="list-style-type: none"><li>“A cyber security incident is an event that had a direct impact on the <b>confidentiality, integrity or availability</b> of information or systems. One or more of the three parameters may be impacted and the reason can be human behaviour or a disruption caused by the natural or manmade environment.”</li></ul>
	<ul style="list-style-type: none"><li>“An unauthorised access or attempted access to a system, or a breach of a system’s security policy in order to affect its <b>integrity or availability</b>”</li></ul>
	<ul style="list-style-type: none"><li>“Cyber incidents occur when events compromise the <b>security, confidentiality, integrity, or availability</b> of an information technology (IT) system, network, or data. ”</li></ul>
	<ul style="list-style-type: none"><li>“A cyber security incident is a single or series of unwanted or unexpected events that have a significant probability of compromising an organisation’s business operations. Cyber security incidents can impact the <b>confidentiality, integrity or availability</b> of a system and the information that it stores, processes or communicates.”</li></ul>

SOURCE: National Cyber Strategy Reports

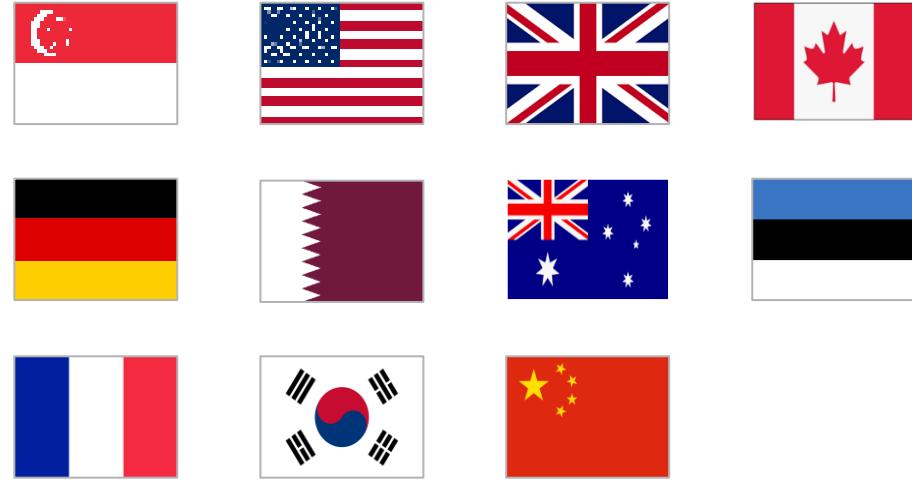
# The C-I-A framework covers most of the recent major cybersecurity attacks around the world

NOT EXHAUSTIVE

Attack	Assessment	
<b>Shamoon virus</b>	<ul style="list-style-type: none"> <li>The virus infiltrates the target, uploads all data into attacker's system, and deletes information on victim system</li> <li>Virus used to attack Saudi Aramco and RasGas</li> </ul>	<ul style="list-style-type: none"> <li><b>Confidentiality</b> of data is compromised</li> <li>By deleting information, the <b>availability</b> of information is affected</li> </ul>
<b>WannaCry</b>	<ul style="list-style-type: none"> <li>Ransomware which encrypted databases and demanded random payments in bitcoin currency</li> <li>Major companies affected include FedEx, National Health Service (UK), and Hitachi</li> </ul>	Locking players out from systems compromised <b>availability</b> of information to authorized users
<b>Sony Pictures hack</b>	<ul style="list-style-type: none"> <li>Database about Sony pictures were leaked by an organization called "Guardians of Peace"</li> <li>Details about inner-workings and private communications within Hollywood was revealed</li> </ul>	<ul style="list-style-type: none"> <li><b>Confidentiality</b> of data is compromised</li> <li>Documents were deleted, compromising <b>integrity</b> and <b>availability</b> of information as well</li> </ul>

# Methodology used to develop the proposed framework for National incident response and recovery

PRELIMINARY

Steps	Source of insight
<b>A</b> Benchmark analysis of key incident response elements defined by 11 benchmark countries	Benchmark analysis of the key elements of Cyber incident response in 11 countries
	
<b>B</b> Alignment with the two most popular incident response frameworks	Analysis of popular industry incident response frameworks: <ul style="list-style-type: none"> <li>NIST Cybersecurity Risk Framework; NIST SP 800-61</li> <li>ISO/IEC 27035: 2011</li> </ul>
	

SOURCE: Team analysis

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# Proposed national incident response and recovery framework

## 1 Victim reporting

**1A**

Single Point  
of Contact



**1B**

Multi-channel  
reporting



**3**

Triage and severity  
assessment



High

Low

Baseline

**2**

Active monitoring  
for Cyber incidents



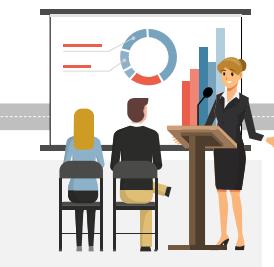
**4**

Agency coordination  
and response



Enablers

**5** Capability  
building



**6**

Effective  
Governance Structure



**7**

Information  
sharing model



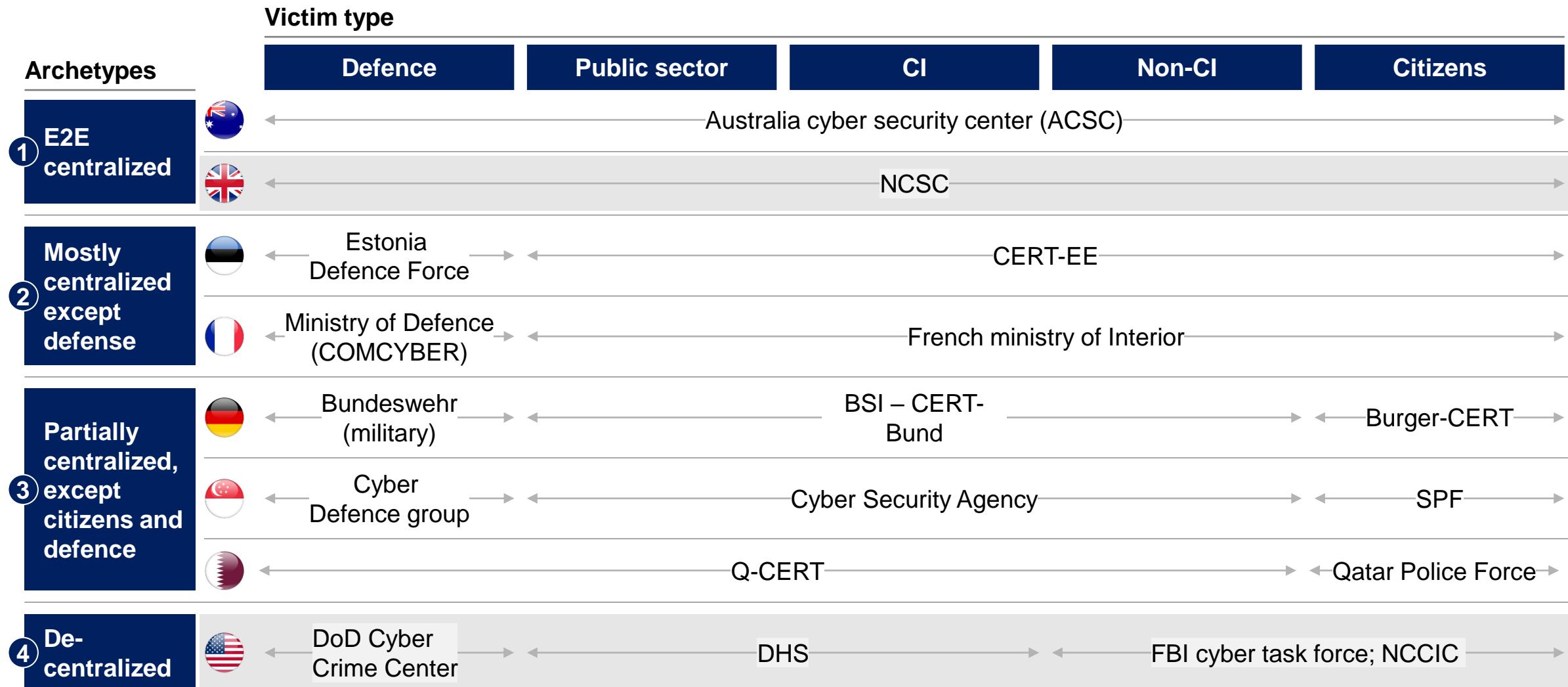
# 1A: Benchmark countries have different archetypes of points of contacts for different types of victims (1/2)

	<b>End-to-End centralized including intelligence and defense</b>	<b>Mostly centralized except intelligence or citizens</b>	<b>Partially centralized, except citizens and defense</b>	<b>Decentralized</b>
<b>Description</b>	  <ul style="list-style-type: none"> <li>One central agency that is the point of contact for all sectors at national level</li> </ul>	  <ul style="list-style-type: none"> <li>One central agency that is the point of contact for most sectors, except for defense</li> </ul>	   <ul style="list-style-type: none"> <li>One central agency that is the point of contact for most sectors, except for citizens and defence</li> </ul>	 <ul style="list-style-type: none"> <li>Multiple different agencies are a lead point of contact for different sectors at a national level</li> </ul>
<b>Appropriate when</b>	<ul style="list-style-type: none"> <li>Strong capabilities concentrated within a specific coordination body</li> </ul>	<ul style="list-style-type: none"> <li>Capabilities spread across multiple entities</li> </ul>	<ul style="list-style-type: none"> <li>Highly skilled workforce, able to employ technical capabilities across several agencies</li> <li>Strong culture of citizens reporting directly to the police</li> </ul>	<ul style="list-style-type: none"> <li>Highly skilled workforce, able to employ technical capabilities across several agencies</li> </ul>

# 1A: Benchmark countries have different archetypes of points of contacts for different types of victims (2/2)

対外厳秘

Detailed next



1 National Cybersecurity and Communications Integration Center

SOURCE: Expert interview, press search

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。



# 1A: Case example – The US has a decentralized incident response model, with different agencies as lead points of contact for different sectors

	Impacted entity	First PoC
<b>Public Sector</b> 	<ul style="list-style-type: none"> <li>• Department of Defense (DoD)</li> <li>• DoD contractors and sub-contractors</li> </ul> <ul style="list-style-type: none"> <li>• All federal, state, local government agencies</li> </ul>	<ul style="list-style-type: none"> <li>• DoD Cyber Crime Center</li> <li>• DoD – Defense Industrial Base (DIB) Cyber Security (CS) program</li> </ul> <ul style="list-style-type: none"> <li>• Department of Homeland Security (US-CERT)</li> </ul>
<b>Critical infrastructure</b> 	<p><b>There are 16 critical infrastructure sectors including:</b></p> <ul style="list-style-type: none"> <li>• Energy</li> <li>• Financial services</li> <li>• Food and agriculture</li> <li>• Healthcare and public health</li> <li>• Nuclear reactors, materials and waste</li> </ul>	<ul style="list-style-type: none"> <li>• Department of Homeland Security</li> </ul>
<b>Non-critical infrastructure</b> 	<ul style="list-style-type: none"> <li>• Businesses</li> <li>• SMEs</li> <li>• Citizens</li> </ul>	<p><b>Any of the following can be reached out to<sup>1</sup>:</b></p> <ul style="list-style-type: none"> <li>• FBI – Internet Crime Complaint Center</li> <li>• FBI - Field Office Cyber Task Forces</li> <li>• National Cybersecurity and Communications Integration Center (NCCIC)</li> </ul>

<sup>1</sup> NCCIC is the key contact for asset response, while all others are for threat response

SOURCE: Expert interview, press search, team analysis

## Key takeaways

- DHS is the most prominent agency that most sectors have to go to
- To provide convenience, the US has retained multiple channels of PoC for non-critical infrastructure
- Defence sector has a dedicated agency to report to, which is separate from the other sectors



# 1A: Case example – The UK has a E2E centralized incident response model, with the NCSC being the single point of contact for all sectors, including Defense

	Impacted entity	First PoC
<b>Public Sector</b> 	<ul style="list-style-type: none"> <li>Ministry of Defense (MoD)</li> <li>MoD contractors and sub-contractors</li> <li>Central government</li> <li>State and local government</li> <li>Public sector organization</li> </ul>	<ul style="list-style-type: none"> <li>NCSC or MoD CERT</li> <li>NCSC or MoD CERT</li> <li>NCSC</li> </ul>
<b>Critical infrastructure</b> 	<p><b>There are 13 critical infrastructure sectors including:</b></p> <ul style="list-style-type: none"> <li>Energy</li> <li>Finance</li> <li>Food</li> <li>Health</li> <li>Civil nuclear communications</li> </ul>	<p><b>For all critical national infrastructure:</b></p> <ul style="list-style-type: none"> <li>Mandatory reporting to the competent authority</li> <li>Cyber Incidence Response Schemes set up by NCSC</li> <li>CareCERT, National Cyber Security Center (NCSC)</li> </ul>
<b>Non-critical infrastructure</b> 	<ul style="list-style-type: none"> <li>Businesses</li> <li>SMEs</li> <li>Citizens</li> </ul>	<ul style="list-style-type: none"> <li>National Cyber Security Center (NCSC)</li> <li>UK Police</li> </ul>

1 NCCIC is the key contact for asset response, while all others are for threat response

SOURCE: Expert interview, press search, team analysis

# 1A: Key learnings from benchmark countries about incident reporting point of contact

対外厳密



## Key learnings from benchmarked countries

- A** Benchmarked countries often have a **separate point of contact for victims in the defense sector**
- B** A **centralized point of contact for non-defense victims** helps to create **clearer accountability in following up on reported incidents**

# Proposed national incident response and recovery framework

## 1 Victim reporting

**1A**

Single Point  
of Contact



**1B**

Multi-channel  
reporting



**3**

Triage and severity  
assessment



Low



**2**

Active monitoring  
for Cyber incidents



**4**

Agency coordination  
and response



Enablers

**5** Capability  
building



**6**

Effective  
Governance Structure



**7**

Information  
sharing model



# 1B: Typically in benchmark countries, there are 5 types of channels to report an incident

 Detailed next

Channels	Description	Pros	Cons
① Hotline	<ul style="list-style-type: none"> <li>Calling directly to an agency to report an incident</li> </ul>	<ul style="list-style-type: none"> <li>Human assistance to understand context and give immediate advice</li> </ul>	<ul style="list-style-type: none"> <li>Tedious to make event log and integrate into response workflow</li> <li>Inconsistent reporting mechanism</li> </ul>
② Online forms	<ul style="list-style-type: none"> <li>Filling out forms online to provide details and description of incident</li> </ul>	<ul style="list-style-type: none"> <li>Consistent, standardized format</li> <li>Easy reporting</li> <li>Convenient to integrate into IR workflow</li> </ul>	<ul style="list-style-type: none"> <li>Vulnerability in sharing confidential company data online</li> </ul>
③ Email	<ul style="list-style-type: none"> <li>Send an email to a centralized address to notify agency of an incident</li> </ul>	<ul style="list-style-type: none"> <li>Convenient to integrate into IR workflow</li> </ul>	<ul style="list-style-type: none"> <li>Higher risk of fake reporting</li> <li>Inconsistent reporting mechanism</li> </ul>
④ Encrypted email	<ul style="list-style-type: none"> <li>Send an email to centralized address to notify agency of an incident, over PGP or RSA secure protocols</li> </ul>	<ul style="list-style-type: none"> <li>Benefits of email reporting, with increased security</li> </ul>	<ul style="list-style-type: none"> <li>Technically challenging to use</li> </ul>
⑤ TAXII / STIX	<ul style="list-style-type: none"> <li>Notify authorities by sending them script information over cyber incident sharing tools</li> </ul>	<ul style="list-style-type: none"> <li>Allows for swift and precise sharing of incident information</li> </ul>	<ul style="list-style-type: none"> <li>Public agencies need to build capabilities to support these platforms</li> <li>Technically challenging to use</li> </ul>

# 1B: Recently, STIX and TAXI have become emerging platforms for cyber incident communications, and more mature government have started to adopt them

STIX and TAXI are new standards created to standardize cyber incident information sharing...

## Overview:

- Having **standard threat information sharing system** helps companies better **prevent, detect, and share information about** an incoming threat.
  - **STIX** assists users to isolate problematic IP address for easier triage and analysis
  - **TAXII** allows allow high volume, secure and fast sharing of cyber threat intelligence across networks of clients and servers running

## Benefits:

- Improved communication:** STIX and TAXI improves quality of communication between peers in the security industry and between security products interoperating with each other
- Low barrier to entry:** STIX and TAXI provide a set of free, available specifications that help with the automated exchange of cyberthreat information
- Creates common structure:** STIX and TAXI helps an organization better define what information should be included within a structured cyber threat indicator and what shouldn't be

... leading to adoption by multiple governments



DHS



CCIRC



JPCERT



ACSC



NCSC



***“CERT-UK has adopted STIX and TAXII because they are open source and free to implement for anyone”***



***“The DHS office of Cybersecurity and Communications, and US-CERT are leading efforts to automate and structure operational cybersecurity information sharing techniques across the globe”***



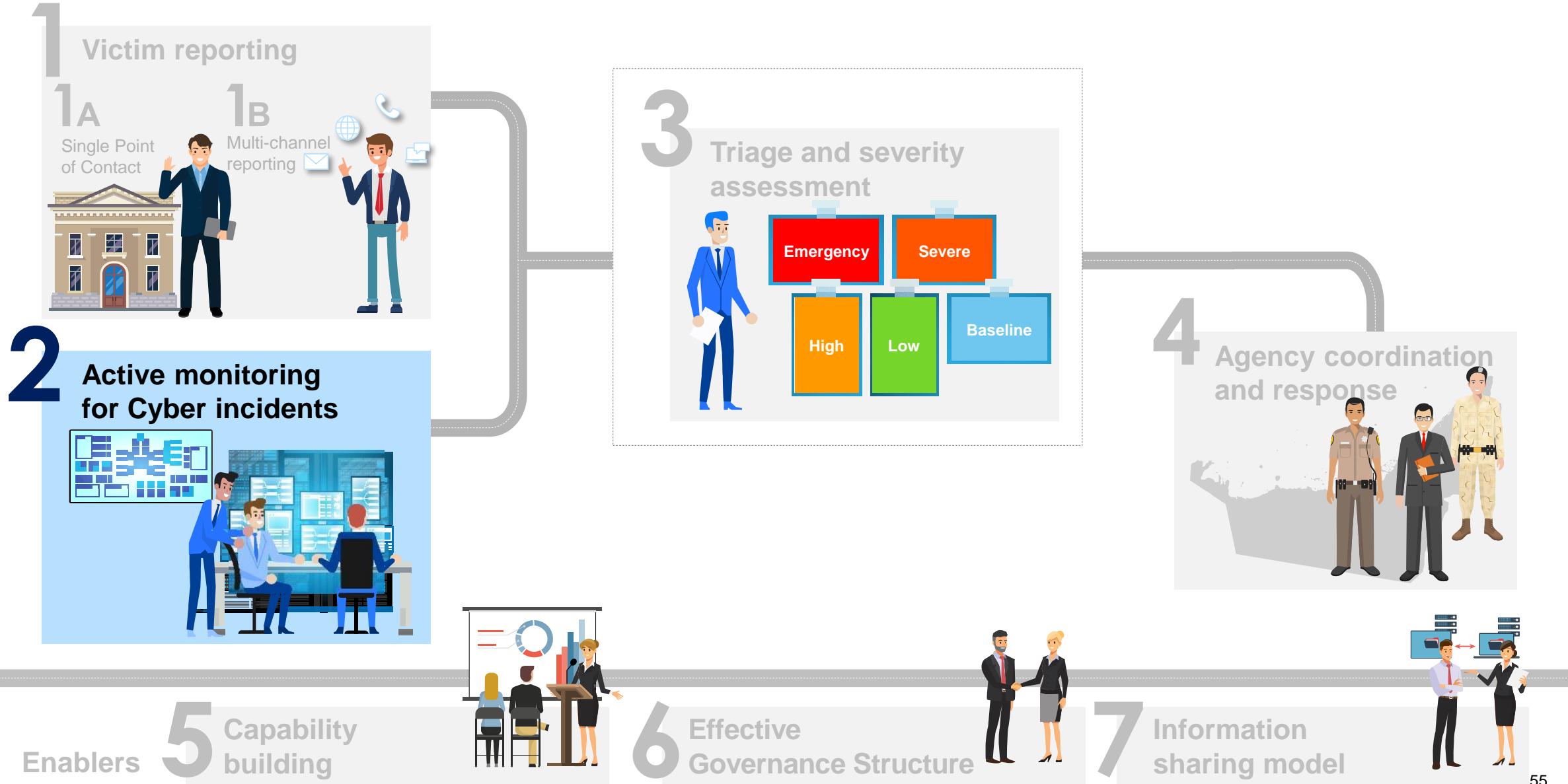
# 1B: Key learnings from benchmark countries about reporting channels



## Key learnings from best in class countries

- A Must leverage multiple channels of reporting (e.g., phone, web and email)**
- B Across all channels and entities, reporting mechanism should be standardized as much as possible**
- C To encourage incident reporting, run national awareness programs about the reporting channels**
- D Many mature countries have started adopting **cyber incident communication standards (STIX, TAXII)**, but these standards remain technically challenging to deploy at scale**
- E To encourage reporting, other than **creating convenience**, government has to position itself as an entity willing to **provide assistance to victims****

# Proposed national incident response and recovery framework



## 2: To enable holistic national-level monitoring, countries typically need both a National CSOC and a National fusion center

NOT EXHAUSTIVE

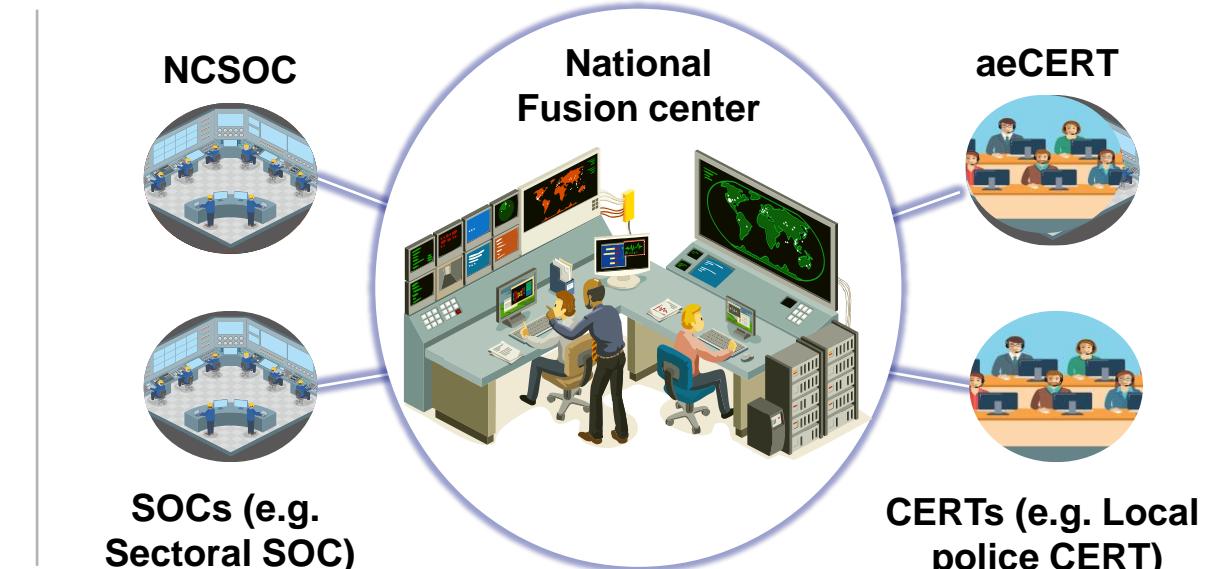
### National Cybersecurity Operations Center (NCSOC)



- Description**
- Monitor network into the country at gateways, to detect malware and botnet-level attack

- Examples**
- National Security Operations Center
  - National Cyber Security Center

### National fusion center



SOURCE: Expert interview

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

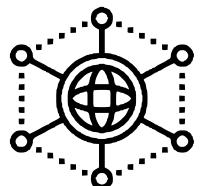
## 2.1: Defense agencies often build a holistic view of network traffic and cyber threats in the country through a National CSOC

Overview of a National Cybersecurity Operations Center (NCSOC)



### Definition

- A national CSOC is a function that **coordinates and leads cyber security monitoring, prevention, detection, and response** for a cybersecurity incident
- It is typically organized as a **Public-Private partnership** with the **Critical Information Infrastructure Operators (CIOOs)**



### Functions

- Maintain **cyber threat intelligence** for the nation
- **Remediate cyber incidents** to minimize business impact
- Regularly **assess and test** critical infrastructure
- Develop **recommendations** to mitigate national-level breaches



### Benefits

- 24/7 operations provides **total situational awareness** for critical national assets
- Continuous monitoring and analysis ensures **timely detection and response** to security incidents

## 2.1: Case example: UK and US employ National CSOC to constantly monitor for risks in their networks

### Case Example – UK NCSC (CSOC)



#### Background

The Cybersecurity SOC (CSOC) was founded under the GCHQ, but has since been transferred to be under the NCSC



#### Functions

The NCSC has the following key functions:

- Provides 24/7 monitoring of the security vulnerabilities in the UK network



#### Notable program

The Active Cyber Defense Programme (ACD) forms partnerships with UK national companies to automatically eradicate threats to citizens. Achievements include:

- Partner with UK ISPs** to block suspicious IP addresses and **scale protection by default**
- Partner with British Telecommunications (BT)** to build a **BGP monitoring platform** to run analytics on routing path data

### Case example – US National Security Operations Center (NSOC)



#### Background

The NSOC is the national SOC of the United States and is housed under the NSA and the US SIGINT System (USSS)



#### Functions

The NSOC has the following key functions:

- Provides 24/7 monitoring of the security vulnerabilities entering the US network
- Combines network patterns with existing military intelligence to assess threat to US



## 2.2: Countries create a near real-time view of cyber threat through National fusion centers

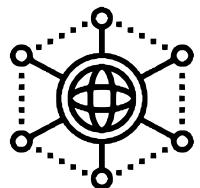
対外厳密

Overview of National fusion center



### Definition

- A cyber threat information sharing system is an agency that **collates, processes, and disseminates** threat information gathered from multiple sources
- Since civilian agencies are usually not authorized to directly monitor networks, this **rapid sharing of operational information** provides civilian agencies a near real-time view of threats as they occur



### Functions

- Create **threat situational awareness** through **information sharing**
- Maintain **network of key SOCs** to share **privileged and operational information**
- **Correlate and triangulate cybersecurity incidents**



### Benefits

- **Consolidate cyber threat intelligence** that is shared from different entities
- Activate network of companies and providers to **disseminate threat information to reduce impact of an attack**

## 2.2: Case example 1: The Fusion Cell in the UK creates a cyber attack monitoring operations room to monitor cyber attacks in real time



### Background

- Announced as part of the UK's Cyber Information Sharing Program, the Fusion Cell empowers cross-sector threat information sharing in the UK



### Functions

- The Fusion Cell is a **monitoring operations room that visualizes the locations of all cyber-attacks against UK-based targets.**



### Notable Features

- The Fusion Cell** will allow public and private sector analysts to work alongside each other to exchange information and techniques and monitor cyber attacks in real time
- The types of information shared included information about attack signatures, attack and reconnaissance methods and successful mitigation strategies.



## 2.2: Case example 2: The Financial Services-ISAC (FS-ISAC) in the US creates a industry forum for cyber and physical threat intelligence analysis and sharing



### Background

- The FS-ISAC was created in the US to **facilitate threat information sharing for critical information infrastructure**
- In 2013, the FS-ISAC's board extended its charter to **share cyber threat information with financial service firms world-wide**



### Functions

- The FS-ISAC provides **anonymous information sharing capability** across the entire financial services industry.
- Upon receiving a threat submission, FS-ISAC experts verify and analyze the threat, and will identify potential solutions to be sent to FS-ISAC members.
- Information sources from FS-ISAC include information from financial services providers, commercial security firms, federal/national, state and local government agencies, law enforcement and other trusted resources



### Notable Features

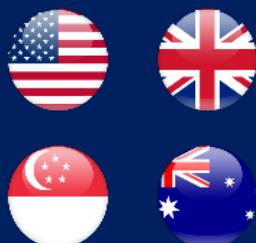
- There are **different subscription tiers** across levels of asset under management (AuM) by the banks. Depending on membership tiers, members can choose to receive a package of services that include **24 x 7 Watch Desk, STIX/TAXII Feeds, and XML Data Feeds**
- Smaller financial institutions are able to sign up for a free FS-ISAC that includes the most **urgent crisis alerts** in the financial services industry



## 2: Key learnings from analysis of benchmark countries that have the ability to actively monitor and detect threats



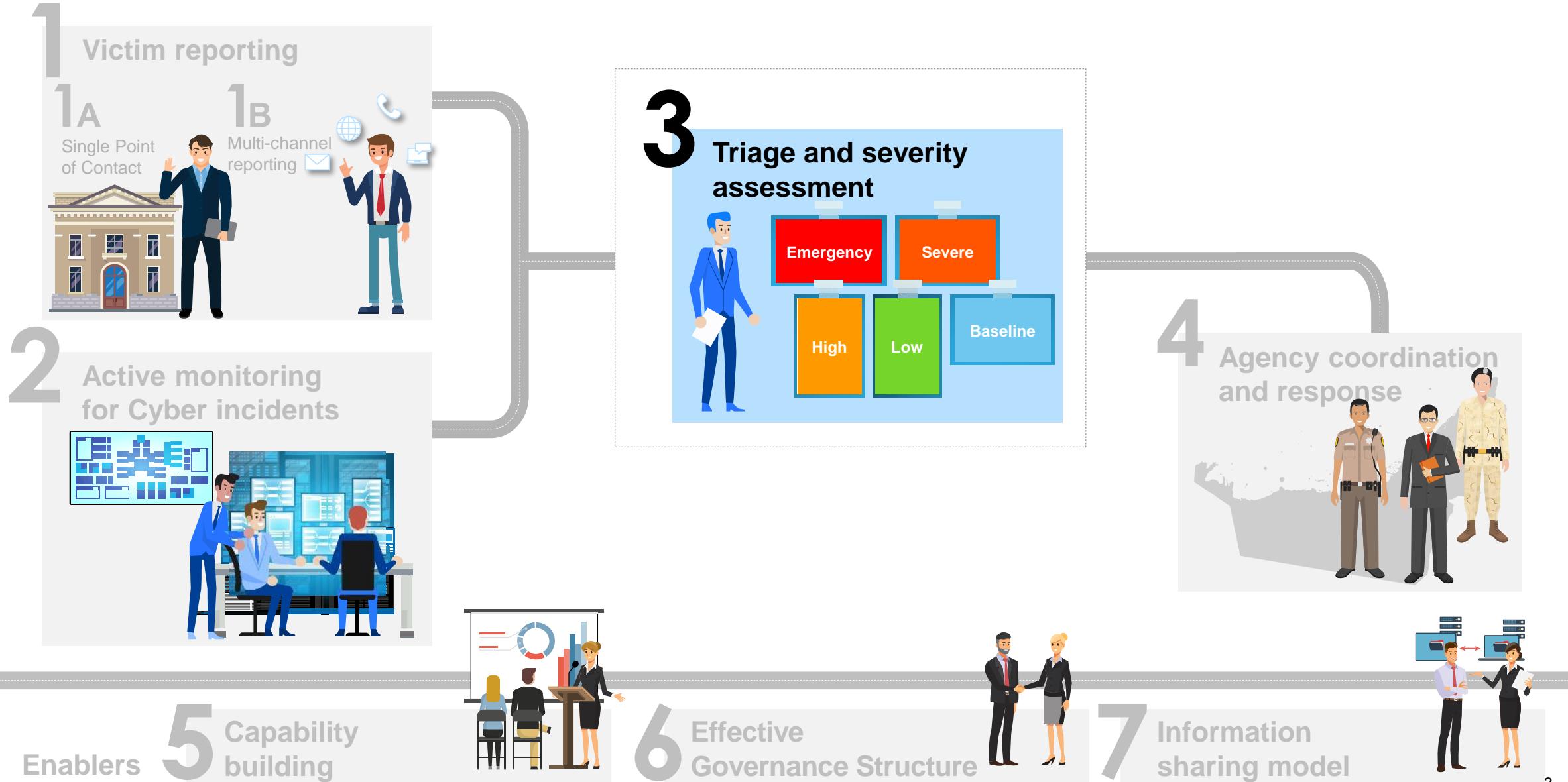
We analyzed 4 benchmark countries for their ability to actively monitor and detect threats



### Key learnings from best in class countries

- A To supplement passive threat intelligence, best in class countries actively monitor and detect threats through national threat monitoring facilities (national SOCs and/or information fusion and analysis centers)**
- B To develop strong situational awareness, the government should create partnerships between national monitoring facilities and critical sector operators (e.g. Telcos, banks, etc.)**
- C The appropriate institution chosen for national threat monitoring varies based on jurisdictional boundaries and respective agency mandates**

# Proposed national incident response and recovery framework



### 3: Benchmark countries typically have a systematic severity classification matrix mapped to multiple economic and social impact indicators

DETAILED NEXT

Dimensions	Description				
1 Loss of life (or public safety)	<ul style="list-style-type: none"> <li>Extent to which people are injured or potentially killed by the cyber incident</li> </ul>	✓	✓	✓	✓
2 National security	<ul style="list-style-type: none"> <li>Type of attacker (e.g. nation state) to determine if an attack has a direct impact on national security</li> </ul>	✓	✓	✓	
3 Public confidence	<ul style="list-style-type: none"> <li>Extent to which the public or businesses will lose confidence in the government or affect international reputation as a result of the incident</li> </ul>	✓	✓	✓	
4 Type of victim	<ul style="list-style-type: none"> <li>Assesses the total potential impact based on the type of victim in terms of its size, criticality and number</li> </ul>	✓	✓	✓	
5 Interdependency	<ul style="list-style-type: none"> <li>Extent of interdependency between the impacted entity and other critical sectors in the country</li> </ul>	✓			✓
6 Recoverability	<ul style="list-style-type: none"> <li>Complexity and time involved for the affected entity to recover from the cyber incident</li> </ul>				✓
7 Economic impact	<ul style="list-style-type: none"> <li>Estimated economic impact directly or indirectly caused by the cyber incident</li> </ul>	✓	✓	✓	✓

SOURCE: Press search, Expert interviews

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

### 3: Case example: The US defines incident severity, and maps incident levels to different parts of the attack lifecycle

対外厳秘

Severity levels

Indicators



Severity levels	General definition
<b>Level 5: Emergency (Black)</b>	<i>Poses an imminent threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons</i>
<b>Level 4: Severe (Red)</b>	<i>Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties</i>
<b>Level 3: High (Orange)</b>	<i>Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence</i>
<b>Level 2: Medium (Yellow)</b>	<i>May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence</i>
<b>Level 1: Low (Green)</b>	<i>Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence</i>
<b>Level 0: Baseline (White)</b>	Unsubstantiated or inconsequential event

The NCICC uses a weighted arithmetic mean across several dimensions to arrive at an incident score

- **Actor Characterization:** initial understanding of the skill levels and intentions of the particular actor set
- **Information (Economic) Impact:** describe the type of information lost, compromised, or corrupted.
- **Recoverability:** the scope of resources needed to recover from the incident
- **Cross-Sector Dependency:** weighting factor that is determined based on cross-sector analyses conducted by the DHS Office of Critical Infrastructure Analysis (OCIA).
- **Potential national Impact:** overall estimated national impact resulting from a total loss of service from the affected entity.

### 3: Case example: The UK has a transparent and clear matrix for incident definition and coordination

対外厳秘

Severity levels

Indicators



#### Severity levels

##### Category 1: National cyber emergency

#### Category definition

- A cyber attack which causes sustained disruption of UK essential services or affects UK national security, leading to severe economic or social consequences or to loss of life

##### Category 2: Highly significant incident

- A cyber attack which has a serious impact on central government, UK essential services, a large proportion of the UK population, or the UK economy

##### Category 3: Significant incident

- A cyber attack which has a serious impact on a large organisation or on wider/local government, or which poses a considerable risk to central government or UK essential services

##### Category 4: Substantial incident

- A cyber attack which has a serious impact on a medium-sized organisation, or which poses a considerable risk to a large organisation or wider/local government

##### Category 5: Moderate incident

- A cyber attack on a small organisation, or which poses a considerable risk to a medium-sized organisation, or preliminary indications of cyber activity against a large organisation or the government

##### Category 6: Localized incident

- A cyber attack on an individual, or preliminary indications of cyber activity against a small or medium-sized organisation

### 3: Key learnings from benchmark countries on severity assessment matrix



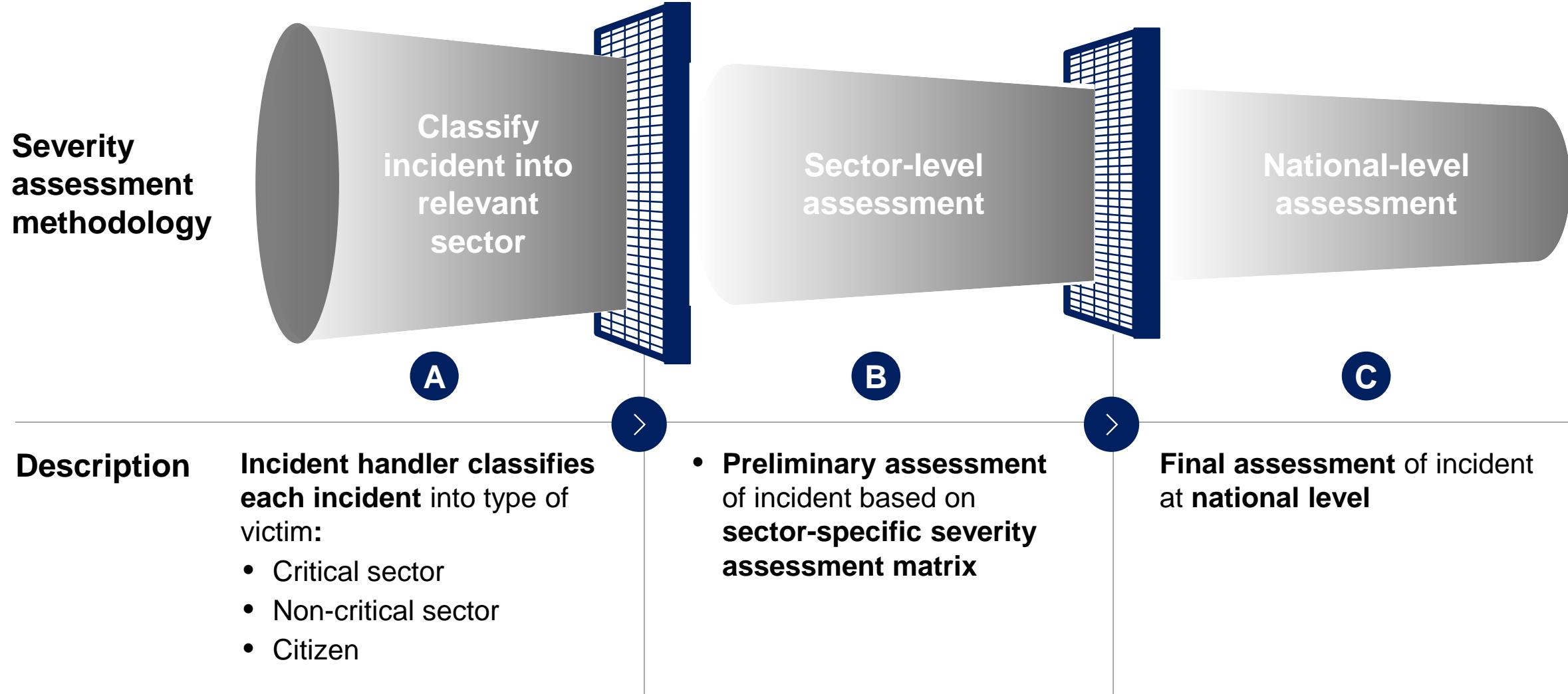
We benchmarked severity assessment systems across 4 benchmark countries



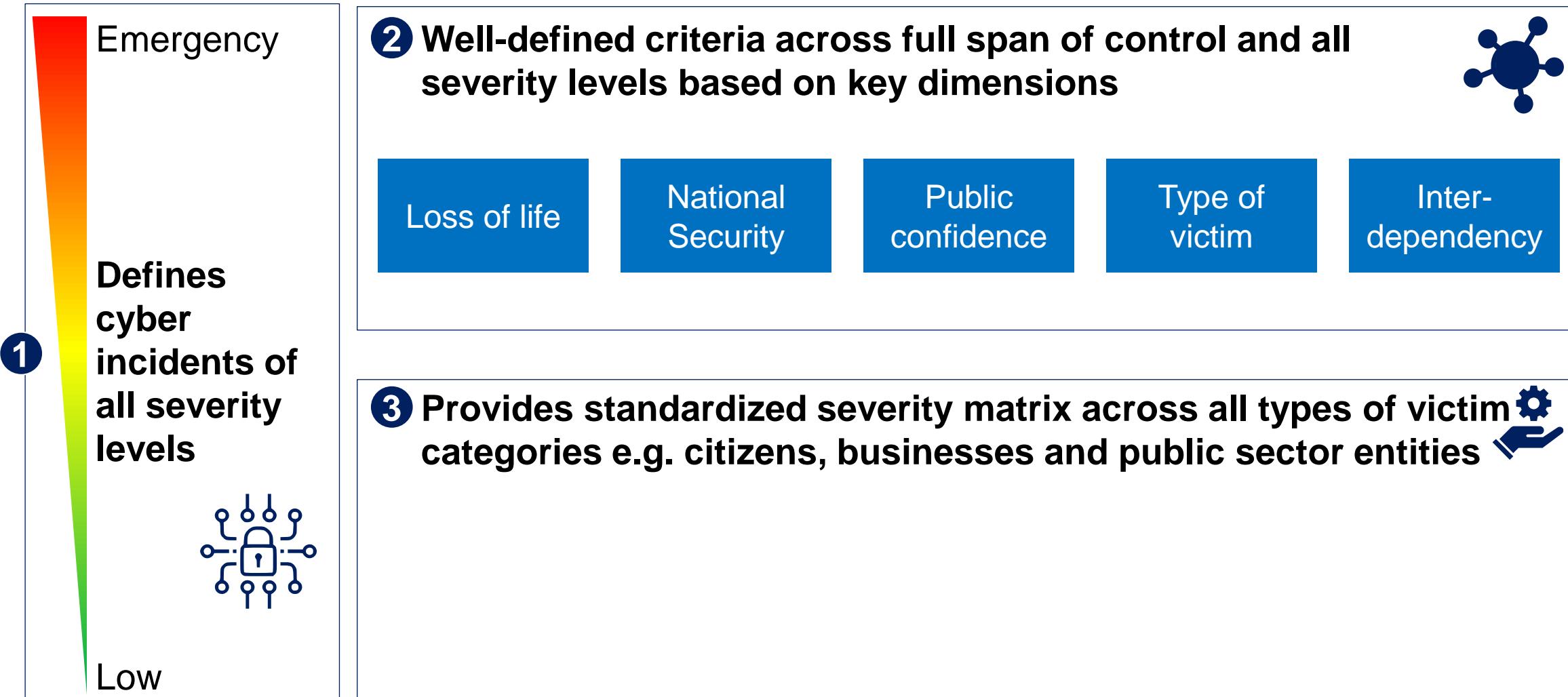
#### Key learnings from best in class countries

- A Severity assessment matrix should provide coverage across all levels of attacks** e.g. attack against a citizen to a large scale national attack
- B Severity assessment matrix must be standardized with common definition and understanding** across all entities in the country
- C Severity assessment matrix should consist of indicators that are critical and relevant for the country** e.g. Public Health or Life, National security, Economic Security, Public confidence, Size & Type of Victim, Population impacted, Recoverability
- D For each of the chosen indicators, the scales should be clearly defined across all levels of the severity matrix**

### 3: We recommend that incident handlers leverage a standardized severity assessment methodology to determine the severity of an incident



### 3: The severity assessment matrix in benchmark countries is typically built on 3 key elements



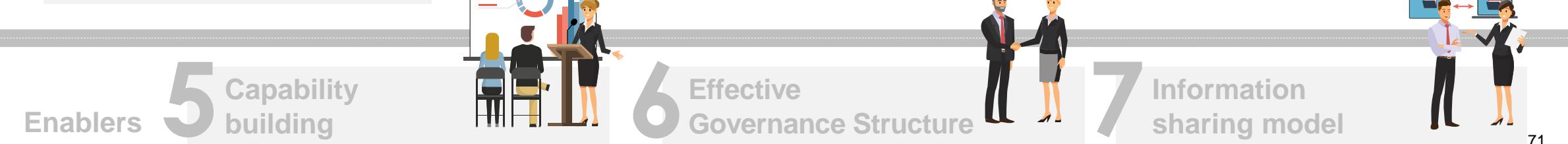
### 3: ILLUSTRATIVE Severity Assessment Matrix



SOURCE: Expert interview, Team analysis

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# Proposed national incident response and recovery framework



# 4: Typically, best in class countries coordinate 7 types of entities to create a comprehensive incident response and recovery

Type of entity	Definition/Description
1 Defense and intelligence agencies	<ul style="list-style-type: none"> <li>Agencies that engage in <b>research, development, and deployment of high-leverage technology</b> for <b>intelligence purposes</b></li> </ul>
2 CERT	<ul style="list-style-type: none"> <li>A national CERT (also known as CIRT/CSIRT) provides the <b>capabilities to identify, defend, respond and manage cyber threats</b> and <b>enhance cyberspace security</b> in the nation state.</li> </ul>
3 Police or Law enforcement	<ul style="list-style-type: none"> <li>A law enforcement agency is a <b>government agency</b> that is responsible for the <b>enforcement of the laws</b></li> </ul>
4 Lead agencies and ministries	<ul style="list-style-type: none"> <li><b>Ministries</b> that are responsible for <b>particular sectors</b> and <b>domains</b> (e.g. Energy, ICT, Water)</li> </ul>
5 SOC	<ul style="list-style-type: none"> <li>A Security Operations Center (SOC) is a facility where <b>enterprise or national information systems</b> are <b>monitored, assessed and defended</b> from cybersecurity threats</li> </ul>
6 NOC	<ul style="list-style-type: none"> <li>A Network Operations Center (NOCs) is a facility where <b>enterprise or national networks</b> are <b>monitored to ensure service availability</b> (e.g. stress-test telecom infrastructure, detect IT infrastructure incidents)</li> </ul>
7 Threat response companies	<ul style="list-style-type: none"> <li>Companies that <b>consolidate, analyze, manage, action, and disseminate intelligence</b> and reports</li> </ul>

# 4: Within benchmarked countries, best-in class countries specify clear procedures for agency coordination based on severity assessment

Country	Coordination systems in place	Pros and cons	Detailed next
<b>Leaders</b>	UK 	Relevant agencies (e.g., lead ministries, cabinet and law enforcement) identified since severity assessment	 Clear identification of lead agencies in response (NCSC)
	US 	Clearly defined agency that will be notified and included in incident response (NCCIC)	 Clear identification of lead agencies in response (DoJ for threat response; DHS for asset response)
	Estonia 	Well-established triage and coordination manual for all events	 Clear identification of lead agencies in response (RIA from “peacetime to war”)
	Canada 	Clearly defined agency that will be notified and included in incident response (CCIRC)	 CCIRC coordinates relevant entities involved in a response
<b>Baseline</b>	Singapore 	Manual for national emergency situations exist, but not for less severe incidents	  Agency coordination done in an adhoc manner through CSA and MinDef
	Germany 	Coordination specification done in broad strokes, without specificity or integration to workflow	  Agency coordination done in an ad-hoc manner through BSI
<b>Laggards</b>	France 	No coordination model, to be improved with set up of Cyber office	 Vague statements about cyber incident response agencies, no clear escalation

SOURCE: Expert interviews

# 4: Case example: UK automatically triggers coordination based on severity assessment matrix

対外厳密



## UK agency coordination

NCSC is the central coordinating body for a cyber incident, and will remain as the central coordinator of incident response

NCSC stays strictly within the cyber domain, and leaves the other domains to other agencies

### In event of cyber attack, Agencies involved

<b>Category 1 National cyber emergency</b>	NCSC coordinating immediate and rapid cross-government response Immediate, with strategic leadership from Ministers / Cabinet Office (COBR), and Law Enforcement
<b>Category 2 Highly significant incident</b>	NCSC coordinating cross-government response with National Crime Agency and Cabinet Office
<b>Category 3 Significant incident</b>	NCSC with National Crime Agency or Regional Organized Crime Units
<b>Category 4 Substantial incident</b>	NCSC with National Crime Agency or Regional Organized Crime Units
<b>Category 5 Moderate incident</b>	Local police force and National Crime Agency or Regional Organized Crime Units
<b>Category 6 Localized incident</b>	Local police force and National Crime Agency or Regional Organized Crime Units

### Key responsibilities

- The NCSC coordinates events that are more severe than Category 4.
- Depending on the severity, the NCSC will decide which level of the government to engage with, and coordinate directly with lead government departments for response
- NCSC's mandate is restricted to the cyber domain, and will leverage lead authorities as appropriate whenever the cyber attack creates physical (non-cyber) impact
- NCSC will lead on mitigating the attack, and will work with lead government departments to deal with the consequences of the attack

### Key learnings

- The NCSC coordinates all cyber attacks **above level 4**, and communicates with local police on proper handover and escalation mechanisms
- Establishment of the NCSC created **clearer responsibility in cyber-related incidents** and helped the UK **craft better response to the public**
- There is **ongoing debate** on whether the NCSC should **expand its mandate** to be involved in incidents related to businesses that are in **category 5 and 6**. Doing so would **create better visibility** across all incidents, but it might **over-stretch** the organization and **hurt its effectiveness in dealing with major incidents**

# 4: Case example: US creates Cyber Unified Coordination Groups to coordinate incident response based on incidents

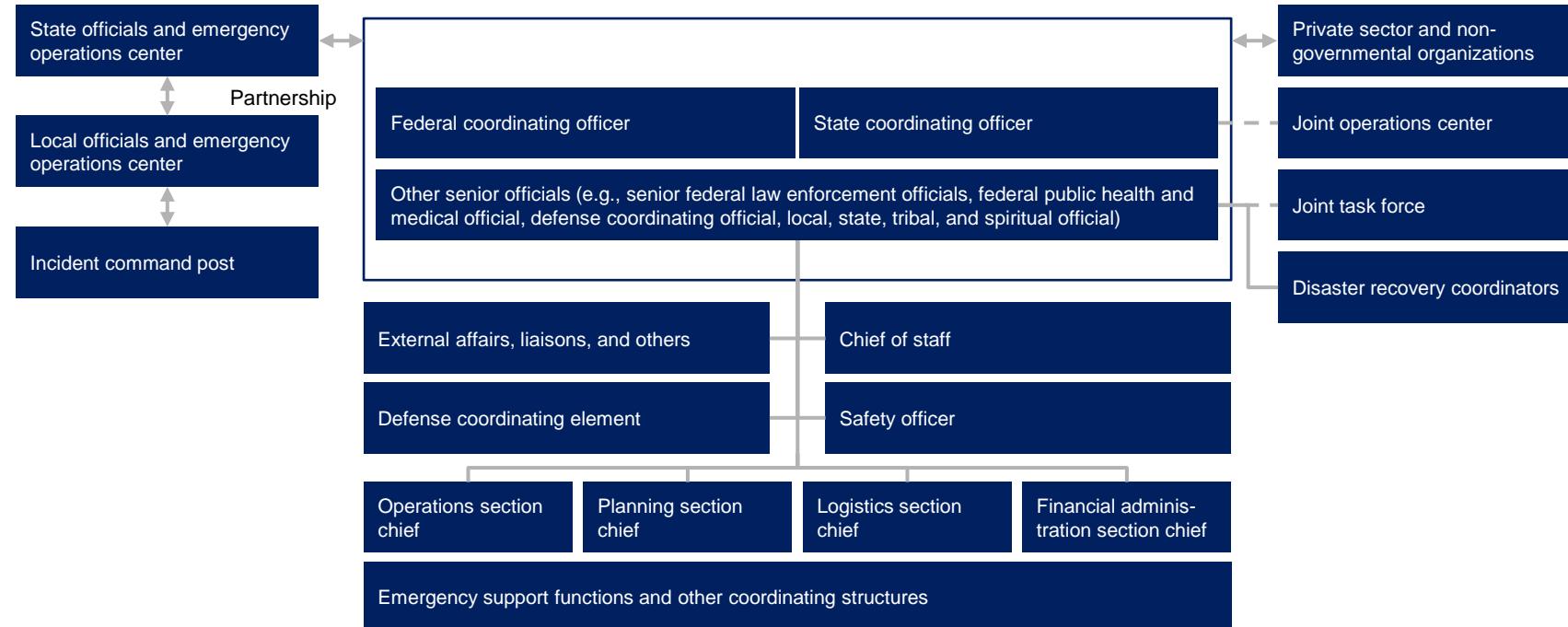
対外厳密



## US agency coordination

- The Department of Justice is lead agency for threat response, while the Department of Homeland Security is lead agency for asset response
- If the event is significant, the National Security Council forms a Cyber Unified Coordination Group (CUG), which coordinates and integrates federal agencies and private sector companies to respond to the incident

## In event of cyber attack, Agencies involved



## Key responsibilities

- The DHS handles incidents below level 3 (highest is level 5)
- If severity of incident is equal to or exceeds level 4, the National Security council will form a CUG to coordinate response across all government agencies.
- In this instance, the CUG (and not the individual agencies) will be responsible for working directly with private sector entities and state officials to share operational intelligence to deal with the threat

## Key learnings

- The UCG is used as a **form of escalation** from DHS, and allows the government to **share sensitive intelligence** for a **coherent response**
- Detailed roles and responsibilities** are specified for each stakeholder that gets mobilized, empowered largely by the structural arrangement coordinated by the UCG

SOURCE: Expert Interviews

# 4: Key learnings from benchmark countries on escalation matrix to mobilize agencies for robust incident response and recovery

対外厳密



We benchmarked  
agency  
mobilization  
across 7 countries



## Key learnings from best in class countries

- A Standardized and commonly understood escalation matrix and agency coordination plan across all key stakeholders**
- B Escalation matrix and agency coordination plan should be clearly mapped to cyber incident severity matrix**
- C Assigning clear accountability for each incident is critical to effective coordination between agencies**
- D Robust information sharing mechanism in place to ensure proper handover between stakeholders**

# 4: ILLUSTRATIVE: Agency mobilization plan linked to the severity assessment matrix

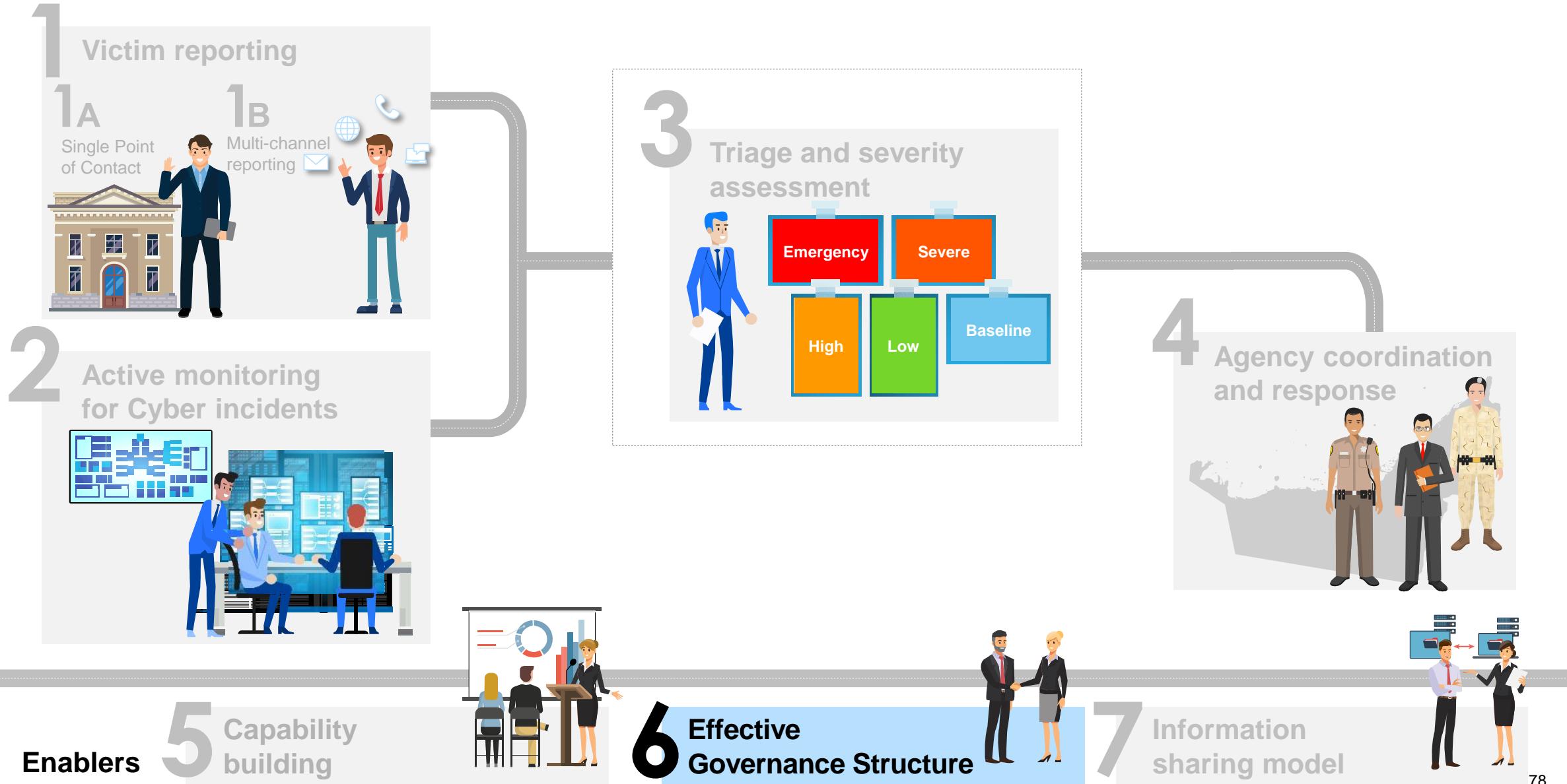
対外厳密



SOURCE: Team analysis

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# Proposed national incident response and recovery framework



# "Cybersecurity Human Resource Development Policy" Overview - Promotion of Industry, Academia, and Government Collaboration for Business Continuity and Value Creation - (NISC Materials)

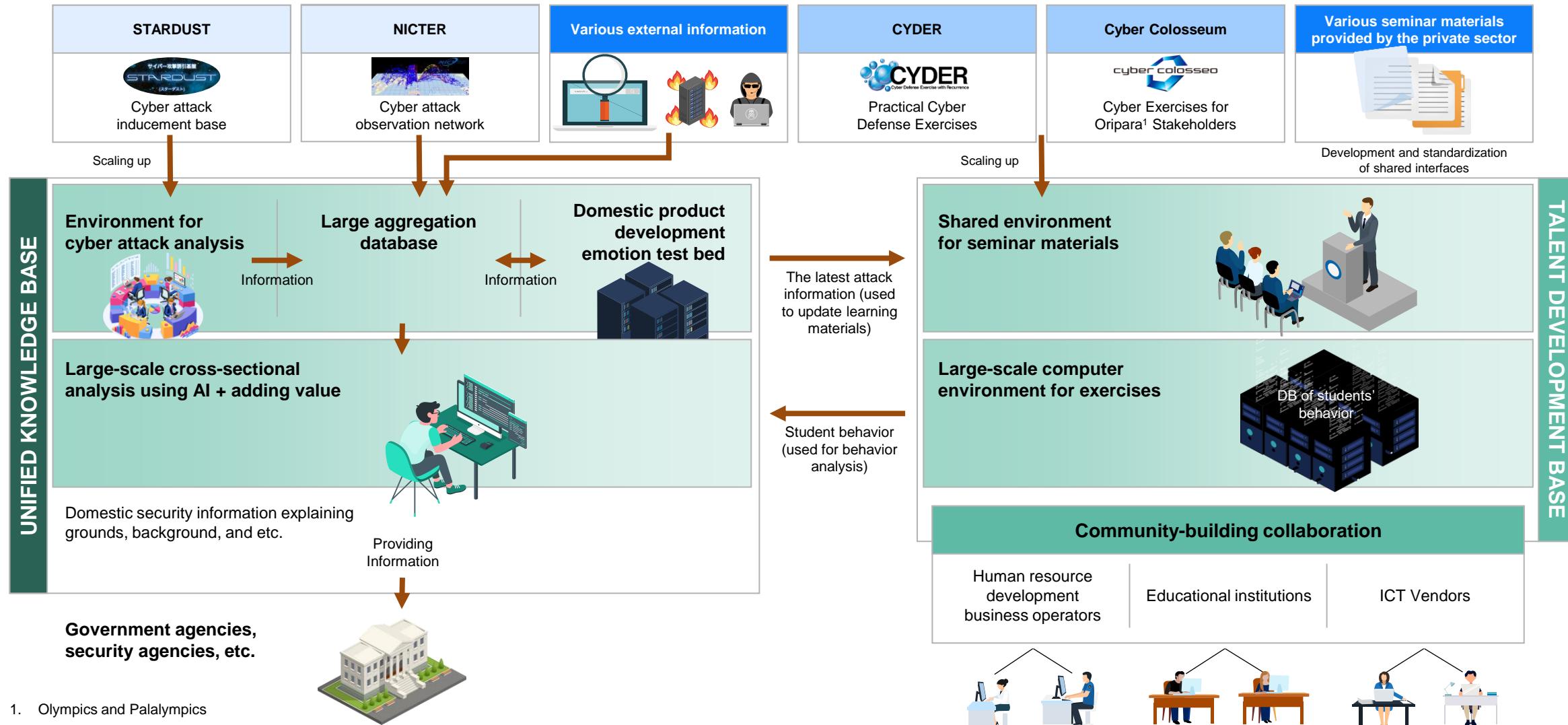
対外厳密



	Executive	Strategic Management	Practitioners and Engineers
Role	<ul style="list-style-type: none"> <li>Implementing important security measures for business continuity and value creation as part of risk management</li> </ul>	<ul style="list-style-type: none"> <li>Planning of measures based on management's policies, and direction of practitioners and engineers</li> <li>Central role in supporting risk management</li> </ul>	<ul style="list-style-type: none"> <li>Planning, construction, and implementation of security measures based on management's policies</li> <li>Human resources which can support management and strategic management and deal with them as part of a team</li> </ul>
Current issues and Direction of initiatives	<ul style="list-style-type: none"> <li><b>Promoting understanding of management and reform of awareness</b> <ul style="list-style-type: none"> <li>Disseminating "The Keidanren Cybersecurity Management Declaration" and holding seminars for executives</li> </ul> </li> <li><b>Developing infrastructure based on differences by industry and type of business</b> <ul style="list-style-type: none"> <li>Developing tools to indicate the level of measures by industry and type of business</li> <li>Considering the arrangement of the corporate Legal System</li> </ul> </li> <li><b>Incentivizing investment</b> <ul style="list-style-type: none"> <li>Promoting information disclosure (formulation of guidelines, etc.)</li> <li>Tax incentives</li> <li>Utilizing cybersecurity Insurance</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li><b>Establishing a strategic management layer in an organization</b> <ul style="list-style-type: none"> <li>Disseminating the significance of the strategic management to the executive</li> <li>Specifying and Clarifying strategic management functions</li> </ul> </li> <li><b>Promoting curriculum development and recurrent education (re-learning)</b> <ul style="list-style-type: none"> <li>starting trial initiatives, etc.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li><b>Developing human resource supporting executive and strategic management</b> <ul style="list-style-type: none"> <li>Implementing curriculum through collaboration among industry, academia, and government</li> <li>Developing human resource related to the use of advanced technologies, etc.</li> <li>Developing knowledge and skills related to the use of cloud and advanced technologies, etc.</li> </ul> </li> </ul>
Enhancing education for young people	<p>&lt;Objective&gt; Help understand the basic mechanisms of ICT and develop logical thinking skills. Information moral education is also important</p> <p>&lt;Initiative&gt; Create opportunities for local governments and companies to freely learn using equipment and tools in addition to launching in-course initiatives at the primary and secondary education</p>		
SMEs' initiatives	<p>&lt;Objective&gt; Knowledge and skills are not sufficient, and it is difficult to invest in security measures. The impact on society will be large</p> <p>&lt;Initiative&gt; Disseminating countermeasures with the usage of cloud system and consideration of incentive mechanisms (tax incentives, etc.)</p>		

# Accelerating collaboration among industry, academia, and government to improve cybersecurity information collection and analysis capabilities (Ministry of Internal Affairs and Communications)

In addition to collecting, accumulating (generating) and providing cybersecurity information, Japan builds a common foundation for fostering cyber security human resources throughout society, open it to industry and academy, and use it as a nod to it to improve cybersecurity capabilities.

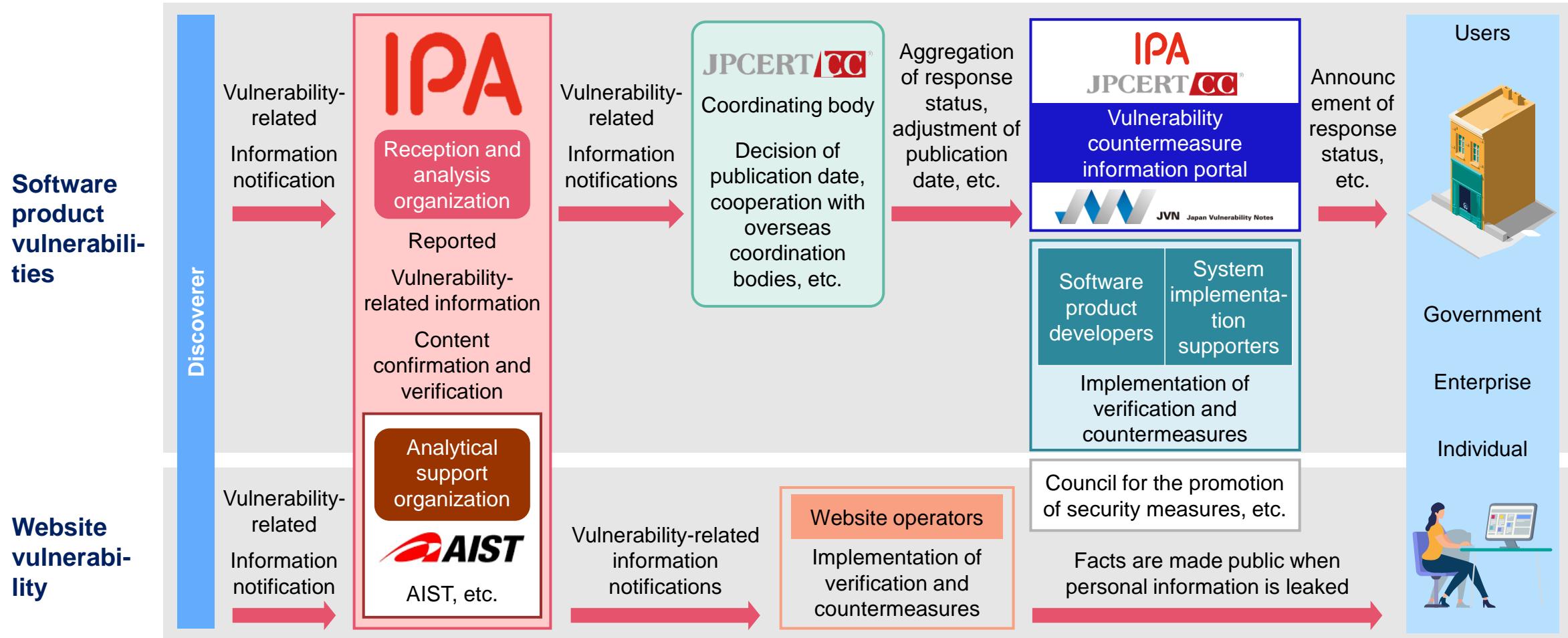


# Notification system for vulnerability-related information, etc. (Ministry of Economy, Trade and Industry materials)

対外厳密



## Information Security Early Warning Partnership

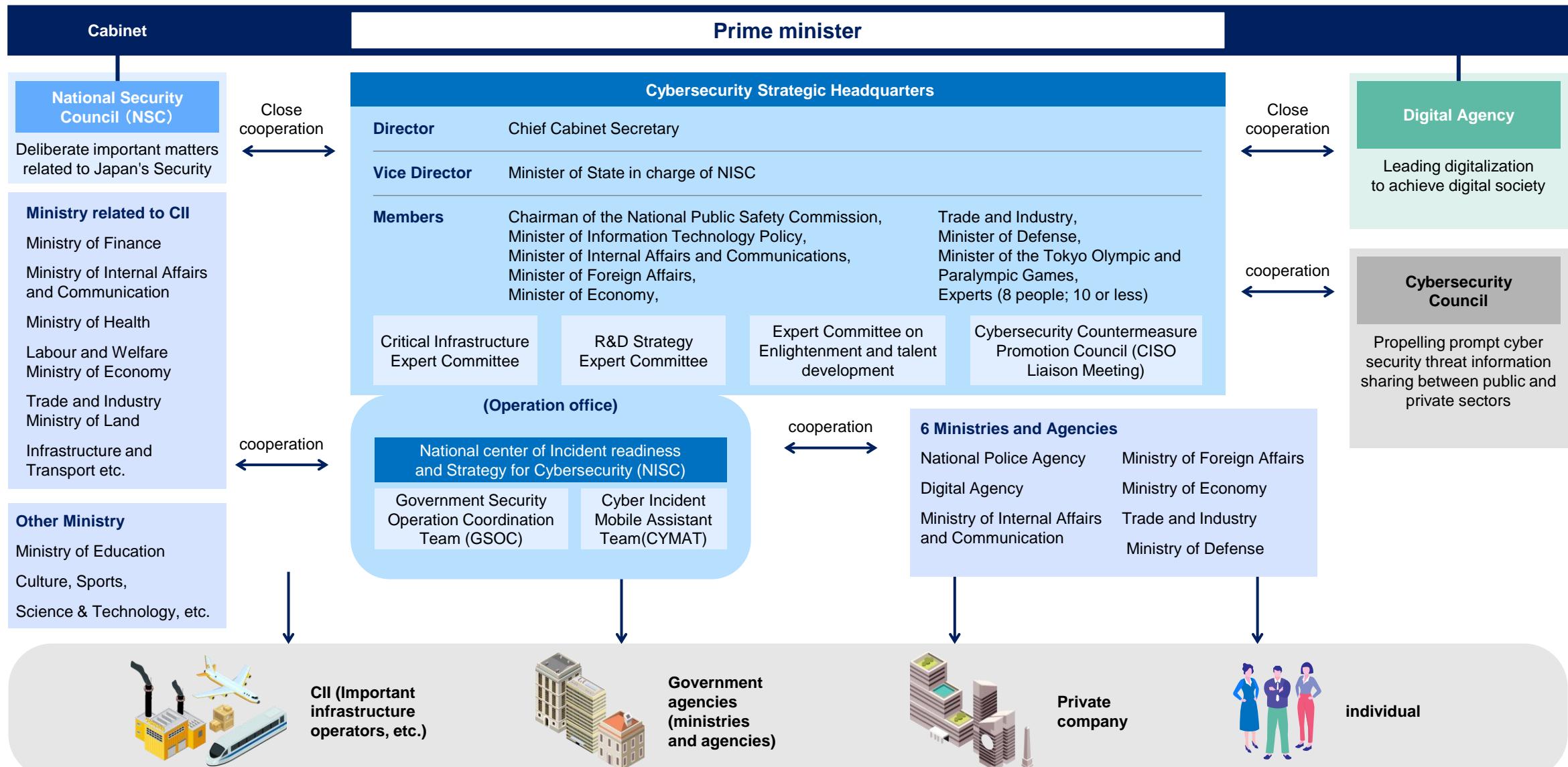


Source: <https://www.ipa.go.jp/files/000073901.pdf>

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。



# Promotion system



# Security personnel development (National Cyber Training Center, Ministry of Internal Affairs and Communications)

対外厳密



## Practical cyber defense exercises for national and local governments, Independent Administrative Institution, and critical infrastructure institutions

⇒ The exercises are held 100 times a year and accommodate a total of 3,000 participants in a year (one-day course and held in all prefectures). A total of 3,090 people attended the course in FY 2019 (a total of 3,009 students attended in FY 2017, and a total of 2,666 students in FY 2018) \*Online courses will be newly established from 2021

## Development of exercise programs and educational content that can respond to new types of cyberattacks



Human resource development that can deal  
with actual cases



Human resource development that can handle  
advanced attacks



## Fostering young security innovators under the age of 25

⇒ Select about 50 students per year and conduct a one-year training course. 45 participants completed the course in FY 2019 (39 in FY 2017 and 46 in FY 2018)



Human resource development at a high level

# Initiatives for the 2020 Tokyo Olympics and Paralympics (National Police Agency)

対外厳密

Ensuring the safe and secure operation of the Games



↔ Cooperation

## Important infrastructure institutions, etc.

Sharing information about cyberattacks



Conducting joint response drills, assuming incidents, etc.

Council for cyber terrorism countermeasures

## Government agencies, etc.

**Police**  
Collecting and analyzing information that contributes to the prevention of cyberattacks  
Investigating cyberattack-related matters, etc.

July 2017, security information center was established.

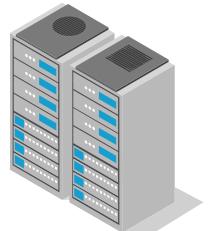
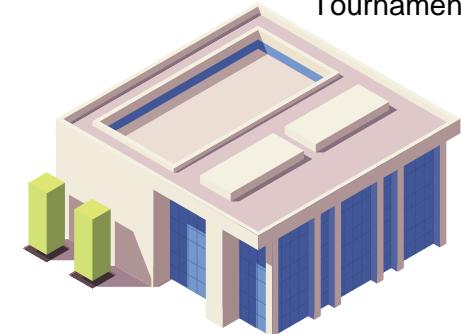
## Overseas organizations

Information exchange  
International Investigation Cooperation

## Tokyo 2020 organizing Committee

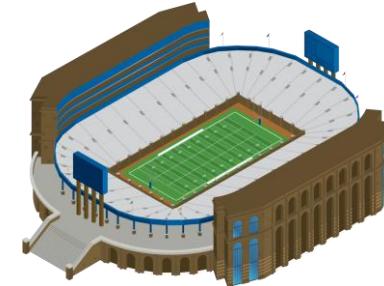
Tournament Management System

Tournament website, media center, etc.



## Security-related businesses, etc.

Sharing information such as unknown malware, unknown vulnerabilities, and unauthorized network connections

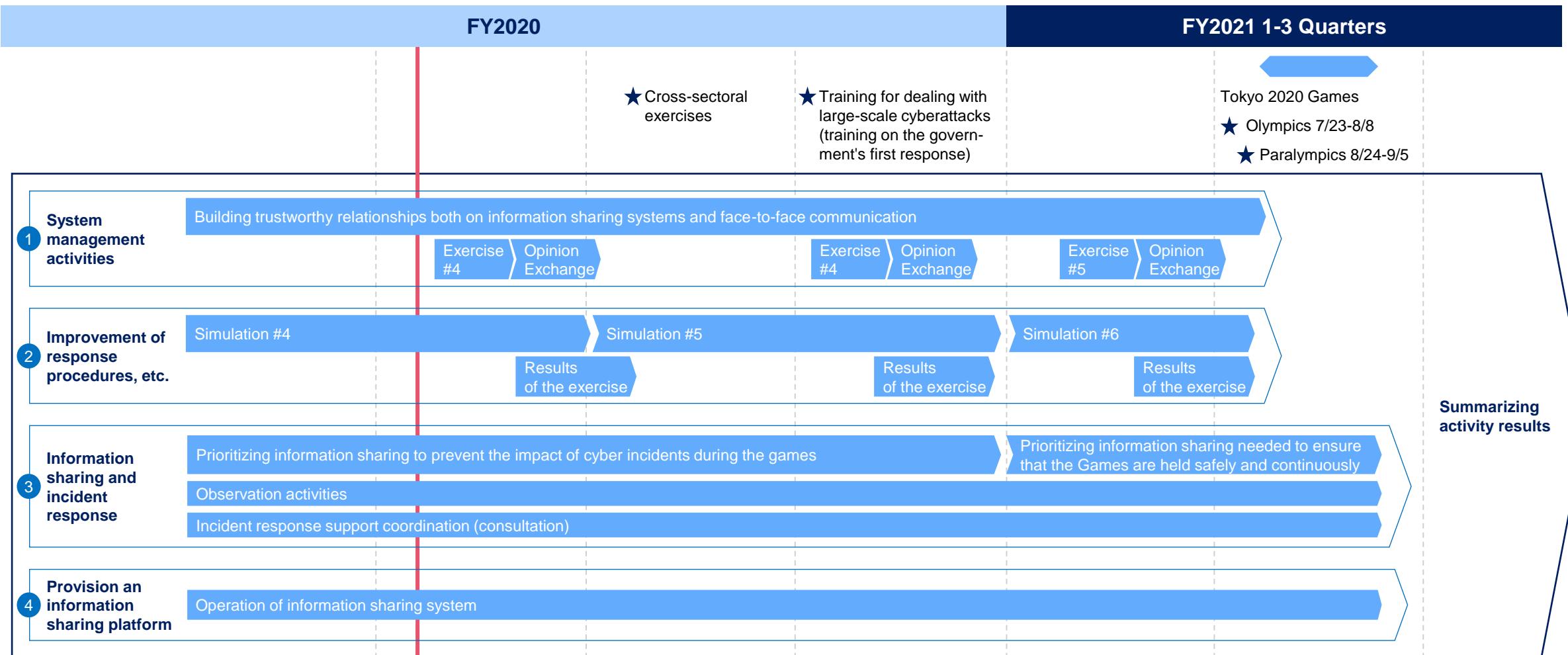


## People involved in the management of Tokyo 2020

Facility managers of the system related to the games, venue facility managers, accommodation hotels for spectators, etc.

# Plans for development of response systems (operation of cybersecurity coordination center, etc.) (NISC materials)

For the Tokyo 2020 Games in FY2021, continuing and improving our system management activities, response procedures, information sharing and incident response, and provision of information sharing platform, and ensuring that the system is fully prepared to deal with the Games



# 3 types of organization typically required to deliver Cybersecurity

	1 National Coordinating body	2 National/Government CERT	3 ISAC
<b>Mission</b>	Often in charge of overall national cybersecurity coordination, focal point in <b>coordinating legitimization, intra-government collaboration and promoting partnerships between industry, academia, and public and private sectors</b>	The main goal is <b>to protect national and economic security, the ongoing operations of a government, and the ability of critical infrastructures to continue to function</b>	The main mission is to <b>enhance the ability of the sector to prepare for and respond to cyber threats, vulnerabilities and incidents</b> , by providing a centralized organization to monitor, disseminate information, and help mitigate cyber security risks and provide protection
<b>Scope of work</b>	<b>National coordination; national defense and response.</b> Typically, acts to coordinate various aspects of national cybersecurity, cybercrime and cyberattack mitigation efforts, through cooperation with civilian agencies, national CERT, infrastructure operators, state and local governments, and international partners. It's also responsible for facilitation and execution <b>national Cybersecurity strategy and policy</b>	The mandatory/core activity includes <b>incident handling, analysis and reporting</b> (subsumed under Incident Management). Additionally, it is advisable that CERTs provide <b>security related information on alerts and warnings and announcements</b> in immediate cases of upcoming threats or other emergencies, and <b>good user practice to building awareness</b> for adding measurable value for the constituency.	There are four major capabilities of an ISAC: <b>Vulnerability and Incident Information Sharing, Threat Analysis, Relationships and Possible Cross-Sector Partnerships, Cyber Security Training.</b> As their primary function, all ISACs have a process in place for <b>gathering and disseminating information to mitigate risks to particular industry sectors.</b> Advanced ISACs may provide incident response through the use of "incident response teams".
<b>Typical Name</b>	<b>No typical name;</b> (i.e.) National cybersecurity councils/ National Cybersecurity and Communications Integration Center	CERT- Computer Emergency Readiness Team CSIRT- Computer Security Incident Response Team	Mostly sector acronym followed by " <b>ISAC</b> "
<b>Examples</b>	 	  	  

# There are 4 design choices to consider while setting up a national cybersecurity agency



We benchmarked 9 **countries** to identify the design choices available while setting up a national cybersecurity agency



## Key design choices

**1** Where does it sit (i.e. within defense and intelligence or is it a civilian body)?



**2** Which level in the government does it report to?



**3** What are the “roles” that it plays?



**4** What is the span of control of the National Cybersecurity Agency?



## Description

**Reporting line and extent of independence** between the national cybersecurity agency and the defense & intelligence community

At what level in the overall government structure, does the **National cybersecurity agency** report to, impacting its authority and influence in the ecosystem

**Roles and responsibilities** that the **National cybersecurity agency owns** (e.g. strategy, policies and regulations, audit and compliance, etc.)

**Set of ecosystem stakeholders** that the **national cybersecurity agency is responsible for** (e.g. Defense, Federal public sector, critical infrastructure, etc.)

# 1 | Benchmark analysis – Archetypes of where the national cybersecurity agency sits

## Archetypes

### 1 Within defense and intelligence

### 2 Within a civilian ministry

	<b>Description</b>	<p><b>The national cybersecurity agency sits within and reports to (or is closely linked to) the defense and intelligence</b></p>	<p><b>The national cybersecurity agency sits outside the defense and intelligence community and reports to a Ministry</b></p>
	<b>Appropriate when</b>	<p><b>Capabilities, resources and partnerships</b> (for intelligence gathering, IR, recovery, etc.) sits primarily within the defense and intelligence community</p>	<p><b>Adequate management, operational and technical capabilities and talent outside of the defense and intelligence community</b></p>
	<b>Benchmark examples</b>		
<p>In the UK, the NCSC reports to the GHQ, within the Intelligence Community</p>			<p>The RIA in Estonia reports to the Ministry of Economic Affairs and Communications</p>

## Key Takeaways

- More **mature economies** have generally set up national cybersecurity agencies either within or very **closely linked to the defense and intelligence communities**

1. In Germany, the BSI reports to the BMI which also has some local intelligence capabilities

## 2 | Benchmark analysis – Archetypes of what level in the government the national cybersecurity agency reports to

### Archetypes

#### 1 Reports to N level of government

#### 2 Reports to N-1 level of government

	<b>Description</b>	<p><b>National cybersecurity agency reports to the highest influential entity</b> (e.g., Prime Minister Office)</p>	<p><b>National cybersecurity agency reports to an entity at the <b>N-1 level</b> of the government</b></p>
	<b>Appropriate when</b>	<p>National cybersecurity agency needs <b>access to budget, resources and the authority to mobilize</b> whole ecosystem to implement strategy</p>	<p>Entity is able to <b>influence</b> all other Ministries <b>indirectly through a law, decree or through another entity</b></p>
	<b>Benchmark examples</b>		
<p>In the US, the national cybersecurity agency is the Department of Homeland Security, at the highest level of the federal government</p>			

### Key Takeaways

- The archetype chosen by benchmark examples depends on what gives the national cybersecurity agency the required authority and influence within the political setup

# 3 | Benchmark analysis – Archetypes of the roles played by the national cybersecurity agency

対外厳密

Archetypes	1 All roles E2E	2 All roles excluding Incident Respond	3 Strategic Role
 <b>Description</b> <ul style="list-style-type: none"> <li>manages cyber security matters in the country <b>E2E from strategy setting and policies, monitoring compliance and IR.</b></li> <li>Typically, national CERT is under this type of agency(coordinating body)</li> </ul>	<p>Across all archetypes, operational aspects of conducting audits are managed by sector regulators or outsourced to private sector entities</p>	<ul style="list-style-type: none"> <li><b>participates in setting the strategy and policies and monitors compliance</b></li> </ul>	<ul style="list-style-type: none"> <li><b>sets the strategy and monitors compliance</b></li> <li>Ministries / regulators set the policies, IR is under Transport &amp; Comm. Ministry</li> </ul>
 <b>Appropriate when</b> <ul style="list-style-type: none"> <li>National cybersecurity agency <b>has appropriate budget, resources and capabilities</b> to play both a strategic and operational role at the same time</li> </ul>	<ul style="list-style-type: none"> <li>Cyber incident response is managed by <b>same entity that is responsible for non-cyber incident response</b></li> </ul>	<ul style="list-style-type: none"> <li><b>Limited budget, resources and capabilities</b> to play both a strategic and operational role at the same time</li> <li><b>Active effort to develop the private sector</b> – spec. cyber security industry</li> </ul>	
 <b>Benchmark examples</b>  <p>The NCSC is involved in the E2E cybersecurity of the UK: it supports the cabinet in setting the strategy, issues policies and regulations (along with the lead government departments), collects compliance from sectors, and has incidence response capabilities</p>	 <p>The CERT in Israel is not part of the National Cyber Directorate and sits in the cybercrime division of the Ministry of public/homeland security</p>	 <p>Qatar's QCERT reports to the Ministry of Transport and Communications, independently from the Cyber Security Coordination Office (CSCO) and the CSCO does not get involved in policies setting</p>	

## Key Takeaways

- All National cybersecurity agencies outsource audit to sector regulators or to private compliance but monitor compliance

1 In the US, policies and regulations are set by the sector regulators with guidance from the DHS, except for the nuclear sector whereby DHS is highly involved in policies and regulations setting

# 4 | Benchmark analysis – Archetypes of scope of control of the national cybersecurity agency

Archetypes	1 Public sector, CI sectors and non-CI sectors	2 Public sector and non-critical sectors	3 E2E except Defense
Description	<ul style="list-style-type: none"> <li>National cybersecurity agency <b>oversees public sector and private sector cybersecurity matters, including critical infrastructure</b></li> </ul>	<ul style="list-style-type: none"> <li>National cybersecurity agency <b>focuses on public sector and on some non critical sectors</b></li> </ul>	<ul style="list-style-type: none"> <li>National cybersecurity agency oversees cybersecurity <b>for all society constituents</b></li> </ul>
Appropriate when	<ul style="list-style-type: none"> <li><b>Citizens are more 'cyber aware'</b> and can manage their own cyber security needs or can leverage a fairly mature private sector cyber security eco-system</li> </ul>	<ul style="list-style-type: none"> <li>Critical infrastructure is managed closely by either the <b>Ministry of Defense or Ministry of Interior</b></li> </ul>	<ul style="list-style-type: none"> <li>Country with <b>need to make a leapfrog</b> in cybersecurity across all sectors</li> <li><b>Nascent private sector</b> cyber security ecosystem with limited abilities to service SMEs and citizens</li> </ul>
Benchmark examples	 X  X  X   ↑  ↑  ↑  X      X      X	 X  X  X  X      ↓ X      ↓ X      ↓  X      X      X	 X  X  X      ↓ X      ↓ X      ↓

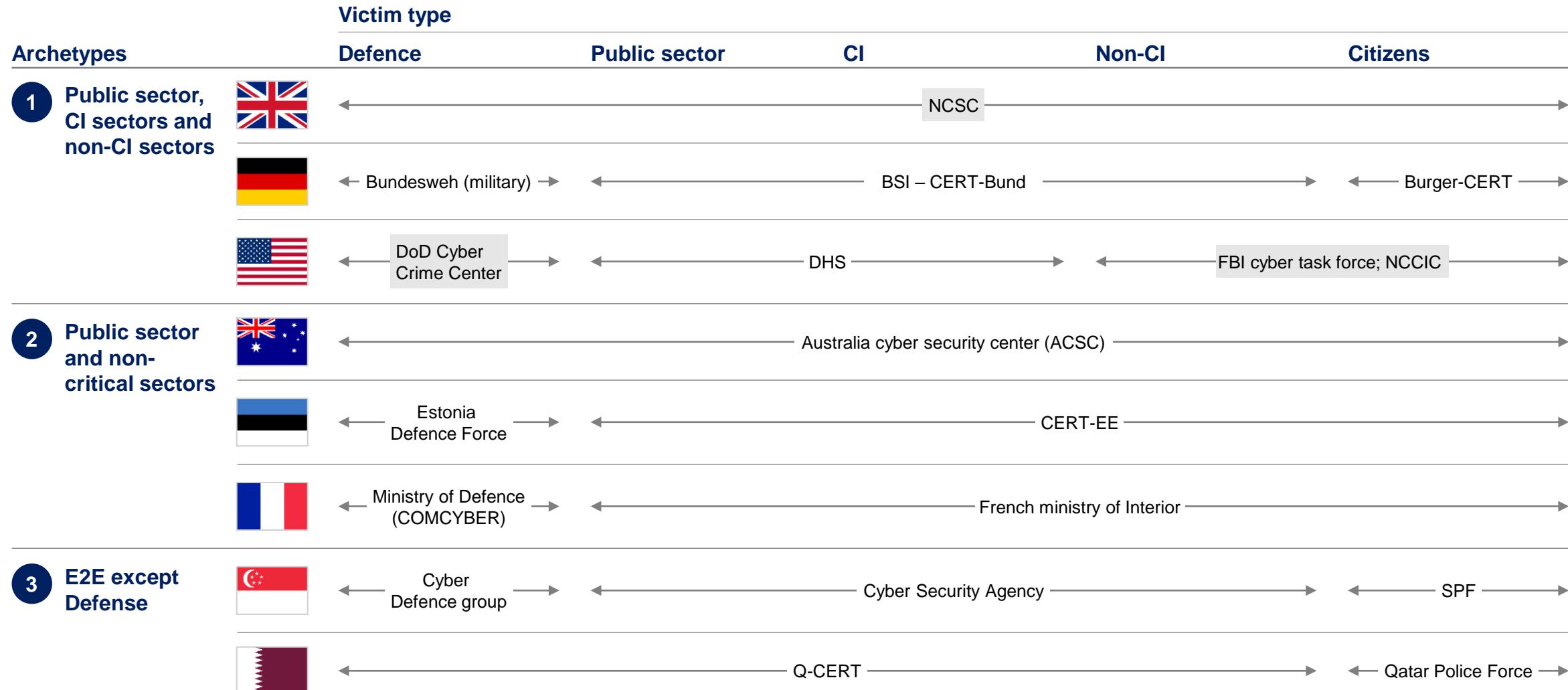
## Key Takeaways

- Benchmark examples that aspire to leapfrog, prefer to have a wide span of control that includes non-critical private sector and citizens

1 In Israel, National Cyber Directorate also manage cybersecurity at the level of defense because it has both a defense and a civilian arm

# 4 | Benchmark countries have different archetypes of points of contacts for different types of victims

Detailed next



1. National Cybersecurity and Communications Integration Center

Source: Expert interview, press search

# Benchmark national coordinating body in charge of overall Cybersecurity

National Cybersecurity strategy element	Singapore 	USA 	Estonia 
① Governance 	A centralized governance body reporting directly to the Prime Minister serves as the owner of cybersecurity strategy both on regulation and execution	National cybersecurity is mainly governed by US DHS and DoD <sup>1</sup> including development and implementation of frameworks	The Cyber Security Council, a committee where all ministries are represented, ensures cooperation and supervises implementation of cyber strategy
② Legal and regulations 	Instruction Manuals provide a framework for mandatory IT security standards, regulations, and best practices, but specific legislations are evolving to address specific regulatory area	The US is at the forefront of developing new cybersecurity legislations and regulations pertaining to emerging technologies	Estonian regulations are comprehensive and innovative in addressing legislative requirements for emerging technologies
③ Talent and people 	<ul style="list-style-type: none"> <li>Singapore cultivates its cyber talent through a variety of awareness and training programs</li> <li>which draw on international standards and certification offerings</li> </ul>	A broad array of federal campaigns and programs to raise public awareness of cybersecurity Certification credentials are a widespread requirement in US agencies and government bodies	Estonia focuses on public awareness programs including SMEs, and on support for cybersecurity higher-education
④ Incident response 	Cybersecurity Agency leads incident response efforts and includes multiple sector-specific NIRCT's, while Cybercrime Command manages the cyber investigation process	Strong coordination in incident situations (e.g., clear roles and procedures, involvement of attacked entities) and focus on data restoration and recovery	Cybersecurity response focuses on providing support to cyber targets; Criminal persecution is secondary
⑤ Partnerships 	Singapore Cybersecurity Agency is a member of several important international partnerships including ASEAN CERT Incident Drill (ACID) and FIRST	Several partnerships exist on regional and international levels incorporating not only public entities but also private institutions to facilitate sharing of cybersecurity best practices	Estonia established broad public-private cooperation at home and is driving international partnerships
⑥ Critical infrastructure 	CII Protection Programme, implemented by Cybersecurity Agency, focuses on protecting assets of 11 critical sectors	National Infrastructure Protection Plan provides strategic guidance to enhance cybersecurity resilience, with several public agencies responsible for critical sectors	Estonia uses a bottom-up approach to supervise critical information infrastructures; with supervised entities are the owners of critical computer networks identified

1. DHS stands for Department of Homeland Security while DoD stands for Department of Defense

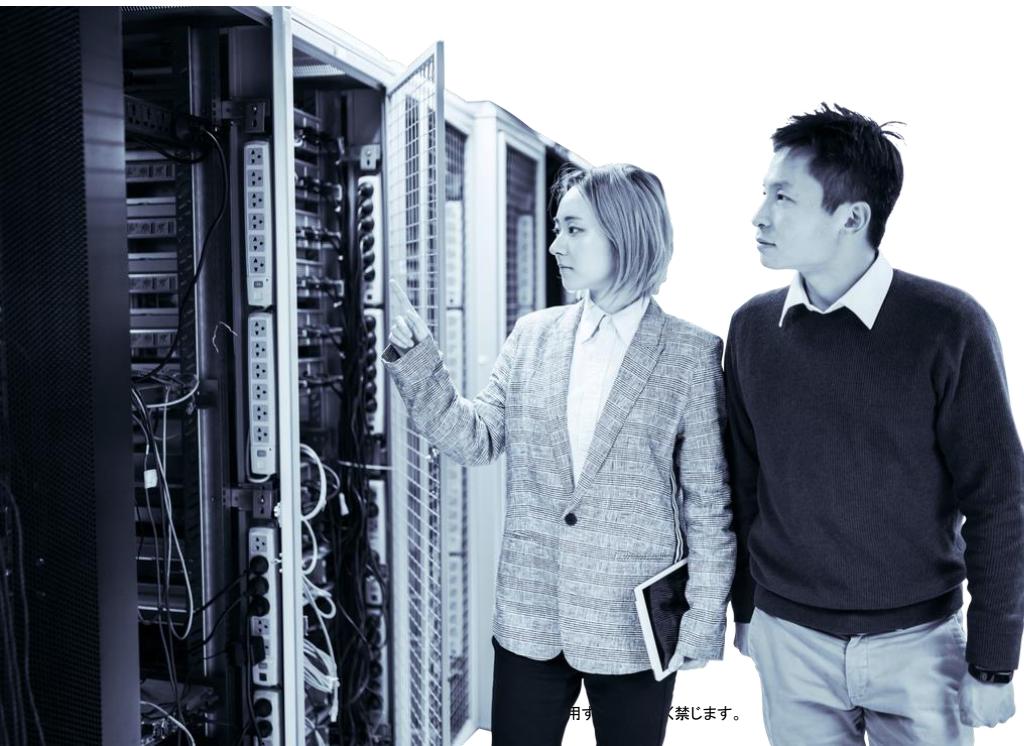
---

# Questions?

---

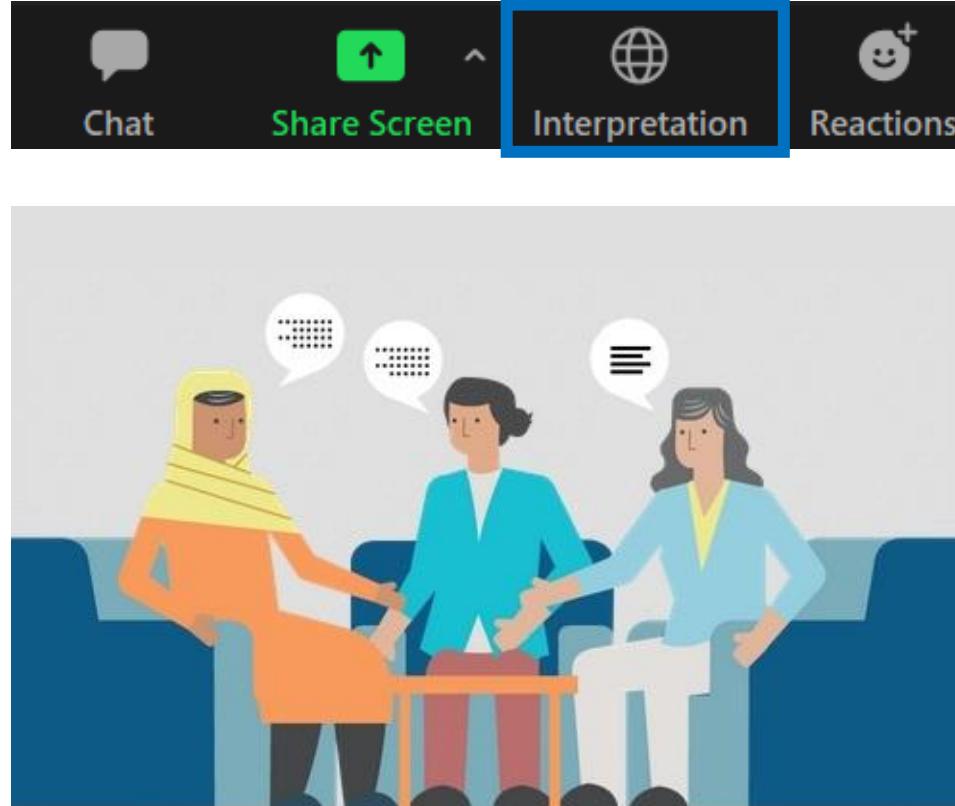


1. Overview of Cyber Security Trend
2. Definition of Cyber threat and national Incident response framework
- 3. Cyber Security Regulation framework**
4. Partnership(Public, Private, Academia, International)
5. Professional training and certification
6. Public awareness and alerts
7. Cyber Security for SME
8. Critical Infrastructure Industry protection
9. CERT/ Resilience
10. Wrap up / Cyber security assessment

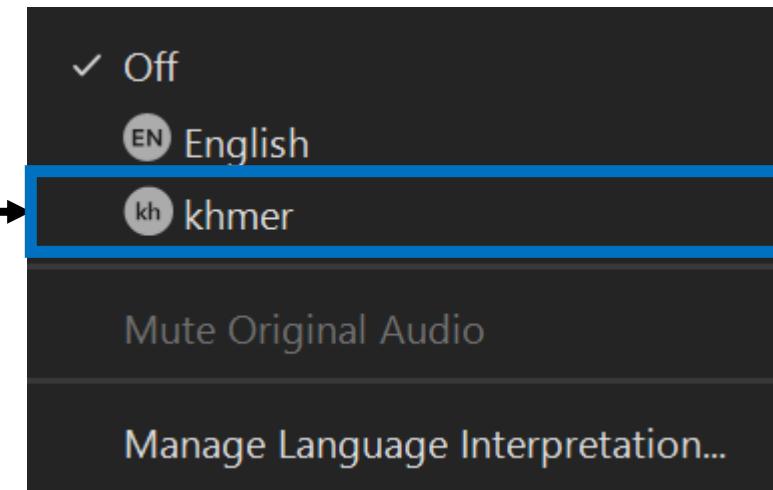


# Khmer simultaneous Interpretation available

Select “Interpretation” on the bottom



Select “Khmer”



- Presentation is simultaneously translated into Khmer
- You can post question in Khmer



## Timeline

## Overview

100 minuets

## Workshop & QA

20 minuets

# Cambodia need to design Cyber security strategy with suggested strategy element

## Cybersecurity strategy element

A Governance	
B Legal and regulations	
E Partnerships	
C Talent and people	
F Critical infrastructure	
D Incident response	

## Insights from benchmarking cybersecurity strategy

#	
• #2	<ul style="list-style-type: none"> <li>Top-performing nations are moving towards <b>centralized governance bodies</b> reporting directly to executive branches of government and serving as <b>E2E owners of cybersecurity strategy implementation</b></li> </ul>
• #3	<ul style="list-style-type: none"> <li><b>Comprehensive legislative frameworks</b> cover mandatory IT security standards, regulations, and best practices, and are enforced through audits and law enforcement</li> <li><b>Specific legislations to address emerging technologies</b> are evolving at fast pace in countries with advanced cybersecurity legislations</li> </ul>
• #4	<ul style="list-style-type: none"> <li><b>Regional and international partnerships</b> are actively used to foster sharing of best practices and enhancing operational and technical capabilities through joint drills &amp; audits</li> </ul>
• #5~7	<ul style="list-style-type: none"> <li><b>Public awareness and training</b> programs, which draw on <b>international standards and offerings</b>, form the basis for cybersecurity talent development</li> </ul>
• #8	<ul style="list-style-type: none"> <li>CII protection programs, executed by national cybersecurity agencies, focus <b>selectively on critical assets</b> in critical sectors with timely involvement of relevant authorities</li> </ul>
• #9	<ul style="list-style-type: none"> <li>National cybersecurity agencies, through <b>specialized incident response teams</b>, lead integrated response efforts with close coordination with impacted assets</li> </ul>

## PRELIMINARY

We benchmarked 6 countries, 1 international treaty, and reports from ITU to identify the key components of cyber security laws and regulations in a country

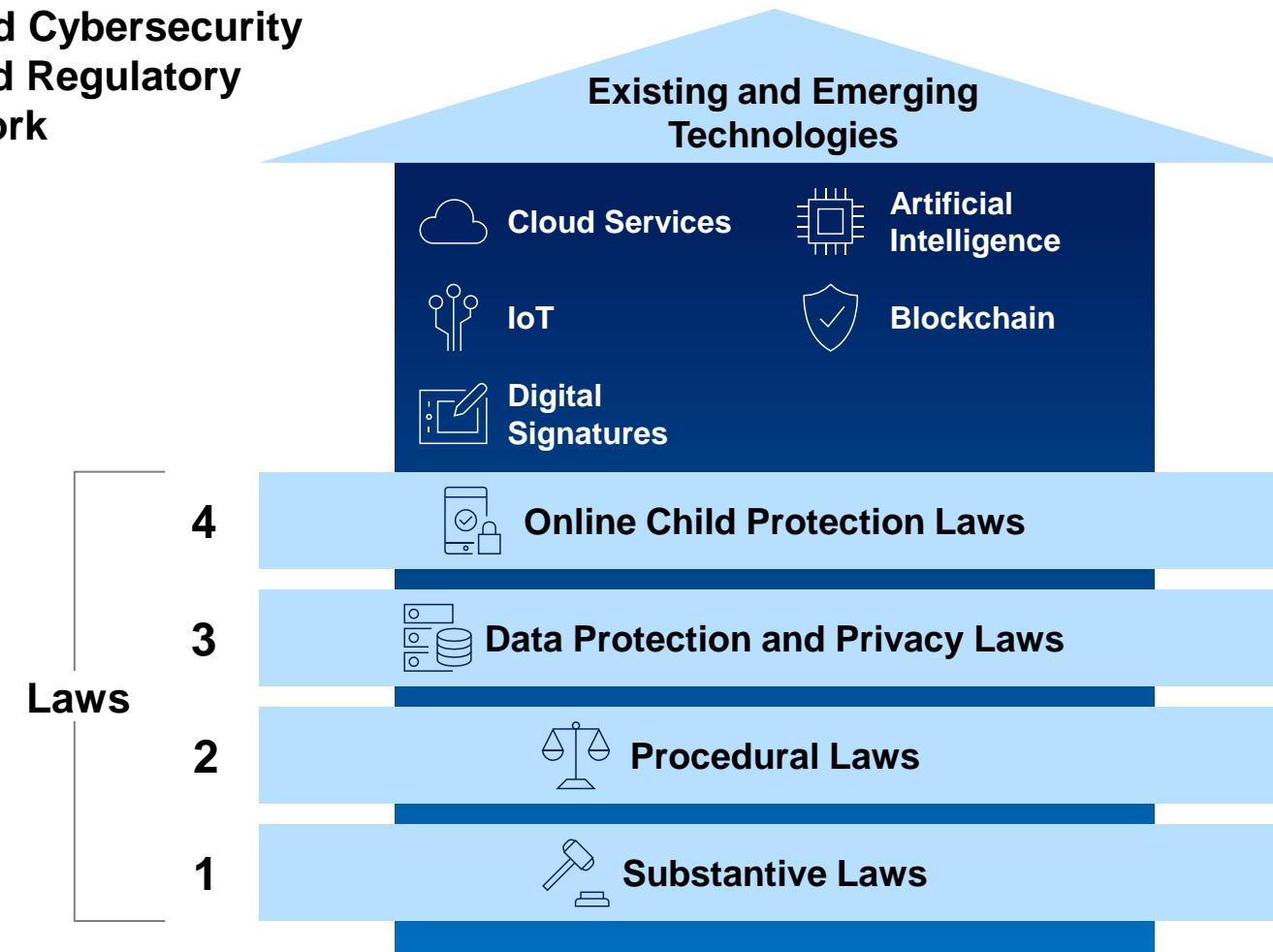


(Signed by 61 countries at Budapest Convention )

Source: Budapest Convention, ITU, Benchmark Analysis

# A comprehensive Cybersecurity Laws and Regulatory framework consists of 4 key components that help secure both existing and emerging technologies

## Proposed Cybersecurity Laws and Regulatory Framework



# 1,2: We benchmarked the Budapest Convention that has developed a comprehensive framework for developing national legislation against cybercrime

PRELIMINARY

## Budapest Convention summary

The Convention on Cybercrime of the Council of Europe (CETS No. 185), known as the Budapest Convention, is an international treaty on cybercrime that is open for signature by the member States and non-member States of the Council of Europe

It serves as a guideline for any country developing comprehensive national legislation against Cybercrime

## 61 Ratified Signatories, including:

### EU Member States



### Non-Member States



Source: coe.int

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。



## Key Components



— 1 —

### Substantive Law

Written statutory rules passed by the legislature to define the cybercrimes and associated punishment



— 2 —

### Procedural Law

Laws that define the procedure, authority and responsibilities to effectively enforce Substantive laws

# 1: As per Budapest Convention, the Substantive laws should cover 10 major categories of electronic crimes (1/2) 対外厳密

PRELIMINARY

**Substantive Laws**  
Written statutory rules passed by the legislature to define the cybercrimes and the associated punishment

Categories	Key aspects covered
1 Illegal access & interception	<ul style="list-style-type: none"><li>Access of a computer system <b>without right</b>, for example, infringing security measures</li><li><b>Interception without right, of non-public transmissions</b> of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data</li></ul>
2 Data & system interference & dissemination	<ul style="list-style-type: none"><li>Damage, deletion, deterioration, alteration or suppression of computer data without right</li><li><b>Hinderance without right of the functioning of a computer system</b> by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data</li><li><b>Dissemination of any electronic data without right</b></li></ul>
3 Computer-related forgery & fraud	<ul style="list-style-type: none"><li><b>Alteration of computer</b> data by any means, resulting in <b>inauthentic data with the intent</b> that it be considered as if it were authentic, regardless whether or not the data is directly readable and intelligible</li><li><b>Alteration or interception</b> of computer data with <b>fraudulent or dishonest intent</b>, causing a loss of property by another person, for economic benefit for oneself or for another person</li></ul>
4 Offences related to child pornography	<ul style="list-style-type: none"><li>Production, procurement or dissemination of <b>child pornography through a computer system</b></li></ul>
5 Offences related to infringements of copyright and related rights	<ul style="list-style-type: none"><li><b>Infringement of copyright</b>, as defined under the domestic law, <b>committed willfully</b>, on a commercial scale and by means of a computer system</li><li><b>Infringement of related rights</b>, as defined under the domestic law, <b>committed willfully</b>, on a commercial scale and by means of a computer system</li></ul>

# 1: As per Budapest Convention, the Substantive laws should cover 10 major categories of electronic crimes (2/2) 对外厳密

PRELIMINARY

## Substantive Laws

Written statutory rules passed by the legislature to define the cybercrimes and the associated punishment

Categories	Key aspects covered
6 Terrorist activities	<ul style="list-style-type: none"><li>• Use of a computer system to carry out or aid in the carrying out of terrorist activities</li></ul>
7 Critical infrastructure and information	<ul style="list-style-type: none"><li>• Access to critical infrastructure or information without right, with the intention to compromise the functioning of the infrastructure</li></ul>
8 Misuse of devices	<ul style="list-style-type: none"><li>• Production, sale, making available or use of any device that is intended to be used to commit any cyber crime defined in legislation</li></ul>
9 Attempt and aiding or abetting	<ul style="list-style-type: none"><li>• Aid or abet of the commission of any of the offences established in accordance with domestic law with intent that such offence be committed</li></ul>
10 Corporate liability	<ul style="list-style-type: none"><li>• Commission of a criminal offence under the domestic cybercrime laws by a natural person acting as part of an organ of the legal person</li></ul>

## 2: As per Budapest convention, cybersecurity laws should cover 10 categories of procedural measures for effective enforcement (1/2)

PRELIMINARY

### Procedural Laws

Laws that define the procedure, authority and responsibilities to effectively enforce Statutory laws

Categories	Key aspects covered
1 Powers and procedures	<ul style="list-style-type: none"> <li>Establish powers and procedures to ensure that the provisions of the enacted laws are enforced efficiently, for example, the establishment of a central body with the duty to enforce the provisions of the laws</li> </ul>
2 Preservation of computer data by competent authorities	<ul style="list-style-type: none"> <li>Enable competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification</li> </ul>
3 Search and seizure of stored computer data	<ul style="list-style-type: none"> <li>Empower competent authorities to search or similarly access a computer system or computer-data storage medium that may be stored in its territory to seize the data when necessary, for example, to maintain the integrity of the relevant stored data</li> </ul>
4 Real-time collection of traffic data	<ul style="list-style-type: none"> <li>Empower competent authorities to compel service providers, within its existing technical capability, to co-operate and assist the authorities in the collection or recording of traffic data in real-time, associated with specified communications in its territory transmitted by means of a computer system</li> </ul>
5 Interception of content data	<ul style="list-style-type: none"> <li>Empower competent authorities to compel service providers, within its existing technical capability, to co-operate and assist the authorities in the collection or recording of content data in real-time, associated with specified communications in its territory transmitted by means of a computer system</li> </ul>

## 2: As per Budapest convention, cybersecurity laws should cover 10 categories of procedural measures for effective enforcement (2/2)

PRELIMINARY

### Procedural Laws

Laws that define the procedure, authority and responsibilities to effectively enforce Statutory laws

	Categories	Key aspects covered
	6 Federal and non-federal agency responsibilities	<ul style="list-style-type: none"> <li>Provide <b>guidance to all relevant federal and non-federal agencies on the responsibilities</b> each agency has in enforcing the provisions of the laws</li> </ul>
	7 Publishing Best practices	<ul style="list-style-type: none"> <li>Enable the competent authorities to <b>publish best cybersecurity practices</b> and update them as and when it becomes necessary</li> </ul>
	8 Reporting of cyber incidences	<ul style="list-style-type: none"> <li>Oblige <b>cybersecurity service providers and digital service providers to report incidences</b> of cybersecurity threats and breaches</li> </ul>
	9 Threat management & incidence response	<ul style="list-style-type: none"> <li>Empower the competent authorities to do <b>whatever is reasonably necessary</b> to prevent, stop or recover from a cybersecurity attack</li> </ul>
	10 Licensing and standards	<ul style="list-style-type: none"> <li><b>Provide standards to all cybersecurity service providers</b> and provide the competent authorities with the powers to evaluate and <b>provide licenses to operate</b> for qualifying cybersecurity service providers</li> </ul>

# 3: We benchmarked best in class countries to identify the 8 key categories that Data Protection and Privacy laws should address (1/2)

PRELIMINARY

We benchmarked 4 countries to identify the key categories of Data Protection and Privacy Laws for cybersecurity



Categories	Key aspects covered
1 Data Gathering	<ul style="list-style-type: none"> <li>Prohibit unauthorized collection of data through a computer system</li> <li>Prohibit the collection of data under false pretenses through a computer system, for example, through phishing emails</li> </ul>
2 Data Usage	<ul style="list-style-type: none"> <li>Prohibit the processing or dissemination of data for unauthorized purposes</li> <li>Provide the right to alter and correct data that has been stored on a computer system or network</li> </ul>
3 Data Storage	<ul style="list-style-type: none"> <li>Regulate the use of adequate data protection controls, such as data encryption, to ensure the privacy of the data and prevent the misuse or unauthorized disclosure of the information</li> <li>Mandate the adoption of comprehensive data security plans to protect information adequately</li> <li>Provide the right to permanently remove data on a computer system</li> </ul>
4 Transparency	<ul style="list-style-type: none"> <li>Mandate that users be informed in a way which is easy to understand about           <ul style="list-style-type: none"> <li>Identity and contact details of the controller</li> <li>Processing of personal data, purpose and legal ground for it</li> <li>Quality of information (mandatory vs. obligatory vs. optional...)</li> <li>Right to lodge a complaint to the supervisory authority</li> <li>Possible data breaches</li> </ul> </li> </ul>

# 3: We benchmarked best in class countries to identify the 8 key categories that Data Protection and Privacy laws should address (2/2)

対外厳密

PRELIMINARY

We benchmarked 4 countries to identify the key categories of Data Protection and Privacy Laws for cybersecurity



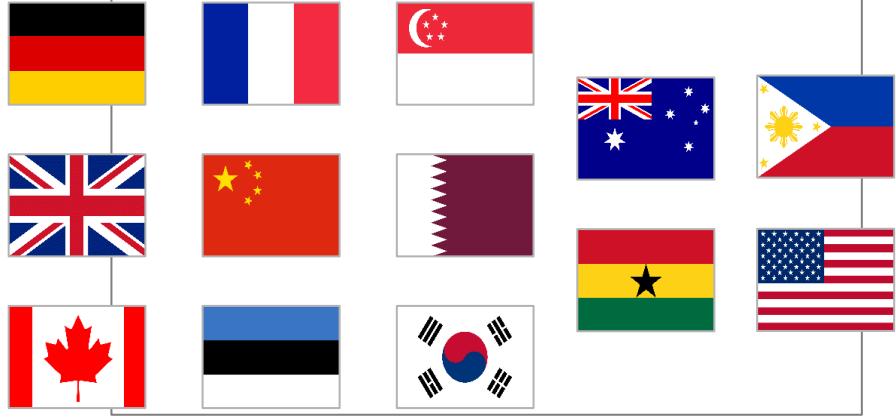
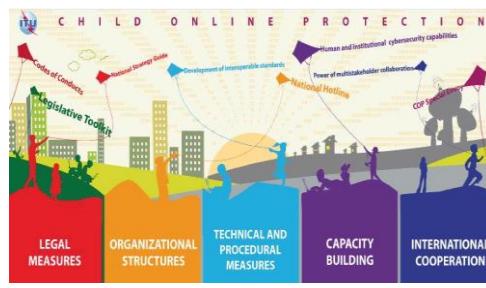
Categories	Key aspects covered
5 Access to Data	<ul style="list-style-type: none"><li>Provide the right to request a copy of stored data</li><li>Provide the right to obtain from the controller at any time information on if and which personal data is processed, purpose, period of storage, transfer and recipients, and information of rights</li></ul>
6 Rectification/erasure (“right to be forgotten”)	<ul style="list-style-type: none"><li>Get rectification of inaccurate data without undue delay</li><li>Right to obtain from controller the erasure of personal data without undue delay in certain circumstances (eg. data is no longer necessary for purposes for which it was collected)</li><li>Notification obligation of controller to data subject on any rectification or erasure of personal data or restriction of processing</li></ul>
7 Right to object/Right to portability	<ul style="list-style-type: none"><li>General right to object to data processing at any time</li><li><b>Right to object to profiling and processing</b> for direct marketing purposes</li><li><b>Right to object to processing for scientific, statistical or historical research purposes</b> unless processing is necessary for reasons of public interest</li><li><b>Right to obtain a copy of personal data from controller</b> in a commonly-used format and have it transferred to another controller without hindrance from original controller</li></ul>
8 Data Sovereignty/Localization	<ul style="list-style-type: none"><li>Provide boundaries for entities to <b>store specified data on</b> computer systems or networks</li><li>Provide <b>conditions when data is not allowed to be stored outside the territorial boundaries</b> of the nation for specific sectors</li></ul>

Source: Benchmark Analysis

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# 4: We benchmarked the 13 countries and global industry frameworks to identify the categories of laws to be enacted for Online Child Protection

PRELIMINARY

Methodology	Description
A <b>Benchmark analysis of intervention programs in 13 countries</b>	Benchmarking of laws enacted to protect children online in 12 global and 1 regional benchmark countries
B <b>Analysis of frameworks adopted by global entities</b>	<p>Analysis of categories of laws for online child protection recommended by the following industry frameworks:</p> <ul style="list-style-type: none"> <li>ITU Child Online Protection (COP) Initiative</li> <li>European Union's EU Kids Online report</li> <li>We Protect Global Alliance to end child sexual exploitation online</li> </ul>   

# 4: Based on benchmark analysis, legal measures are required to protect children against the most common cyber risks

PRELIMINARY

## Child Online Protection

The laws that protect children and young people from any type of abuse on the web, whether through social networks, playing online games or using mobile phones

Categories	Key aspects covered
1 Cyberbullying	• Use of information and communication <b>technologies</b> by individuals or groups deliberately and repeatedly to harm others
2 Cyber grooming	• Use of the internet by an <b>adult</b> to form a <b>trusting relationship</b> with a <b>child</b> with the intent of having <b>sexual contact</b>
3 Cyber stalking	• Type of <b>online harassment</b> in which a single individual's conduct in an extreme form of online pursuit involving repeated contact and malicious threats
4 Personal information	• <b>Collection of personal data</b> online automatically, upon request by an information service provider, or voluntarily when filling in an online form presents a risk that information may be used for <b>privacy-invasive practices</b> including online monitoring, profiling and identity theft
5 Excessive use	• Use of the internet excessively and obsessively, which may have <b>damaging effects</b> on children's and young people's <b>health and/or social skills</b>
5 Inappropriate or harmful content	• Production of online material that is <b>inappropriate for the age and stage</b> of development of children and youth, or is harmful to children and is defined by national or regional cultures and societal values
5 Marketing of inappropriate products	• Marketing and advertising of services such as gambling and dating sites can <b>trigger minors' curiosity and foster risky behavior</b> which might lead to financial loss or set the scene for sexual solicitation

# Benchmark analysis of 6 countries cybersecurity laws and regulations (1/4)

## 1: Substantive Law

PRELIMINARY

Categories						
• Illegal access & interception	✓	✓	✓	✓	✓	✓
• Data & System interference & dissemination	✓	✓	✓	✓	✓	✓
• Corporate Liability	✓	✓	✓	✓	✓	✓
• Computer-related forgery & fraud	✓	✓	✓	✓	✓	✓
• Misuse of devices	✓	✓	✓	✓	✓	✓
• Attempt and aiding or abetting	✓	✓	✓	✓	✓	✓
• Terrorist Activities	✓	✓	✓	✓	✓	✓
• Offences related to infringements of copyright and related rights	✓	✓	✓	✓	✓	✓
• Critical infrastructure and information	✓	✓	✓	✓	✓	✓
• Offences related to child pornography	✓	✗	✓	✓	✓	✓

Source: Benchmark analysis, team analysis

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# Benchmark analysis of 6 countries cybersecurity laws and regulations (2/4)

## 2: Procedural Law

PRELIMINARY

Categories						
• Powers and procedures	✓	✓	✓	✓	✓	✓
• Federal and non-federal agency responsibilities	✓	✓	✓	✓	✓	✓
• Search and seizure of stored computer data	✓	✓	✓	✓	✓	✓
• Real-time collection of traffic data	✓	✓	✓	✓	✓	✓
• Interception of content data	✓	✓	✓	✓	✓	✓
• Preservation of computer data by competent authorities	✗	✓	✗	✗	✓	✓
• Licensing and standards	✗	✓	✓	✓	✗	✓
• Publishing best practices	✓	✓	✓	✓	✓	✓
• Reporting of cyber incidences	✓	✓	✗	✓	✓	✓
• Threat management & Incidence Response	✓	✓	✓	✓	✓	✓

Source: Benchmark analysis, team analysis

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# Benchmark analysis of 6 countries cybersecurity laws and regulations (3/4)

## 3: Data Protection and Privacy Laws

PRELIMINARY

Categories						
• Data Gathering	✓	✓	✓	✓	✓	✓
• Data Storage	✓	✓	✓	✓	✓	✓
• Data Usage	✓	✓	✓	✓	✓	✓
• Transparency	✓	✓	✓	✓	✓	✓
• Access to Data	✓	✓	✓	✓	✓	✓
• Rectification/ erasure	✓	✓	✓	✓	✓	✓
• Right to object/Right to portability	✓	✓	✓	✓	✓	✓
• Data Sovereignty/ Localization	✓	✓	✓	✓	✓	✓

# Benchmark analysis of 6 countries cybersecurity laws and regulations (4/4)

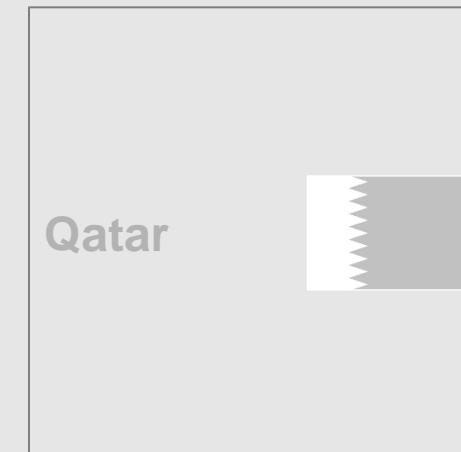
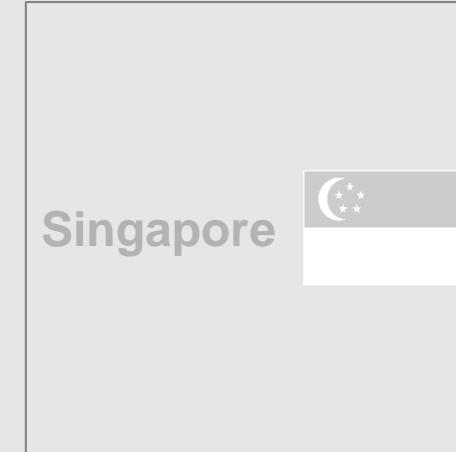
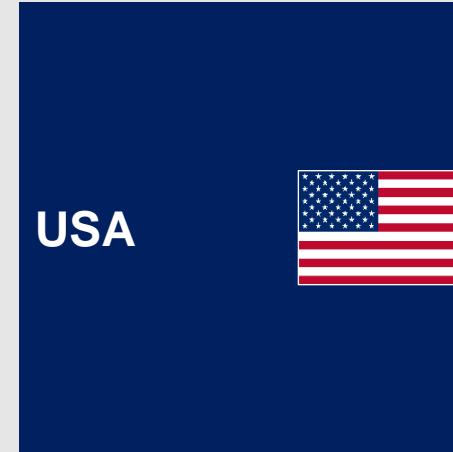
## 4: Online Child Protection

PRELIMINARY

Categories						
• Cyberbullying	✓	✓	✓	✓	✓	✗
• Cyber Grooming	✓	✓	✓	✓	✓	✗
• Cyber Stalking	✓	✓	✓	✓	✓	✗
• Personal Information	✓	✓	✓	✓	✓	✓
• Excessive use	✓	✓	✓	✓	✗	✓
• Inappropriate or harmful content	✓	✓	✓	✓	✓	✓
• Marketing of inappropriate products	✓	✓	✓	✓	✗	✓

PRELIMINARY

# Benchmark analysis of cybersecurity laws of 6 countries





# Benchmark analysis of USA cybersecurity laws (1/6)

PRELIMINARY

Categories	Laws/ Regulations	Description
<b>1 Sustantive and 2 Procedural Laws</b>	<b>Cybersecurity Enhancement Act 2014</b>	<ul style="list-style-type: none"> <li>An Act to provide for an ongoing, <b>voluntary public-private partnership</b> to improve cybersecurity, and to <b>strengthen cybersecurity research and development, workforce development and education, and public awareness and preparedness</b>, and for the advancement of cybersecurity <b>technical standards</b></li> </ul>
	<b>Cybersecurity Act 2015</b>	<ul style="list-style-type: none"> <li>The Act is divided into two primary subparts, cybersecurity information sharing and national cybersecurity advancement</li> <li><b>Cybersecurity Information Sharing establishes the core cybersecurity information sharing framework:</b> a voluntary framework for real-time information sharing of cyber threat indicators and defensive measures between non-federal entities (defined to include State, tribal, or local governments) and federal entities and provides liability protections and an antitrust exemption, such that “no cause of action shall lie or be maintained in any court against any private entity” for the monitoring, sharing, or receipt of cyber threat indicators or defensive measures in accordance with the Act</li> <li><b>National Cybersecurity Advancement includes Subtitle A entitled “National Cybersecurity and Communications Integration Center”</b> and its functions include, among other things, sharing cyber threat indicators, defensive measures, and other information related to cybersecurity risks and incidents with Federal and non-Federal entities engaging with international partners to collaborate on cybersecurity information sharing and enhance the security and resilience of global cybersecurity, designating an agency contact for non-Federal entities, and entering into voluntary information sharing relationships with non-Federal entities. <b>Subtitle B, Federal Cybersecurity Enhancement</b>, establishes new cybersecurity-related requirements for the federal government or amends existing laws to improve federal network security, advance internal defences, and establishes specific reporting requirements on government agencies</li> </ul>



# Benchmark analysis of USA cybersecurity laws (2/6)

PRELIMINARY

Categories	Laws/ Regulations	Description
<b>1 Sustantive and 2 Procedural Laws</b>	<b>National Cybersecurity Protection Act 2014</b>	<ul style="list-style-type: none"> <li>The NCPA <b>codifies</b> the existing cybersecurity and communications operations center at DHS, known as the <b>National Cybersecurity and Communications Integrity Center (NCCIC)</b></li> <li>The bill directs the NCCIC to provide a number of services, including sharing information about cybersecurity risks and incidents, and providing technical assistance, risk management support, and incident response capabilities to federal and non-federal entities</li> </ul>
	<b>Federal Cybersecurity Enhancement Act 2016</b>	<ul style="list-style-type: none"> <li>This bill seeks to improve federal network security by <b>mandating that federal agencies adopt cybersecurity best practices</b>, and accelerating the use of the <b>Dept. of Homeland Security's (DHS) intrusion detection and prevention system</b> across the federal governments</li> </ul>
	<b>Federal Information Security Modernization Act</b>	<ul style="list-style-type: none"> <li>The <b>Act updates the Federal Government's cybersecurity practices</b> by: <ul style="list-style-type: none"> <li>Codifying Department of Homeland Security (DHS) authority to administer the implementation of information security policies for non-national security federal Executive Branch systems, including providing technical assistance and deploying technologies to such systems;</li> <li>Amending and clarifying the Office of Management and Budget's (OMB) oversight authority over federal agency information security practices; and by</li> <li>Requiring OMB to amend or revise OMB A-130 to "eliminate inefficient and wasteful reporting."</li> </ul> </li> </ul>



# Benchmark analysis of USA cybersecurity laws (3/6)

PRELIMINARY

Categories	Laws/ Regulations	Description
<b>1 Sustantive and 2 Procedural Laws</b>	<b>Fourth Amendment to the U.S. Constitution</b>	<ul style="list-style-type: none"> <li>The amendment protects the party only when the party maintains a reasonable expectation of privacy</li> <li>A search warrant may be issued by the Commissioner only on condition that there is probable cause to believe that the media contains evidences of crime, the fruits of a crime or was used as an instrument in committing the crime</li> </ul>
	<b>Federal Rules of Criminal Procedure</b>	<ul style="list-style-type: none"> <li>Rule 41 outlines the criminal procedure regarding search and seizure of property</li> <li>Rule 41 allows any type of property to be search and seized pursuant to a warrant being obtained</li> </ul>
	<b>Communications Assistance for Law Enforcement Act</b>	<ul style="list-style-type: none"> <li>CALEA's purpose is to enhance the ability of law enforcement agencies to conduct lawful interception of communication by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have built-in capabilities for targeted surveillance, allowing federal agencies to selectively wiretap any telephone traffic; it has since been extended to cover broadband Internet and VoIP traffic</li> </ul>



# Benchmark analysis of USA cybersecurity laws (4/6)

PRELIMINARY

Categories	Laws/ Regulations	Description
3 Data Protection and Privacy Laws	Gramm-Leach-Bliley Act (GLBA), 1999	<ul style="list-style-type: none"> <li>GLBA requires companies and organizations to <b>ensure the security for Personally Identifiable Information (PII)</b> of customers. It includes following rules:             <ul style="list-style-type: none"> <li>Provide each customer with privacy notice</li> <li>Develop written plan for security program</li> <li>Prohibits use of fraudulent statements to collect customer data</li> </ul> </li> <li>The <b>penalties</b> include:             <ul style="list-style-type: none"> <li>Financial Institution can be fined up to \$100,000 for each violation</li> <li>The officers can be fined up to \$10,000 for each violation</li> <li>Imprisonment for up to 5 years, a fine, or both</li> </ul> </li> </ul>
	Payment Card Industry Data Security Standard (PCI DSS)	<ul style="list-style-type: none"> <li>PCI DSS standard protects cardholders against misuse of their personal information</li> <li>The <b>penalties</b> include:             <ul style="list-style-type: none"> <li>\$5,000 to \$100,000 per month until compliant</li> </ul> </li> </ul>
	NERC – CIP regulation	<ul style="list-style-type: none"> <li>Set of requirements designed to secure the assets required for operating North America's Bulk Electric Systems (BES)</li> <li>The <b>penalties</b> include:             <ul style="list-style-type: none"> <li>\$1-2mn, based on recent settlements</li> </ul> </li> </ul>
	Federal Information Security Management Act (FISMA)	<ul style="list-style-type: none"> <li>Requires each U.S. federal government agency to implement and support standardized IT security controls, as defined by the National Institute of Standards and Technology, for all agency IT systems that support the operations and assets of the agency</li> <li>The <b>penalties</b> include:             <ul style="list-style-type: none"> <li>Agencies are graded on their FISMA compliance, and FISMA scorecards are publicly available</li> </ul> </li> </ul>



# Benchmark analysis of USA cybersecurity laws (5/6)

PRELIMINARY

Categories	Laws/ Regulations	Description
<b>1 Data Protection and Privacy Laws</b>	ENCRYPT Act	<ul style="list-style-type: none"> <li>The Act <b>has not been enacted yet</b> and would <b>prevent U.S. states and local governments from compelling companies to weaken their encrypted products</b> or store decryption keys for use on demand by law enforcement if it came to pass, and it would also prevent states from prohibiting the sale and offering of certain devices and services based solely on their encryption capabilities</li> </ul>
	HIPPA, 1996	<ul style="list-style-type: none"> <li>Provides data privacy and security provisions for safeguarding all "individually identifiable health information"</li> <li>The <b>penalties</b> include: <ul style="list-style-type: none"> <li>Fine of \$100-50,000 per record, maximum penalty of \$1.5mn per year</li> </ul> </li> </ul>
	Sarbanes-Oxley Act(SOX), 2002	<ul style="list-style-type: none"> <li>Designed with the goal of improving accuracy and reliability of corporate disclosures. Security related sections state <ul style="list-style-type: none"> <li>302 – List all deficiencies in internal controls</li> <li>404 – Third party auditing must review assessment of effectiveness of internal controls</li> </ul> </li> <li>The <b>penalties</b> include: <ul style="list-style-type: none"> <li>Formal penalty for non-compliance of SOX includes fines and removal from the listing on public stock exchanges</li> <li>CEOs and CFOs who can face fines of \$5mn and up to 20 years in jail</li> </ul> </li> </ul>
	Secure Data Act	<ul style="list-style-type: none"> <li>The Act <b>forbids any government agency from demanding</b> that "a manufacturer, developer, or seller of covered products design or <b>alter the security functions in its product or service to allow the surveillance</b> of any user of such product or service, or to allow the physical search of such product, by any agency"</li> <li>The Act has not been enforced yet, but it is seen to be a bill to protect the integrity of encryption systems</li> </ul>



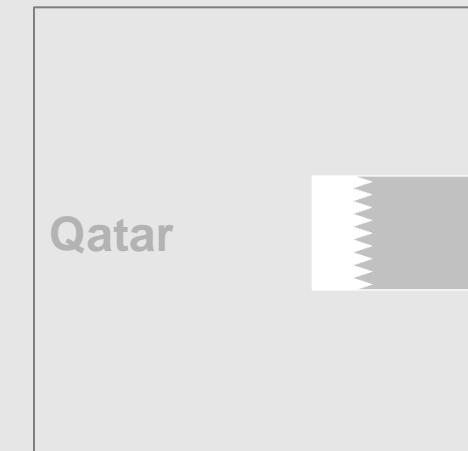
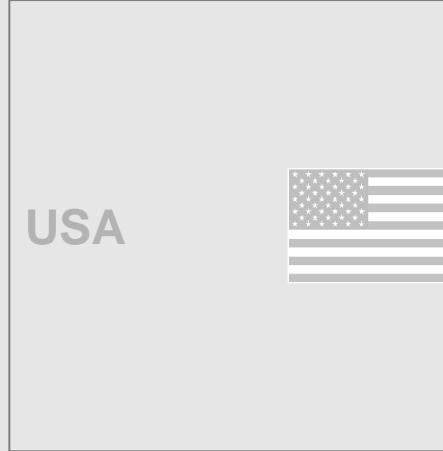
# Benchmark analysis of USA cybersecurity laws (6/6)

PRELIMINARY

Categories	Laws/ Regulations	Description
4 Online Child Protection	Children's Online Privacy Protection Act (COPPA)	<ul style="list-style-type: none"> <li>Limits the ability of websites to collect personal information about children below the age of thirteen without explicit parental consent</li> </ul>
	Other laws	<ul style="list-style-type: none"> <li><b>Harmful Children's Internet Protection Act (CIPA)</b> of 2000 requires that K-12 schools and libraries in the US to use Internet filters and implement other measures to protect children from harmful online content as a condition for federal funding</li> <li><b>Protect Our Children Act</b> makes it a crime to offer or solicit sexually explicit images of children</li> <li><b>Securing Adolescents from Exploitation Online Act, February 2007</b> requires anybody offering a Wi-Fi connection to the public, who obtains actual knowledge of illegal visual media such as child pornography being transmitted over that connection, must report it</li> <li><b>Cyber Bullying:</b> Almost all the US states have criminal laws that cover contact risks like cyberbullying and cyber stalking. For example, according to the California Penal code 653.2, every person who, with intent to place another person in reasonable fear for his or her safety by means of an electronic communication device is guilty of a misdemeanour punishable by up to one year in a county jail and or a fine of \$1000</li> <li><b>Cyber Stalking:</b> Under 18 U.S.C. 875(c), it is a federal crime, punishable by up to 5 years and a fine of up to \$250,000 to transmit a threat to injure another person via an electronic device</li> <li><b>Cyber Grooming:</b> Keeping the Internet Devoid of Sexual Predators Act of 2008 requires convicted sex offenders to register online identifiers in a central database which can be queried by social media and other online websites</li> </ul>

PRELIMINARY

# Benchmark analysis of cybersecurity laws of 6 countries





# Benchmark analysis of Singapore cybersecurity laws (1/2)

PRELIMINARY

Categories	Laws/ Regulations	Description
<b>1 Sustantive and 2 Procedural Laws</b>	<b>Cyber-security Act 2018</b>	<ul style="list-style-type: none"> <li>The Act creates a <b>regulatory framework for the monitoring and reporting of cybersecurity threats</b> to essential services in Singapore through the appointment of the Commissioner of Cybersecurity</li> <li>The Act creates a licensing regime that will require certain data <b>security service providers in Singapore to be registered</b></li> <li>The <b>11 critical sectors of essential services that are identified</b> in the Act are: Energy, Info-communications, Water, Healthcare, Banking and finance, Security and emergency services, Aviation, Land transport, Maritime, Government and Media</li> </ul>
	<b>Singapore Spam Control Act 2007</b>	<ul style="list-style-type: none"> <li>The Act contains the framework for regulating <b>unauthorised electronic messages</b> which are regarded as commercial electronic messages for the purposes of the Act, sent by the traditional method of electronic mail ('e-mail'), text and multimedia messaging to mobile telephone numbers.</li> <li>Prohibited Activities that the Act defines include to send electronic messages to e-mail addresses or mobile telephone numbers randomly generated or obtained through harvesting software. In the circumstances, to protect the interests of the Spammer it is proposed that the Spammer is obliged to ensure the e-mail addresses or mobile telephone numbers used in the Spam are not harvested through prohibited means.</li> </ul>
	<b>Cybersecurity Bill 2017</b>	<ul style="list-style-type: none"> <li>An Act to require or authorise the taking of measures to prevent, manage and respond to cybersecurity threats and incidents, to regulate owners of critical information infrastructure, to establish a framework for the sharing of cybersecurity information, to regulate cybersecurity service providers, and for matters related thereto, and to make related amendments to certain other written laws</li> </ul>
	<b>Copyright law</b>	<ul style="list-style-type: none"> <li>Criminal offences under copyright law include the following: <ul style="list-style-type: none"> <li>Manufacture of infringing copies for commercial purposes</li> <li>Sale of infringing copies</li> <li>Possession or importation of infringing copies for commercial purposes</li> <li>Distribution of infringing copies for commercial purposes</li> </ul> </li> <li>In any of the instances above, it must be proved that the infringing party knows or ought reasonably to know that the copies are infringing ones</li> </ul>



# Benchmark analysis of Singapore cybersecurity laws (2/2)

PRELIMINARY

Categories	Laws/ Regulations	Description
3 Data Protection and Privacy Laws	Personal Data Protection Act 2012 - PDPA ( Data Privacy)	<ul style="list-style-type: none"> <li>• The PDPA covers personal data stored in electronic and non-electronic forms</li> <li>• The PDPA takes into account the following concepts: <ul style="list-style-type: none"> <li>– <b>Consent:</b> Organizations may collect, use or disclose personal data only with the individual's knowledge and consent (with some exceptions);</li> <li>– <b>Purpose:</b> Organizations may collect, use or disclose personal data in an appropriate manner for the circumstances, and only if they have informed the individual of purposes for the collection, use or disclosure; and</li> <li>– <b>Reasonableness:</b> Organizations may collect, use or disclose personal data only for purposes that would be considered appropriate to a reasonable person in the given circumstances.</li> </ul> </li> </ul>
4 Online Child Protection	Criminal code of Singapore	<ul style="list-style-type: none"> <li>• Section 293 of the criminal code of Singapore prohibits the sale, let to hire, distribution or circulation of <b>obscene objects</b> such as books to any person under the age of 21</li> <li>• Section 11 of the Undesirable Publications Act prohibits any person from creating, distributes or sells <b>obscene publications</b></li> <li>• Section 31 of the Films Act prohibits the advertising of a film with <b>obscene content</b></li> <li>• Section 376E of Singapore's criminal code provides that any person of 21 years or older is prohibited from <b>sexual grooming of a minor that is under 16 years of age</b></li> </ul>

# AI and Blockchain use cases entail a number of cybersecurity risks (1/2)

NOT EXHAUSTIVE

	Industries	AI use cases	Examples of cyber risks
<b>Artificial Intelligence (AI)</b> 	 Transportation	Autonomous transportation	<ul style="list-style-type: none"> <li>• <b>Illegal access into the car systems</b> to manipulate the application can create havoc in a traffic network consisting of autonomous vehicles</li> </ul>
	 Entertainment and Social Media	Recommender systems	<ul style="list-style-type: none"> <li>• <b>System interference and manipulation</b> of recommendation engines algorithms can create <b>echo chambers</b> that can allow the spread of misinformation (e.g. “Fake News” on Twitter and Facebook)</li> </ul>
	 Home services	Robotics	<ul style="list-style-type: none"> <li>• <b>Misuse of a robot by manipulating software</b> to commit crimes by portraying as if it was unable to perform care functions adequately (e.g. assist an elderly person from a fall)</li> </ul>
	 Retail	Chat bots	<ul style="list-style-type: none"> <li>• <b>Manipulation of chat bots to bully children online</b> and send inappropriate messages</li> </ul>
	 Healthcare	Healthcare analytics and prediction	<ul style="list-style-type: none"> <li>• <b>Data protection</b> for consumers. Healthcare equipment providers cannot allow data to leak to other companies which can <b>adversely affect patients</b> (e.g. insurance providers having record of lifestyle)</li> </ul>

# AI and Blockchain use cases entail a number of cybersecurity risks (2/2)

NOT EXHAUSTIVE

	Example of cyber risks	Description
<b>Blockchain</b> 	<b>1 Data privacy and protection</b>	<ul style="list-style-type: none"> <li>It is difficult to establish who is <b>responsible for protecting personal data</b> and complying with data privacy regulations once it has been recorded into a blockchain</li> <li>Since the data is immutable, a user may no longer have the right to have personal data deleted or corrected</li> </ul>
	<b>2 Illegal access and interception</b>	<ul style="list-style-type: none"> <li>Similar to all data storage systems, the user has access with a unique secure method, and in the case of a blockchain, it could be a cryptographic key. If the <b>user is careless</b>, that key can be stolen from them and the data used for malicious purposes</li> </ul>
	<b>3 Data Storage</b>	<ul style="list-style-type: none"> <li>The safety of private keys is questionable as it might not be generated with enough randomness, and once a <b>private key is lost, it cannot be recovered</b></li> <li>If a private key is stolen, it is difficult to track the criminal's behaviors and track the criminal's behavior</li> </ul>
	<b>4 Terrorist activities</b>	<ul style="list-style-type: none"> <li>Theoretically, a blockchain can be <b>manipulated if 51%</b> of the nodes conspire to commit fraud on the blockchain</li> </ul>
	<b>5 Corporate liability</b>	<ul style="list-style-type: none"> <li><b>Poorly written software</b> and coding flaws compromise the safety of blockchain</li> </ul>
	<b>6 Misuse of devices/software</b>	<ul style="list-style-type: none"> <li>Malicious software may be stored on a user's computer to <b>monitor the browsing activity</b> of the user and ultimately committing crimes such as phishing, cryptojacking and using ransomware including stealing blockchain keys</li> <li>Software can also be installed to maliciously <b>mine cryptocurrencies</b></li> </ul>

# Bibliography -- Laws, Regulations and Policies

PRELIMINARY

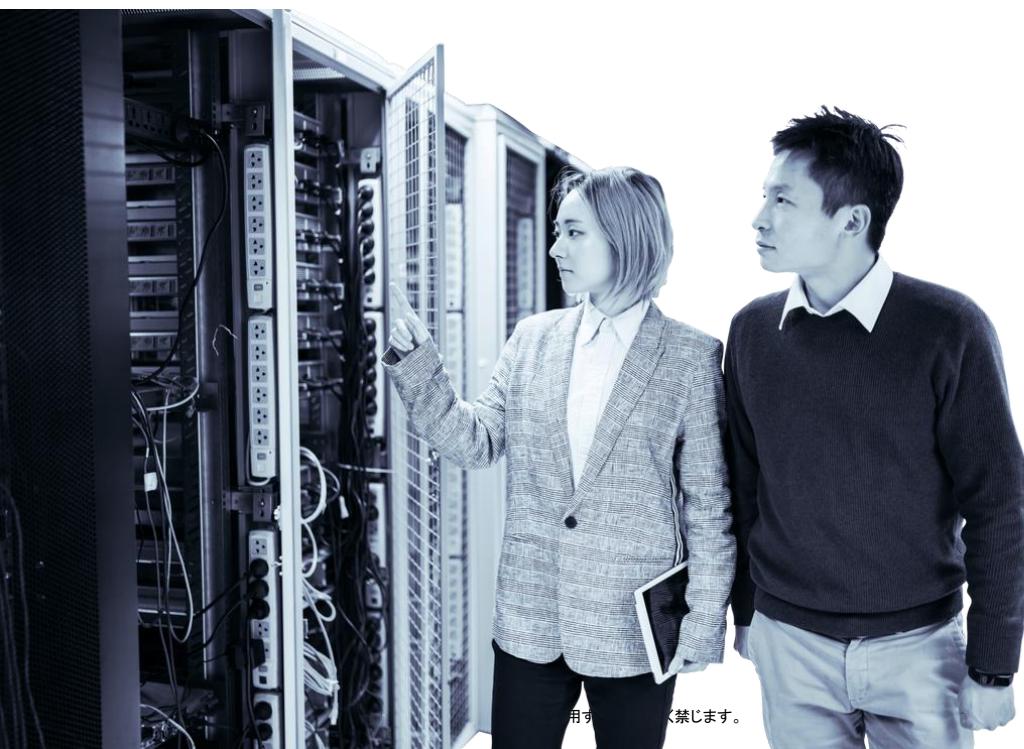
	Description	Created by
1 Federal Law	<ul style="list-style-type: none"> <li>Federal constitution represents the highest legal authority within a country</li> <li>Federal laws must be followed by every state in a country</li> <li>Federal laws do not cover all areas of the law, and in those instances, state or local laws will control</li> </ul>	<ul style="list-style-type: none"> <li>Federal Government</li> </ul>
2 State Law	<ul style="list-style-type: none"> <li>State constitution represents the highest legal authority within a state</li> <li>State laws may be enacted, which apply to everyone within the state, however, may not violate the state constitution, the federal constitution, or federal law</li> </ul>	<ul style="list-style-type: none"> <li>State Government</li> </ul>
3 Regulation	<ul style="list-style-type: none"> <li>Authorized by statutes, regulations (sometimes called rules or administrative laws) have the effect of law</li> <li>Regulations are designed to increase flexibility and efficiency in the operation of laws and most are developed and enacted through a rule making process with public input</li> </ul>	<ul style="list-style-type: none"> <li>Executive Agencies Designated by Laws</li> </ul>
4 Policies	<ul style="list-style-type: none"> <li>Guidelines created and issued at all levels of governances – from national bodies to entities</li> <li>Every law and regulation created is informed by a policy</li> </ul>	<ul style="list-style-type: none"> <li>All levels</li> </ul>

---

# Questions?

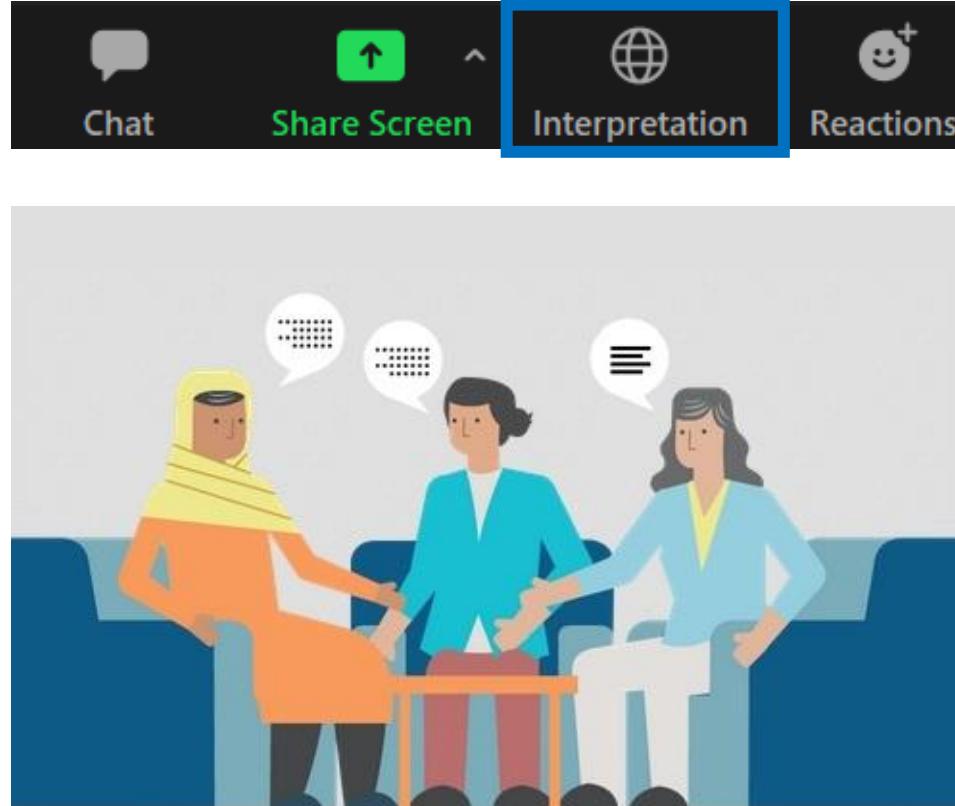
---



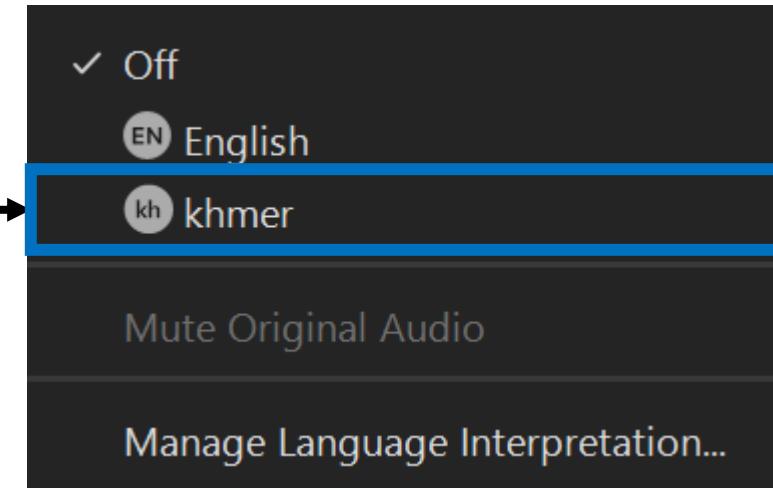
- 
1. Overview of Cyber Security Trend
  2. Definition of Cyber threat and national Incident response framework
  3. Cyber Security Regulation framework
  - 4. Partnership(Public, Private, Academia, International)**
  5. Professional training and certification
  6. Public awareness and alerts
  7. Cyber Security for SME
  8. Critical Infrastructure Industry protection
  9. CERT/ Resilience
  10. Wrap up / Cyber security assessment

# Khmer simultaneous Interpretation available

Select “Interpretation” on the bottom



Select “Khmer”



- Presentation is simultaneously translated into Khmer
- You can post question in Khmer



## Timeline

## Overview

100 minuets

## Workshop & QA

20 minuets

# Cambodia need to design Cyber security strategy with suggested strategy element

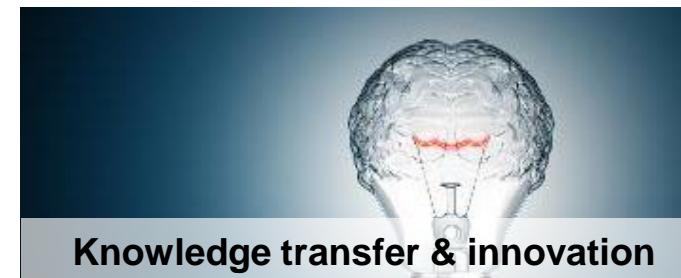
Cybersecurity strategy element	Insights from benchmarking cybersecurity strategy	#
A Governance 	<ul style="list-style-type: none"> <li>Top-performing nations are moving towards <b>centralized governance bodies</b> reporting directly to executive branches of government and serving as <b>E2E owners of cybersecurity strategy implementation</b></li> </ul>	• #2
B Legal and regulations 	<ul style="list-style-type: none"> <li><b>Comprehensive legislative frameworks</b> cover mandatory IT security standards, regulations, and best practices, and are enforced through audits and law enforcement</li> <li><b>Specific legislations to address emerging technologies</b> are evolving at fast pace in countries with advanced cybersecurity legislations</li> </ul>	• #3
E Partnerships 	<ul style="list-style-type: none"> <li><b>Regional and international partnerships</b> are actively used to foster sharing of best practices and enhancing operational and technical capabilities through joint drills &amp; audits</li> </ul>	• #4
C Talent and people 	<ul style="list-style-type: none"> <li><b>Public awareness and training</b> programs, which draw on <b>international standards and offerings</b>, form the basis for cybersecurity talent development</li> </ul>	• #5~7
F Critical infrastructure 	<ul style="list-style-type: none"> <li>CII protection programs, executed by national cybersecurity agencies, focus <b>selectively on critical assets</b> in critical sectors with timely involvement of relevant authorities</li> </ul>	• #8
D Incident response 	<ul style="list-style-type: none"> <li>National cybersecurity agencies, through <b>specialized incident response teams</b>, lead integrated response efforts with close coordination with impacted assets</li> </ul>	• #9

# Partnerships are a core enabler in jointly achieving cybersecurity goals and ambitions

## Definition of partnerships

A cybersecurity partnership is a long term agreement between two or more public and /or private sector entities **to jointly create value by sharing information, skills, risk, scale and funding to achieve a common set of cyber security goals and ambitions**

## Benefits of partnerships



# Benchmark analysis reveals that the central coordination body typically enters into 4 types of partnerships...

	Partnership types	Description	Key examples
 <p>We benchmarked 6 countries to identify partnership models and purposes that the central coordination body leverages</p>      	<b>National</b>	<b>1. Public sector</b>  Partnership with <b>federal/state/city government entities</b> , and other public sector agencies	 Partner with other government agencies to create policies, standards and respond to threats
		<b>2. Private sector<sup>2</sup></b>  Partnerships made directly with <b>large enterprises, industry associations, quasi-govt. firms, SMEs, cross-sectorial agencies</b>	 German public-private partnership for CIIP program
	<b>Inter-national</b>	<b>3. Academia</b>  Partnership with local <b>universities</b> and other <b>educational institutes</b> (typically to address cyber-talent gap and join R&D)	 Partner with University of Tulsa to do cybersecurity R&D
		<b>4. Inter-national<sup>3</sup></b>  Bilateral and/or multi-lateral <b>agreements</b> between countries, typically build on top of <b>existing regional unions</b> and relationships	 International treaty "Budapest convention" on cyber security laws and policies

1. Israeli National Cyber Bureau; 2. Including sector specific and cross-sectorial agencies; 3. Other countries or international organizations

Source: Team analysis, Press search

# ...which are usually for 5 different types of purposes

Partnership purposes

1 Develop and enforce laws and standards



2 Cybersecurity awareness



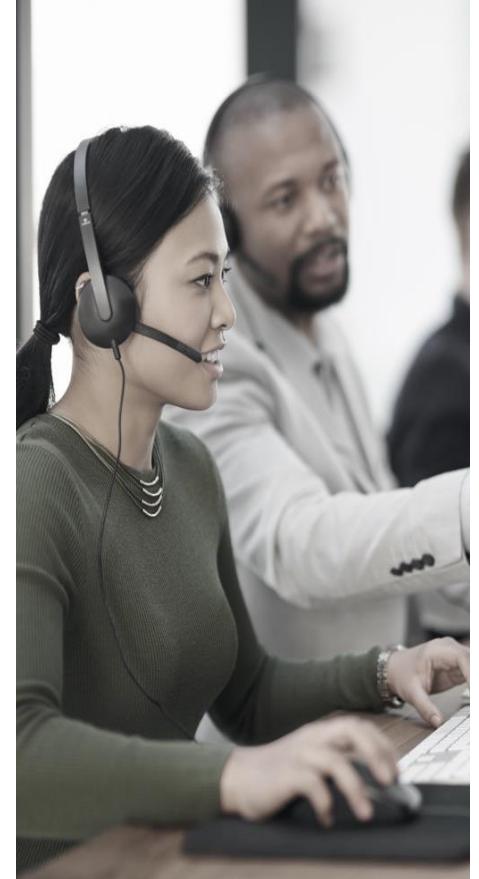
3 Capacity and capability building



4 Cybersecurity ecosystem



5 Incident response



# Game changing partnerships observed in benchmark countries (1/4)

	Game changing partnerships	Benchmark country
Private sector 	<ul style="list-style-type: none"> <li>“Cyber Essentials” is an initiative of the UK government that helps organizations protect themselves against common online threats and in return gives them preference for certain government contracts.</li> <li>To enable auditing and certification of private sector entities, the UK government has accredited multiple private sector players as accreditation bodies</li> </ul>	
	<ul style="list-style-type: none"> <li>Cyber Defense League is an innovative model of the Estonian government to involve volunteers in national cyber defence. It focuses on partnering with patriotic individuals with IT skills, including youth who are ready to contribute to cyber security, and specialists in other fields that concern cyber security (lawyers, economists etc). Their objectives include: <ul style="list-style-type: none"> <li>Development of cooperation among qualified volunteer IT specialists</li> <li>Raising the level of cyber security for critical information infrastructure through the dissemination of knowledge and training</li> <li>Creation of a network which facilitates public private partnership and enhances preparedness in operating during a crisis situation</li> <li>Education and training in information security</li> <li>Participation in international cyber security training events</li> </ul> </li> </ul>	
International 	<ul style="list-style-type: none"> <li>The Budapest Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer related fraud, child pornography and violations of network security.</li> <li>Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation</li> </ul>	

# Game changing partnerships observed in benchmark countries (2/4)

	Game changing partnerships	Benchmark country
<b>Public sector</b> 	<ul style="list-style-type: none"> <li>Estonia's <b>crime prevention project "Web constables"</b>, created as part of government cybersecurity strategy under Police department with the objective of <ul style="list-style-type: none"> <li><b>Raising awareness about security of internet</b></li> <li><b>Protecting children and young people online</b></li> </ul> </li> <li>Web constables, funded by Police department work <b>in social media channels with their professional accounts (e.g. photo, name), participate in online discussions, join groups or forums with special focus on youth/pupils/students</b></li> </ul>	
	<ul style="list-style-type: none"> <li>Singapore government is officially partnering with <b>private bug bounty facilitators</b> to invite white hat hackers <b>to test and identify vulnerabilities</b> on selected internet facing systems with the objective of <ul style="list-style-type: none"> <li>Identifying cyber blind spots in internet facing systems</li> <li>Benchmark its defences against skilled hackers</li> <li>Bring together a community of cyber defenders who share common goal of making cyber space safer and more resilient</li> <li>Drive cyber innovation in the country</li> </ul> </li> </ul>	
<b>Private sector</b> 	<ul style="list-style-type: none"> <li><b>Region's first cybersecurity entrepreneur hub</b> "Innovation cybersecurity ecosystem" (ICE71) created from partnership between government, SingTel and NUS with the objective to <b>drive cybersecurity entrepreneurship</b> and uplift cybersecurity industry</li> <li>SingTel innov8, VC arm of SingTel group provides funding and resources from world-wide start-ups while NUS Enterprise, entrepreneurial arm of NUS act as academy's bridge to industry</li> </ul>	

# Game changing partnerships observed in benchmark countries (3/4)

	Game changing partnerships	Benchmark country
Private sector 	<ul style="list-style-type: none"> <li>Cybersecurity innovation arena “CyberSpark”, is a partnership between Israeli National Cyber Bureau in the Prime Minister’s Office, Beer Sheva Municipality, Ben Gurion University of the Negev and leading companies in the cybersecurity industry to bring together academic research and start-ups with investors, multi-nationals.</li> <li>Objectives of this non-profit organization are: <ul style="list-style-type: none"> <li>to leverage the region and maximize its potential as a global cyber centre</li> <li>to encourage joint academia industry partnerships</li> <li>to support the plans for drawing other companies (international or Israeli)</li> <li>to establish projects or base themselves in the region</li> </ul> </li> </ul>	
Academia 	<ul style="list-style-type: none"> <li>CyberCorps – <b>Scholarship for service</b> program is a partnership between government and selected universities with the objective to increase and <b>strengthen the cadre</b> of federal information assurance professionals and <b>attract students to the cybersecurity/information assurance fields</b></li> <li>Scholarships funded through grants awarded by National Science Foundation cover tuition fees and student stipends of \$22K – \$34K</li> <li>In return, recipients must agree to <b>work after graduation for a government agency</b> in a position related to cybersecurity for a period equal to the length of the scholarship</li> </ul>	

# Game changing partnerships observed in benchmark countries (3/4)

	Game changing partnerships	Benchmark country
Private sector	<ul style="list-style-type: none"> <li>“UP KRITIS” is a public-private sector partnership on both strategic and operational level objectives including:             <ul style="list-style-type: none"> <li>Information sharing</li> <li>Incident response</li> <li>Cyber security incident drills</li> <li>Joint assessment of situation</li> <li>Coordinated crisis response and management</li> </ul> </li> <li>National council of ISACs (NCI) is a cross-sector partnership, providing a forum for sharing cyber and physical threats and mitigation strategies among sectoral ISACs and with government</li> <li>The main objectives of NCI are             <ul style="list-style-type: none"> <li>Maximize information flow between government and private sector</li> <li>Share threat and mitigation strategies during steady-state and incident response</li> <li>Drills and exercises, including participation in national cyber exercises</li> </ul> </li> <li>Sharing and coordination done via <b>calls, reports, request for information, monthly meetings and other activities as per the situation requirements</b></li> </ul>	
International	<ul style="list-style-type: none"> <li>NATO Cyber Defence is a partnership among NATO members, allies, EU, industry and academia with the objective of conducting <b>cyber defence drills and exercises</b> for testing and training the cyber defenders from across the alliance.</li> <li>The first one happened in Estonia, which had multiple tests (e.g. attacks via social media, mobile devices) and training options:             <ul style="list-style-type: none"> <li>Testing of operational and legal procedures</li> <li>Exchange of information and work with industry and partners</li> </ul> </li> </ul>	

# Benchmark analysis of partnerships leveraged across 6 benchmark countries

対外厳密

USA



UK



Singapore



Estonia



Israel



Germany



# Benchmark analysis of partnerships – Homeland Security's Cyber Security Division (1/2)

対外厳密



Homeland  
Security

Not available in public domain

Type of entity	Develop and enforce laws and standards	Cybersecurity awareness	Capacity and capability building
Public sector entities	 <ul style="list-style-type: none"><li>Conducts government led cyber security exercise "CyberStorm" across public and private sector agencies to identify gaps</li></ul>	 <ul style="list-style-type: none"><li>National Cybersecurity <b>Summit</b> bring together govt, agencies, FBI, academia and industry CEOs to lay out a vision <b>for a collective defence model</b> to protect our nation's critical infrastructure</li></ul>	 <ul style="list-style-type: none"><li>NICCS<sup>2</sup> created with other govt. agencies provide <b>online cybersecurity training</b></li><li>Federal virtual training environment provides <b>free, online, on-demand cybersecurity training</b> to federal and SLTT<sup>3</sup> government personnel</li></ul>
Private sector (including sector specific & cross-sectorial)	 <ul style="list-style-type: none"><li>Multiple working groups are created at the sector level for CII protection and compliance (e.g. CII Vetting, Cyber incident data analysis,</li></ul>	<ul style="list-style-type: none"><li>SECIR<sup>1</sup> programs cultivate public, private partnerships to provide support and <b>build resilience across CII</b></li><li>Stop.Think.Connect <b>campaign build public awareness</b> on cybersecurity</li></ul>	<ul style="list-style-type: none"><li>National initiative for cybersecurity education partner with government, academia, and private sector to focus on <b>cybersecurity education</b></li><li>Conduct <b>CII protection exercise DECIDE<sup>4</sup></b> with FSSCC<sup>5</sup> to <b>develop cyber talent</b> in financial sector</li></ul>
Academia	 <ul style="list-style-type: none"><li>Homeland security <b>academic advisory council</b> meets twice a year to <b>consult</b> with academic experts on <b>cybersecurity</b></li></ul>		<ul style="list-style-type: none"><li>CyberCorps <b>scholarship for students</b> at select colleges and universities in return for service in federal or SLTT<sup>3</sup> governments upon graduation</li><li>Collegiate cyber <b>defence challenge</b> promotes cybersecurity curriculum</li></ul>
International			

1. Stakeholder Engagement and Cyber Infrastructure Resilience;

2. National Initiative for Cybersecurity Careers and Studies;

3. State, local, tribal and territorial;

4. Distributed environment for Critical infrastructure decision-making exercise;

5. Financial services sector coordinating council

# Benchmark analysis of partnerships – Homeland Security's Cyber Security Division (2/2)

対外厳密



Homeland  
Security

Not available in public domain



Type of entity	Cybersecurity ecosystem	Incident response
Public sector entities		<ul style="list-style-type: none"><li>CISCP<sup>1</sup> enables <b>unclassified information exchange</b> public-private sectors</li><li>Partner with 16 CII sector agencies, Budget office to <b>address threats, risks</b> across agencies</li><li>Cyber unified coordination group <b>coordinates multiple federal agencies</b> in incident response</li><li>Partner with regional teams via <b>fusion centres and task forces</b></li></ul>
Private sector (including sector specific & cross-sectorial)		<ul style="list-style-type: none"><li>Silicon valley innovation program <b>fund start-ups</b> to make cybersecurity software</li><li>Partnered with 418 Intelligence Corporation to develop <b>cybersecurity controls information sharing platform</b></li><li>NCCIC<sup>2</sup> provides <b>information-sharing hub</b> for cross-sector cooperation</li><li>National risk management centre <b>ameliorate persistent threats</b> targeting public, private and critical infrastructure sectors</li><li>23 sector based ISACs make up National council of ISACs(NSI) to collect, analyse and share cyber threat intelligence with DHS</li></ul>
Academia		<ul style="list-style-type: none"><li><b>Awarded funding</b> to University of Tulsa for <b>cybersecurity research</b> to improve value-based decision-making</li><li>Partnered with Yale University for <b>Data Privacy Research</b></li></ul>
International		<ul style="list-style-type: none"><li>International partnerships with 13 countries and EU to do <b>joint cybersecurity research</b></li><li>US-Dutch <b>bilateral R&amp;D partnership</b> between CSD and Netherland's NCSC on cybersecurity</li><li>IMPACT<sup>3</sup> project between US and Netherlands to <b>enable empirical data and information sharing</b> among countries</li><li>MoU between US and India CERTs to cooperate and <b>exchange information</b></li><li><b>Informal cyber agreements</b> via NATO, Interpol, Europol</li><li>Bilateral <b>cybersecurity agreement</b> with <b>China</b> to prevent cyber espionage</li></ul>

1. Cyber Information Sharing and Collaboration Program;

3. Information Marketplace for Policy and Analysis of Cyber-risk and Trust

2. National Cybersecurity and Communications Integration Centre;

# Benchmark analysis of partnerships leveraged across 6 benchmark countries

対外厳秘

USA



UK



Singapore



Estonia



Israel



Germany



# Benchmark analysis of partnerships – National Cyber Security Centre of UK (1/2)

対外厳秘



National Cyber  
Security Centre  
a part of GCHQ

Not available in public domain

Type of entity	Develop and enforce laws and standards	Cybersecurity awareness	Capacity and capability building
Public sector entities	 <ul style="list-style-type: none"><li>NCSC worked with Crown Commercial Services to establish a central technical and qualitative evaluation “CyberEssentials” to procure cyber services for public sector.</li><li>Independent evaluation of cybersecurity professionals “Certified professional scheme” to give them eligibility to work on CII projects</li></ul>	 <ul style="list-style-type: none"><li>Digital government loft events conducted across cities for educating govt. entity teams (up to 80 people attending each event)</li></ul>	
Private sector (including sector specific & cross-sectorial)	 <ul style="list-style-type: none"><li>Promote security best practices through multi-stakeholder internet governance organisations (e.g. ICANN that coordinates the DNS)</li><li>Competent authorities audit operators of essential services for non-compliance</li><li>NCSC’s decentralized accreditation program to ensure cybersecurity compliance through 3rd party auditors (e.g. capula, Knox)</li></ul>	<ul style="list-style-type: none"><li>Partner with trade bodies to launch campaigns (e.g. “Would you be ready”)</li><li>Partner with British Retail Consortium (BRC) to raise cyber resilience capability (e.g. Cyber security toolkit)</li></ul>	<ul style="list-style-type: none"><li>Industry 100 allows UK businesses to let its employees do secondment at NCSC<sup>1</sup> (for NCSC to pool niche skills)</li></ul>
Academia			<ul style="list-style-type: none"><li>CyberFirst Bursary project provides cyber-security training with annual stipend for students</li><li>Sponsor PhD students in cybersecurity research via academic CoE with 15+ universities</li><li>Certification of masters' degrees in cybersecurity at specific universities</li></ul>
International	 <ul style="list-style-type: none"><li>Worked with EU parliament members to form Network Information Security directive</li><li>Implement ISO standard for information security management system (ISO 27001) in local firms</li></ul>	<ul style="list-style-type: none"><li>OSCE<sup>2</sup> used to improve confidence building measures and cybersecurity awareness among its members</li><li>Partner and support the cybersecurity norms initiative by UN Group of Governmental experts</li></ul>	<ul style="list-style-type: none"><li>Cybersecurity master's degree program set up with NATO</li><li>Cyber capacity building program with ASEAN, MENA, Brazil, India, Mexico</li></ul>

1. Department for Digital, Culture, Media and Sport; 2. Organization for security and cooperation in Europe

Source: Team analysis, Press search

# Benchmark analysis of partnerships – National Cyber Security Centre of UK (2/2)

対外厳秘



National Cyber  
Security Centre  
a part of GCHQ

Not available in public domain



Type of entity	Cybersecurity ecosystem	Incident response
Public sector entities	<ul style="list-style-type: none"><li>Partner with Department for Digital, Culture, Media and Sport, and Cyber accelerator to <b>encourage start-ups and facilitate investments</b></li></ul>	<ul style="list-style-type: none"><li>National and regional cybercrime units act as <b>regional contacts</b> of NCSC for <b>providing cybersecurity support</b> to organizations</li><li>Work with public sector agencies to <b>provide cybersecurity service</b> free of charge in supporting role</li></ul>
Private sector (including sector specific & cross-sectorial)	<ul style="list-style-type: none"><li>CyberInvest <b>brings investment from industry</b> on cyber security research in UK academia</li></ul>	<ul style="list-style-type: none"><li>CiSP<sup>1</sup> provides <b>confidential information sharing platform</b> for its members</li><li>Cyber defence alliance, organization to <b>protect bank's customers</b> from cybercrime is run collaboratively with GCHQ</li></ul>
Academia	<ul style="list-style-type: none"><li>Cybergrowth partnership with academia allows <b>showcasing of products and capabilities</b> to UK and overseas buyers</li></ul>	
International	<ul style="list-style-type: none"><li>NATO <b>secondment opportunity</b> for UK cyber security experts to share and learn with/from other global experts</li></ul>	<ul style="list-style-type: none"><li>FVEY<sup>2</sup> alliance for <b>intelligence sharing</b> and cooperation</li><li>ENISA<sup>3</sup> conducts <b>cybersecurity challenges and exercises</b> at pan-European level</li><li>Share cybersecurity information and reports with NATO members</li></ul>

1. Cybersecurity information sharing platform;  
information security;

2. Five Eyes (UK, USA, Canada, Australia, New Zealand);

3. European union agency for network and

# Benchmark analysis of partnerships leveraged across 6 benchmark countries

USA



UK



Singapore



Estonia



Israel



Germany



# Benchmark analysis of partnerships – Cyber Security Agency of Singapore (1/2)

对外厳秘



Not available in public domain

Type of entity	Develop and enforce laws and standards	Cybersecurity awareness	Capacity and capability building
Public sector entities			
Private sector (including sector specific & cross-sectorial)		<ul style="list-style-type: none"><li>Partner with private bug bounty facilitators to invite white hat hackers to <b>test and identify vulnerabilities</b> on selected internet facing systems</li><li>Partnership with ISACA<sup>1</sup> to launch <b>cybersecurity readiness and risk-based assessment</b> based on capability maturity model integration (CMMI)</li></ul>	<ul style="list-style-type: none"><li><b>Cyber security awareness alliance</b> brings multiple government agencies, private entities and professional associations together to promote adoption of essential cybersecurity practices</li></ul>
Academia			<ul style="list-style-type: none"><li><b>Consulted with academics</b>, cybersecurity experts, professionals and public in drafting the Cybersecurity Bill for the protection of CIs</li></ul>
International			<ul style="list-style-type: none"><li>Police partner with local research institutes to <b>develop new cybercrime investigations and forensic capabilities</b> (e.g. Temasek Advanced Learning, Nurturing and Testing Lab)</li><li>ASEAN <b>Cyber Capacity Development Project</b> funded by Japan and implemented by INTERPOL</li><li>Singapore-United States Third Country <b>Training Programme</b></li></ul>

1. Information Systems Audit and Control Association

Source: Team analysis, Press search

# Benchmark analysis of partnerships – Cyber Security Agency of Singapore (2/2)

对外厳秘



Not available in public domain



Type of entity	Cybersecurity ecosystem	Incident response
Public sector entities	<ul style="list-style-type: none"><li>CSA partnered with Economic Development Board (EDB) to <b>build cybersecurity industry</b> and <b>attract top talent</b></li><li>National Cybersecurity R&amp;D (NCR) programme to <b>bring together govt. agencies and academia</b> on cyber R&amp;D</li></ul>	<ul style="list-style-type: none"><li>Conducts multi-sector Exercise Cyber Star, to <b>test Singapore's cyber incident management</b> and emergency response plans</li><li>Partner with Police, ISPs and Telcos to <b>protect private businesses and individuals</b></li></ul>
Private sector (including sector specific & cross-sectorial)	<ul style="list-style-type: none"><li>MoU with multiple organizations (e.g. SingTel, BAE) for <b>joint R&amp;D</b></li><li><b>Start-up hub</b> “Innovation cybersecurity ecosystem” <b>launched</b> with Innov8 VC, National University of Singapore and Cylon<sup>1</sup></li><li>Cybersecurity <b>centre of excellence</b> launched with partners (e.g. StarHub, EY)</li></ul>	<ul style="list-style-type: none"><li><b>Information sharing</b> facilitated by sectoral SOCs <b>mandate</b> cybersecurity related <b>data collection and analysis</b></li><li><b>Information sharing MoUs</b> with key industry players ( e.g. SingTel, FireEye, BAE Systems, Microsoft, Palo Alto Networks)</li><li>MoU with FS-ISAC<sup>2</sup> for better <b>joint cyber-security efforts and threat intelligence sharing</b> in financial sector</li></ul>
Academia	<ul style="list-style-type: none"><li>Cyber Risk Management (CyRIM) <b>R&amp;D project</b> launched by Nanyang University with CSA</li><li><b>Cybersecurity laboratory</b> launched by ST Electronics and Singapore University of Technology and Design</li></ul>	
International	<ul style="list-style-type: none"><li>Led INTERPOL Operational expert groups to make Singapore the <b>global hub of INTERPOL's cybercrime unit</b></li></ul>	<ul style="list-style-type: none"><li>Partner with INTERPOL to tackle cybercrime and Asia Pacific CERT to <b>enhance cyber incident reporting and response linkages</b></li><li>Conducts annual exercise, ASEAN CERT Incident Drill (ACID) aimed at <b>strengthening cooperation among CERTs</b> in ASEAN and its Partners</li><li><b>MoUs</b> with 6 countries France, India, Netherlands, UK, USA and Germany <b>to cooperate on cybersecurity intelligence sharing</b></li></ul>

1. European cybersecurity accelerator;

2. Financial Services – Information Sharing and Analysis Centre

Source: Team analysis, Press search

# ISAC



## Mission

Improve preparedness and resilience toward cyber attacks through information sharing and collaboration

## Scope of work

Share threats, incidents, vulnerabilities, mitigating measures and also about the best practices and tools.  
Usually do not have an operational role to respond during a cyber incident

## Governance

2 key models:

1. PPP between government and private sector entities
2. Private sector led ISACs

## Typical members

Relevant government ministries, national or sector CERTs, private organizations, law enforcement, national intelligence authorities

# Information sharing platforms vary across countries and sectors, with different levels of involvement by government

対外厳密



National ISAC



Sector ISAC



International ISAC

**Scope of work** Members of ISACs **exchange information about threats, incidents, vulnerabilities, mitigating measures and also about the best practices and tools.**

The experts in ISACs provide technical expertise to:

- identify and analyze emerging threats, including their impact on various communication and information networks and systems
- analyze the impact of cyber incidents (including security breaches, network failures, service interruptions)
- Implement coordinated measures to be prepared for and mitigate such threats and risks
- set up internal and joint procedures to continually review the implementation of adopted measures

Purpose	National(counties) level	Sector(Industry) level	Region(international) level
<b>Function</b>	Share information on threats related to electronic/physical attacks, malfunction of systems, interdependencies among sectors and natural disasters	Share information on threats related to electronic/physical attacks, malfunction of systems, and natural disasters relevant to a specific sector	Promote international cooperation on cybersecurity
<b>Example</b>	UK's Cyber Security Information Sharing Partnership (CiSP)	USA's Financial Sector ISAC (FS-ISAC) Automobile, Utility, Oil & Gas, Pragmatical	European ISAC in Aviation sector

# National ISAC : The UK has had succeeded with its Cyber information Sharing Program (CiSP) which boasts membership from 30 different sectors

対外厳秘



## Overview



The Cyber Security Information Sharing Partnership (CiSP) is a **joint initiative between government and industry** to provide a secure environment to share information on cyber threats

**Representation from 30+ sectors** on this platform

CiSP **works closely with the National Cyber Security Center (NCSC)**

## Key responsibilities



Platform supports **collaboration between industry, Security Service, GCHQ<sup>1</sup>, National Crime Agency and NCSC**

**Share assessments and advisories** during steady state and during a cyber incident

Members receive **network monitoring reports** customized to their organizations

Members also receive an **early warning of cyber threats**

Initially targeted at private sector organizations have partnered with Center for Protection of National Infrastructure. Eventually **extended to SMEs and all interested organizations**

## Role of government(s)



Set up, as a part of CiSP, a Fusion Cell – a **team of experts across industry, law enforcement and intelligence communities** to provide threat analysis

1. Government Communications Headquarters
2. Once an organization is granted membership, the staff of the organization can also get individual access

Source: CiSP, NCSC; Press search

## Overall impact

Platform received 4,000+ visitors per month

Between 2016 and 2017

Organization membership increased by 43%

Individual membership<sup>2</sup> increased by 60%

During the WannaCry ransomware attack, CiSP provided mitigation advice and discredited false rumors/news

NCSC and CiSP together produce regular threat reports that discuss the latest threats and vulnerabilities



# Sector ISAC : The US uses sector ISACs to share digital forensics information between government and industry

対外厳秘



## Overview



**Sector-based Information Sharing and Analysis Centers (ISACs)** collaborate and coordinate with each other via the National Council of ISACs (NCI)

NCI consists of **24 organizations** which have been designated as information-sharing operational arms, by their sectors

ISACs are normally **funded by their member organizations**

## Key responsibilities



**Help critical infrastructure owners and operators** safeguard facilities, personnel and clients from cyber and physical threats

Most ISACs have **24x7 threat warning and incident reporting capability**, and classify the threat level based on the sector

ISACs **promote information sharing** through annual meetings, technical exchanges and webinars

The 24 ISACs **collaborate and share threat and mitigation related information** with each other and partners through NCI

## Role of government(s)



**Federal agencies work with ISACs** and other partners to improve action during steady-state and incident response

ISACs **collaborations extend to governments of other countries**, to share knowledge on cyber threats and incident response

## Overall impact

Several ISACs have **shared relevant information** and helped the government respond to incidents more quickly

ISACs can build capabilities by **developing and customizing trainings** to the industry

ISACs provide member organizations with regular updates, **industry best practices**, and working groups

There are **15,000+ active users** on the secure member portal of the financial service ISAC

## Member<sup>1</sup> ISACs



1. Not exhaustive

Sectors: Automotive, aviation, communication, defense industrial base, defense security information exchange, downstream natural gas, emergency management and response, electricity, financial services, healthcare, IT, Maritime, Multi-state, national health, oil and natural gas, over-the-road bus, public transportation, real estate, research & education, retail, supply chain, surface transportation and water

Source: National Council of ISACs; Press search

# Sector ISAC : The Financial Services-ISAC (FS-ISAC) in the US creates a industry forum for cyber and physical threat intelligence analysis

対外厳密



## Background

The FS-ISAC was created in the US **to facilitate threat information sharing for critical information infrastructure**

In 2013, the FS-ISAC's board extended its charter to **share cyber threat information** with **financial service firms world-wide**



## Functions

The FS-ISAC provides **anonymous information sharing capability** across the entire financial services industry.

Upon receiving a threat submission, FS-ISAC experts verify and analyze the threat, and will identify potential solutions to be sent to FS-ISAC members.

Information sources from FS-ISAC include information from financial services providers, commercial security firms, federal/national, state and local government agencies, law enforcement and other trusted resources



## Notable Features

There are **different subscription tiers** across levels of asset under management (AuM) by the banks depending on membership tiers, members can choose to receive a package of services that include **24 x 7 Watch Desk, STIX/TAXII Feeds, and XML Data Feeds**

Smaller financial institutions are able to sign up for a free FS-ISAC that includes the most **urgent crisis alerts** in the financial services industry



# International ISAC : The EU has several sectoral ISACs to leverage private sector expertise in security

対外厳秘



## Overview

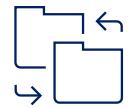


**Sector operators create Information Sharing and Analysis Centers (ISACs)** to leverage information and security experts within the sector

These ISACs are becoming a **platform for shared services**

Sector-specific ISACs are normally set in **countries where the private sector is strong** and has well defined goals in cyber security

## Information shared



Information sharing structure is decided by the sector operator

**Pre incident:** Early-warning systems, real-time security data and analysis, protection mechanisms, vulnerabilities, and incidents

**During incident:** Not clear

**Post incident:** Details of attempted and successful attacks; patches to plug vulnerabilities; methods for remedying vulnerabilities and recovering from incidents



## Key outcomes



**83% of commercial banks in Poland are members** of the Banking Cybersecurity

The government of Norway funded the HealthCERT, provided resources and decided what services this CERT would offer

Energy Analytic Security Exchange (EASE) tied up with the European Energy-Information Sharing & Analysis Centre (EE-ISAC) in Oct 2018. They will share intelligence on international threats, with the aim to protect the global utilities

## Role of government

**Government plays a passive role when ISACs are run by sector operators**

In some countries, the **government also facilitates** the ISACs through National ISACs and by playing a secretariat and/or financier role (Finland, Belgium, Netherlands)

# Benchmark example : Singapore Talent Development Strategy

Initiatives	Name of organization	Initiative	Description of initiative
Central coordinating body		Cybersecurity Professional Scheme	<ul style="list-style-type: none"> <li>CSA has implemented a Cybersecurity Professional Scheme to <b>groom skilled cybersecurity manpower for the public sector</b></li> </ul>
		CSA academy	<ul style="list-style-type: none"> <li>CSA developed a new academy to <b>train cybersecurity professionals in government and CII sectors</b> in partnership industry players</li> <li>The Academy <b>provides intermediate to advanced, niche training to cyber defenders</b> in the government, and also invites selected parties in the CII sectors to join in the training through FireEye, its first training partner</li> </ul>
		MoC with UK	<ul style="list-style-type: none"> <li>Singapore and the United Kingdom signed a <b>Memorandum of Cooperation (MoC) on Cybersecurity Capacity Building</b></li> <li>With Association of <b>Information Security Professionals (AISP)</b> and <b>CREST International</b>, CSA signed Memorandum of Intent (MOI) to work together to introduce <b>CREST certifications</b> for penetration testing in Singapore in 2016. By introducing the certification, the aim is to help <b>grow local skills and capabilities and provide assurance</b> for professionals and service providers that perform penetration tests.</li> <li>The present MoC will see both countries cooperating to <b>deliver cybersecurity capacity building programmes to Commonwealth Member States for a two-year period</b> beginning September 2018, and in addition, the UK will also actively participate in Singapore's ASEAN Cyber Capacity Programme that was launched in 2016</li> </ul>
		DOI with US	<ul style="list-style-type: none"> <li>Singapore and US signed a Declaration of Intent (<b>DOI</b>) to <b>collaborate on a Singapore-US Cybersecurity Technical Assistance Program for ASEAN Member States</b></li> <li>The DOI aims to deliver cybersecurity <b>training workshops for government employees</b> and key industry partners across South East Asia</li> </ul>

# Benchmark example : Singapore Talent Development Strategy

Initiatives	Name of organization	Initiative	Description of initiative
Central coordinating body	 	<b>Cybersecurity Centre of Excellence</b>	<ul style="list-style-type: none"> <li>Deputy Prime Minister Teo Chee Hean Announced at the third annual Singapore International Cyber Week, Singapore will set up an Asean-Singapore Cybersecurity Centre of Excellence to <b>strengthen ASEAN members' cyber strategy development, legislation and research capabilities</b></li> <li>The centre will also <b>train national Computer Emergency Response Teams (Certs) in the region</b>, and promote Cert-to-Cert open-source information sharing</li> </ul>
		<b>National Cyber-security Postgraduate Scholarship</b>	<ul style="list-style-type: none"> <li>National Cybersecurity Postgraduate Scholarship (NCPS) is jointly offered by NRF and IMDA under NCR, a prestigious <b>scholarship for graduates and working professionals</b> who are keen to contribute and commit to the protection of Singapore's cyberspace</li> <li>Applicants may pursue their <b>Masters and/or Doctoral degrees</b></li> </ul>

# Benchmark analysis of capability building initiatives in the US

Initiatives	Name of organization	Initiative	Description of initiative
Central coordinating body	 <b>Homeland Security</b>	<b>National Initiative for Cybersecurity Careers &amp; Studies</b>	<ul style="list-style-type: none"> <li>• NICCS is the <b>nation's one-stop shop for cybersecurity careers and studies</b> that connects the public with information on cybersecurity awareness, degree programs, training, careers, and talent management</li> <li>• As of September 2018, the <b>Training Catalog</b> connects the public to over 4,000 courses every day</li> </ul>
		<b>Federal Virtual Training Environment</b>	<ul style="list-style-type: none"> <li>• FedVTE provides <b>free online cybersecurity training to U.S. government employees, Federal contractors, and veterans</b></li> <li>• Course proficiency ranges <b>from beginner to advanced levels</b> and several courses align with a variety of IT certifications such as Network +, Security +, and Certified Information Systems Security Professional (CISSP)</li> </ul>
	 <b>NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION</b>	<b>Cybersecurity competitions</b>	<ul style="list-style-type: none"> <li>• CCDC's mission is to provide institutions with an information assurance or a computer security curriculum controlled, competitive environment to assess their student's depth of understanding and operational competency in managing the challenges inherent in protecting a corporate network infrastructure and business information systems</li> <li>• <b>CCDC Events are designed to:</b> <ul style="list-style-type: none"> <li>– Build a meaningful mechanism by which institutions of higher education may evaluate their programs</li> <li>– <b>Provide an educational venue in which students are able to apply the theory and practical skills</b> they have learned in their course work</li> <li>– Foster a spirit of teamwork, ethical behavior, and effective communication both within and across teams</li> <li>– <b>Create interest and awareness</b> among participating institutions and students</li> </ul> </li> </ul>

# Benchmark analysis of capability building initiatives in the US

Initiatives	Name of organization	Initiative	Description of initiative
Central coordinating body	 	NICE Working Group	<ul style="list-style-type: none"> <li>NICE Working Group (NICEWG) has been established <b>to provide a mechanism in which public and private sector participants</b> can develop concepts, design strategies, and pursue actions that <b>advance cybersecurity education, training, and workforce development</b></li> <li>NICE Working Group is comprised of <b>six sub-working groups</b>. Each subgroup meets independent of the NICEWG and reports out at the NICEWG Meetings. The subgroups are: <b>apprenticeship, collegiate, competitions, K-12, training and certifications and workforce management</b></li> </ul>
		NICE Interagency Coordinating Council	<ul style="list-style-type: none"> <li>NICE Interagency Coordinating Council (ICC) convenes federal government partners of NICE for <b>consultation, communication, and coordination of policy initiatives and strategic directions</b> related to cybersecurity education, training, and workforce development</li> <li>Current NICE ICC membership includes members from the following departments and agencies amongst others: Department of Commerce, Department of Defense, Department of Education, Department of Energy and Department of Health and Human Services</li> </ul>

# Benchmark analysis of capability building initiatives in the US

Initiatives	Name of organization	Initiative	Description of initiative
Central coordinating body	 <b>Homeland Security</b>  	<b>National Centers of Academic Excellence in Cyber Defense</b>	<ul style="list-style-type: none"> <li>The goal of the program is to <b>reduce vulnerability</b> in the US national information infrastructure by <b>promoting higher education and research in cyber defense and producing professionals</b> with cyber defense expertise</li> <li>The CAE-CD program comprises the following designations:             <ul style="list-style-type: none"> <li>Four-Year Baccalaureate/Graduate Education (CAE-CDE)</li> <li>Two-Year Education (CAE2Y)</li> <li>Research (CAE-R)</li> </ul> </li> </ul>
		<b>National Centers of Academic Excellence in Cyber Operations</b>	<ul style="list-style-type: none"> <li>NSA's CAE in Cyber Operations (CAE-CO) program <b>supports</b> the President's National Initiative for Cybersecurity Education (<b>NICE</b>): Building a Digital Nation, and furthers the goal to broaden the pool of skilled workers capable of supporting a cyber-secure nation</li> <li>CAE-CO program is a <b>deeply technical, inter-disciplinary, higher education program</b> firmly grounded in the computer science, computer engineering, and/or electrical engineering disciplines, with extensive opportunities for hands-on applications via labs and exercises</li> </ul>

---

# Questions?

---



# Theme of Cyber Strategy PoC (19-28 July)

Session by Kirirom institute of technology (KIT)

Session by FPT Software

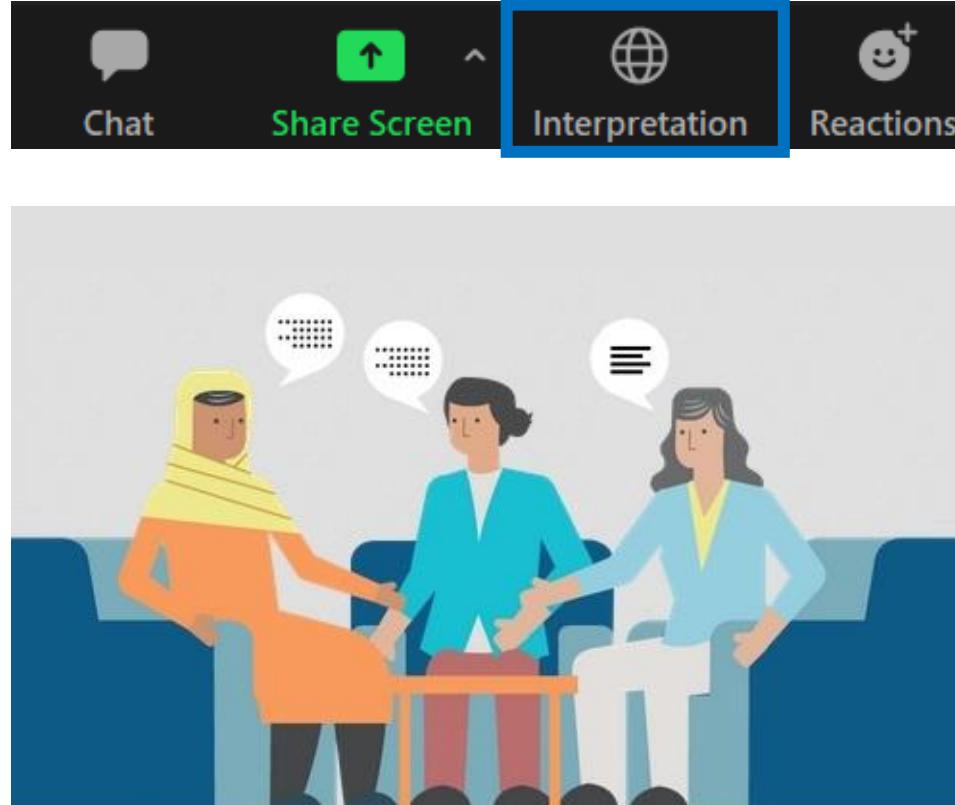
<b>Day</b>	<b>KHM</b>	<b>JST</b>	<b>Theme</b>
<b>19-Jul</b>	9:00-11:00	11:00-13:00	1. Overview of Cyber Security Trend
	13:00-15:00	15:00-17:00	2. Definition of Cyber threat and national Incident response framework
<b>20-Jul</b>	9:00-11:00	11:00-13:00	3. Cyber Security Regulation framework
	13:00-15:00	15:00-17:00	4. Partnership(Public, Private, Academia, International)
<b>21-Jul</b>	9:00-11:00	11:00-13:00	5. Professional training and certification
	13:00-15:00	15:00-17:00	6. Public awareness and alerts
<b>26-Jul</b>	9:00-11:00	11:00-13:00	7. Cyber Security for SME
	13:00-15:00	15:00-17:00	8. Critical Infrastructure Industry protection
<b>28-Jul</b>	9:00-11:00	11:00-13:00	9. CERT/ Resilience
	13:00-15:00	15:00-17:00	10. CamCERT

1. Overview of Cyber Security Trend
2. Definition of Cyber threat and national Incident response framework
3. Cyber Security Regulation framework
4. Partnership(Public, Private, Academia, International)
- 5. Professional training and certification**
6. Public awareness and alerts
7. Cyber Security for SME
8. Critical Infrastructure Industry protection
9. CERT/ Resilience
10. Wrap up / Cyber security assessment

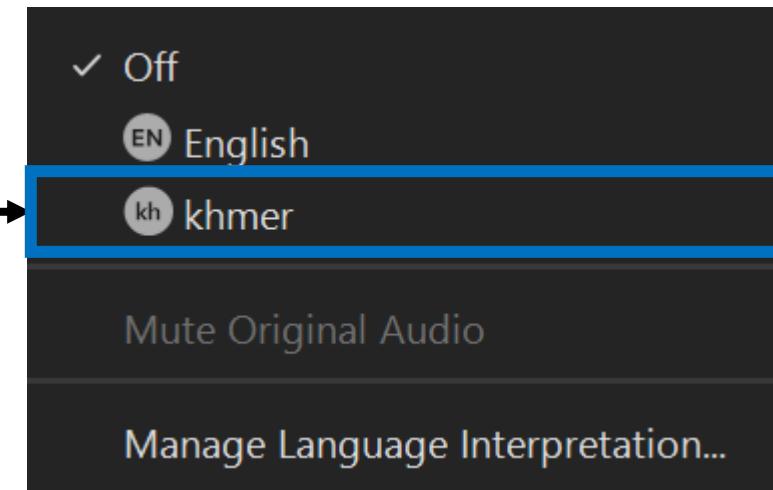


# Khmer simultaneous Interpretation available

Select “Interpretation” on the bottom



Select “Khmer”



- Presentation is simultaneously translated into Khmer
- You can post question in Khmer



## Timeline

## Overview

100 minuets

## Workshop & QA

20 minuets

# Cambodia need to design Cyber security strategy with suggested strategy element

Cybersecurity strategy element	Insights from benchmarking cybersecurity strategy	#
A Governance 	<ul style="list-style-type: none"> <li>Top-performing nations are moving towards <b>centralized governance bodies</b> reporting directly to executive branches of government and serving as <b>E2E owners of cybersecurity strategy implementation</b></li> </ul>	• #2
B Legal and regulations 	<ul style="list-style-type: none"> <li><b>Comprehensive legislative frameworks</b> cover mandatory IT security standards, regulations, and best practices, and are enforced through audits and law enforcement</li> <li><b>Specific legislations to address emerging technologies</b> are evolving at fast pace in countries with advanced cybersecurity legislations</li> </ul>	• #3
E Partnerships 	<ul style="list-style-type: none"> <li><b>Regional and international partnerships</b> are actively used to foster sharing of best practices and enhancing operational and technical capabilities through joint drills &amp; audits</li> </ul>	• #4
C Talent and people 	<ul style="list-style-type: none"> <li><b>Public awareness and training</b> programs, which draw on <b>international standards and offerings</b>, form the basis for cybersecurity talent development</li> </ul>	• #5~7
F Critical infrastructure 	<ul style="list-style-type: none"> <li>CII protection programs, executed by national cybersecurity agencies, focus <b>selectively on critical assets</b> in critical sectors with timely involvement of relevant authorities</li> </ul>	• #8
D Incident response 	<ul style="list-style-type: none"> <li>National cybersecurity agencies, through <b>specialized incident response teams</b>, lead integrated response efforts with close coordination with impacted assets</li> </ul>	• #9

# Contents

 Detailed next

- 1 THE NEED FOR CYBERSECURITY CAPABILITIES**
- 2 PROPOSED NATIONAL CYBERSECURITY CAPABILITY BUILDING FRAMEWORK**
- 3 BENCHMARK ANALYSIS OF GLOBAL CAPABILITY BUILDING INITIATIVES**
- 4 RECOMMENDED NATIONAL INITIATIVES**



# Globally, entities today are more vulnerable to cyber incidents than ever before primarily due to 4 key reasons

 Detailed next

## Key Reasons

1 Increased frequency and severity of cyber attacks



2 More entry points vulnerable to attack



3 Growing sophistication of attackers



4 Non-compliance and user behavior as contributing factors



## Details/ Examples

- Ransomware attacks worldwide **increased by 36 percent in 2017** – with more than 100 new malware families introduced by hackers **1 in 131 emails** contain a malware
- The average cost of a data breach will exceed \$150 million by 2020 – and by 2019, cybercrime will cost businesses over \$2 trillion – **a four-fold increase from 2015**

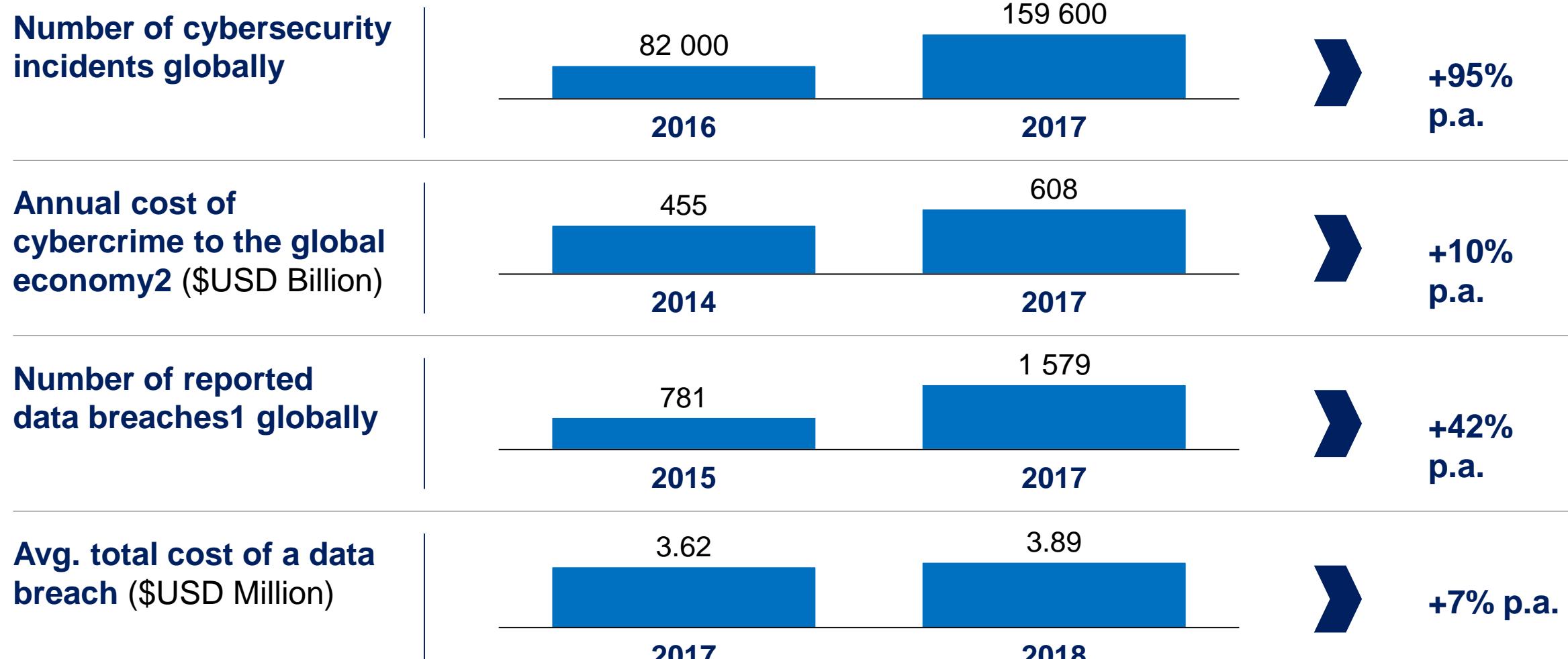
- 3.8 B Internet users** in 2017 (51% of the population), up from 2 B in 2015
- Microsoft estimates that data volumes online will **increase 50x** between 2016 and 2020
- New attacks are being powered by the spread of **unsecured IoT devices** – in 2016, IoT devices were responsible for the biggest DDoS attack ever seen

- The average size of distributed denial-of-service (DDoS) attacks is **4X larger** than what cybercriminals were launching two years ago – and more than 40 percent of DDoS incidents in 2017 exceed a whopping 50Gbps, up from 10 percent of cases in 2015
- Networks of attack robots** can automatically and systematically run attack scripts against any device connected to a network

- Over 75% of websites** have unpatched vulnerabilities
- Approximately 15% of people tested** click on links in a phishing email
- 66% of malware** installed via malicious email attachments

# The number of cybersecurity incidents has doubled in the past year, resulting in significant cost to global economy

PRELIMINARY



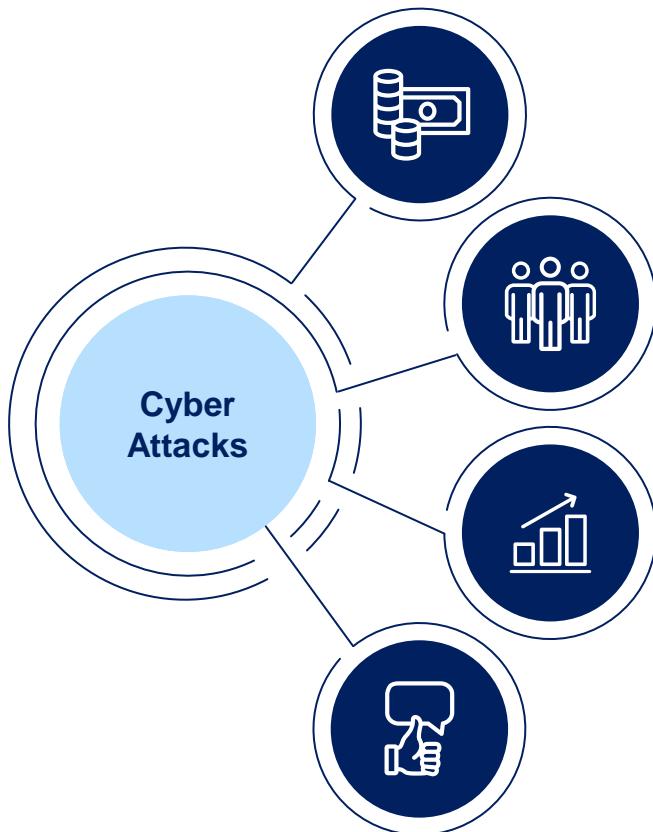
<sup>1</sup> Defined by ITRC as an incident in which Personally Identifiable Information, user names, passwords or email addresses are potentially put at risk because of exposure

<sup>2</sup> Based on a combination of high level estimates done by Allianz and McAfee for 2014 and Juniper Research for 2019

# However, the impact of cybersecurity incidents, extends beyond just the economic losses

PRELIMINARY

## Potential impact of cybersecurity incidents



## Recent Examples



### 1 Direct Financial Impact



### 2 Client Impact



### 3 Impact on Services



### 4 Reputational Impact

## Impact of cybersecurity incidents

- **Supervisory Fines and Remediation Cost** imposed for insufficient cyber security
- **Theft of Funds or loss of revenues** directly relating to hacker activism and cyber fraud
- **Stock Price Impact** reflecting market concerns over governance failures, legal recuperations, or financial impact
- **Theft of client funds** from client accounts and transfer to 3rd party accounts as well as the use of client data for purchases
- **Theft of sensitive client data** including personal information as well as card numbers and security codes
- **Publication of confidential client information** such as investment holdings, earnings, or credits
- **Down Time** of service critical or client facing systems (e.g. website) prohibiting the proper functioning of services
- **Operational chaos** during and after attacks as clients cannot access services and internal processes break down
- **Data Manipulation** in the firm's ledgers may cause sustained malfunctions and service inaccuracies
- **Reputation with Clients** suffers as the security of sensitive and confidential personal data gets questioned
- **Public image and effect on investors** as major security breaches break headlines and worsen reputation
- **Supervisory relations** get strained and cause close scrutiny by authorities going forward

# This rapid growth in cybersecurity incidents has been observed across industries

対外厳秘

PRELIMINARY

## Manufacturing



22% average year-on-year increases in **industrial** control systems vulnerabilities

## Banking



+ 64% increase in **internet banking** fraud, which covers fraudulent payments taken from a customer's bank account in 2015

## Healthcare



85% of **healthcare organizations** had at least one data breach involving the loss or theft of patient data in 2015 and 2016

## Financial Services



89% of data breaches in 2015 had a **financial** or espionage motive

# Case examples: Cybersecurity incidents across the world

PRELIMINARY

## Ukraine Power Outage



**80,000** people lost power when hackers hacked 2 power distribution companies in Ukraine in 2015. Hackers sabotaged the managed systems, which forced workers to travel to substations to manually turn the power back on

## WannaCry Ransomware attack



**230,000** computers infected in over 150 countries within 24 hours. A ransomware crypto-worm, which targeted computers running the Microsoft Windows encrypting data and demanding ransom payments in the Bitcoin cryptocurrency

## Shamoon virus – Aramco and Saudi government



**35,000** computers partially wiped or totally destroyed at Aramco by a spear phishing email Shamoon, a spear phishing email containing a malicious link. It took Aramco 5 months to get its systems back online on a newly secured computer network. In Nov 2016, Shamoon 2 affected 15 private institutions and government agencies in KSA

## Cosmos Bank Hack



**10mn** Indian rupees stolen via 12,000 fraudulent transactions through ATMs over the weekend using 450 cloned cards in 28 countries. Criminals conducted extensive reconnaissance to understand the target's infrastructure well and leveraged a mix of known (and zero-day) malware. Exploited the internal and ATM systems using a 'man-in-the-middle' technique and self-approved fraudulent transactions

# In fact, globally there is a shortage of ~2.93M cybersecurity workers today

PRELIMINARY

Overview of the Global Information Security Workforce Study

- Online survey conducted every two years by the Center for Cyber Safety and Education and (ISC)<sup>2</sup>
- The survey aims at examining the state of the response to developing global cybersecurity risks and capabilities
- The 2018 edition of the survey gauged the opinions of 1,500 information security professionals



1 Assuming that the growth in the cybersecurity workers

Source: Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens, (ISC)<sup>2</sup> CYBERSECURITY WORKFORCE STUDY, 2018

# Contents

 Detailed next

- 1 THE NEED FOR CYBERSECURITY CAPABILITIES**
- 2 PROPOSED NATIONAL CYBERSECURITY CAPABILITY BUILDING FRAMEWORK**
- 3 BENCHMARK ANALYSIS OF GLOBAL CAPABILITY BUILDING INITIATIVES**
- 4 RECOMMENDED NATIONAL INITIATIVES**



# The US and Canada leverage the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework to identify and build cyber capabilities

PRELIMINARY



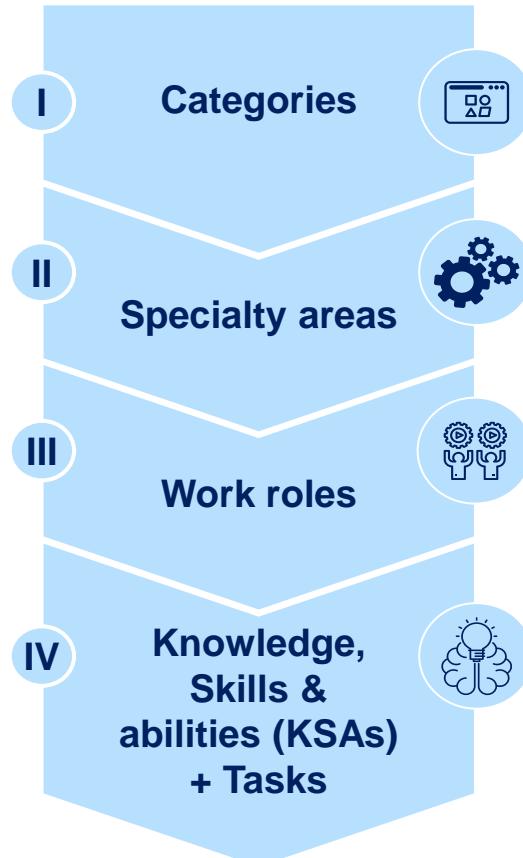
- We have identified the National Initiative for Cybersecurity Education (**NICE**) Cybersecurity Workforce Framework **developed by NIST** to be the most **comprehensive cyber capability building framework**
- The NICE Cybersecurity Workforce Framework is **employed by the US and Canadian governments**



## NICE cybersecurity workforce framework

### Framework elements

### Description



- There are **7 overarching categories** that act as framework pillars. These 7 categories are aligned to the **full cycle of a cybersecurity profession**, from protecting and managing digital assets to incident response and analysis
- There are **33 specialty areas** **Represent types of jobs** that exist in the cybersecurity sector (grouped by type of work and functions undertaken)
- Attributes required to perform jobs**, based on:
  - Requirement of knowledge, skills & abilities
  - Expectation of tasks to be carried about
- Helps **match employers and workers needs**
- KSAs and tasks define the attributes required to perform a work role:**
  - KSAs:** Attributes required to perform a job, generally demonstrated through relevant experience, education, or training
  - Tasks:** Outlines work required to be done to in a specific specialty area or work role

# I: The framework specifies 7 overarching categories of capabilities in cybersecurity

对外厳秘

Defining categories	Categories are the pillars of the NICE cybersecurity workforce framework that group types of jobs in a cybersecurity ecosystem					
1 	2 	3 	4 	5 	6 	7 
Operate and maintain	Securely Provision	Protect and Defend	Collect and operate	Investigate	Oversee and Govern	Analyze
<ul style="list-style-type: none"><li>Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security</li></ul>	<ul style="list-style-type: none"><li>Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development</li></ul>	<ul style="list-style-type: none"><li>Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks</li></ul>	<ul style="list-style-type: none"><li>Provides specialized denial and deception operations and collection of cyber-security information that may be used to develop intelligence</li></ul>	<ul style="list-style-type: none"><li>Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.</li></ul>	<ul style="list-style-type: none"><li>Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work</li></ul>	<ul style="list-style-type: none"><li>Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.</li></ul>

## II: Under the 7 overarching categories lie 33 different specialty areas

対外厳秘

Defining specialty areas		Specialty areas represent types of jobs within cybersecurity sector											
1		2		3		4		5		6		7	
Operate and maintain		Securely Provision		Protect and Defend		Collect and operate		Investigate		Oversee and Govern		Analyze	
Data administration		Risk management		Cybersecurity defense analysis		Cyber operations		Digital forensics		Cybersecurity management		Threat analysis	
Knowledge management		Software Development		Cyber incident response		Cyber Operational Planning		Cyber investigation		Legal Advice and Advocacy		Exploitation analysis	
Customer Service and Technical Support		Systems Architecture		Vulnerability assessment and management		Collection Operations				Training, Education, and Awareness		All-Source Analysis	
Network services		Technology R&D		Cyber Defense Infrastructure Support						Strategic Planning and Policy		Targets	
Systems analysis		Systems Requirements Planning								Executive Cyber Leadership		Language Analysis	
Systems Administration		Test and Evaluation								Program/Project Management (PMA) and Acquisition			
		Systems Development											

# III: Specialty areas translate into 52 different work roles

对外厳秘

Defining work roles		Specialty areas represent types of jobs within cybersecurity sector																		
1		Operate and maintain	2		Securely Provision	3		Protect and Defend	4		Collect and operate	5		Investigate	6		Oversee and Govern	7		Analyze
		<ul style="list-style-type: none"><li>Database Administrator</li><li>Data Analyst</li><li>Knowledge Manager</li><li>Technical Support Specialist</li><li>Network Operations Specialist</li><li>System Administrator</li><li>Systems Security Analyst</li></ul>		<ul style="list-style-type: none"><li>Authorizing Official</li><li>Security Control Assessor</li><li>Software Developer</li><li>Secure Software Assessor</li><li>Enterprise Architect</li><li>Security Architect</li><li>R&amp;D Specialist</li><li>Systems Req. Planner</li><li>System Testing and Evaluation Specialist</li><li>Information Systems Security Developer</li><li>Enterprise Architect</li></ul>		<ul style="list-style-type: none"><li>Cyber Defense Analyst</li><li>Cyber Defense Infrastructure Support Specialist</li><li>Cyber Defense Incident Responder</li><li>Vulnerability Assessment Analyst</li></ul>		<ul style="list-style-type: none"><li>Cyber Operator</li><li>Cyber Intel Planner</li><li>Cyber Ops Planner</li><li>Partner Integration Planner</li><li>All Source-Collection Manager</li><li>All Source-Collection Req. Manager</li></ul>		<ul style="list-style-type: none"><li>Cyber Crime Investigator</li><li>Law Enforcement/ Counter intelligence Forensics Analyst</li><li>Cyber Defense Forensics Analyst</li></ul>		<ul style="list-style-type: none"><li>Cyber Legal Advisor</li><li>Privacy Officer</li><li>Cyber Instructional Curriculum Developer</li><li>Cyber Instructor</li><li>Information Systems Security Manager</li><li>Communications Security Manager</li><li>Cyber Workforce Developer &amp; Manager</li><li>Cyber Policy and Strategy Planner</li><li>Executive Cyber Leadership</li><li>Program Manager</li><li>IT Project Manager</li><li>Product Support Manager</li><li>IT Investment/ Portfolio Manager</li><li>IT Program Auditor</li></ul>		<ul style="list-style-type: none"><li>Threat/Warning Analyst</li><li>Exploitation Analyst</li><li>All-Source Analyst</li><li>Mission Assessment Specialist</li><li>Target Developer</li><li>Target Network Analyst</li><li>Multi-Disciplined Language Analyst</li></ul>						

# 1: The “Operate and Manage” category consists of 7 work roles

対外厳密

Key role for Cyber

Category	Specialty area	Work Role	Work Role Description
Operate & maintain 	Data administration	Database Administrator	Administers databases and/or data management systems that allow for the secure storage, query, protection, and utilization of data
		Data Analyst	Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes
	Knowledge management	Knowledge Manager	Responsible for the management and administration of processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
	Customer Service and Technical Support	Technical Support Specialist	Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable)
	Network services	Network Operations Specialist	Plans, implements, and operates network services/systems, to include hardware and virtual environments
	Systems Administration	System Administrator	Responsible for setting up and maintaining a system or specific components of a system (e.g. for example, installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures)
	Systems Analysis	Systems Security Analyst	Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security

## 2: The “Securely provision” category consists of 11 work roles

対外厳密

Key role for Cyber

Category	Specialty area	Work Role	Work Role Description
Securely provision	Risk management	Authorizing Official/Designating Representative	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009).
		Security Control Assessor	Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).
	Software Development	Software Developer	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.
		Secure Software Assessor	Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.
	Systems Architecture	Enterprise Architect	Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.
		Security Architect	Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes.
	Technology R&D	Research & Development Specialist	Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems
	Systems Requirements Planning	Systems Requirements Planner	Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions
	Test and Evaluation	System Testing and Evaluation Specialist	Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results
	Systems Development	Information Systems Security Developer	Designs, develops, tests, and evaluates information system security throughout the systems development life cycle
		Enterprise Architect	Designs, develops, tests, and evaluates information systems throughout the systems development life cycle

### 3: The “Protect and Defend” category consists of 4 work roles

対外厳秘

Key role for Cyber

Category	Specialty area	Work Role	Work Role Description
 Protect and Defend	Cyber-security defense analysis	Cyber Defense Analyst	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats
	Cyber incident response	Cyber Défense Infrastructure Support Specialist	Tests, implements, deploys, maintains, and administers the infrastructure hardware and software
	Vulnerability assessment and management	Cyber Defense Incident Responder	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave
	Cyber Defense Infrastructure Support	Vulnerability Assessment Analyst	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities

# 4: The “Collect and Operate” category consists of 6 work roles

対外厳密

Key role for Cyber

Category	Specialty area	Work Role	Work Role Description
Collect and operate 	Cyber operations	Cyber Operator	Conducts collection, processing, and/or geolocation of systems to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executes on-net operations
	Cyber Operational Planning	Cyber Intel Planner	Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace
		Cyber Ops Planner	Develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions
		Partner Integration Planner	Works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions
Cyber Operational Planning	All Source-Collection Manager		Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan
	All Source-Collection Requirements Manager		Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations

# 5: The “Investigate” category consists of 3 work roles

対外厳密

Key role for Cyber

Category	Specialty area	Work Role	Work Role Description
Investigate 	Digital forensics	Cyber Crime Investigator	Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques
	Cyber investigation	Law Enforcement/Counter-intelligence Forensics Analyst	Conducts detailed investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents
		Cyber Defense Forensics Analyst	Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation

# 6: The “Oversee and Govern” category consists of 14 work roles

対外厳秘

Key role for Cyber

Category	Specialty area	Work Role	Work Role Description
Oversee and Govern 	Legal Advice and Advocacy	Cyber Legal Advisor	Provides legal advice and recommendations on relevant topics related to cyber law
		Privacy Officer/Compliance Manager	Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams
	Training, Education, and Awareness	Cyber Instructional Curriculum Developer	Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs
		Cyber Instructor	Develops and conducts training or education of personnel within cyber domain
	Cybersecurity management	Information Systems Security Manager	Responsible for the cybersecurity of a program, organization, system, or enclave
		Communications Security (COMSEC) Manager	Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009) or key custodian for a Crypto Key Management System (CKMS)
	Strategic Planning and Policy	Cyber Workforce Developer and Manager	Develops cyberspace workforce plans, strategies, and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements
	Cyber Workforce Developer & Manager	Cyber Policy and Strategy Planner	Develops and maintains cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance
	Executive Cyber Leadership	Executive Cyber Leadership	Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations
	Program/Project Management (PMA) and Acquisition	Program Manager	Leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with agency or enterprise priorities
		IT Project Manager	Directly manages information technology projects
		Product Support Manager	Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components
		IT Investment/Portfolio Manager	Manages a portfolio of IT investments that align with the overall needs of mission and enterprise priorities
		IT Program Auditor	Conducts evaluations of an IT program or its individual components to determine compliance with published standards

# 7: The “Analyze” category consists of 7 work roles

对外厳密

Key role for Cyber

Category	Specialty area	Work Role	Work Role Description
Analyze	Threat analysis	Threat/Warning Analyst	Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber threat/warning assessments
	Exploitation analysis	Exploitation Analyst	Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks
	All-Source Analysis	All-Source Analyst	Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations
		Mission Assessment Specialist	Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness
Targets		Target Developer	Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation
		Target Network Analyst	Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks, and the applications on them
Language Analysis		Multi-Disciplined Language Analyst	Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates and maintains language-specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects

# IV: The NICE Cybersecurity Workforce Framework clearly specifies the tasks as well as the knowledge, skills, and abilities (KSAs) required to perform each work role

ILLUSTRATIVE

Defining work roles

Specialty areas represent types of jobs within cybersecurity sector

## NICE cybersecurity workforce framework Components for each work role

- For each of the 52 work roles across 7 categories, the NICE cybersecurity workforce framework defines the following:
- Tasks:** Specific defined piece of work that, combined with other identified Tasks, composes the work in a specific specialty area or work role
- Knowledge:** Body of information applied directly to the performance of a function.
- Skills:** Skills needed for cybersecurity rely on applying tools, frameworks, processes and controls that have an impact on the cybersecurity posture of an organization or individual
- Abilities:** Competence to perform a behavior that results in an observable product

## Sample Work role specifications<sup>1</sup>

<b>Work Role Name</b>	Cyber Operator
<b>Work Role ID</b>	CO-OPS-001
<b>Specialty Area</b>	Cyber Operations (OPS)
<b>Category</b>	Collect and Operate (CO)
<b>Work Role Description</b>	Conducts collection, processing, and/or geolocation of systems to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executing on-net operations.
<b>Tasks</b>	T0566, T0567, T0598, T0609, T0610, T0612, T0616, T0618, T0619, T0620, T0623, T0643, T0644, T0664, T0677, T0696, T0697, T0724, T0740, T0756, T0768, T0774, T0796, T0804, T0828, T0829
<b>Knowledge</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0021, K0051, K0109, K0142, K0224, K0363, K0372, K0373, K0375, K0379, K0403, K0406, K0420, K0423, K0428, K0427, K0429, K0430, K0433, K0438, K0440, K0452, K0468, K0481, K0485, K0486, K0480, K0516, K0528, K0530, K0531, K0536, K0560, K0565, K0573, K0608, K0609
<b>Skills</b>	S0062, S0183, S0236, S0182, S0190, S0192, S0202, S0206, S0221, S0242, S0243, S0252, S0255, S0257, S0266, S0267, S0270, S0275, S0276, S0281, S0282, S0293, S0295, S0298, S0299, S0363
<b>Abilities</b>	A0095, A0097, A0099, A0100

1 Refer to the NICE cybersecurity workforce framework for detailed list of Tasks, Knowledge, Skills, and Abilities for all work roles

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# Countries could leverage the NICE cybersecurity workforce framework to build comprehensive cybersecurity capabilities and a common lexicon for cybers roles

PRELIMINARY

Framework elements	Uses
Categories and Specialty areas	<p><b>1 Guidelines for the national capability building program:</b> The specialty areas can be used to build comprehensive cyber security capabilities across whole value chain of cybersecurity ecosystem</p>
Work roles	<p><b>2 Build common lexicon:</b> Publish and promote a framework to enable clearer communication between cybersecurity educators, trainers/certifiers, employers, and employees</p>
Knowledge, Skills & abilities (KSAs) + Tasks	<p><b>3 Provide guidance</b> to public and private sector entities on <b>roles, responsibilities and proficiencies</b> required for cyber security roles including:</p> <ul style="list-style-type: none"><li>– <b>Perform criticality analysis:</b> Identifying knowledge, skills and abilities, and tasks required to successfully build national capabilities</li><li>– <b>Perform proficiency analysis:</b> Assessing types of candidates required (entry-level, experienced, etc.) based on capability assessment and critical analysis exercises</li></ul>

# Contents

 Detailed next

- 1 THE NEED FOR CYBERSECURITY CAPABILITIES**
- 2 PROPOSED NATIONAL CYBERSECURITY CAPABILITY BUILDING FRAMEWORK**
- 3 BENCHMARK ANALYSIS OF GLOBAL CAPABILITY BUILDING INITIATIVES**
- 4 RECOMMENDED NATIONAL INITIATIVES**



# In benchmark countries, national cyber security capability building programs are typically delivered through 3 channels

对外厳秘

PRELIMINARY



Training channel	Benchmark example	Benchmark example
1 Central coordinating body	<ul style="list-style-type: none"><li>CSA developed a new academy to <b>train cybersecurity professionals in government and CII sectors</b> in partnership industry players</li><li>Working to establish an online school and a research institute for <b>cyber studies</b></li></ul>	Singapore – CSA Academy
2 Formal education institutions	<ul style="list-style-type: none"><li>Estonian Information Technology College opened a new curricula, <b>Cyber Security Engineering</b>, which is designed to provide broad-based higher education in the area of cyber security engineering</li><li><b>More than 15 universities</b> in the UK offer cybersecurity degrees that have been <b>certified by the NCSC</b></li></ul>	Israel – National Cyber Bureau online school
3 Private sector training providers	<ul style="list-style-type: none"><li>SANS is the world's <b>largest and most trusted source for cyber security training</b>, certification and research</li><li>COMAT, offers <b>end-to-end cyber security training</b> in Singapore and information security certification that caters to all levels of employment</li></ul>	United States – SANS Singapore – COMAT training

Source: Benchmark analysis, team analysis

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# Summary of Game changing initiatives in benchmark countries

对外厳秘

PRELIMINARY

Training channel	Description	Benchmark countries
Central coordinating body 	<ul style="list-style-type: none"><li>Develop a cybersecurity scheme that develops a core of cybersecurity specialists to be deployed across agencies</li><li>Build an academy to train cybersecurity professionals in government and CII sectors in partnership industry players</li><li>Create international partnerships to build capabilities in cooperation with other countries through knowledge sharing and cross-training</li><li>Develop a one-stop shop for cybersecurity careers and studies that connects the public with information on cybersecurity awareness, degree programs, training, careers, and talent management</li><li>Encourage the next generation of cyber professionals by creating competitions and hackathons targeted at high school and elementary school students</li></ul>	 CSA Cybersecurity Professional Scheme  CSA Academy  Cybersecurity online school  CSA – UK MOC  Cybersecurity Career Mentoring Program  Federal Virtual Training Environment  CyberFirst  Nuti Labor
Formal education institutions 	<ul style="list-style-type: none"><li>Develop degrees dedicated to cybersecurity designed to provide higher education in the area of cybersecurity engineering by integrating the software development and information system administration</li></ul>	 TALtech cybersecurity engineering degree
Private sector training providers 	<ul style="list-style-type: none"><li>The NCSC accredits a large number of training providers and is working on setting up a Cybersecurity council that creates a collaboration between private and public sector entities and academia to unify cybersecurity certifications</li></ul>	 NCSC accreditations

Source: Team analysis

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# Benchmark analysis of cybersecurity capability building initiatives

対外厳秘

PRELIMINARY

A



Singapore

B



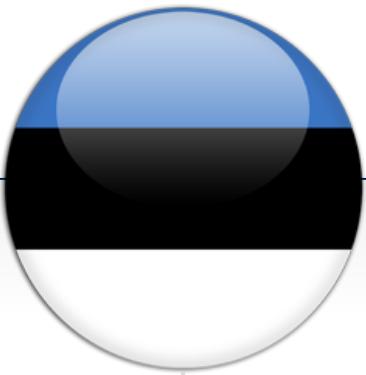
US

C



UK

D



Estonia

E



Israel

# A: Benchmark analysis of capability building initiatives in Singapore



对外厳秘

PRELIMINARY

Training channel	Name of organization	Initiative	Description of initiative
Central coordinating body		Cybersecurity Professional Scheme	<ul style="list-style-type: none"><li>CSA has implemented a Cybersecurity Professional Scheme to <b>groom skilled cybersecurity manpower for the public sector</b></li></ul>
		CSA academy	<ul style="list-style-type: none"><li>CSA developed a new academy to <b>train cybersecurity professionals in government and CII sectors</b> in partnership industry players</li><li>The Academy <b>provides intermediate to advanced, niche training to cyber defenders</b> in the government, and also invites selected parties in the CII sectors to join in the training through FireEye, its first training partner</li></ul>
		MoC with UK	<ul style="list-style-type: none"><li>Singapore and the United Kingdom signed a <b>Memorandum of Cooperation (MoC) on Cybersecurity Capacity Building</b></li><li>The MoC <b>builds on and extends</b> the close cooperation already existing between the two countries under the Memorandum of Understanding (<b>MoU on Cybersecurity Cooperation</b>, signed between the Cyber Security Agency of Singapore (CSA) and the UK Cabinet Office in 2015)</li><li>The present MoC will see both countries cooperating to <b>deliver cybersecurity capacity building programmes to Commonwealth Member States for a two-year period</b> beginning September 2018, and in addition, the UK will also actively participate in Singapore's ASEAN Cyber Capacity Programme that was launched in 2016</li></ul>
		DOI with US	<ul style="list-style-type: none"><li>Singapore and US signed a Declaration of Intent (<b>DOI</b>) to collaborate on a <b>Singapore-US Cybersecurity Technical Assistance Program for ASEAN Member States</b></li><li>The DOI aims to deliver cybersecurity <b>training workshops for government employees</b> and key industry partners across South East Asia</li></ul>

Source: csa.gov.sg, mfa.gov.sg, press search

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# A: Benchmark analysis of capability building initiatives in Singapore



对外厳秘

PRELIMINARY

Training channel	Name of organization	Initiative	Description of initiative
Central coordinating body		Cybersecurity Centre of Excellence	<ul style="list-style-type: none"><li>Deputy Prime Minister Teo Chee Hean Announced at the third annual Singapore International Cyber Week, Singapore will set up an Asean-Singapore Cybersecurity Centre of Excellence to <b>strengthen ASEAN members' cyber strategy development, legislation and research capabilities</b></li><li>The centre will also <b>train national Computer Emergency Response Teams (Certs) in the region</b>, and promote Cert-to-Cert open-source information sharing</li></ul>
		National Cyber-security Postgraduate Scholarship	<ul style="list-style-type: none"><li>National Cybersecurity Postgraduate Scholarship (NCPS) is jointly offered by NRF and IMDA under NCR, a prestigious <b>scholarship for graduates and working professionals</b> who are keen to contribute and commit to the protection of Singapore's cyberspace</li><li>Applicants may pursue their <b>Masters and/or Doctoral degrees</b></li></ul>
Formal education institutions		Computer and information security degrees	<ul style="list-style-type: none"><li><b>6 institutions in Singapore offer computer and information security degrees:</b><ul style="list-style-type: none"><li>National University of Singapore</li><li>Singapore University of Technology and Design</li><li>SMF Institute of Higher Learning</li><li>Nanyang Polytechnic</li><li>Ngee Ann Polytechnic</li><li>Temasek Polytechnic</li></ul></li></ul>

Source: csa.gov.sg, mfa.gov.sg, press search

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# A: Benchmark analysis of capability building initiatives in Singapore



对外厳秘

PRELIMINARY

Training channel	Name of organization	Initiative	Description of initiative
Private sector training providers		MoU with CSA	<ul style="list-style-type: none"><li>Singapore Telecommunications Limited (Singtel) and the Cyber Security Agency of Singapore (CSA) signed a Memorandum of <b>Understanding (MOU) to develop and strengthen Singapore's cyber security capabilities</b> Under the MOU, Singtel and CSA will <b>cooperate</b> in three areas:<ul style="list-style-type: none"><li><b>Build up local capabilities and deliver advanced cyber security services</b> and;</li><li>Develop industry's cyber security <b>talent capabilities and capacity</b> to meet fast growing demand, and</li><li>Develop <b>indigenous research and development</b> (R &amp; D), including joint R &amp; D with institutes of higher learning and research institutes</li></ul></li></ul>
		MoU with CSA	<ul style="list-style-type: none"><li>ISACA and CSA have signed a memorandum of understanding (MOU) to <b>jointly enhance Singapore's cyber security capabilities and workforce, using ISACA-developed training, assessment tools and certification</b></li><li>MOU formalizes the collaboration between the two parties through an initial three-year period. <b>ISACA is a leading professional body with members in 188 countries</b></li></ul>
		Cybersecurity Career Mentoring Programme	<ul style="list-style-type: none"><li>Cybersecurity Career Mentoring Programme is a joint initiative by the CSA and SCS, and supported by the Association of Information Security Professionals</li><li>The programme aims to provide a <b>platform for students and professionals to receive career guidance and support</b> from experienced cybersecurity mentors and industry experts, through activities such as talks and panel discussions</li></ul>

# A: Benchmark analysis of capability building initiatives in Singapore



对外厳秘

PRELIMINARY

Training channel	Name of organization	Initiative	Description of initiative
Private sector training providers	<b>EC-Council</b> Hackers are here. Where are you?	Computer security courses	<ul style="list-style-type: none"><li>EC-Council (International Council of Electronic Commerce Consultants) is the <b>world leader in IT Security Courses</b> – Information Security, Network Security, Computer Security and Internet Security Certification and Training</li><li>EC-Council <b>organizes sessions on various topics of information security</b> pertaining to certified ethical hacking Singapore, pen testing, basic system security, internet security etc across various locations</li></ul>
	<b>COMAT</b>	End-to-end training	<ul style="list-style-type: none"><li>COMAT, a division under ST Electronics (e-Services) offers <b>end-to-end cyber security training</b> in Singapore and <b>information security certification that caters to all levels of employment</b></li><li>COMAT has developed an <b>eco-system to help organizations build capability and capacity</b> in cybersecurity, to make IT security courses in Singapore relevant to business management, which focuses on 3 main areas:<ul style="list-style-type: none"><li><b>Partner network</b></li><li><b>Training and certification programs</b></li><li><b>Performance support system</b></li></ul></li></ul>

Source: csa.gov.sg, mfa.gov.sg, press search

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。



# APCERT was established in 2003, formally known as APSIRC, to strengthen CERT network across Asia Pacific region

## Overview



APSIRC (Asia Pacific Security Incident Response Coordination) change name to **APCERT in February 2003**. Asia Pacific Incident Response Teams propose the establishment of a group called **Asia Pacific CERT (APCERT)**. APCERT would have an operational focus and be open to all suitably qualified CERTs and CSIRTS in the Asia Pacific region.

## Mission & Vision

**APCERT will maintain a trusted contact network of computer security experts in the Asia Pacific region to improve the region's awareness and competency in relation to computer security incidents through:**

- Enhancing Asia Pacific regional and international cooperation on information security
- Jointly developing measures to deal with large-scale or regional network security incidents
- Facilitating information sharing and technology exchange, including information security, computer virus and malicious code among its members
- Promoting collaborative research and development on subjects of interest to its members
- Assisting other CERTs and CSIRTS in the region to conduct efficient and effective computer emergency response
- Providing inputs and/or recommendations to help address legal issues related to information security and emergency response across regional boundaries

## ASEAN members



LaoCERT



MNCERT/CC, MonCIRT



ThaiCERT



CERT-PH



SingCERT



CyberSecurity Malaysia



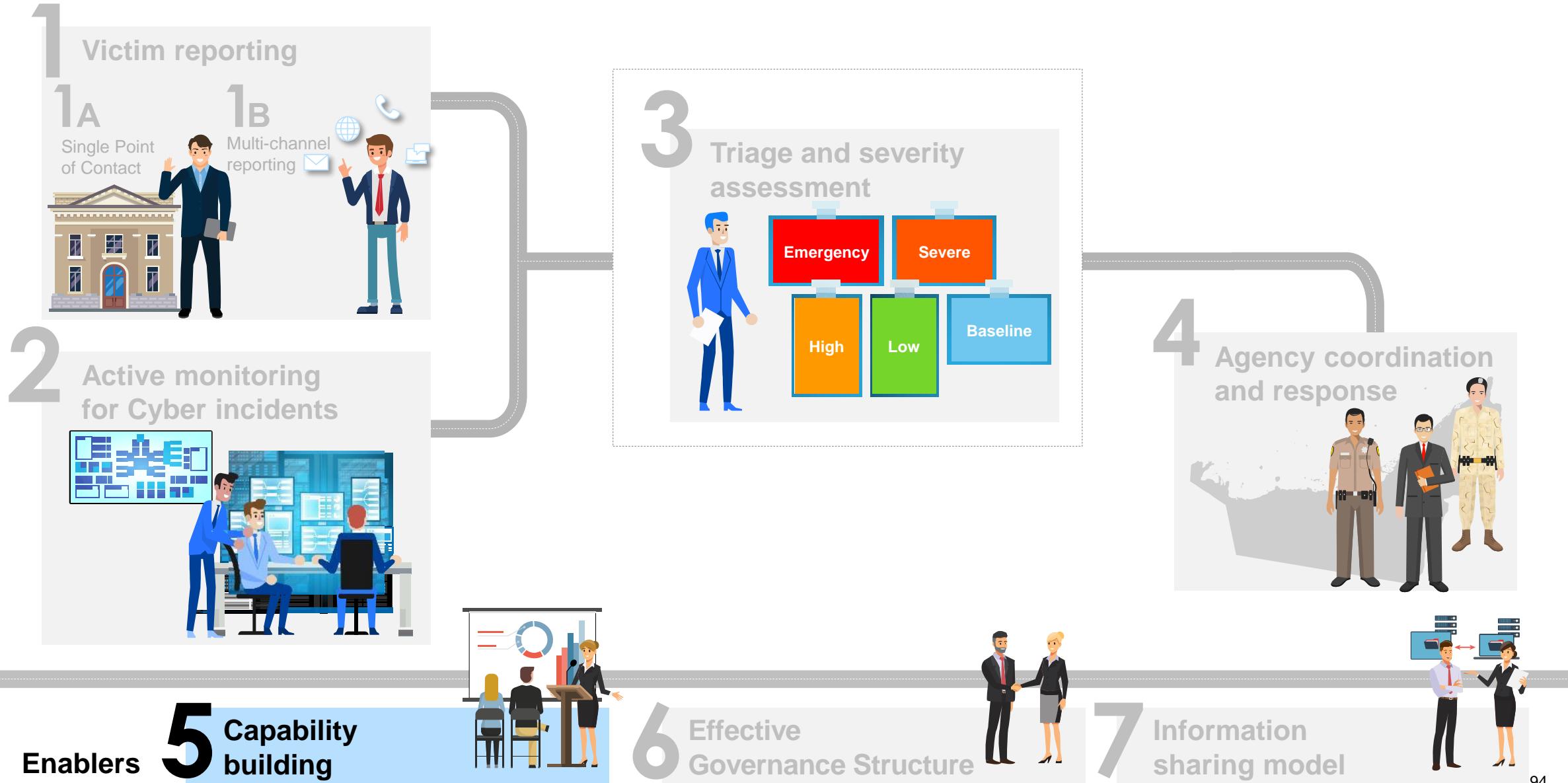
VNCERT/CC



ID-CERT / ID-SIRTII/CC

**(Total 33 Teams / 23 Economies)**

# Proposed national incident response and recovery framework



# 5: The NICE Workforce Framework highlights capabilities that are required across the value chain of incident response

	We benchmarked <b>models of cyber capability building programs</b> and identified the <b>NICE Workforce Framework</b> to be the <b>most comprehensive</b>
	Created by <b>NIST</b> , the NICE Workforce framework is employed by the <b>DHS</b> and the <b>US Government</b>
 National Institute of Standards and Technology U.S. Department of Commerce	

Categories	Descriptions	Attack lifecycle	Capabilities relevant to incident response
<b>Securely Provision (SP)</b>	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.	Pre-attack	<ul style="list-style-type: none"> <li>• Cyber Defense Analysis</li> <li>• Cyber Defense Infrastructure Support</li> <li>• Vulnerability Assessment and Management</li> <li>• Exploitation Analysis</li> <li>• All-Source Analysis</li> <li>• Cyber Operational Planning</li> </ul>
<b>Operate and Maintain (OM)</b>	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.		
<b>Oversee and Govern (OV)</b>	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.		
<b>Protect and Defend (PR)</b>	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks		
<b>Analyze (AN)</b>	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.	During attack	<ul style="list-style-type: none"> <li>• Incident Response</li> <li>• Cyber Operations</li> </ul>
<b>Collect and Operate (CO)</b>	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.		
<b>Investigate (IN)</b>	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.	Post-attack	<ul style="list-style-type: none"> <li>• Cyber Investigation</li> <li>• Digital Forensics</li> <li>• Threat Analysis</li> </ul>

# 5: Throughout the lifecycle of incident response, different skillsets are required across multiple stakeholders in the ecosystem (1/3)

对外厳密

PRELIMINARY

	<b>Capability</b>	<b>Description</b>	<b>Sample certification courses</b>
1. Pre-attack	<b>Cyber Defense Analysis</b>	Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network to protect information, information systems, and networks from threats	<ul style="list-style-type: none"><li>• Cyber Defense Analysis Certificate of Mastery</li><li>• Certified Security Analyst Training</li></ul>
	<b>Cyber Defense Infrastructure Support</b>	Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.	<ul style="list-style-type: none"><li>• Certified Network Defender (CND) Certification Training</li><li>• Cisco Certified Network Associate (CCNA) Security</li><li>• Computer Network and Defense Fundamentals</li></ul>
	<b>Vulnerability Assessment and Management</b>	Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations	<ul style="list-style-type: none"><li>• Android Security Vulnerabilities, Testing, and Enterprise Considerations</li><li>• CompTIA Cybersecurity Analyst (CSA+)</li><li>• Applied Wireless Network Security</li></ul>
	<b>Exploitation Analysis</b>	Analyzes collected information to identify vulnerabilities and potential for exploitation.	<ul style="list-style-type: none"><li>• Cyber Threat Counter Exploitation</li><li>• Exploit Development</li></ul>

SOURCE: Press search, benchmark analysis, team analysis, NICCS

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# 5: Throughout the lifecycle of incident response, different skillsets are required across multiple stakeholders in the ecosystem (2/3)

对外厳密

PRELIMINARY

	<b>Capability</b>	<b>Description</b>	<b>Sample certification courses</b>
1. Pre-attack	All-Source Analysis	Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications	<ul style="list-style-type: none"><li>Certified Cyber Threat Intelligence Analyst</li><li>Certified Expert Fusion Analyst (CEFA)</li></ul>
	Cyber Operational Planning	Performs in-depth joint targeting and cybersecurity planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.	<ul style="list-style-type: none"><li>Cyber Warfare for Management</li><li>Cyber Operations and Planning</li></ul>
2. During attack	Incident Response	Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities	<ul style="list-style-type: none"><li>CyberSec First Responder: Threat Detection and Response</li><li>Business Continuity and Disaster Recovery</li><li>Behavioral Malware Analysis</li><li>Certified Disaster Recovery Engineer</li><li>Cyber Incident Analysis &amp; Response</li></ul>
	Cyber Operations	Performs activities to gather evidence on criminal or foreign intelligence entities to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.	<ul style="list-style-type: none"><li>Certificate in Cyber Operations</li><li>(ISC)<sup>2</sup> Certified Information Systems Security Professional (CISSP)</li><li>(ISC)<sup>2</sup> Systems Security Certified Practitioner (SSCP)</li><li>Cyber Warfare for Practitioners</li><li>CyberSAFE</li></ul>

SOURCE: Press search, benchmark analysis, team analysis, NICCS

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# 5: Throughout the lifecycle of incident response, different skillsets are required across multiple stakeholders in the ecosystem (3/3)

对外厳密

PRELIMINARY

Capability	Description	Sample certification courses
<b>3. Post attack</b>	<b>Cyber investigation</b>  Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering	<ul style="list-style-type: none"><li>• Intrusion Detection In-Depth: Compliance, Security, Forensics and Troubleshooting</li><li>• Attack Vectors and Mitigations</li><li>• Basics of Fraud Investigations</li></ul>
<b>Digital forensics</b>	Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.	<ul style="list-style-type: none"><li>• Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response</li><li>• Computer Hacking Forensic Investigator (CHFI)</li><li>• Root Cause Analysis</li></ul>
<b>Threat Analysis</b>	Identifies and assesses the capabilities and activities of cybersecurity criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities	<ul style="list-style-type: none"><li>• Certified Cyber Threat Intelligence Analyst</li><li>• Emerging Threats &amp; defenses</li><li>• Malware Analysis/Reverse Engineering</li></ul>

SOURCE: Press search, benchmark analysis, team analysis, NICCS

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# 5 - Case: The US-CERT and NCCIC adopts the NICE framework and accredits providers to offer these classes

対外厳秘



Government accreditation and cooperation helps the US create a robust capability building program



- The NICCS Education and Training Catalog offers more than 3,000 cybersecurity-related courses from over 125 different providers
- The NICCS Supervisory Office sets vetting criteria to ensure quality of accredited courses
- For government employees, the DHS manages a Federal Virtual Training Environment (FedVTE) for online, on-demand cybersecurity training
- The DHS and NSA jointly sponsor the National Centers of Academic Excellence (CAE) program to develop capabilities

Attack lifecycle	Capability relevant to incident response	Sample certification courses	Sample providers
Pre-attack	Cyber Operational Planning	<ul style="list-style-type: none"><li>Cyber Warfare for Management</li><li>Cyber Operations and Planning</li></ul>	<ul style="list-style-type: none"><li>Phoenix TS</li><li>Lunarline Inc</li></ul>
	Cyber Defense Analysis	<ul style="list-style-type: none"><li>Cyber Defense Analysis Certificate of Mastery</li><li>Certified Security Analyst Training</li></ul>	<ul style="list-style-type: none"><li>Security University</li><li>CyberTraining365</li></ul>
	Vulnerability Assessment and Management	<ul style="list-style-type: none"><li>Android Security Vulnerabilities, Testing, and Enterprise Considerations</li><li>CompTIA Cybersecurity Analyst (CSA+)</li><li>Applied Wireless Network Security</li></ul>	<ul style="list-style-type: none"><li>Skillsoft</li><li>University of Virginia - School of Continuing &amp; Professional Studies</li></ul>
During attack	Incident Response	<ul style="list-style-type: none"><li>CyberSec First Responder: Threat Detection and Response</li><li>Behavioral Malware Analysis</li><li>Cyber Incident Analysis &amp; Response</li></ul>	<ul style="list-style-type: none"><li>Logical operations</li><li>Systems IT, Inc.</li><li>Focal Point Academy</li></ul>
	Cyber Operations	<ul style="list-style-type: none"><li>(ISC)2 Systems Security Certified Practitioner (SSCP)</li><li>Cyber Operations Analyst</li><li>Cyber Warfare for Practitioners</li></ul>	<ul style="list-style-type: none"><li>UMBC training center</li><li>LeapFox Learning</li></ul>
Post-attack	Cyber Investigation	<ul style="list-style-type: none"><li>Attack Vectors and Mitigations</li><li>Basics of Fraud Investigations</li></ul>	<ul style="list-style-type: none"><li>Merritt college</li><li>Skillsoft</li></ul>
	Digital Forensics	<ul style="list-style-type: none"><li>Computer Hacking Forensic Investigator (CHFI)</li><li>Root Cause Analysis</li></ul>	<ul style="list-style-type: none"><li>SANS Institute</li><li>Federal Virtual Training Environment (FedVTE)</li></ul>

SOURCE: Press search, Expert interview

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# 5 - Case: ENISA creates a series of trainings to build capabilities for CERTs across Europe, which maps across the NICE Framework

対外厳密



## ENISA Creating capabilities for CERTS all across Europe



- European Network and Information Security Agency (ENISA) was founded in 2005 as a **center of network and information security expertise for the EU**
- ENISA actively promotes **cybersecurity capability building** across **all CERTs in Europe**. Beyond conducting trainings courses, it has also proposed activities such as:
  - Provide **certification paths** for cyber capabilities
  - Conduct '**Fire Drills**' for the CERT community
  - Establish **ENISA CERT Training Hubs (ECTH)**

Attack lifecycle	NICE capabilities for incident response	Sample ENISA courses <sup>1</sup>
Pre-attack	Cyber Operational Planning	<ul style="list-style-type: none"><li>• Processing and storing artefacts</li><li>• Social networks used as an attack vector for targeted attacks</li></ul>
	Cyber Defense Analysis	<ul style="list-style-type: none"><li>• Building artefact handling and analysis environment</li><li>• Using indicators to enhance defense capabilities</li></ul>
	Vulnerability Assessment and Management	<ul style="list-style-type: none"><li>• Vulnerability handling</li><li>• Common framework for artefact analysis activities</li></ul>
During attack	Incident Response	<ul style="list-style-type: none"><li>• Incident handling during an attack on Critical Information Infrastructure</li><li>• Incident Handling Management</li><li>• Automation in incident handling</li></ul>
	Cyber Operations	<ul style="list-style-type: none"><li>• Advanced Persistent Threat incident handling</li><li>• Developing CSIRT infrastructure</li><li>• CERT participation in incident handling related to the Article 13a obligations</li></ul>
Post-attack	Cyber Investigation	<ul style="list-style-type: none"><li>• Cooperation with Law Enforcement Agencies - Advising in Cyber Crime Cases</li></ul>
	Digital Forensics	<ul style="list-style-type: none"><li>• Network forensics</li><li>• Forensic analysis: Webserver Analysis New</li></ul>

<sup>1</sup> ENISA organizes their courses according to Technical, Operational, CSIRT building, and Legal and Cooperation capabilities

SOURCE: Press search, benchmark analysis

# 5: Key learnings from capability building programs in benchmarked countries

対外厳密



## Key learnings from best in class countries

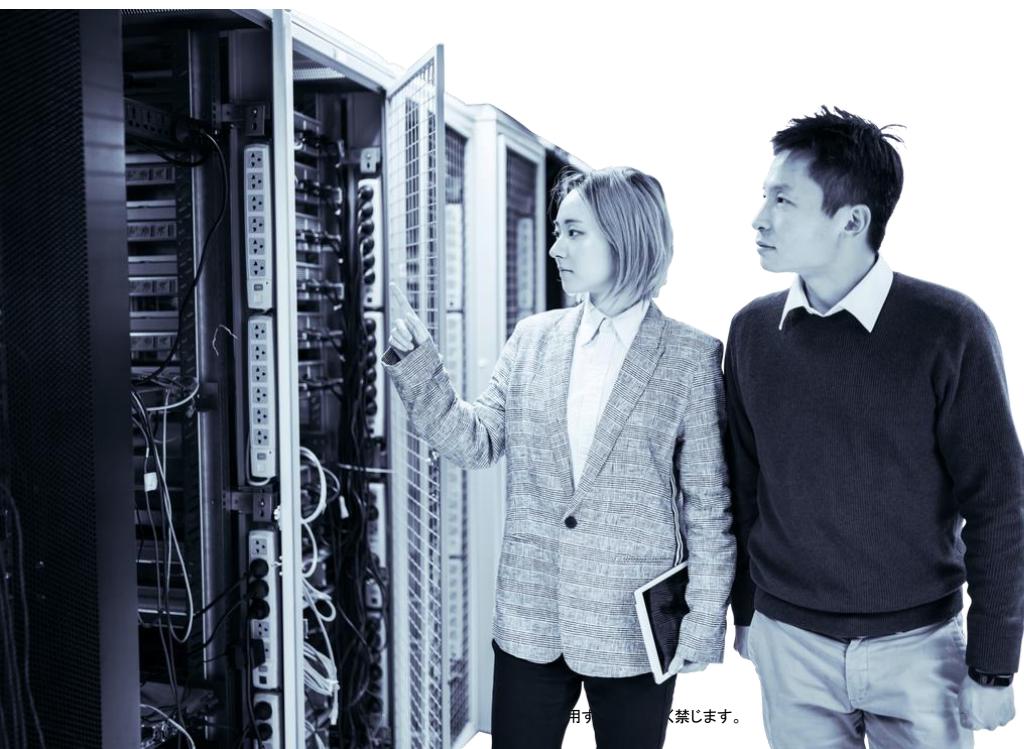
- A** The **NICE framework** provides a **comprehensive methodology** for **national capability building in incident response**
- B** Capability building programs can be **delivered** in a **centralized, targeted way** (e.g. ENISA to CERTS), or be **broad-based** and customizable to each organizations need (e.g. UK, US)

---

# Questions?

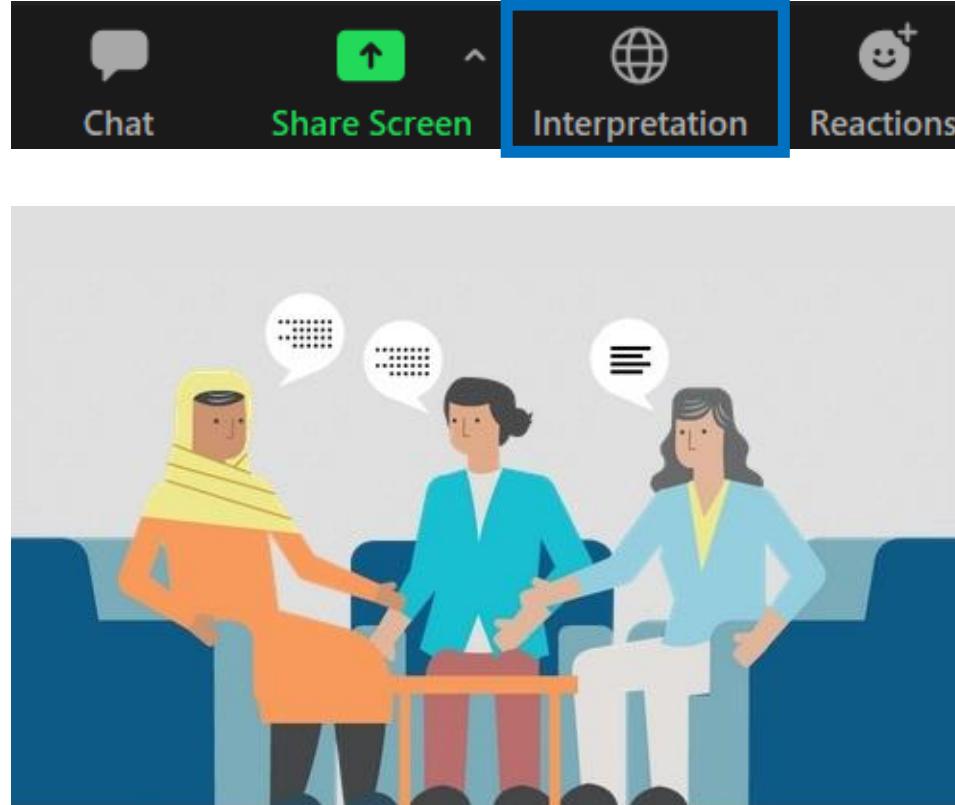
---



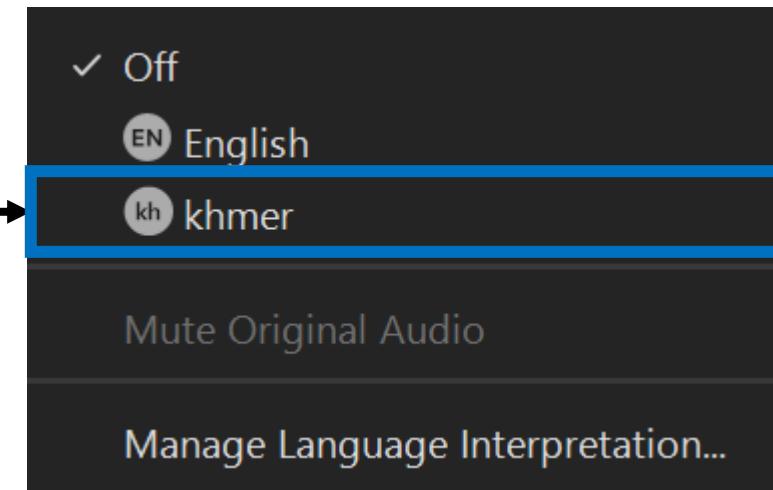
- 
1. Overview of Cyber Security Trend
  2. Definition of Cyber threat and national Incident response framework
  3. Cyber Security Regulation framework
  4. Partnership(Public, Private, Academia, International)
  5. Professional training and certification
  - 6. Public awareness and alerts**
  7. Cyber Security for SME
  8. Critical Infrastructure Industry protection
  9. CERT/ Resilience
  10. Wrap up / Cyber security assessment

# Khmer simultaneous Interpretation available

Select “Interpretation” on the bottom



Select “Khmer”



- Presentation is simultaneously translated into Khmer
- You can post question in Khmer



## Timeline

## Overview

100 minuets

## Workshop & QA

20 minuets

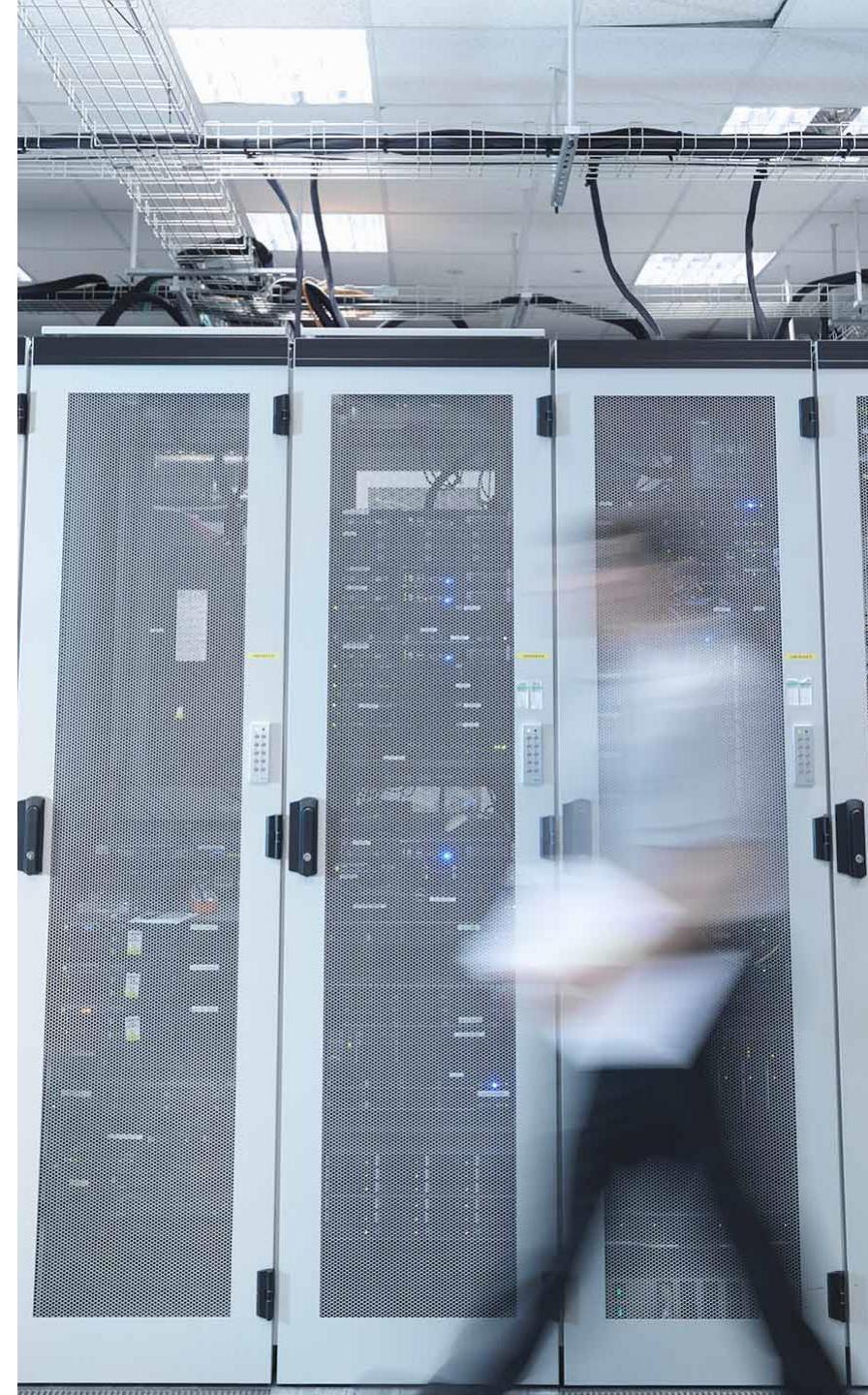
# Cambodia need to design Cyber security strategy with suggested strategy element

Cybersecurity strategy element	Insights from benchmarking cybersecurity strategy	#
A Governance 	<ul style="list-style-type: none"> <li>Top-performing nations are moving towards <b>centralized governance bodies</b> reporting directly to executive branches of government and serving as <b>E2E owners of cybersecurity strategy implementation</b></li> </ul>	• #2
B Legal and regulations 	<ul style="list-style-type: none"> <li><b>Comprehensive legislative frameworks</b> cover mandatory IT security standards, regulations, and best practices, and are enforced through audits and law enforcement</li> <li><b>Specific legislations to address emerging technologies</b> are evolving at fast pace in countries with advanced cybersecurity legislations</li> </ul>	• #3
E Partnerships 	<ul style="list-style-type: none"> <li><b>Regional and international partnerships</b> are actively used to foster sharing of best practices and enhancing operational and technical capabilities through joint drills &amp; audits</li> </ul>	• #4
C Talent and people 	<ul style="list-style-type: none"> <li><b>Public awareness and training</b> programs, which draw on <b>international standards and offerings</b>, form the basis for cybersecurity talent development</li> </ul>	• #5~7
F Critical infrastructure 	<ul style="list-style-type: none"> <li>CII protection programs, executed by national cybersecurity agencies, focus <b>selectively on critical assets</b> in critical sectors with timely involvement of relevant authorities</li> </ul>	• #8
D Incident response 	<ul style="list-style-type: none"> <li>National cybersecurity agencies, through <b>specialized incident response teams</b>, lead integrated response efforts with close coordination with impacted assets</li> </ul>	• #9

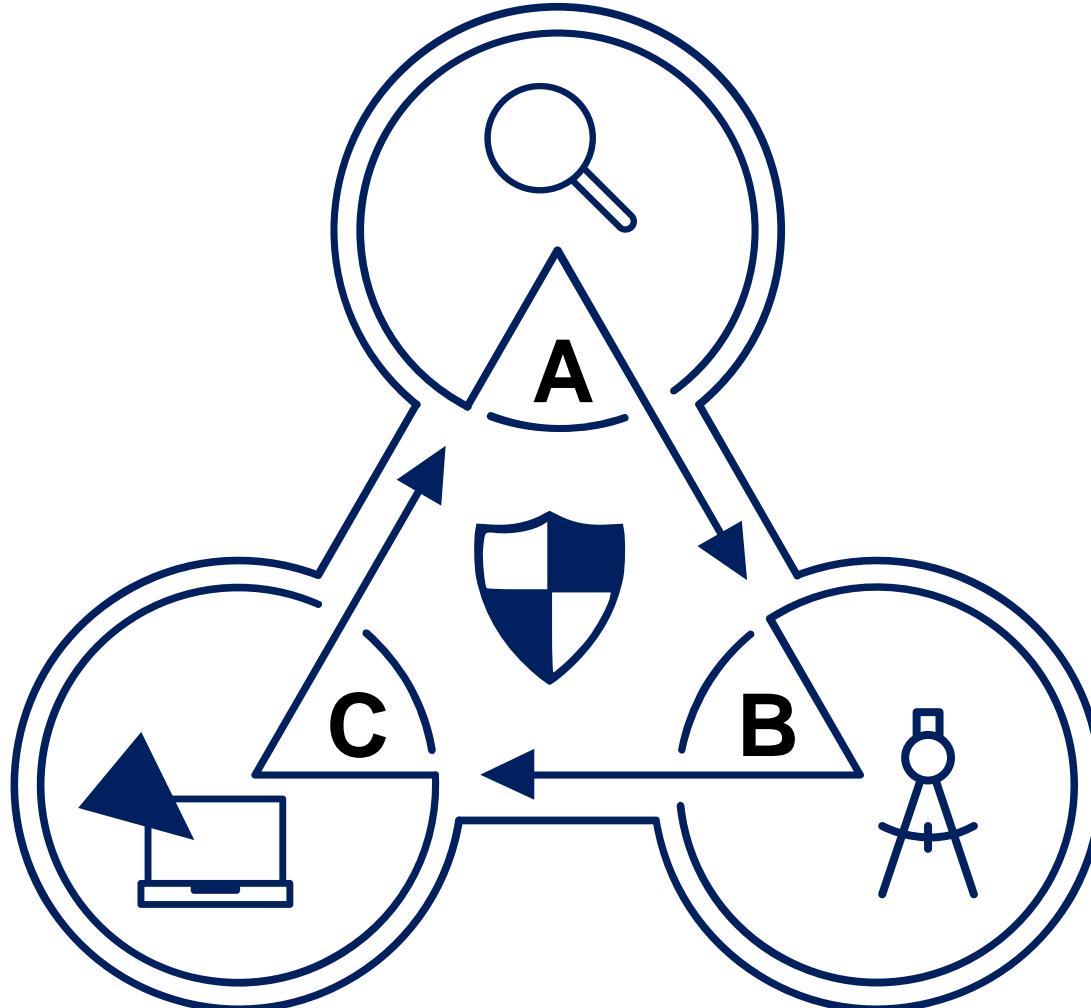
“ ”

**...The weakest link in the security chain is the human element...**

Kevin Mitnick, Computer Security Author and Hacker



In order to promote better cybersecurity awareness, we have developed a National cyber security awareness program using a 3 step approach



- A** Identify high priority cyber security topics, based on attack trends and benchmark analysis
- B** Design a National cyber security awareness program using McKinsey's Influence Model
- C** Launch prioritized initiatives track progress

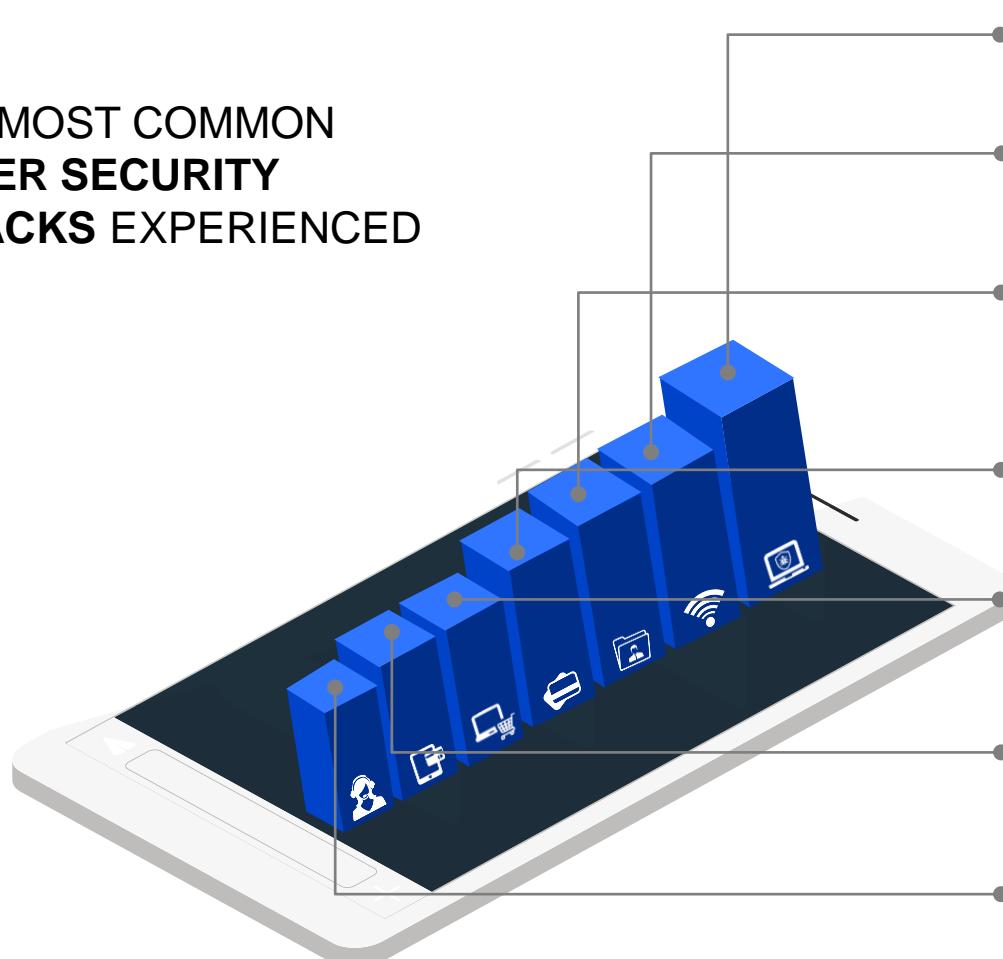
In order to promote better cybersecurity awareness, we have developed a National cyber security awareness program using a 3 step approach



- A** Identify high priority cyber security topics, based on attack trends and benchmark analysis
- B** Design a National cyber security awareness program using McKinsey's Influence Model
- C** Launch prioritized initiatives track progress

# A: Cybercrime victims experience a variety of different cyber security attacks, which should be addressed by the cyber awareness programs

## THE MOST COMMON CYBER SECURITY ATTACKS EXPERIENCED



Topic to be addressed	
Devices infected by malware	Mobile and computer devices
Home Wi-Fi cracked into without permission	Wi-Fi Passwords
Personal information compromised after a data breach	Data storage (e.g. Cloud) Internet browsing Social Media
Personal and financial information being shared in reply to a bogus email	Email Online Shopping/ Banking
Fraudulent online purchases	Online Shopping/ Banking Internet browsing
Payment information stolen from their phones	Mobile and computer devices Online Shopping/ Banking
Technical support scams	Email Mobile and computer devices

# A: We validated the key topics to be addressed with focus areas of cybersecurity awareness programs offered in 5 benchmark countries

NOT EXHAUSTIVE



## Cross-cutting cybersecurity hygiene



1  
Mobile and computer devices



2  
Wi-Fi



3  
Passwords



4  
Internet browsing



5  
Data storage (e.g. Cloud)

## Activity-specific cybersecurity hygiene



6  
Online Shopping/Banking



7  
Social Media



8  
Online Gaming



9  
Email

List of topics will be refreshed with ongoing threats and attacks

# A: For each topic, we identified risky behaviors that people often possess and need to change (1/5)

对外厳密



## BEHAVIORS TO CHANGE

### 1 Mobile and Computer devices

#### Mobile devices

- 1 Lock your NFC-equipped phone with a PIN when it is not in use
- 2 Verify legitimacy of incoming calls
- 3 Report lost or stolen device immediately
- 4 Disable Bluetooth on devices when not in use
- 5 Install latest OS and app updates (e.g., on iPhone, iPad, Android)
- 6 Check security review of apps before downloading them
- 7 Disable automatic downloads of software and applications

#### Computer devices

- 8 Use a privacy screen on laptop when in public
- 9 When leaving laptop unattended, always shut down or hibernate (to enable full disk encryption)
- 10 Reboot laptop every day to allow for automatic updates
- 11 Install and enable comprehensive antivirus software and keep it updated regularly

### 2 Wi-Fi

- 12 Connect to public WiFi (hotel, airport) only when absolutely necessary
- 13 Don't use WiFi if "Cannot Verify Server Identity" error pops up when trying to connect
- 14 Choose semi-open or closed public wi-fi networks where passwords are not given out freely
- 15 Choose your network wisely by verifying the network name with staff

# A: For each topic, we identified risky behaviors that people often possess and need to change (2/5)

对外厳秘



## BEHAVIORS TO CHANGE

### 2 Wi-Fi

- 16 Be wary of using personal information, such as cellphone numbers and email address, to sign up to public wi-fi, and if necessary, do not use primary information, rather use information such as secondary email address
- 17 Enable MAC address filtering to only allow home equipment to connect to the home network
- 18 Position the router or access strategically to avoid its range reaching homes nearby or outside your home, for example placing it at the center of your home instead of near windows to minimize signal leakage
- 19 Enable the built in firewalls and security software of your router
- 20 Turn off your home network during extended periods of non-use
- 21 Secure sensitive information on reliable cloud services

### 3 Data storage

- 22 Back up data on safe cloud
- 23 Employ a backup strategy that consists of full and incremental backups.
- 24 Test the recovery abilities of your backup cloud provider
- 25 If storing data hard drive, ensure that the hard disk is encrypted
- 26 Do not store backup copies of data on pen drive as it can be corrupted
- 27 Limit the number of devices your hard disk is connected to minimize the chances of an infection

# A: For each topic, we identified risky behaviors that people often possess and need to change (3/5)



## BEHAVIORS TO CHANGE

<b>4</b> Malware, Botnets and Ransom- ware	28	Remember that a genuine bank or other organization will never ask you for your password via email, text, instant message or phone call
	29	Don't write down your password anywhere
	30	Use strong passwords
	31	Use a password manager
	32	Do not use "secret words" that can be easily guessed through social engineering
	33	Do not share your password with anyone, even with your trusted friend
	34	Enable a multi-factor verification system on your password protected apps and devices
	35	Use comprehensive security software that will protect you from keyloggers and other similar malware
	36	Do not save your passwords on devices that you do not control
	37	Look for certificate warnings and spoofed websites; don't proceed if unsure
<b>5</b> Internet browsing	38	Look at the URL bar for HTTPS or lock symbol to ensure site is secure
	39	Read certificate warnings carefully. Don't automatically allow.
	40	Do not enter personal or financial information on a website to which you have been directed from a QR code
	41	Hover over links to see the true address of the link and check whether it is consistent with what the link is name
	42	Get professional advice before pursuing opportunities on websites that promise high returns in a short period of time
	43	Carry out a web search for user reviews if you suspect a website to be fraudulent
	44	Use trusted download websites
	45	Do not disclose sensitive information to people met online

# A: For each topic, we identified risky behaviors that people often possess and need to change (4/5)

对外厳秘



## BEHAVIORS TO CHANGE

6	Online Shopping / Banking	46 Make online purchases from secure sites only 47 Conduct research before purchasing for the first time on a website, for example, by reading the reviews of previous customers 48 Use safe payment options – credit cards are generally the safest option as the seller can easily refund the buyer in the case of complications 49 Do not shop over unsecure wi-fi connections such as public wi-fi 50 Double check all purchase details before making a payment 51 Check credit card and bank statements carefully after shopping to ensure that the correct amount has been debited
7	Social media	52 Do not post sensitive or private information online 53 Create a username that does not include any personal information 54 Do not readily click on links in texts or posts/tweets from unknown sources, this could lead to viruses or your confidential information being compromised 55 Do not let peer pressure or what other people are doing on these sites convince you to do something you are not comfortable with 56 Keep your profile closed and only allow friends to view your profile 57 Use the privacy features to restrict strangers' access to your profile 58 Be on your guard against phishing, including fake friend requests and posts from individuals or companies inviting you to visit other pages or site 59 Report incidences that make you uncomfortable or incidences that you feel are inappropriate to the service provider

# A: For each topic, we identified risky behaviors that people often possess and need to change (5/5)

对外厳秘



## BEHAVIORS TO CHANGE

### 8 Online Gaming

- 60 Play only with authorized versions of games which you have purchased from the correct sources and for which you have a license
- 61 Choose a user name that does not reveal any personal information
- 62 Do not reveal any personal information to other players
- 63 Watch out for scams and cons when buying or selling 'property' that exists inside a computer game, in the real world
- 64 Delete all personal information when disposing of the game

### 9 Email

- 65 Be wary about attachments in emails from unknown or untrusted sources
- 66 Report suspicious emails to the relevant authorities
- 67 Don't click on links when source is unknown or can't be trusted
- 68 Use webmail services from well-known and trusted companies
- 69 Enable spam filtering or switch to a webmail provider that can do this
- 70 Do not reply to unsolicited or spam emails from companies or individuals you do not recognize

# A: The topics that national cyber security awareness programs focus on, will need to be revised on an annual basis based on global and local trends

	 Sources of insights	 Description of insight	 Review frequency
<b>Ecosystem stakeholders</b>	Interviews with national CERT	Types of cyber incidents being reported in the country  Insights from active monitoring of cyber incidents in the country	Quarterly
	Interviews with the Police force	Cybercrime and fraud statistics  Insights from actual investigation cases being handled	Quarterly
<b>Reports</b>	Cyber security reports and survey results published by leading entities like:	Statistics on the most common cyber security incidents  Survey results from actual consumers	Annual
	   		

Source: Team analysis, Press search

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

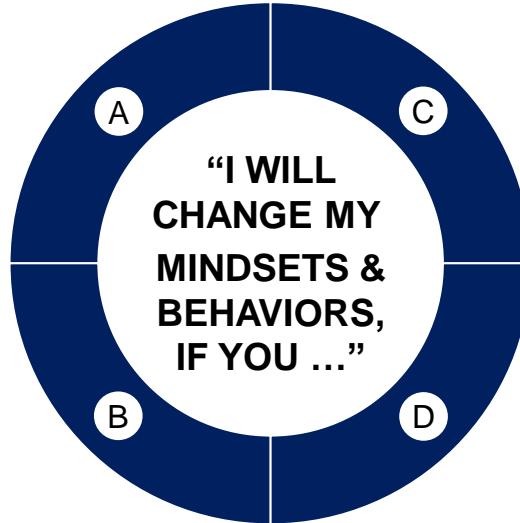
In order to promote better cybersecurity awareness, we have developed a National cyber security awareness program using a 3 step approach



- A** Identify high priority cyber security topics, based on attack trends and benchmark analysis
- B** Design a National cyber security awareness program using McKinsey's Influence Model
- C** Launch prioritized initiatives track progress



# Best-in-class awareness programs require initiatives around all 4 dimensions of the Influence Model to shift mindsets and behaviors



Influence Model	Program menu
A Role-modelling 	<ul style="list-style-type: none"> <li>1 Cyber safety demonstrations at road shows</li> <li>2 Appointing cybersecurity ambassadors at schools and companies</li> <li>3 Volunteer-based "cyber defenders" program</li> </ul>
B Developing talent and skills 	<ul style="list-style-type: none"> <li>4 Cybersecurity portal</li> <li>5 Embed cyber security awareness in education curriculum</li> </ul>
C Fostering understanding and conviction 	<ul style="list-style-type: none"> <li>6 Infomercials on social media</li> <li>7 Posters and billboard infographics</li> <li>8 Cyber awareness campaigns on government websites</li> <li>9 Awareness activities for homemakers and retirees</li> </ul>
D Reinforcing with formal mechanisms 	<ul style="list-style-type: none"> <li>10 Cyber awareness messages at consumer touchpoints</li> <li>11 Phishing campaigns in critical sector entities</li> <li>12 Cybersecurity awareness month (incl. career-related events and cybersecurity-themed blogs)</li> </ul>



## Key takeaways

Although government has conducted some cyber awareness programs, they are **informational in nature** and should be **reinforced through formal mechanisms and role-modeling**

Existing awareness channels focus on **generic cybersecurity topics**, making it **difficult to generate substantial behavior change**

# c2: National cyber security awareness program with 4 segment-specific initiatives (1/4)

対外厳密



Initiative name	Description	Benchmarked examples (if any)	Segments
 <b>Role-modelling</b>	<b>1 Cyber safety demonstrations at road shows</b> Live hacking demonstrations outside major malls (e.g. how hackers can take over cellphones through phishing)	 National Cyber Security Alliance (NCSA) conducts <b>roadshows</b> for <b>small and medium business</b> to increase <b>cybersecurity awareness</b>	
	<b>2 Appointing cyber-security ambassadors at schools and companies</b> Cybersecurity awareness “ambassadors” award given out in schools to encourage students to spread messages about online safety	N.A.	Youth and students Tertiary and pre-professionals
	<b>3 Volunteer-based “cyber defenders” program</b> “Cyber defenders” program that accepts trains police force members to become defenders of cyber-space. Program provides training and deployment for roles to spread cybersecurity awareness.	 Estonia RIA works with Police and Border Guard Board to create <b>web constables</b> for increasing <b>cybersecurity awareness</b>	

# c2: National cyber security awareness program with 4 segment-specific initiatives (2/4)

対外厳密



Initiative name	Description	Benchmarked examples (if any)	Segments
 <b>Developing talent and skills</b>	<b>4 Cybersecurity portal</b>  Online portal that publishes advisories and guidelines on how to use technology better. The portal will also contain cyber training programs that will help the public and companies learn how to practice better data and digital hygiene  Content can be tailored to specific segments and spread through social media channels	 Cyber Aware and Get Safe Online campaign to <b>drive behavior change amongst small businesses and individuals</b>	
		 <b>Gosafeonline</b> provides Singaporean citizens with tips and tricks to <b>browse securely</b>	
		 Get Cyber Safe is a <b>national public awareness campaign</b> created to <b>educate Canadians about Internet security</b>	
<b>5 Embed cyber security awareness in education curriculum</b>	Cybersecurity and online safety curriculum embedded into schools from Grade 1-12	 Singapore created a <b>cyber wellness program</b> for schools to adopt <b>cybersecurity awareness modules</b> in the <b>formal curriculum</b>	Youth and students
		 Tiger leap foundation works with <b>schools</b> to <b>create modules in information security</b>	

# c2: National cyber security awareness program with 4 segment-specific initiatives (3/4)

対外厳密



Initiative name	Description	Benchmarked examples (if any)	Segments
 <b>Fostering understanding and conviction</b>	<p><b>6 Infomercials on social media</b></p> <p>Short infomercials and multimedia messages to be aired on social media channels and influencers to inform the public about cybersecurity topics</p> <p>Leverage social media channels such as Instagram and snapchat tools</p> <p>A social media hashtag can be created to brand online outreach efforts</p>	 The National Crime Prevention Council (NCPC) and the Singapore Police Force (SPF) launched <b>anti-scam commercials</b> focusing on <b>cyber crimes</b>	
<b>7 Posters and billboard infographics</b>	Posters and billboards put up around prominent areas to garner attention	 STOP.THINK.CONNECT campaign creates <b>anti-cybercrime posters</b> that the public can download and distribute	
<b>8 Cyber awareness campaigns on government websites</b>	Nation-wide campaign to insert cybersecurity-related information on major government websites	 Gov.UK has a <b>dedicated page on cybersecurity</b> under the "Government" tab	
<b>9 Awareness activities for homemakers and retirees</b>	Cyber awareness information events in community centers	N.A.	Homemakers Retirees

# c2: National cyber security awareness program with 4 segment-specific initiatives (4/4)

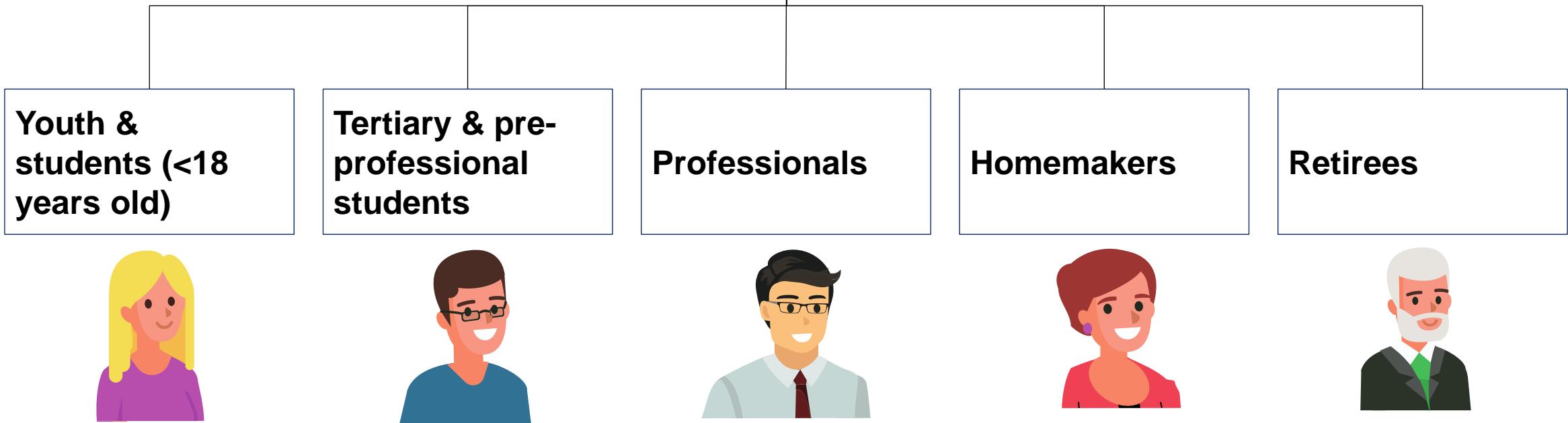
対外厳密



Initiative name	Description	Benchmarked examples (if any)	Segments
 <b>Reinforcing with formal mechanisms</b>	<b>⑩ Cyber awareness messages at consumer touchpoints</b> Leverage private sector players to insert cyber awareness messages around key consumer decision making moments Content can be tailored to specific segments	N.A.	
	<b>⑪ Phishing campaigns in critical sector entities</b> Phishing campaign across public agencies and critical sector operators to educate them about phishing	 UK's "Would you be ready" campaigns gives <b>tips to business leaders</b> on how to <b>safeguard their assets</b> online, including running phishing simulation campaigns	Professionals
	<b>⑫ Cybersecurity awareness month (incl. career-related events and cybersecurity-themed blogs)</b> One full month of events, activities, and carnivals dedicated to cybersecurity awareness topics	 Canada designated <b>October</b> as <b>cybersecurity awareness month</b> . Activities during the month include <b>university research show-cases</b> , targeted week-by-week <b>cybersecurity-themed blogs</b> (e.g. "Buy Secure"), and a <b>tool-kit for companies</b> to launch cyber campaigns	
		 The US designated <b>October</b> as <b>cybersecurity awareness month</b> , and include cybersecurity <b>career-related events</b> , <b>social media conversations</b> , and <b>cybersecurity curricula</b> for teachers	

# Targeted approach to cyber awareness can be formulated by reaching out to specific citizen archetypes

There are 5 citizen archetypes that need to be made cyber aware



# B: We recommend a National cyber security awareness program consisting of 8 cross-cutting initiatives and 4 segment-specific initiatives (1/5)

## Cross cutting initiatives

Initiative name	Description	Benchmarked examples (if any)
<b>Cyber safety demonstrations at road shows</b>	Live hacking demonstrations outside major malls (e.g. how hackers can take over cellphones through phishing)	 National Cyber Security Alliance (NCSA) conducts <b>roadshows for small and medium business to increase cybersecurity awareness</b>
<b>Cyber awareness messages at consumer touchpoints</b>	Leverage private sector players to insert cyber awareness messages around key consumer decision making moments  Content can be tailored to specific segments	N.A.
<b>Volunteer-based “cyber defenders” program</b>	“Cyber defenders” program that accepts trains police force members to become defenders of cyber-space. Program provides training and deployment for roles to spread cybersecurity awareness.	 Estonia RIA works with Police and Border Guard Board to create <b>web constables for increasing cybersecurity awareness</b>

# B: We recommend a National cyber security awareness program consisting of 8 cross-cutting initiatives and 4 segment-specific initiatives (2/5)

## Cross cutting initiatives

Initiative name	Description	Benchmarked examples (if any)
Cybersecurity portal	<p>Online portal that publishes advisories and guidelines on how to use technology better. The portal will also contain cyber training programs that will help the public and companies learn how to practice better data and digital hygiene</p> <p>Content can be tailored to specific segments and spread through social media channels</p>	 Cyber Aware and Get Safe Online campaign to <b>drive behavior change amongst small businesses and individuals</b>  <b>Gosafeonline</b> provides Singaporean citizens with tips and tricks to <b>browse securely</b>  Get Cyber Safe is a <b>national public awareness campaign</b> created to <b>educate Canadians about Internet security</b>
Infomercials on social media	<p>Short infomercials and multimedia messages to be aired on social media channels and influencers to inform the public about cybersecurity topics</p> <p>Leverage social media channels such as Instagram and snapchat tools</p> <p>A social media hashtag can be created to brand online outreach efforts</p>	 The National Crime Prevention Council (NCPC) and the Singapore Police Force (SPF) launched <b>anti-scam commercials</b> focusing on <b>cyber crimes</b>

# B: We recommend a National cyber security awareness program consisting of 8 cross-cutting initiatives and 4 segment-specific initiatives (3/5)

## Cross cutting initiatives

Initiative name	Description	Benchmarked examples (if any)
<b>Posters and billboard infographics</b>	Posters and billboards put up around prominent areas to garner attention	 STOP.THINK.CONNECT campaign creates <b>anti-cybercrime posters</b> that the <b>public can download and distribute</b>
<b>Cyber awareness campaigns on government websites</b>	Nation-wide campaign to insert cybersecurity-related information on major government websites	 <b>Gov.UK</b> has a <b>dedicated page on cybersecurity</b> under the "Government" tab
<b>Cybersecurity awareness month (incl. career-related events and cybersecurity-themed blogs)</b>	One full month of events, activities, and carnivals dedicated to cybersecurity awareness topics	 <b>Canada</b> designated <b>October</b> as <b>cybersecurity awareness month</b> . Activities during the month include <b>university research show-cases</b> , targeted week-by-week <b>cybersecuri-ty-themed blogs</b> (e.g. "Buy Secure"), and a <b>tool-kit for companies</b> to launch cyber campaigns  <b>The US</b> designated <b>October</b> as <b>cybersecurity awareness month</b> , and include cybersecurity <b>career-related events</b> , <b>social media conversations</b> , and <b>cybersecurity curricula</b> for teachers

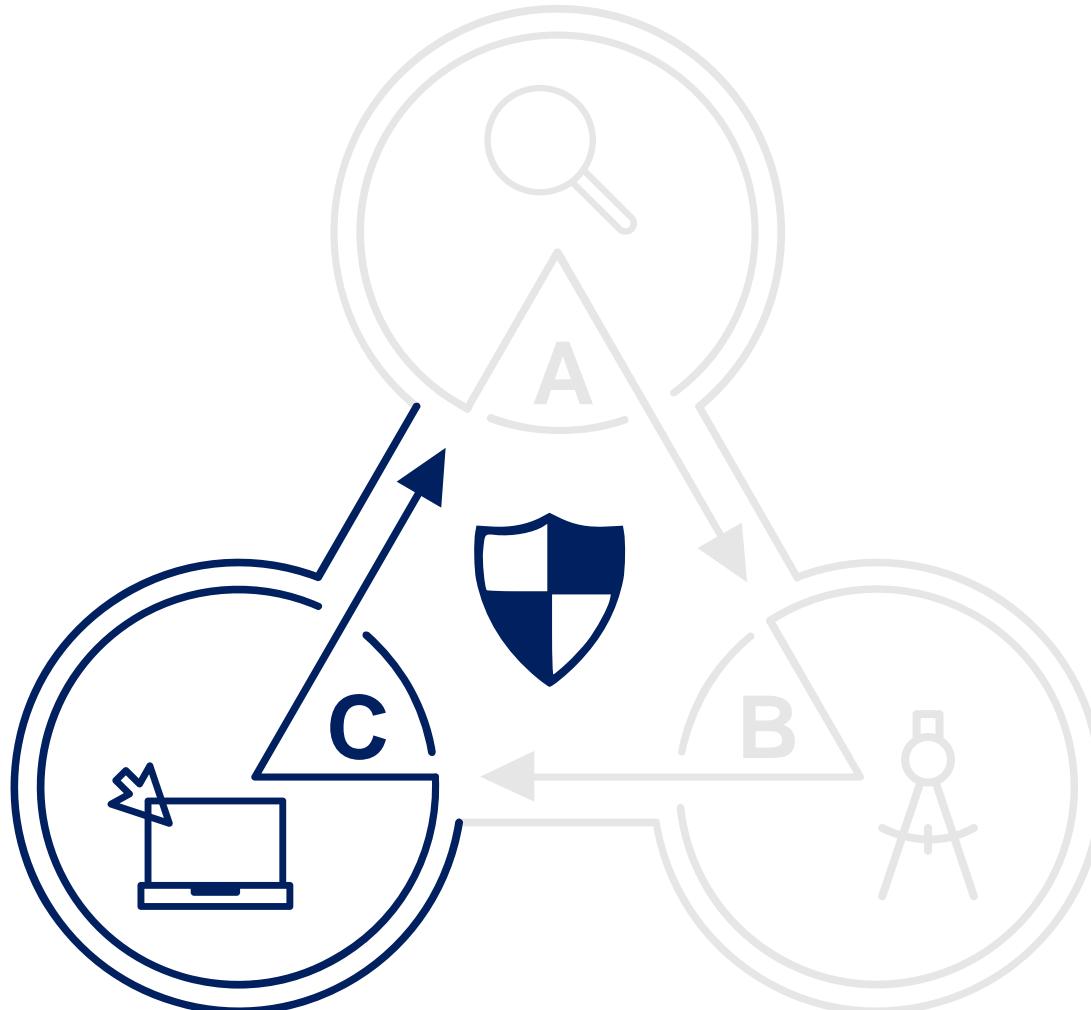
# B: We recommend a National cyber security awareness program consisting of 8 cross-cutting initiatives and 4 segment-specific initiatives (4/5)

Cross cutting initiatives	Initiative name	Description	Benchmarked examples (if any)	
	<b>Phishing campaigns in critical sector entities</b>	Phishing campaign across public agencies and critical sector operators to educate them about phishing	 UK's "Would you be ready" campaigns gives <b>tips to business leaders</b> on how to <b>safeguard their assets</b> online, including running phishing simulation campaigns	Professionals
	<b>Appointing cybersecurity ambassadors at schools and companies</b>	Cybersecurity awareness "ambassadors" award given out in schools to encourage students to spread messages about online safety	 Global phishing companies <b>PhishMe</b> and <b>Wombat</b> provide <b>phishing simulation services</b> that contain <b>customizable email templates</b> and <b>educational videos</b>	Youth and students Tertiary and pre-professionals

# B: We recommend a National cyber security awareness program consisting of 8 cross-cutting initiatives and 4 segment-specific initiatives (5/5)

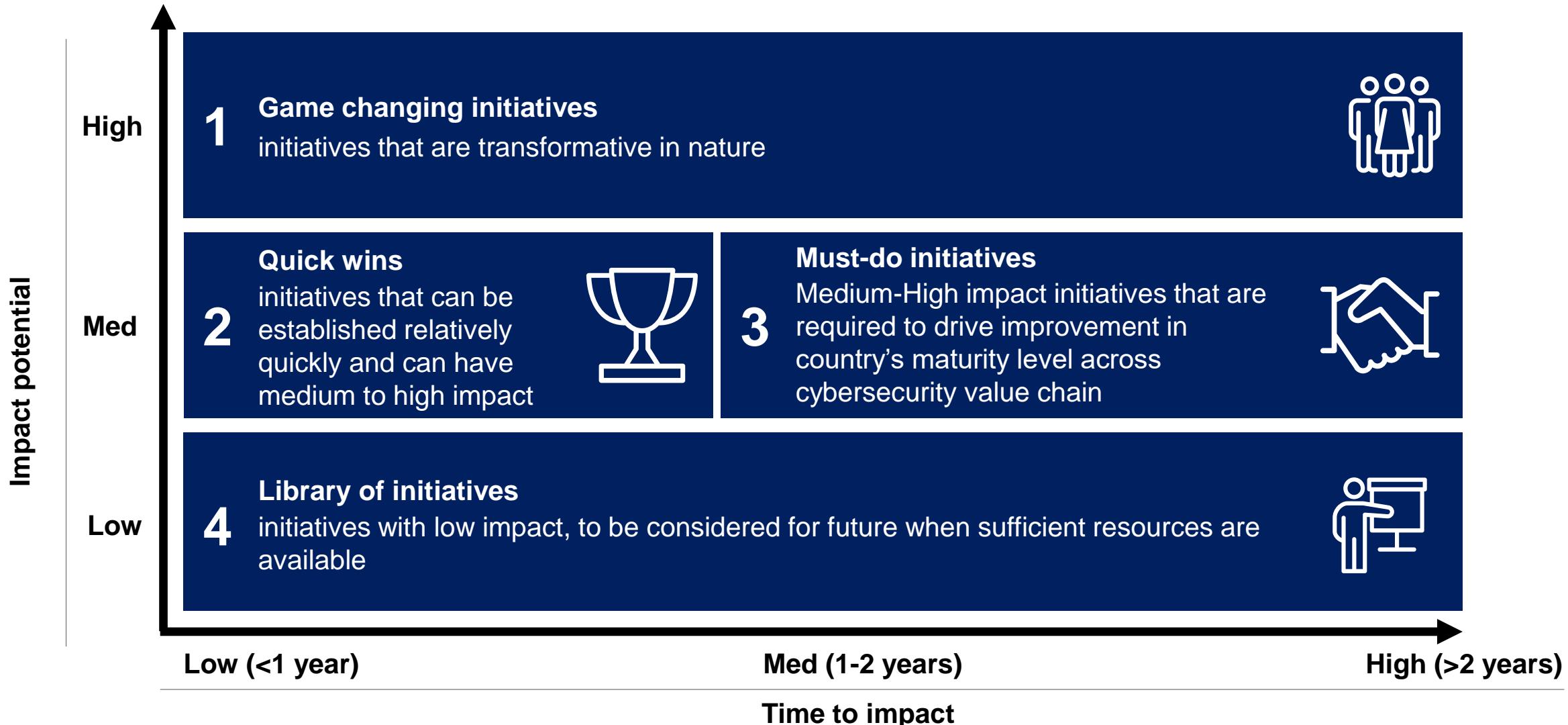
Cross cutting initiatives	Initiative name	Description	Benchmarked examples (if any)
	<b>Embed cyber security awareness in education curriculum</b>	Cybersecurity and online safety curriculum embedded into schools from Grade 1-12	 Singapore created a <b>cyber wellness program</b> for schools to adopt <b>cybersecurity awareness modules</b> in the <b>formal curriculum</b>  Tiger leap foundation works with <b>schools</b> to <b>create modules in information security</b>
	<b>Awareness activities for homemakers and retirees</b>	Cyber awareness information events in community centers	N.A. Homemakers Retirees

In order to promote better cybersecurity awareness, we have developed a National cyber security awareness program using a 3 step approach



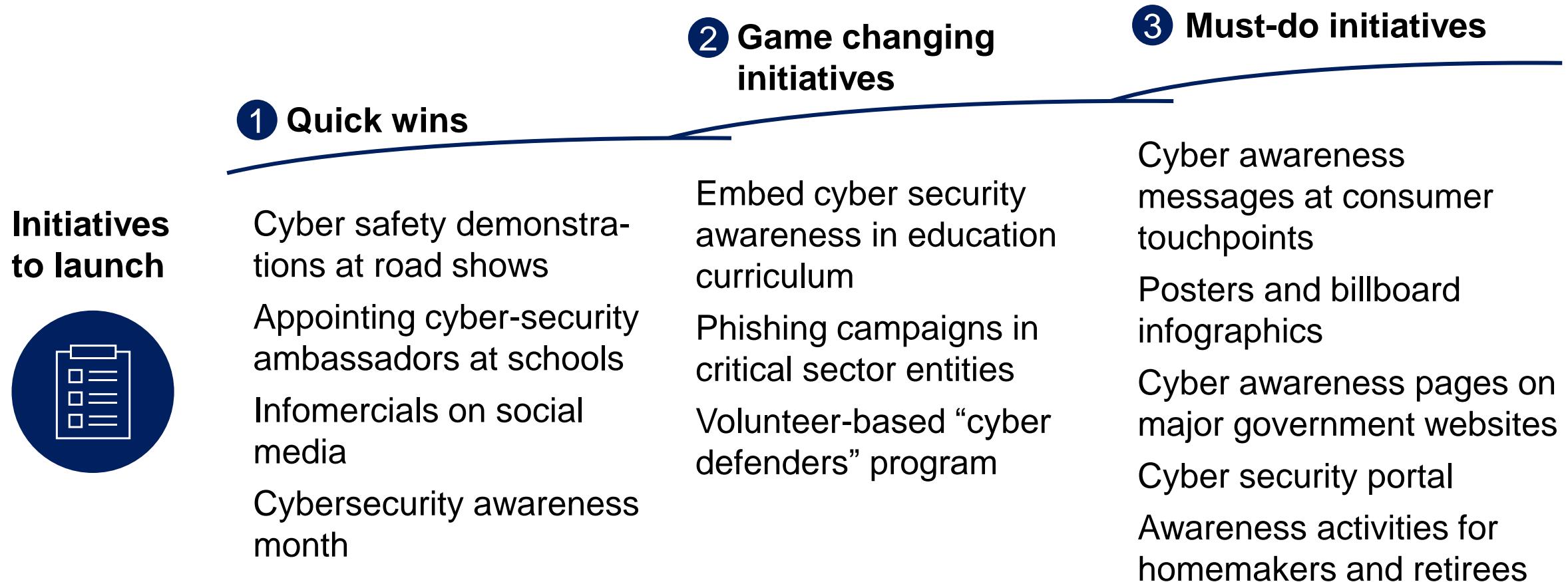
- A** Identify high priority cyber security topics, based on attack trends and benchmark analysis
- B** Design a National cyber security awareness program using McKinsey's Influence Model
- C** Launch prioritized initiatives track progress

# C: We have prioritized the recommended initiatives across the dimensions of potential impact and time to impact



# C: Initiatives should be launched in phases, beginning with quick wins and game changing initiatives

対外厳秘



# C: Following KPIs must be tracked to measure effectiveness of awareness program on annual basis

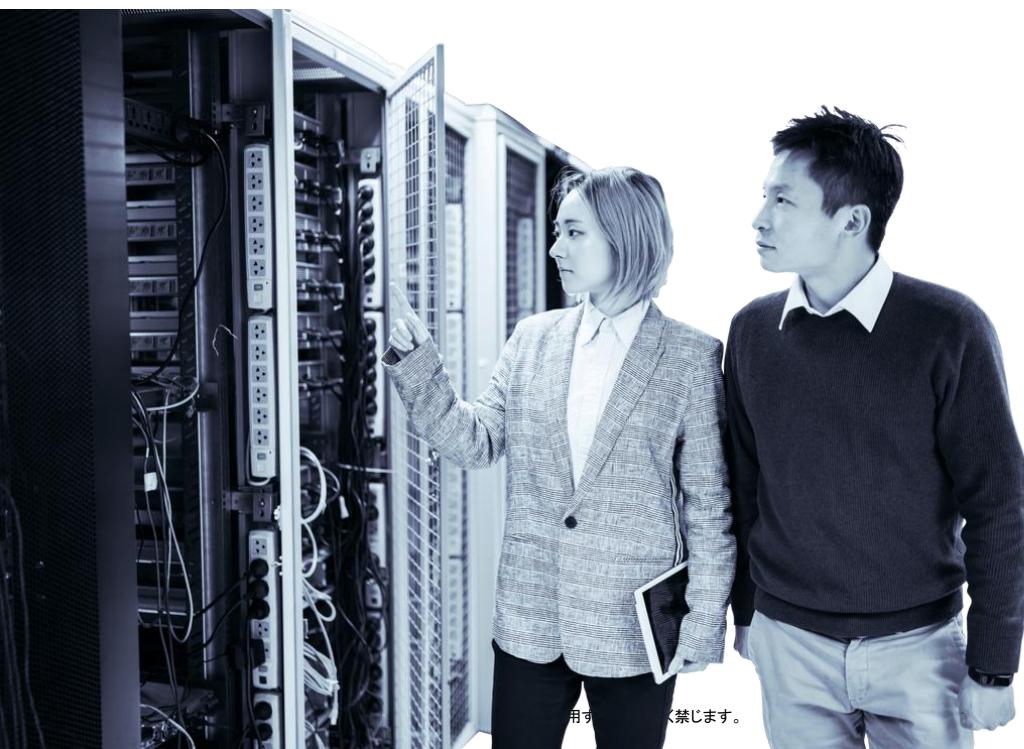
Segment	KPI	Measurement method
Youth (<18 years old) & students	 <ul style="list-style-type: none"> <li>% score in cybersecurity simulation game / survey</li> <li>User engagement for social media posts(e.g., # of shares, retweets, etc.)</li> </ul>	<ul style="list-style-type: none"> <li>Annual game / survey given out during end of awareness month</li> <li>Social media engagement metrics</li> </ul>
Tertiary & pre-professional students	 <ul style="list-style-type: none"> <li>% score in cybersecurity simulation game / survey</li> <li>User engagement for social media posts(e.g., # of shares, retweets, etc.)</li> </ul>	<ul style="list-style-type: none"> <li>Annual game / survey given out during end of awareness month</li> <li>Social media engagement metrics</li> </ul>
Professionals	 <ul style="list-style-type: none"> <li>% of employees clicking phishing emails</li> <li>% of suspicious emails reported</li> </ul>	Quantitative assessment through phishing test administrator
Homemakers	 <ul style="list-style-type: none"> <li>Number of people reached through awareness program</li> </ul>	Sampling assessment of audience reach through infomercials, awareness month and portals
Retirees	 <ul style="list-style-type: none"> <li>Number of people reached through awareness program</li> </ul>	Sampling assessment of audience reach through infomercials, awareness month and portals

---

# Questions?

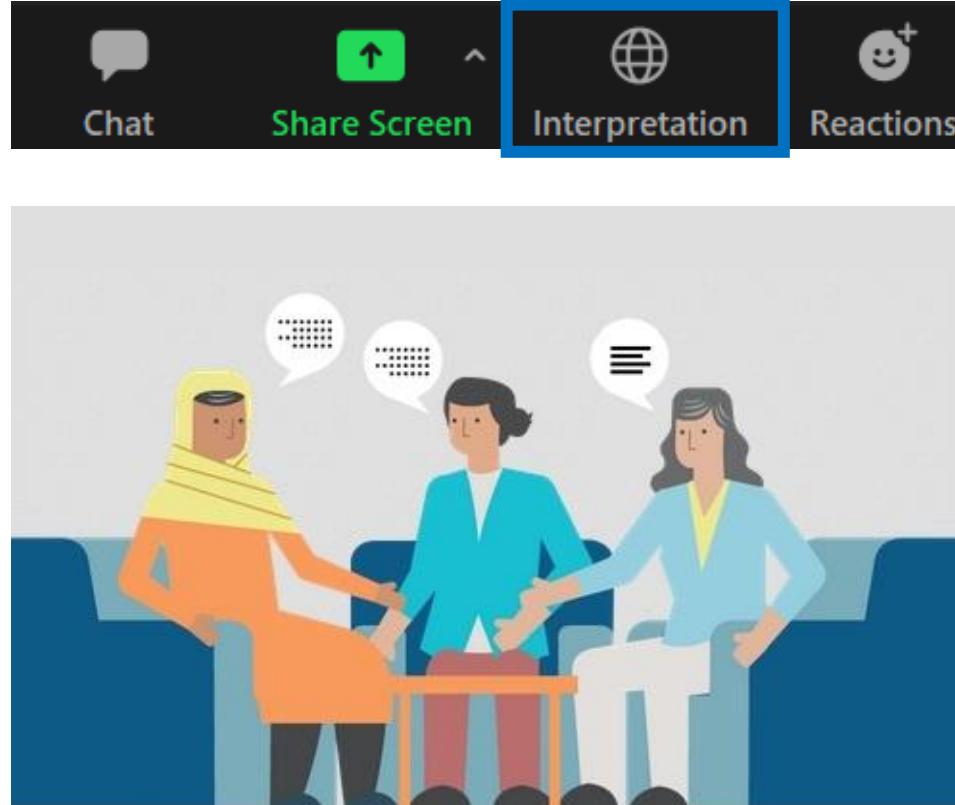
---



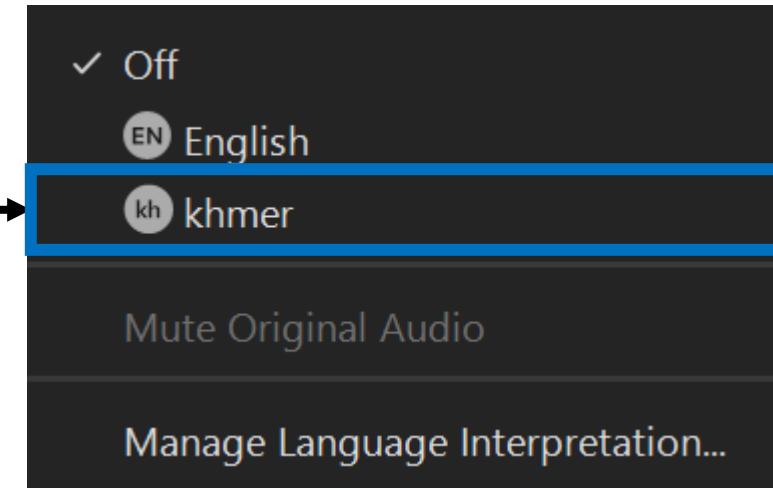
- 
1. Overview of Cyber Security Trend
  2. Definition of Cyber threat and national Incident response framework
  3. Cyber Security Regulation framework
  4. Partnership(Public, Private, Academia, International)
  5. Professional training and certification
  6. Public awareness and alerts
  - 7. Cyber Security for SME**
  8. Critical Infrastructure Industry protection
  9. CERT/ Resilience
  10. Wrap up / Cyber security assessment

# Khmer simultaneous Interpretation available

Select “Interpretation” on the bottom



Select “Khmer”



- Presentation is simultaneously translated into Khmer
- You can post question in Khmer



## Timeline

## Overview

100 minuets

## Workshop & QA

20 minuets

# Cambodia need to design Cyber security strategy with suggested strategy element

Cybersecurity strategy element	Insights from benchmarking cybersecurity strategy	#
A Governance 	<ul style="list-style-type: none"> <li>Top-performing nations are moving towards <b>centralized governance bodies</b> reporting directly to executive branches of government and serving as <b>E2E owners of cybersecurity strategy implementation</b></li> </ul>	• #2
B Legal and regulations 	<ul style="list-style-type: none"> <li><b>Comprehensive legislative frameworks</b> cover mandatory IT security standards, regulations, and best practices, and are enforced through audits and law enforcement</li> <li><b>Specific legislations to address emerging technologies</b> are evolving at fast pace in countries with advanced cybersecurity legislations</li> </ul>	• #3
E Partnerships 	<ul style="list-style-type: none"> <li><b>Regional and international partnerships</b> are actively used to foster sharing of best practices and enhancing operational and technical capabilities through joint drills &amp; audits</li> </ul>	• #4
C Talent and people 	<ul style="list-style-type: none"> <li><b>Public awareness and training</b> programs, which draw on <b>international standards and offerings</b>, form the basis for cybersecurity talent development</li> </ul>	• #5~7
F Critical infrastructure 	<ul style="list-style-type: none"> <li>CII protection programs, executed by national cybersecurity agencies, focus <b>selectively on critical assets</b> in critical sectors with timely involvement of relevant authorities</li> </ul>	• #8
D Incident response 	<ul style="list-style-type: none"> <li>National cybersecurity agencies, through <b>specialized incident response teams</b>, lead integrated response efforts with close coordination with impacted assets</li> </ul>	• #9

# Out of the different types of SMEs, the National Cyber Security Strategy may focus on medium-scale companies for maximum impact

Enterprise scale	# of employees	Revenue (Million USD/year)	Typical % SME GDP contribution
1 Medium	100-250	30-70	45%
2 Small	11-100	3-30	35%
3 Micro	1-10	0-3	20%

Medium scale enterprises should be the focus for SME cybersecurity since they:

- Typically represent roughly half (~45%) of the SME economy
- Higher risk due to larger cyber footprint e.g. ERP, CRM systems, etc.
- Higher likelihood of being targeted by cyber criminals since medium scale companies are more in the public eye

# Typically, SMEs are particularly vulnerable to cybersecurity incidents since they face 4 key challenges in safeguarding themselves

PRELIMINARY

Despite the availability of multiple cybersecurity standards, SMEs face cybersecurity challenges due to multiple reasons such as ...

1

Lack of clearly defined guidelines



- SMEs often lack awareness on:
  - Key **cyber vulnerabilities** affecting them
  - **Security standard** to implement and **Controls to be prioritized** to achieve minimum level of cybersecurity

2

Limited budget



- SMEs **do not have enough security-related operating budget** to dedicate towards buying the **needed hardware, software or hiring technical personnel** to implement cybersecurity controls

3

Lack of clear incentives to implement cybersecurity



- **Lack of clearly articulated benefits** for the SMEs to implement cybersecurity controls **results in a reactive mindset instead of a proactive mindset** for implementing cybersecurity controls

4

Lack of technical capabilities



- SMEs have **challenges accessing the cybersecurity professionals with required technical skills** and capabilities

# Benchmark countries have taken multiple initiatives to address some of these key cybersecurity challenges for SMEs

PRELIMINARY

SME cybersecurity challenges	UK	Germany	Australia	Potential solution
① Lack of clear regulations or cybersecurity guidelines	Defined Cyber Essentials standard with clear guidelines	Defined IT Grundschutz Standard which is the IT baseline standard for organizations	Not defined/recommended any specific standard	Essential Cybersecurity standard for SMEs
② Lack of security operational budget	Broad scope of implementation of security controls	Cyber Essentials defines 5 key control areas that narrows cybersecurity implementation scope to bring the cost down	IT Grundschutz customizes ISO27001 for SMEs which are primarily from manufacturing sector	No specific initiative to narrow down the scope of implementation for SMEs
	Cost of certification and penetration testing	UK offers minimum certification fee (300 GBP) for SMEs to achieve Cyber Essentials certification	No specific initiative	Offers grants of up to \$2000 for SMEs to avail penetration testing services from approved service providers
③ Lack of clear incentives for certification	Eligibility for certain national and local government projects require Cyber Essentials Plus certification	No specific initiatives	No specific initiatives	Incentive programs to encourage certification

# CASE EXAMPLE: Australia offers grants to SMEs to subsidize cybersecurity testing from the approved service providers

PRELIMINARY



## Overview

Australia's **Cyber Security Small Business Program** is an integrated element of the Cyber Security Strategy to improve cyber security for Australia's small businesses with **2 linked components**:

- **Grant to the Council of Registered Ethical Security Testers Australia New Zealand (CREST ANZ)**
- **Grants of up to \$2,100 to co-fund small businesses to have their cyber security tested by CREST ANZ approved service providers**

## Objectives

**Help Australian small businesses test their cyber security, and increase their awareness of their cybersecurity risk**

**Increase small business confidence** in the credentials of the service providers they approach for help and the cyber security products and services they use

**Help CREST ANZ expand its range of cyber security services to include small business services** and the infrastructure for Members to use the services in the small business market

## Intended Outcomes

### For SMEs:

Attain thorough knowledge of cybersecurity vulnerabilities their businesses are exposed to

### For CREST ANZ:

- **Grow its current pool of CREST ANZ -approved service providers** to meet the demand of businesses accessing their services
- **Diversify its services to include the certification of the skills and capabilities required to provide services (including assessment services) for small business**

# Based on benchmark analysis, we recommend 3 key initiatives for the countries to help mitigate the cybersecurity challenges of the SMEs

对外厳秘

PRELIMINARY

01



Define Essential  
cybersecurity  
standard for SMEs

02



Create incentives  
for SMEs to  
implement  
cybersecurity

03



Provide  
cybersecurity  
training to SMEs

# Based on benchmark analysis, we recommend 3 key initiatives for the countries to help mitigate the cybersecurity challenges of the SMEs

对外厳秘

PRELIMINARY

01



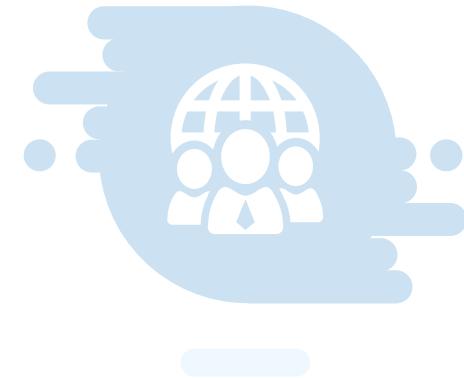
Define Essential  
cybersecurity  
standard for SMEs

02



Create incentives  
for SMEs to  
implement  
cybersecurity

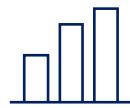
03



Provide  
cybersecurity  
training to SMEs

# Benchmark analysis shows that to establish clear guidelines for SMEs, countries define an Essential cybersecurity standard that follows 4 key principles

PRELIMINARY



We **benchmarked 2 countries and their cybersecurity essential standards for SMEs** to identify the key principles for a Cybersecurity Essential standard



## Examples from benchmark countries

### UK Cyber Essentials



Government scheme encouraging organizations to adopt good practice in information security.

Includes an **assurance framework and a simple set of security controls to protect information from internet based threats**

**Defines 5 key categories** for SMEs to safeguard themselves

### German IT Grundschutz



IT-Grundschutz approach from the German FSI is a **methodology to identify and implement computer security measures** in an organization with the aim of **achieving an adequate and appropriate level of security for IT systems**

Focusses on a general organization, and is better suited for mid-scale manufacturing enterprises which form majority portion of Germany's SME GDP

## Key learnings to develop Essential Cybersecurity standard for SMEs

1



Cover majority of the cybersecurity threats

2



Focus on **prioritized list of controls** that cover majority of attacks

3



Communicate guidance in simplified language

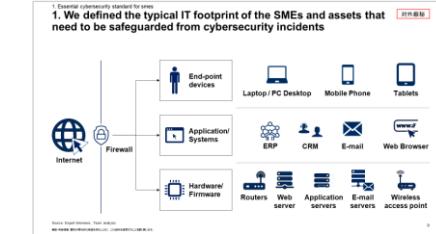
# In order to develop the Essential cybersecurity standard for the SMEs, 3 key steps were followed

## Steps

### 1 Define the typical IT footprint for SMEs

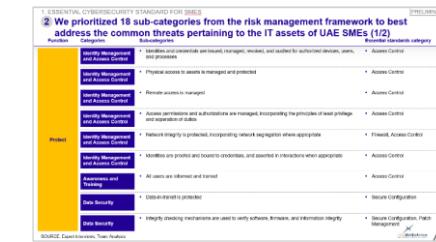
## Description

**Define the typical IT assets that SMEs use** (i.e. types of systems, hardware, software) would need to safeguard against cybersecurity incidents



### 2 Identify prioritized set of controls that protect SMEs from majority of threats

Based on the threats to the identified IT assets, **prioritize the applicable control families** from the proposed risk management framework to focus on most controls that provide coverage against majority of the threats

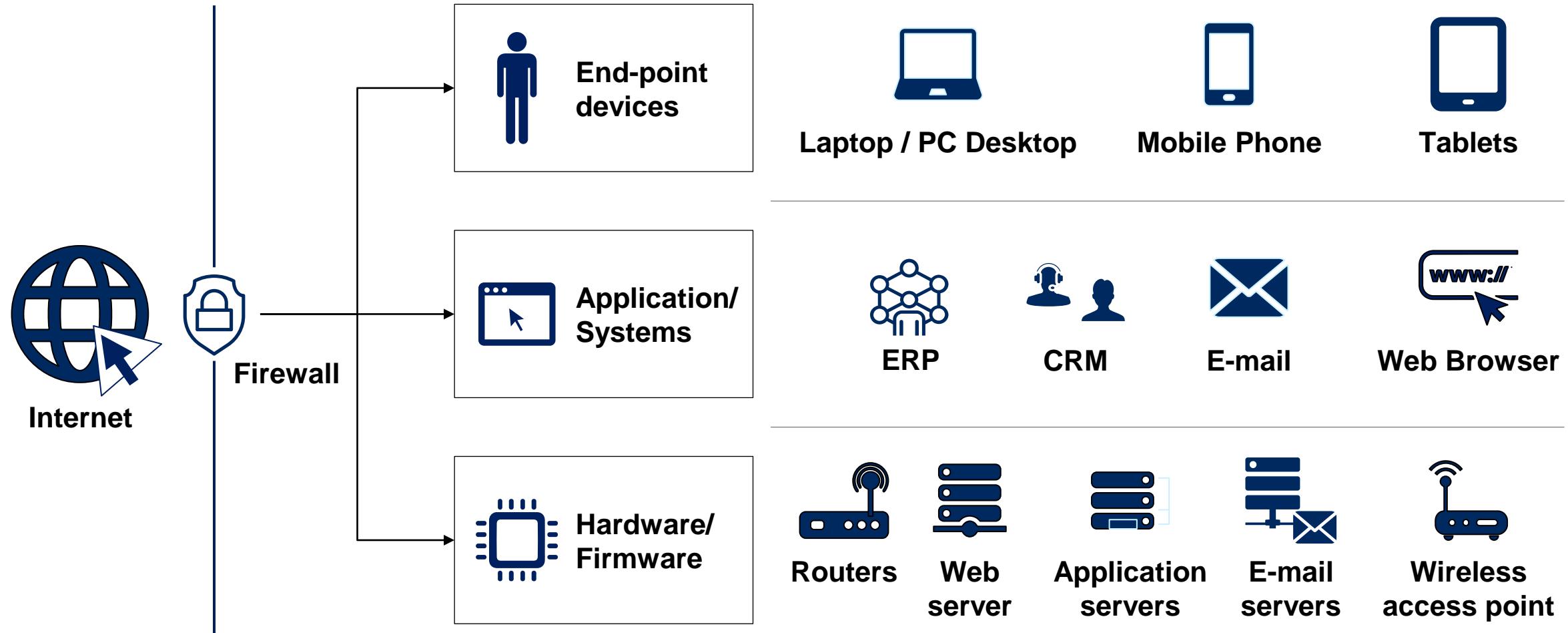


### 3 Develop simplified guidelines for prioritized controls

**Distill the technical controls into simplified language that can be easily communicated to and understood by the SMEs** that may not have very mature cybersecurity personnel or capabilities



# 1. We defined the typical IT footprint of the SMEs and assets that need to be safeguarded from cybersecurity incidents



## 2. We prioritized 18 sub-categories from NIST CSF to best address the common threats pertaining to the IT assets of the SMEs (1/2)

対外厳密

PRELIMINARY

Function	Categories	Sub-categories	Essential standards category
Protect	Identity Management and Access Control	Identities and credentials are issued, managed, revoked, and audited for authorized devices, users, and processes	Access Control
		Physical access to assets is managed and protected	Access Control
		Remote access is managed	Access Control
		Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	Access Control
		Network integrity is protected, incorporating network segregation where appropriate	Firewall, Access Control
	Awareness and Training	Identities are proofed and bound to credentials, and asserted in interactions when appropriate	Access Control
Data Security		All users are informed and trained	Access Control
		Data-in-transit is protected	Secure Configuration
		Integrity checking mechanisms are used to verify software, firmware, and information integrity	Secure Configuration, Patch Management

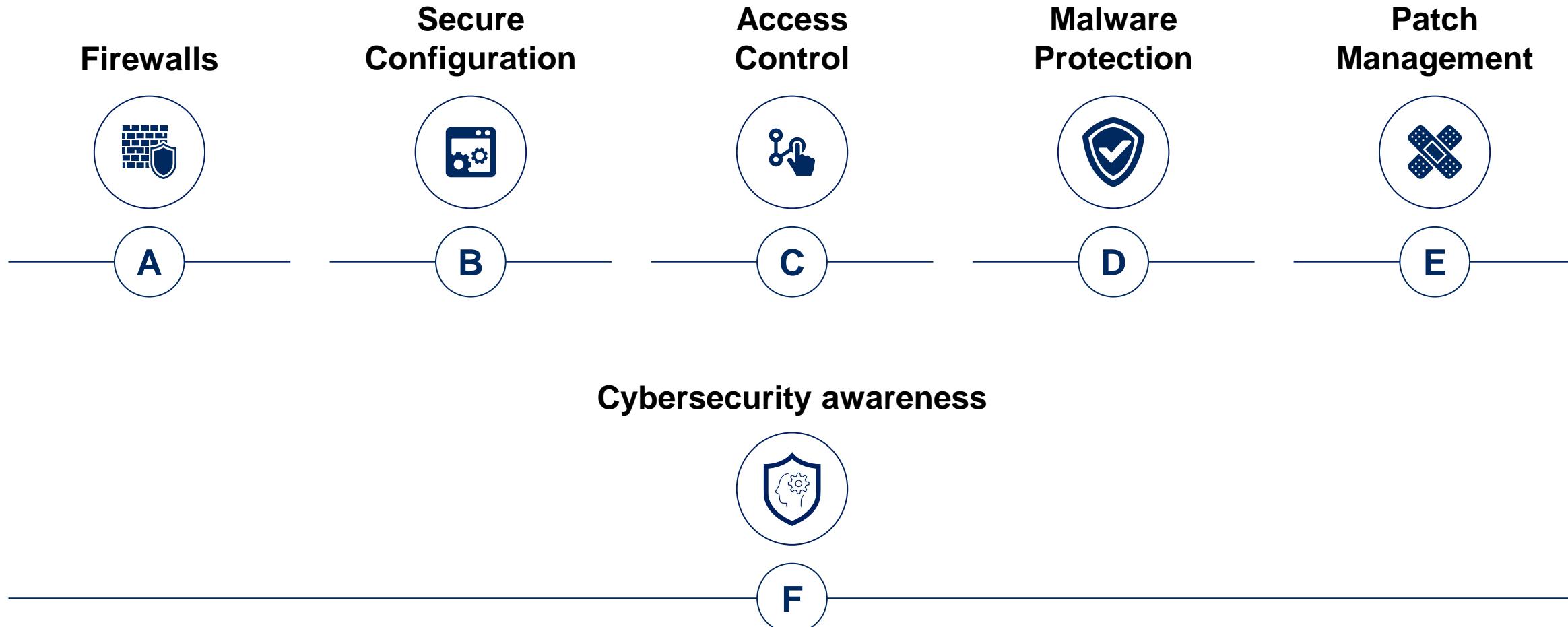
## 2. We prioritized 18 sub-categories from NIST CSF to best address the common threats pertaining to the IT assets of the SMEs (2/2)

対外厳密

PRELIMINARY

Function	Categories	Sub-categories	Essential standards category
Protect	Information Protection	Backups of information are conducted, maintained, and tested periodically	Secure Configuration
		Data is destroyed according to policy	Secure Configuration
	Protective Technology	Removable media is protected and its use restricted according to policy	Secure Configuration
		The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	Secure Configuration
		Communications and control networks are protected	Firewall, Secure Configuration
	Security Continuous Monitoring	The physical environment is monitored to detect potential cybersecurity events	Secure Configuration
		Malicious code is detected	Malware Protection, Patch Management
		Unauthorized mobile code is detected	Access Control, Malware Protection
		Monitoring for unauthorized personnel, connections, devices, and software is performed	Secure Configuration, Malware Protection

### 3. The technical controls for the 18 prioritized sub-categories can be synthesized into 6 key areas of Essential cybersecurity standard for simplified communication



## 3A. Essential Cybersecurity Standard for SMEs - Firewalls



	<b>Applies to</b>	Boundary firewalls; desktop computers; laptop computers; routers; servers
	<b>Objective</b>	Ensure that only safe and necessary network services can be accessed from the Internet
	<b>Requirements</b>	<p>Every device that is in scope must be protected by a correctly configured firewall (or equivalent network device)</p> <p>For all firewalls (or equivalent network devices), the organization must routinely:</p> <p><b>Change any default administrative password</b> to an alternative that is difficult to guess (see Password-based authentication) — or disable remote administrative access entirely</p> <p><b>Prevent access to the administrative interface</b> (used to manage firewall configuration) from the Internet, unless there is a clear and documented business need and the interface is protected by one of the following controls:</p> <ul style="list-style-type: none"> <li>• A second authentication factor, such as a one-time token</li> <li>• An IP whitelist that limits access to a small range of trusted addresses</li> </ul> <p><b>Block unauthenticated inbound connections by default</b></p> <p><b>Ensure inbound firewall rules are approved and documented</b> by an authorized individual (i.e., business need/purpose of the rule, services, users and devices it affects, date when the rule was added, expiry date of the rule (if applicable))</p> <p><b>Remove or disable permissive firewall rules quickly, when they are no longer needed.</b> Use a host-based firewall on devices which are used on untrusted networks, such as public Wi-Fi hotspots</p> <p><b>Upgrade the firewall software</b> and firmware by installing all the latest patches</p> <p><b>Establish and follow a change procedure for firewall configuration</b> (i.e., change request, testing, deployment, validation and documentation)</p>

## 3B. Essential Cybersecurity Standard for SMEs - Secure Configuration



	<b>Applies to</b>	Email, web, and application servers; desktop computers; laptop computers; tablets; mobile phones; firewalls; routers
	<b>Objective</b>	Ensure that computers and network devices are properly configured to: <ul style="list-style-type: none"> <li>Reduce the level of inherent vulnerabilities</li> <li>Provide only the services required to fulfil their role</li> </ul>
	<b>Requirements</b>	<p><b>Computers and network devices:</b></p> <ul style="list-style-type: none"> <li>Remove and disable unnecessary user accounts (such as guest accounts and administrative accounts that won't be used)</li> <li>Change any default or guessable account passwords to something non-obvious</li> <li>Remove or disable unnecessary software (including applications, system utilities and network services)</li> <li>Disable any auto-run feature which allows file execution without user authorization (such as when they are downloaded from the Internet)</li> <li>Authenticate users before allowing Internet-based access to commercially or personally sensitive data, or data which is critical to the running of the organization</li> </ul> <p><b>Password-based authentication:</b></p> <p>Protect against brute-force password guessing, by using at least one of the following methods:</p> <ul style="list-style-type: none"> <li>Lock accounts after no more than 10 unsuccessful attempts</li> <li>Limit the number of guesses allowed in a specified time period to no more than 10 guesses within 5 minutes</li> <li>Create Password Blacklist by creating a database of most common passwords (e.g., dictionary words, passwords that have been already cracked)</li> </ul> <p>Set a minimum password length of at least 8 characters, and no maximum password length</p> <p>Change passwords promptly when the organization knows or suspects they have been compromised</p> <p>Have a password policy that tells users:</p> <ul style="list-style-type: none"> <li>How to avoid choosing obvious passwords (such as those based on easily-discoverable information like the name of a favorite pet)</li> <li>Not to choose common passwords — this could be implemented by technical means, using a password blacklist</li> <li>Not to use the same password anywhere else, at work or at home</li> <li>Where and how they may record passwords to store and retrieve them securely — for example, in a sealed envelope in a secure cupboard</li> <li>If they may use password management software — if so, which software and how</li> <li>Which passwords they really must memorize and not record anywhere</li> </ul> <p>Apply end-to-end non-reversible password encryption for the storage and transit of passwords over the network</p>

## 3C. Essential Cybersecurity Standard for SMEs - Access Control



### Applies to

Email, web and application servers; desktop computers; laptop computers; tablets; mobile phones



### Objective

Ensure user accounts:

Are assigned to authorized individuals only

Provide access to only those applications, computers and networks actually required for the user to perform their role



### Requirements

The organization must be in control of its user accounts and the access privileges granted to each user account. It must also understand how user accounts authenticate and control the strength of that authentication. The organization must:

Have a user account creation and approval process

Authenticate users before granting access to applications or devices, using unique credentials (see Password-based authentication)

Remove or disable user accounts when no longer required (when a user leaves the organization or after a defined period of account inactivity, for example)

Implement two-factor authentication, where available

Use administrative accounts to perform administrative activities only (no emailing, web browsing or other standard user activities that may expose administrative privileges to avoidable risks)

Remove or disable special access privileges when no longer required (when a member of staff changes role, for example)

## 3D. Essential Cybersecurity Standard for SMEs - Malware Protection (1/2)



### Applies to

Desktop computers; laptop computers; tablets; mobile phones



### Objective

Restrict execution of known malware and untrusted software, to prevent harmful code from causing damage or accessing sensitive data



### Requirements

The organization must:

- **Keep browser plugins patched**
- **Block P2P usage:** Create and enforce a no-P2P policy, including home usage of a company machine. Enforce the policy at the gateway and/or desktop
- **Turn off AutoRun**
- **Limit the use of network shares** (mapped drives. If possible limit permissions to read-only rather than read-write)
- **Review mail security and gateway blocking effectiveness:** Deploy a mail security solution which updates frequently to detect the latest bad sender IPs, spam and malware threats at the mail gateway. Implement a web security solution that will protect against Web 2.0 threats, including malicious URLs and malware
- The organization must implement a malware protection mechanism on all devices that are in scope. For each such device, the organization must use at least one of the three mechanisms listed below:

## 3D. Essential Cybersecurity Standard for SMEs - Malware Protection (2/2)



### Requirements

#### 1. Anti-malware software

- The software (and all associated malware signature files) must be kept up to date, with signature files updated at least daily. This may be achieved through automated updates, or with a centrally managed deployment.
- The software must be configured to scan files automatically upon access. This includes when files are downloaded and opened, and when they are accessed from a network folder.
- The software must scan web pages automatically when they are accessed through a web browser (whether by other software or by the browser itself).
- The software must prevent connections to malicious websites on the Internet (by means of blacklisting, for example) — unless there is a clear, documented business need and the organization understands and accepts the associated risk

#### 2. Application whitelisting

- Only approved applications, restricted by code signing, are allowed to execute on devices. The organization must:
- Actively approve such applications before deploying them to devices
- Maintain a current list of approved applications Users must not be able to install any application that is unsigned or has an \* invalid signature

#### 3. Application sandboxing

- All code of unknown origin must be run within a 'sandbox' that prevents access to other resources unless permission is explicitly granted by the user. This includes:
- Other sandboxed applications
- Data stores, such as those holding documents and photos
- Sensitive peripherals, such as the camera, microphone and GPS
- Local network access

## 3E. Essential Cybersecurity Standard for SMEs - Patch Management



 <b>Applies to</b>	Web, email and application servers; desktop computers; laptop computers; tablets; mobile phones; firewalls; routers
 <b>Objective</b>	Ensure that devices and software are not vulnerable to known security issues for which fixes are available
 <b>Requirements</b>	<p>The organization must keep all its software up to date. Software must be:</p> <ul style="list-style-type: none"><li>• Licensed and supported</li><li>• Removed from devices when no longer supported</li><li>• Patched within 14 days of an update being released, where the patch fixes a vulnerability with a severity the product vendor describes as 'critical' or 'high risk'</li></ul>

## 3F. Essential Cybersecurity Standard for SMEs – Cybersecurity awareness



	<b>Applies to</b>	Web, email and application servers; desktop computers; laptop computers; tablets; mobile phones;
	<b>Objective</b>	Provide cybersecurity training to everyone in the organization to raise awareness on threats and best practices
	<b>Requirements</b>	<p>The organization must provide periodic cybersecurity training to its employees to raise their awareness on:</p> <ul style="list-style-type: none"><li>• Ensure training provided to employee at the time of onboarding includes a module on cybersecurity awareness and best practices</li><li>• Conduct a cybersecurity awareness day annually where cybersecurity awareness programs are offered to all employees</li><li>• Run regular phishing awareness campaigns</li><li>• Share best cybersecurity practices with the employee via emails, posters and info graphs on a periodic basis</li><li>• Provide technical cybersecurity training to the IT team</li></ul>

# Based on benchmark analysis, we recommend 3 key initiatives for the countries to help mitigate the cybersecurity challenges of the SMEs

对外厳秘

PRELIMINARY

01



Define Essential  
cybersecurity  
standard for SMEs

02



Create incentives  
for SMEs to  
implement  
cybersecurity

03



Provide  
cybersecurity  
training to SMEs

# CASE EXAMPLE: UK NCSC offers 2 types of certifications for the entities with clearly mapped benefits for each certification



## Overview

To incentivize entities to implement cybersecurity, UK offers 2 types of certification with clearly mapped benefits

UK adopted a 2-pronged approach for successful implementation:

**Encouraging government entities to mandate Cyber Essentials Plus certification for suppliers**

**Creating a smooth and easy certification process** for entities

### Benefits for the compliant organizations

Reassure customers that organization is committed IT security and securing customer's data against cyber attack

Attract new business with the promise you take cyber security seriously

Build a relationship with a trusted IT supplier

Qualify for certain local & national government contracts that require Cyber Essentials certification

### Cyber Essentials (Self-assessment based)



### Cyber Essentials Plus (Audit based)



# We recommend taking 2 actions to enable incentives for the SMEs to implement cybersecurity

Detailed next

1 Encourage government agencies to mandate certification for suppliers

2 Create a simple and streamlined certification mechanism



# Countries should incentivize SMEs with two types of certifications while clearly communicating the benefits of each certification

[Detailed next](#)

Certification types	Benefits	Certification mechanism
<b>1</b>  <b>Gold Certification (self-assessment based)</b>	<p><b>Reassure customers</b> that organization is committed IT security and securing customer's data against cyber attack</p> <p><b>Attract new customers</b> with the promise you take cyber security seriously</p>	<p><b>Light touch</b> mechanism where the: Entity performs a <b>self-assessment by filling a questionnaire</b> Certification body <b>evaluates the responses and grants Gold Certification</b> if the entity passes the evaluation</p>
<b>2</b>  <b>Platinum Certification (Audit based)</b>	<p><b>All benefits of self-assessment</b></p> <p><b>Qualify for certain local &amp; national government contracts</b> that require Platinum certification</p>	<p><b>High touch</b> mechanism where the: Entity <b>volunteers to be audited</b> by one of the Certification bodies</p> <p>Certification body <b>verifies the control implementation and grants Platinum Certification</b> if the entity meets the standard</p>

# Countries should incentivize SMEs with two types of certifications while clearly communicating the benefits of each certification

对外厳秘

		Steps to be taken by the SME		Steps to be taken by the accredited auditor	
Certification types		Mechanism			
1	 Gold Certification (self-assessment based)	1 <b>Implements the controls</b> prescribed in the Essential cybersecurity standard	2 <b>Chooses a certification body</b> from the website of the accreditation body	3 <b>Fills out and submits the self-reporting questionnaire</b> on the accreditation body's website	4 <b>Evaluates the responses</b> and determines if the entity has met the requirements
2	 Platinum Certification (Audit based)	1 <b>Implements the controls</b> prescribed in the Essential cybersecurity standard	2 <b>Chooses a certification body</b> from the website of the accreditation body	3 <b>Requests and schedules an audit</b> from the Certification Body	4 <b>Visits the entity</b> and verifies entity's implementation of controls as prescribed by the standard

# Based on benchmark analysis, we recommend 3 key initiatives for the countries to help mitigate the cybersecurity challenges of the SMEs

对外厳秘

PRELIMINARY

01



Define Essential  
cybersecurity  
standard for SMEs

02



Create incentives  
for SMEs to  
implement  
cybersecurity

03



Provide  
cybersecurity  
training to SMEs

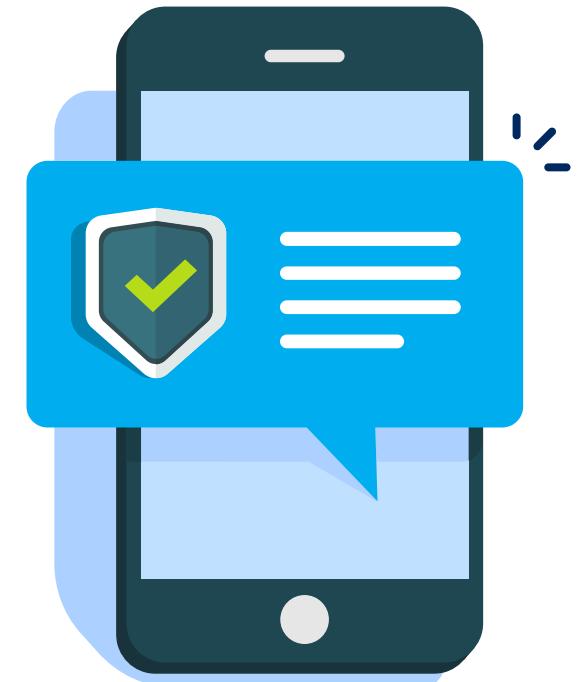
# Countries should offer an online portal with free courses for SMEs to help them implement the guidance of Essential cybersecurity standards and mitigate the talent gap

Dedicated portal to provide **free online on-demand cybersecurity courses** to SMEs that help them implement the needed controls and follow best practices related to the following 5 categories:

- Firewalls
- Access Control
- Secure Configuration
- Malware Protection
- Patch Management

In addition, portal would consist of

- Forum for submitting queries regarding the standard and compliance process
- FAQ section
- Information on details of the requirements of Essential cybersecurity standards
- Contact information of the accreditation bodies and certification bodies
- Benefits of getting Gold or Platinum certification

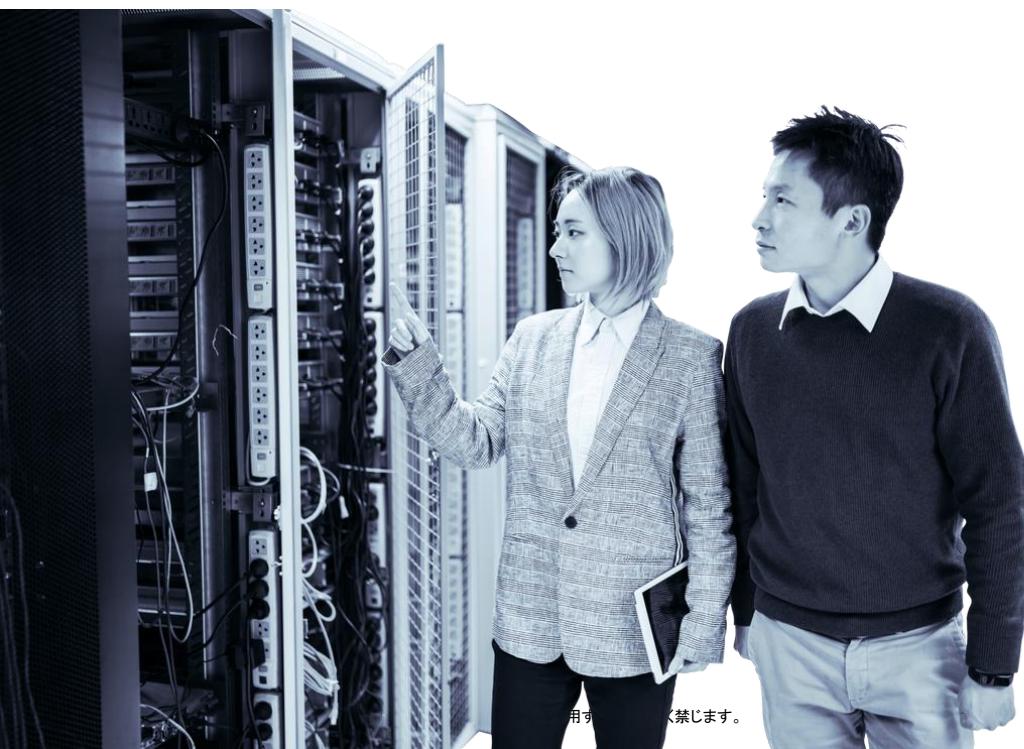


---

# Questions?

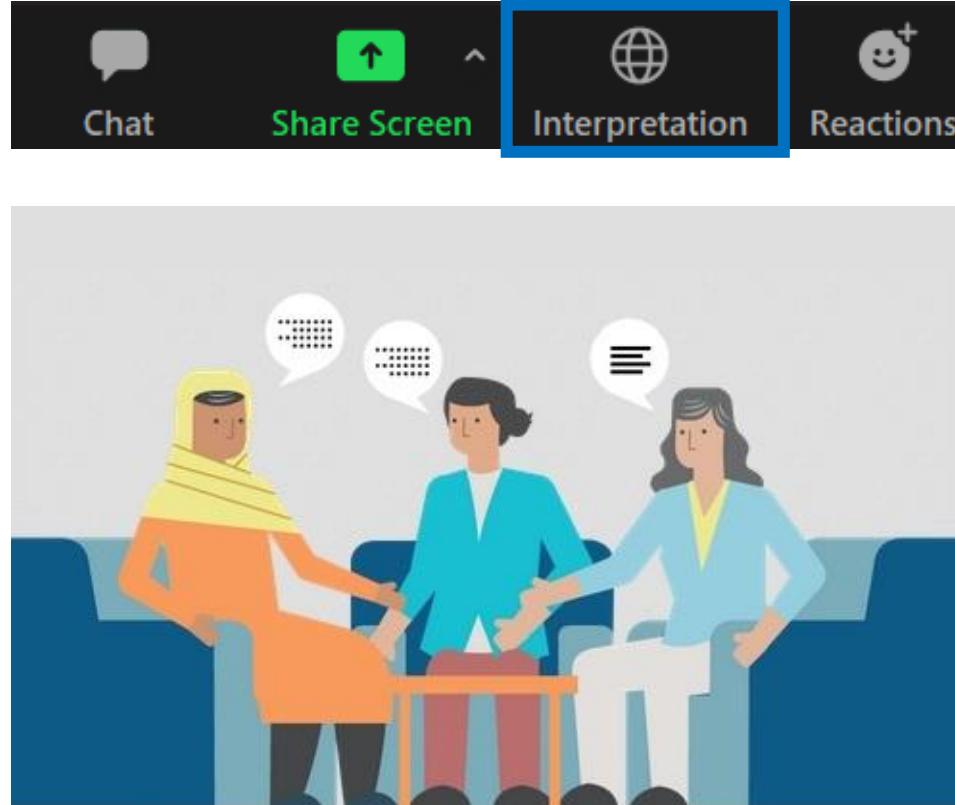
---



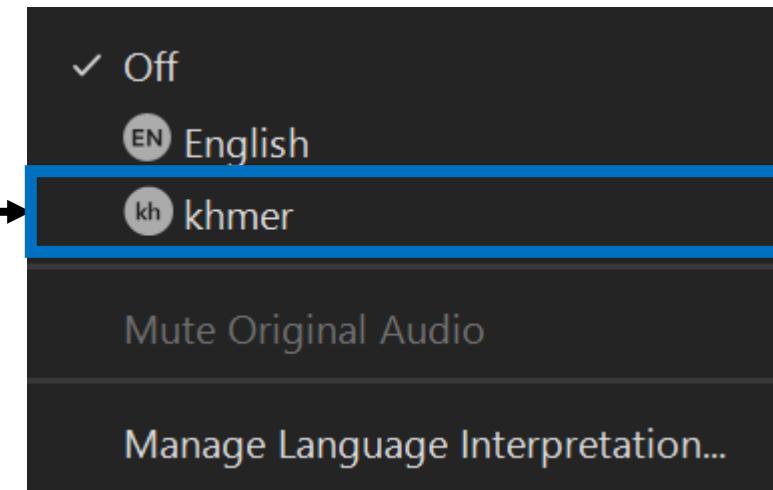
- 
1. Overview of Cyber Security Trend
  2. Definition of Cyber threat and national Incident response framework
  3. Cyber Security Regulation framework
  4. Partnership(Public, Private, Academia, International)
  5. Professional training and certification
  6. Public awareness and alerts
  7. Cyber Security for SME
  - 8. Critical Infrastructure Industry protection**
  9. CERT/ Resilience
  10. Wrap up / Cyber security assessment

# Khmer simultaneous Interpretation available

Select “Interpretation” on the bottom



Select “Khmer”



- Presentation is simultaneously translated into Khmer
- You can post question in Khmer



## Timeline

## Overview

100 minuets

## Workshop & QA

20 minuets

# Cambodia need to design Cyber security strategy with suggested strategy element

Cybersecurity strategy element	Insights from benchmarking cybersecurity strategy	#
A Governance 	<ul style="list-style-type: none"> <li>Top-performing nations are moving towards <b>centralized governance bodies</b> reporting directly to executive branches of government and serving as <b>E2E owners of cybersecurity strategy implementation</b></li> </ul>	• #2
B Legal and regulations 	<ul style="list-style-type: none"> <li><b>Comprehensive legislative frameworks</b> cover mandatory IT security standards, regulations, and best practices, and are enforced through audits and law enforcement</li> <li><b>Specific legislations to address emerging technologies</b> are evolving at fast pace in countries with advanced cybersecurity legislations</li> </ul>	• #3
E Partnerships 	<ul style="list-style-type: none"> <li><b>Regional and international partnerships</b> are actively used to foster sharing of best practices and enhancing operational and technical capabilities through joint drills &amp; audits</li> </ul>	• #4
C Talent and people 	<ul style="list-style-type: none"> <li><b>Public awareness and training</b> programs, which draw on <b>international standards and offerings</b>, form the basis for cybersecurity talent development</li> </ul>	• #5~7
F Critical infrastructure 	<ul style="list-style-type: none"> <li>CII protection programs, executed by national cybersecurity agencies, focus <b>selectively on critical assets</b> in critical sectors with timely involvement of relevant authorities</li> </ul>	• #8
D Incident response 	<ul style="list-style-type: none"> <li>National cybersecurity agencies, through <b>specialized incident response teams</b>, lead integrated response efforts with close coordination with impacted assets</li> </ul>	• #9

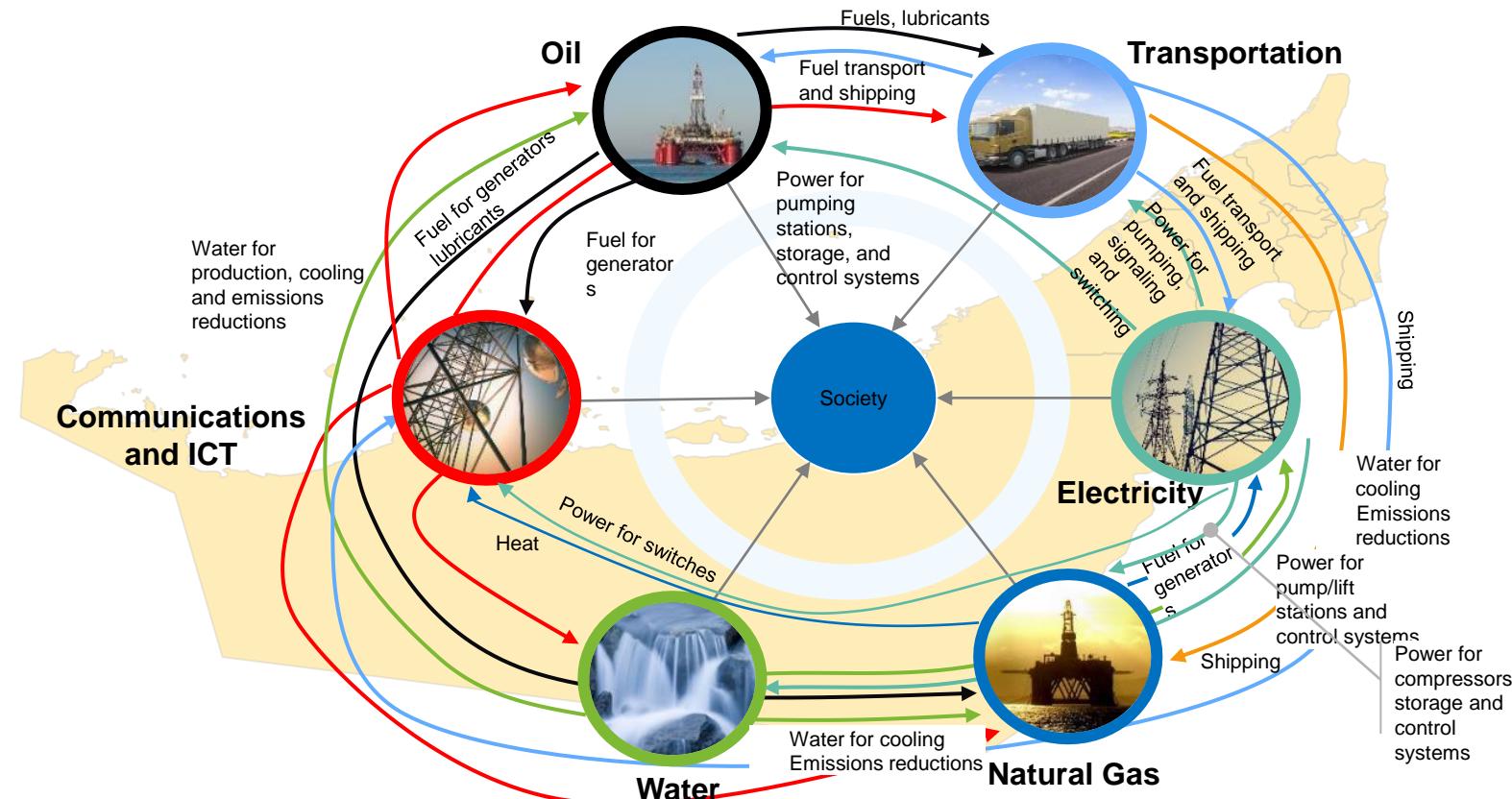
# We benchmarked 6 countries to define Critical Information Infrastructure (CII) (1/2)

  
Benchmark  
countries



**Definition:** All physical or virtual assets of ICT systems such as data, systems, facilities, network and computers that support carrying-out of a **critical function** and the **delivery of a critical service**, the **disruption** or **destruction** of which may have a **debilitating impact** on the **national security, economy, society** or any combination of these

## Examples of critical sectors and their interdependencies

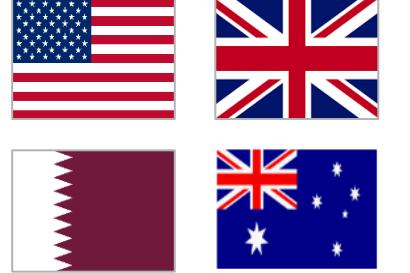


# We benchmarked 6 countries to define Critical Information Infrastructure (CII) (2/2)

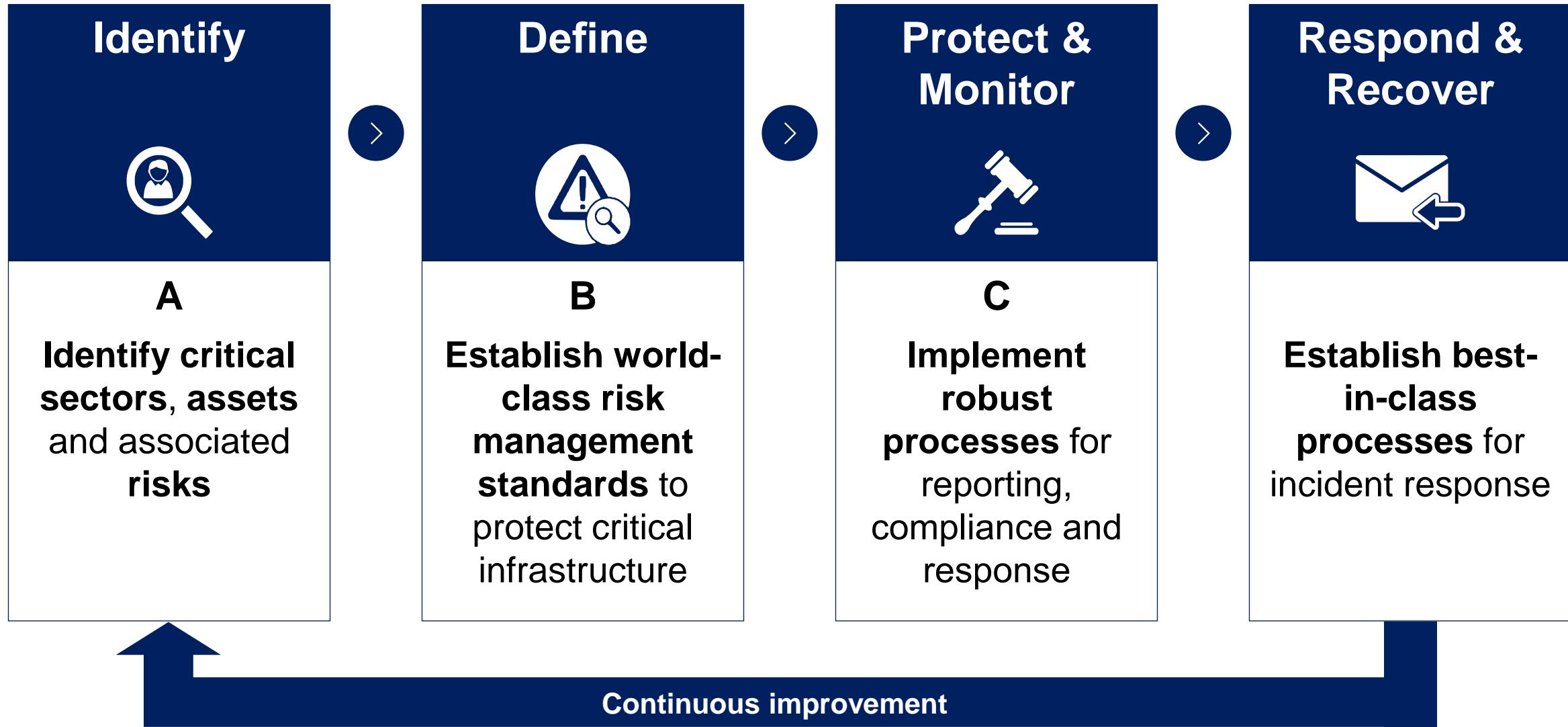
**Definition:** All physical or virtual assets of ICT systems such as data, systems, facilities, network and computers that support carrying-out of a **critical function and the delivery of a critical service**, the **disruption or destruction** of which may have a **debilitating impact** on the **national security, economy, society** or any combination of these

1	Germany		Critical Infrastructure are organizations or institutions with major importance for the public good, whose failure or damage would lead to sustainable supply bottlenecks, <b>considerable disturbance of public security or other dramatic consequences</b>
2	US		Critical infrastructure are the sectors whose <b>assets, systems, and networks, whether physical or virtual</b> , are considered so <b>vital to the United States</b> that their incapacitation or destruction would have a <b>debilitating effect on security, national economic security, national public health or safety</b> , or any combination thereof
3	UK		Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in: a) Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could <b>result in significant loss of life or casualties – taking into account significant economic or social impacts</b> ; and/or b) <b>Significant impact on national security, national defense, or the functioning of the state.</b>
4	Singapore		Physical infrastructure and assets that are vital to the continued delivery of the essential services upon which Singapore relies, the loss or compromise of which would lead to a <b>debilitating impact on security, economy or public health and safety</b>
5	Australia		Those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly <b>impact on the social or economic wellbeing of the nation</b> , or affect Australia's ability to conduct national defense and ensure national security
6	Canada		The processes, systems, facilities, technologies, networks, assets and <b>services essential to the health, safety, security or economic well-being</b> of Canadians and the <b>effective functioning of the government</b>

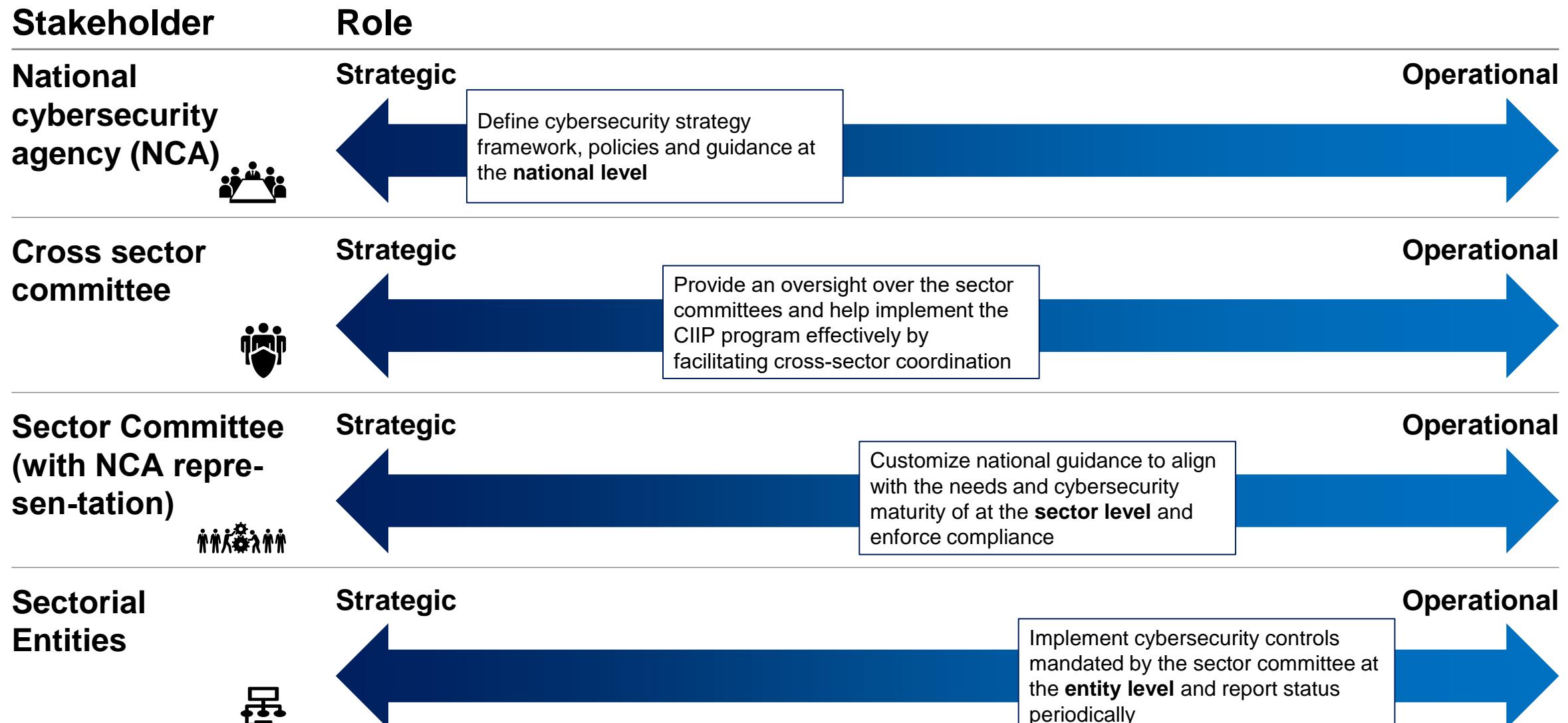
# Methodology used to develop CIIP Program

Steps	Source of insight	
A Key program components defined by 7 benchmark countries	Benchmark analysis of the key components of CIIP programs in 7 countries	 
B Alignment with the two most popular risk management frameworks	<p>Analysis of popular industry risk management frameworks:</p> <ul style="list-style-type: none"> <li>NIST Cybersecurity Risk Framework</li> <li>ISO 27001:2013</li> </ul>	 

# Proposed National Risk Management Framework for CIIP Program



# An effective governance mechanism for CIIP is established through close coordination of 4 key stakeholders



Source: Expert Interviews, Benchmarking, Team analysis

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# We have identified 3 key factors that make sectorial committees effective in the benchmark countries

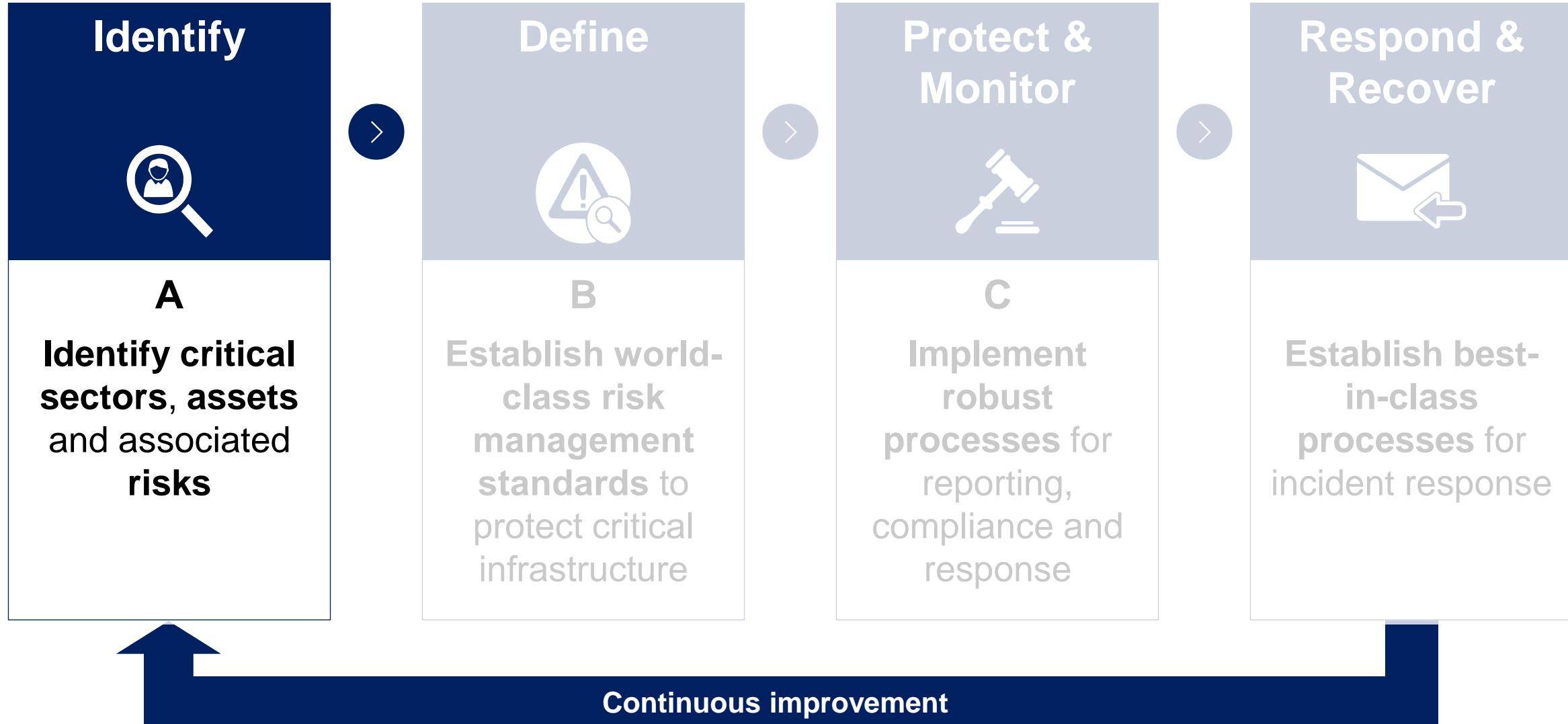
  
**Majority of the benchmarked countries have constituted sectorial committees** to customize policies per sector needs and enforce compliance



Key success factors for sector committees		Examples from benchmark countries
<b>1</b>	<b>Clear top-down communication of guidance and policies from a single agency/stakeholder</b>	While GCC and SCC for each sector help define the policies and implementation plan, each SSA takes the charge of issuing the directive Sector committee for healthcare issues all directives related to cyber after the WannaCry incident, as against multiple agencies issuing confusing (and often contradictory) directive to the hospitals
<b>2</b>	<b>Central coordination agency regulates through sectors regulators/lead govt. agencies with authoritative power to take action in case of non-compliance</b>	Cybersecurity commissioner appointed for each sector has significant powers to respond to, and prevent, cybersecurity incidents affecting Singapore. These powers include the powers of investigation such as the power to examine persons, require the production of evidence and to seize evidence Sector lead govt. agency representative appointed as asst. commissioner CII owners have to comply with codes and directions, and report incidents to the Commissioner, and conduct regular audits and risk assessments for cybersecurity vulnerabilities. There are significant criminal and civil penalties for failing to comply with these obligations
<b>3</b>	<b>Cybersecurity maturity/expertise within the sector committee</b>	For sectors such as Banking and Transport that have high maturity level for cybersecurity, the sector committee has the needed cyber expertise to issue sector specific directives. For sectors such as Food, Retail etc. which lack the cyber maturity, NCSC provides the needed technical expertise to the committees to bridge the gaps

# Proposed national risk management framework for CIIP program

Detailed next



# A: 'Identify' component of CIIP includes 3 key steps

 Detailed next

Key Steps	Methodology	Owner	Sources of insight
1 <b>Identify critical sectors in the country</b>	<ul style="list-style-type: none"> <li>Identify the sectors considered <b>critical by majority benchmark countries</b></li> <li><b>Align with the priority sectors</b> defined in the national strategies</li> </ul>	NCA	             
2 <b>Identify critical assets for each sector</b>	<ul style="list-style-type: none"> <li>Define <b>social and economic thresholds</b> to determine the criticality of the assets by gauging the impact of their degradation or failure</li> <li><b>Use the thresholds to assess and identify</b> if an asset is critical</li> </ul>	Sector Committee	      
3 <b>Identify critical systems in each of the critical assets</b>	<ul style="list-style-type: none"> <li>Define a <b>risk rating methodology to assign a risk rating</b> for the systems within each asset</li> <li>Identify the critical systems by <b>assessing the risk rating for each system</b> based on the defined methodology</li> </ul>	NCA/Sector Committee	International risk assessment frameworks    <b>OWASP Risk Rating Methodology</b>

Source: Benchmarking, Expert Interviews, Team analysis

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# A1: Benchmark analysis of critical sectors across 13 countries

Critical for majority of the 12 benchmarked countries

Sectors													
We benchmarked 13 countries to identify 11 Critical sectors that are vital for majority of the countries													
Energy	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ICT	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Health	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Water and Wastewater	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Finance and Insurance	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Transportation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Government (State & Administration)	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗	✓	✓
Food and Agriculture	✓	✓	✓	✓	✗	✗	✗	✓	✓	✓	✓	✓	✗
Media and Culture	✓	✗	✗ <sup>1</sup>	✗	✗ <sup>1</sup>	✗	✗ <sup>1</sup>	✓	✓	✗	✓	✗	✗
Nuclear Reactors, Materials & Waste	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓
Emergency Services	✗	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗	✓	✓
Chemicals	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗
Space	✗	✗	✓	✗	✗	✗	✗	✓	✗	✓	✗	✓	✗
Defense Industrial Base	✗	✓	✓	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗
Critical Manufacturing	✗	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✓	✗
Dams	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗
Environment	✗	✗	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗
Commercial Facilities	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Economy	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗

1. Partially included in Communications as the Broadcasting sub-sector 2. Included in Energy as a sub-sector 3. Included in Water as a sub-sector

Source: Germany: Cybersecurity Strategy for Germany; US: <https://www.dhs.gov/critical-infrastructure-sectors>; UK: <https://www.cpni.gov.uk/critical-national-infrastructure-0>; Singapore: <https://www.apec-epwg.org/public/uploadfile/act/98c54734e9ad749df3fc174a50491c2.pdf>; [https://publicwiki01.fraunhofer.de/CIPedia/index.php/Critical\\_Infrastructure\\_Sector](https://publicwiki01.fraunhofer.de/CIPedia/index.php/Critical_Infrastructure_Sector)

# A: 'Identify' component of CIIP includes 3 key steps

[Detailed next](#)

Key Steps	Methodology	Owner	Sources of insight
1 <b>Identify critical sectors in the country</b>	<ul style="list-style-type: none"> <li>Identify the sectors considered <b>critical by majority benchmark countries</b></li> <li><b>Align with the priority sectors</b> defined in the national strategies</li> </ul>	NCA	
2 <b>Identify critical assets for each sector</b>	<ul style="list-style-type: none"> <li>Define <b>social and economic thresholds</b> to determine the criticality of the assets by gauging the impact of their degradation or failure</li> <li><b>Use the thresholds to assess and identify</b> if an asset is critical</li> </ul>	<b>Sector Committee</b> <b>Sector Entities</b>	 
3 <b>Identify critical systems in each of the critical assets</b>	<ul style="list-style-type: none"> <li>Define a <b>risk rating methodology to assign a risk rating</b> for the systems within each asset</li> <li>Identify the critical systems by <b>assessing the risk rating for each system</b> based on the defined methodology</li> </ul>	<b>NCA/Sector Committee</b> <b>Sector Entities</b>	International risk assessment frameworks  <p><b>OWASP Risk Rating Methodology</b></p>

Source: Benchmarking, Expert Interviews, Team analysis

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

## A2: To identify CII assets within each sector, thresholds will be defined by sectorial committee



We benchmarked **6 countries** to determine the criteria to identify critical assets within each critical sector



### Key steps

- 1. Setup sectorial committees**  
for each of the 9 critical sectors with representatives from:
  - NCA
  - Lead Govt. Agency
  - Select major entities in the respective sector
- 2. Each sectorial committee defines the thresholds** to identify the critical assets within their sector, typically through social and economic metrics such as:
  - **# of goods/services impacted**
  - **\$ value of economic loss**
  - **# of people impacted**
- 3. Each sectorial entity identifies itself as the critical asset or not** based on the decided thresholds defined by the committee, and informs the Lead Govt. Agency

## A2: Example - Thresholds to identify CII assets in Health sector

ILLUSTRATIVE – TO BE FINALIZED BY SECTORIAL COMMITTEES

<b>Asset</b>	<b>Asset category</b>	<b>Threshold value</b>
<b>In-patient care</b>	Hospital	30 000 patients in full-time hospital care /year
<b>Supply of directly life-sustaining medical products which are consumer goods</b>	Production site	90,68 million turnover in euros /year
	Dispensary	90,68 million turnover in euros /year
<b>Supply of prescription drugs and blood and plasma concentrates for use in or on the human body</b>	Production site	4 650 000 packages placed on the market/year
	Facility or system for taking and further processing blood donations	34 000 products produced or placed on the market/year
	Operations and storage room	4 650 000 packages handled / year
	Facility or system for distributing prescription drugs	4 650 000 packages transported [year
	Pharmacy	4 650 000 packages dispensed /year
<b>Laboratory diagnostics</b>	Transport system	1500 000 cumulated no. of requests of laboratories in the group year
	Communications system for sending requests and test results	1500 000 requests/year
	Laboratory	1500 000 requests /year

# A: 'Identify' component of CIIP includes 3 key steps

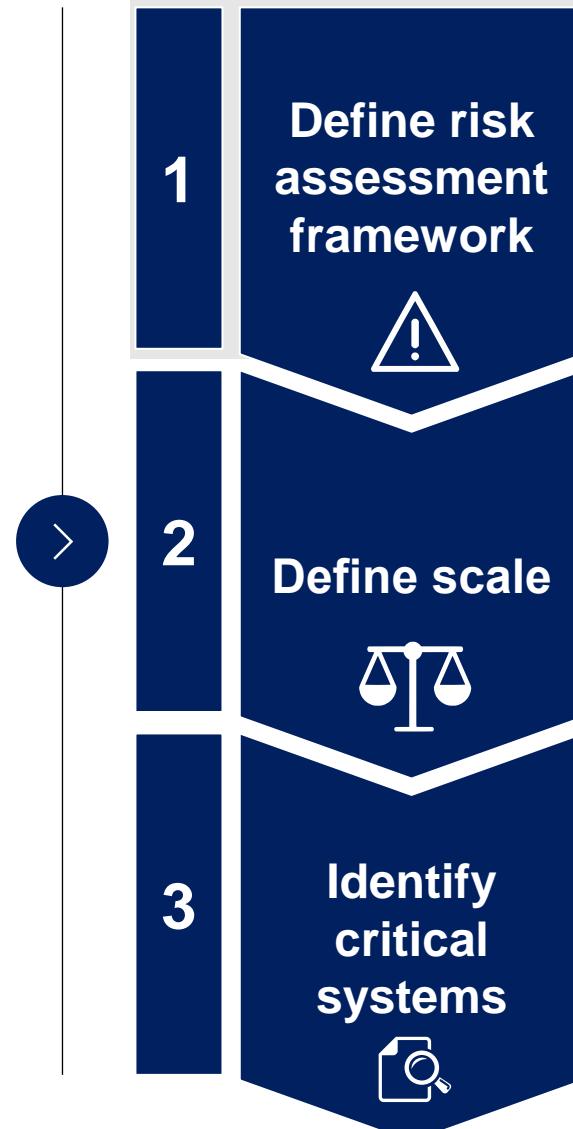
[Detailed next](#)

Key Steps	Methodology	Owner	Sources of insight
1 <b>Identify critical sectors in the country</b>	<ul style="list-style-type: none"> <li>Identify the sectors considered <b>critical by majority benchmark countries</b></li> <li><b>Align with the priority sectors</b> defined in the national strategies</li> </ul>	NCA	
2 <b>Identify critical assets for each sector</b>	<ul style="list-style-type: none"> <li>Define <b>social and economic thresholds</b> to determine the criticality of the assets by gauging the impact of their degradation or failure</li> <li><b>Use the thresholds to assess and identify</b> if an asset is critical</li> </ul>	<b>Sector Committee</b> <b>Sector Entities</b>	 
3 <b>Identify critical systems in each of the critical assets</b>	<ul style="list-style-type: none"> <li>Define a <b>risk rating methodology to assign a risk rating</b> for the systems within each asset</li> <li>Identify the critical systems by <b>assessing the risk rating for each system</b> based on the defined methodology</li> </ul>	<b>NCA/Sector Committee</b> <b>Sector Entities</b>	International risk assessment frameworks   <b>OWASP Risk Rating Methodology</b>

# A3: To Within each critical asset, critical systems are identified by risk score prioritization

 Detailed next

  
We benchmarked  
**6 countries** to  
determine the  
process of  
identifying critical  
systems



- NCA to define the risk assessment framework that is in line with the internationally recognized frameworks

NCA

- Sector committees define the scale for impact severity and likelihood of incidence in the risk assessment framework for their respective sector

Sector Committee

- Sector Committee to ask entities to self-assess their systems to identify critical systems based on the risk assessment frameworks and scale
- Sector Entities to complete the assessment & share list of critical systems with Sector Committee

Sectorial Entity

# A. 3.1: Within each critical asset, critical systems are identified through a risk assessment framework

対外厳密

 Detailed next



We validated proposed risk rating framework against internationally recognized and accepted risk rating methodologies such as **ISO 27005** and **OWASP**



**OWASP Risk Rating Methodology**

## Proposed risk rating framework:

### 1. Create systems inventory



- **List of systems are gathered** from all the departments and business units
- Systems are **organized by their asset class** (e.g., PII)

### 2. Calculate risk rating



- For each asset, threats are determined by **listing types of attackers, purpose of the attack and the attack type** (C-I-A)
- **Severity across 6 key impact dimensions** and the **likelihood of incidence** are determined for each threat
- Risk rating is determined as a **product of impact severity and likelihood of incidence**

### 3. Prioritize and determine critical systems



- **Systems are prioritized** in the descending order of their risk score
- Systems with a **risk rating of moderate or higher** are classified as **critical systems**

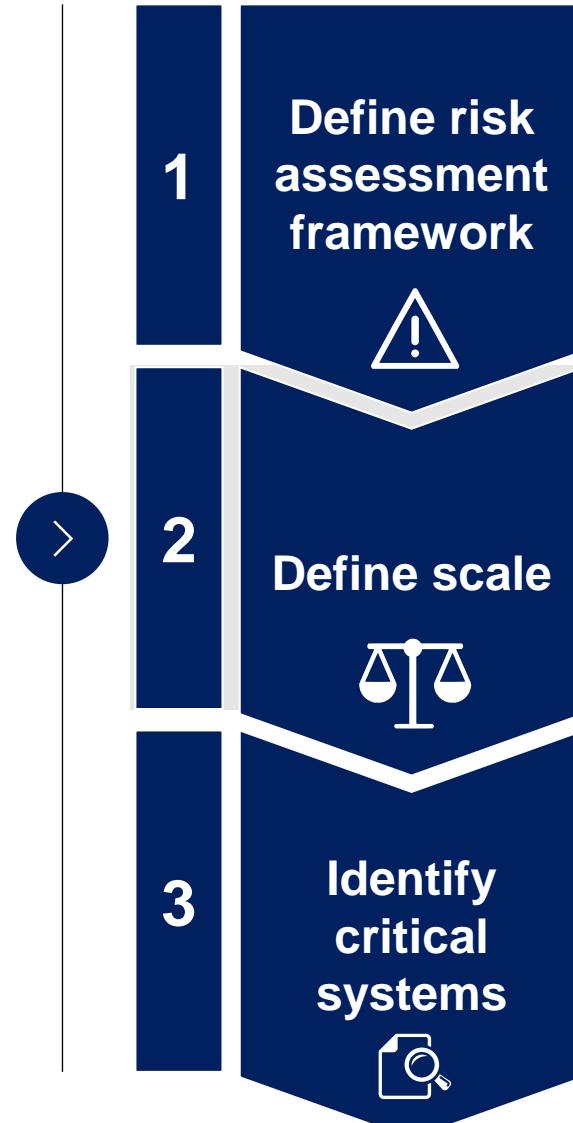
# A. 3.1: Example worksheet to be filled out by the entities to calculate risk rating and prioritize their systems

			Impact severity								Risk calculation		
Asset info		Attack description			17%	17%	17%	17%	17%	17%	Overall Impact	Likelihood	Risk score
#	Asset Class	Asset	Attackers/ Potential threat actors	Motive	Attack type (CIA)	Financial	Safety/ Injury	Regulatory /Legal	Reputational (National Image)	Operational (business continuity)	Interdependency for other assets		
1	Personal Identifiable Information												
2	Financial information												
3	Strategic planning												
4	Intellectual property												

# A3: Within each critical asset, critical systems are identified by risk score prioritization

 Detailed next

  
We benchmarked  
**6 countries** to  
determine the  
process of  
identifying critical  
systems



- NCA to define the risk assessment framework that is in line with the internationally recognized frameworks

NCA

- Sector committees define the scale for impact severity and likelihood of incidence in the risk assessment framework for their respective sector

Sector Committee

- Sector Committee to ask entities to self-assess their systems to identify critical systems based on the risk assessment frameworks and scale
- Sector Entities to complete the assessment and share list of critical systems with Sector Committee

Sectorial Entity

## A. 3.2: Example of scale for impact severity

ILLUSTRATIVE – TO BE DEFINED BY SECTORIAL COMMITTEE GROUPS

Impact Areas	1 -- Incidental	2 -- Minor	3 -- Moderate	4 -- Major	5 -- Severe
<b>Financial</b>	<ul style="list-style-type: none"> <li>0.025% to 0.25% deviation in expense and/or revenue budget</li> </ul>	<ul style="list-style-type: none"> <li>0.25% to 1% deviation in expense and/or revenue budget</li> </ul>	<ul style="list-style-type: none"> <li>1% to 2% deviation in expense and/or revenue budget</li> </ul>	<ul style="list-style-type: none"> <li>2% to 5% deviation in expense and/or revenue budget</li> </ul>	<ul style="list-style-type: none"> <li>More than 5% deviation in overall expense and/or revenue budget</li> </ul>
<b>Regulatory and Compliance</b>	<ul style="list-style-type: none"> <li>Isolated, quickly remedied noncompliance standards, regulations or contracts terms</li> <li>&lt;=50,000 AED legal claim</li> </ul>	<ul style="list-style-type: none"> <li>Isolated, quickly remedied noncompliance standards, regulations or contracts terms</li> <li>&gt;50,000 AED and &lt;=250,000 AED legal claim</li> </ul>	<ul style="list-style-type: none"> <li>Repeated, slowly remedied standard, contractual or regulatory noncompliance</li> <li>&gt;250,000 AED and &lt;=0.5M AED legal claim</li> </ul>	<ul style="list-style-type: none"> <li>Material non-compliance with standards regulations or contract terms</li> <li>&gt;0.5M AED and &lt;=2M AED legal claim</li> </ul>	<ul style="list-style-type: none"> <li>Material non-compliance with standards, regulations or contract terms</li> <li>&gt;2M AED legal claim</li> </ul>
<b>Reputational</b>	<ul style="list-style-type: none"> <li>Minor, adverse attention from local community, and local media; quickly remedied in hours</li> </ul>	<ul style="list-style-type: none"> <li>Adverse attention from the local community and local media; remediated within few days</li> </ul>	<ul style="list-style-type: none"> <li>Criticism from the local community and local media; remediated within 1 to 2 weeks</li> </ul>	<ul style="list-style-type: none"> <li>Significant adverse attention from the regional community, and regional media; remediated within 2 to 4 weeks</li> </ul>	<ul style="list-style-type: none"> <li>Very serious adverse attention from international community; sustained, negative international coverage; difficulties to remediate within a month</li> </ul>
<b>Interdependency for other sectors</b>	<ul style="list-style-type: none"> <li>No impact on other dependent critical sectors</li> </ul>	<ul style="list-style-type: none"> <li>Minor impact on other dependent critical sectors</li> </ul>	<ul style="list-style-type: none"> <li>Moderate impact on other dependent critical sectors</li> </ul>	<ul style="list-style-type: none"> <li>Significant impact on other dependent critical sectors</li> </ul>	<ul style="list-style-type: none"> <li>Debilitating impact on other dependent critical sectors</li> </ul>
<b>Business Continuity</b>	<ul style="list-style-type: none"> <li>&lt;=1 hour Partial building closure or Data Centers discontinuity</li> </ul>	<ul style="list-style-type: none"> <li>&gt;1 hour and &lt;=3 hours Partial building closure or Data Centers discontinuity</li> </ul>	<ul style="list-style-type: none"> <li>&gt;3 hours and &lt;=5 hours Partial building closure or Data Centers discontinuity</li> </ul>	<ul style="list-style-type: none"> <li>&gt;5 hours and &lt;=7 hours Partial building closure or Data Centers discontinuity</li> </ul>	<ul style="list-style-type: none"> <li>&gt;7 hours Partial building closure or Data Centers discontinuity</li> </ul>
<b>Stakeholders Satisfaction</b>	<ul style="list-style-type: none"> <li>&lt;=1% variance in results from last Employees, Customers, or Vendors Satisfaction Survey score</li> <li>&lt;=1% Employees turnover</li> </ul>	<ul style="list-style-type: none"> <li>&gt;1% and &lt;=2% variance in results from last Employees, Customers, or Vendors Satisfaction Survey score</li> <li>&gt;1% and &lt;=2% Employees turnover</li> </ul>	<ul style="list-style-type: none"> <li>&gt;2% and &lt;=3% variance in results from last Employees, Customers, or Vendors Satisfaction Survey score</li> <li>&gt;2% and &lt;=3% Employees turnover</li> </ul>	<ul style="list-style-type: none"> <li>&gt;3% and &lt;=5% variance in results from last Employees, Customers, or Vendors Satisfaction Survey score</li> <li>&gt;3% and &lt;=5% Employees turnover</li> <li>Loss of any Executive</li> </ul>	<ul style="list-style-type: none"> <li>&gt;5% variance in results from last Employees, Customers, or Vendors Satisfaction Survey score</li> <li>&gt;5% Employees turnover</li> <li>Loss of multiple Executives</li> </ul>

Source: McKinsey CRI, ISO 27005, OWASP risk rating methodology, Expert interviews

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

## A. 3.2: Example of scale for the likelihood of incidence

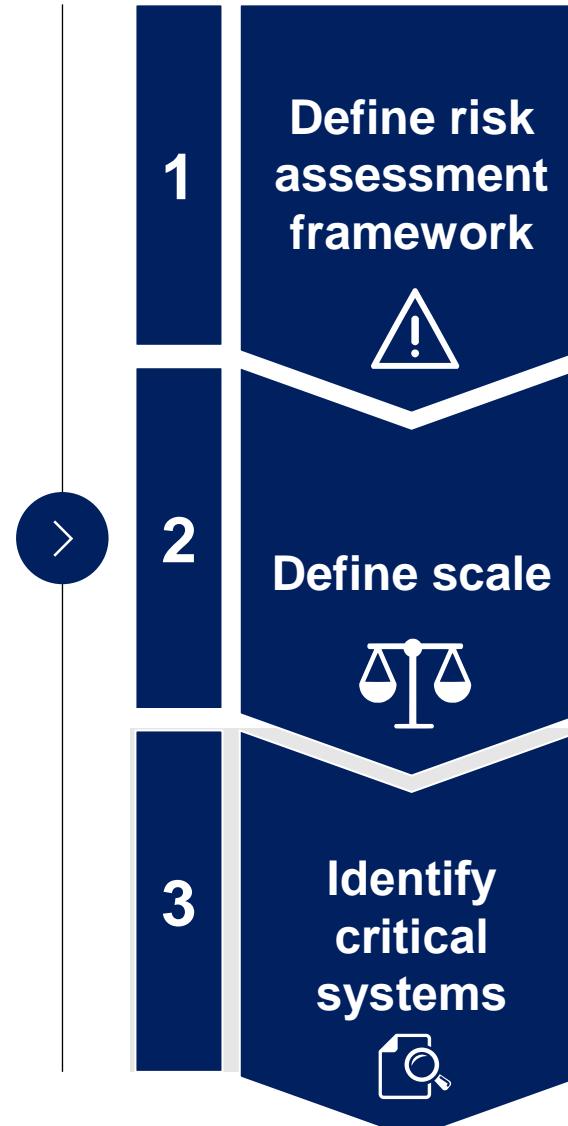
ILLUSTRATIVE – TO BE DEFINED BY SECTORIAL COMMITTEES

<b>Description</b>	
<b>1.Almost impossible</b>	<ul style="list-style-type: none"><li>• Almost no motivated threat actors</li><li>• Strong protection in place with no clearly identified vulnerabilities</li></ul>
<b>2.Unlikely</b>	<ul style="list-style-type: none"><li>• Some moderately motivated threat actors with low sophistication</li><li>• Strong protection in place with no clearly identified vulnerabilities</li></ul>
<b>3.Possible</b>	<ul style="list-style-type: none"><li>• Some highly motivated threat actors with low sophistication</li><li>• Partially tested infrastructure with reasonable protection</li></ul>
<b>4.Very likely</b>	<ul style="list-style-type: none"><li>• Sophisticated threat actors with high motivations</li><li>• Partially tested infrastructure with reasonable protection</li></ul>
<b>5.Almost Certain</b>	<ul style="list-style-type: none"><li>• Sophisticated threat actors with high motivations and the ability to conduct zero day attack</li><li>• Untested technology stack with high incidents of vulnerabilities</li></ul>

# A3: Within each critical asset, critical systems are identified by risk score prioritization

 Detailed next

  
We benchmarked  
**6 countries** to  
determine the  
process of  
identifying critical  
systems



- NCA to define the risk assessment framework that is in line with the internationally recognized frameworks

NCA

- Sector committees define the scale for impact severity and likelihood of incidence in the risk assessment framework for their respective sector

Sector Committee

- Sector Committee to ask entities to self-assess their systems to identify critical systems based on the risk assessment frameworks and scale
- Sector Entities to complete the assessment and share list of critical systems with Sector Committee

Sectorial Entity

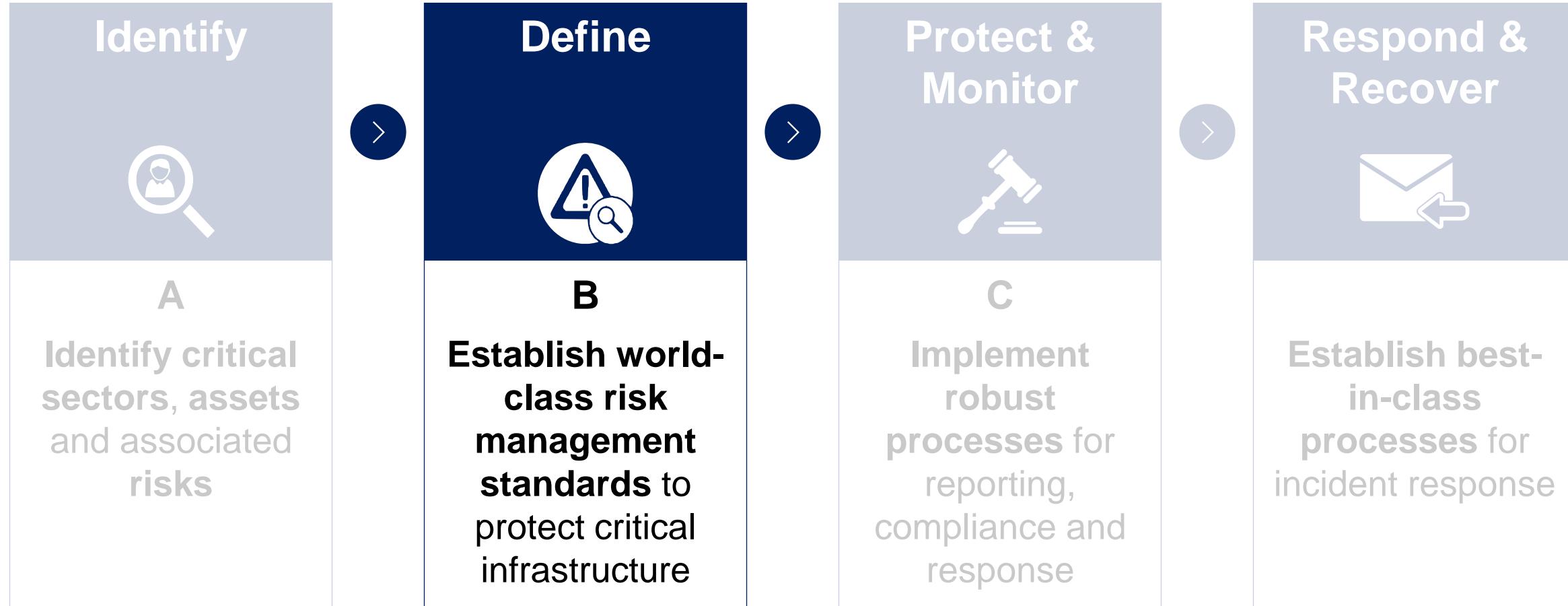
# A. 3.3: Example of the filled self-assessment template that the sectorial working group will receive from each of the sectorial entities listing out their critical systems

Low	Medium
High	Very High

#	Asset info		Attack description			Impact severity							Risk calculation			
	Asset Class	Asset	Attackers/ Potential threat actors	Motive	Attack type (CIA)	17%	17%	17%	17%	17%	17%	Operational (business continuity)	Interdependency for other assets	Overall Impact	Likelihood	Risk score
1	Personal Identifiable Information	Customer account information	Competitors Hacktivists Market Traders Suppliers	To gain competitive advantage by obtaining confidential patient records for gaining business/competitive advantage	Confidentiality	4	3	4	5	2	2	3	4	12		
2	Financial information	Transaction records information	Competitors Hacktivists Market Traders Suppliers	Integrity	Integrity	5	2	3	3	2	1	3	4	12		
3	Strategic planning	Internal PMO information	Competitors Market Traders Suppliers Insiders	Confidentiality	Confidentiality	3	1	3	1	2	1	2	3	6		
4	Control system	Locker monitoring system	Insiders Customers Hacktivists Organized Criminals	Availability	Availability	4	2	1	3	3	1	2	3	6		

# Key components of the CIIP

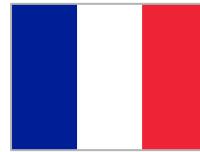
Detailed next



# B: Key learnings from benchmark countries on cybersecurity standards implementation



We benchmarked **6 countries** to understand the implementation of risk standards in order to manage the risks in critical sectors



## Key learnings from best in class countries



**Recommend a suite of standards** instead of being prescriptive on a single standard



**Leverage globally recognized standards** (e.g. ISO, NIST, etc.) which are regularly updated by dedicated global teams



**Empower Sector Committees with flexibility to customize the standards and controls** as per the unique requirements of sector

## B: ‘Define’ component of CIIP includes 2 key steps

 Detailed next

Key Steps	Methodology	Owner	Sources of insight
<b>1</b> Recommend general and sector-specific standards 	Recommend a suite of <b>general and sector-specific risk management standards</b> for cybersecurity controls organized by domains, from which entities in the critical sectors can choose from to protect their systems	NCA	       <b>NATIONAL ELECTRONIC SECURITY AUTHORITY</b> <small>UNITED ARAB EMIRATES</small>  
<b>2</b> Customize domains and standards for each sector 	Based on sector specific requirements, each of the 9 sector committees to: <ul style="list-style-type: none"> <li>Decide whether to be prescriptive about specific general risk management standards for entities to use <b>or give entities the flexibility</b> to choose from the suite of recommended standards</li> <li>Choose and recommend sector-specific standards to address the unique needs of the sector</li> <li>Identify which domains are mandatory versus optional for entities to implement</li> </ul>	Sector Committee	     

# B1: In addition, NCA should recommend a suite of sector-specific standards for the sectorial committee to choose from (1/3)

	<b>Organization</b>	<b>Number/Name</b>	<b>Description</b>	<b>Focus</b>
<b>① Energy</b>	AGA	AGA 12-1	Cryptographic Protection of SCADA Communications	Encryption
	API	API 1164	Pipeline SCADA Security	Control System
	IEC	IEC 62351	Data and Communications Security	Communications
	IEEE	IEEE 1402	IEEE Guide for Electric Power Substation Physical and Electronic Security	Physical and Control System
	NERC	NERC 1200	Cyber Security	Control System
	NERC	NERC CIP-002 through 009	Cyber Security	Control System
	NERC	NERC Security Guidelines	Security Guidelines for the Electricity Sector	Control System
<b>② Chemical</b>	CIDX	Version 2.0	Guidance for Addressing Cybersecurity in the Chemical Sector	Control System
	CFAT	Chemical facilities anti-terrorism standards (CFATS) risk-based performance standard 8	Provides standards on how to deter cyber sabotage, including by preventing unauthorized onsite or remote access to Chemicals of Interest (COI) critical process controls, such as Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCSs), Process Control Systems (PCPs), Industrial Control Systems (ICs), critical business system and other sensitive computerized systems at chemical facilities	Cyber Sabotage
<b>③ Finance &amp; Insurance</b>	PCI	DSS	A joint venture by the major credit card companies, the Payment Card Industry security council's Data Security Standard is a set of policies and procedures intended to improve the security of card transactions and cardholder data.	Payment cards

Source: US DHS Cybersecurity Framework Implementation Guidance for Chemicals; Process Control System Cyber Security Standards – an Overview – Idaho National Laboratory; CISO Survey, Expert Interviews

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# B1: In addition, NCA should recommend a suite of sector-specific standards for the sectorial committee to choose from (2/3)

	<b>Organization</b>	<b>Number/Name</b>	<b>Description</b>	<b>Focus</b>
<b>3 Finance &amp; Insurance</b>	American Institute of Certified Public Accountants	SSAE18	SSAE 18 defines a subservice organization as a service organization used by another service organization to perform some of the services provided to user entities that are likely to be relevant to those user entities' internal control over financial reporting	Financial Reporting
	New York Dept. of Financial Services	NYDFS500	The NYDFS Cybersecurity Regulation works by imposing strict cybersecurity rules on covered organizations, including the installment of a detailed cybersecurity plan, the designation of a Chief Information Security Officer (CISO), the enactment of a comprehensive cybersecurity policy, and the initiation and maintenance of an ongoing reporting system for cybersecurity events. These components are all made up of several sub-regulations and requirements	...
<b>4 Telecom</b>	ISO	27011	Information security controls for the telecoms industry based on ISO 27002	Control System
<b>5 Nuclear</b>	RG	RG 5.71	Cyber Security Programs for Nuclear Facilities	Control System cyber security
	NEI	NEI 04-04	Cyber Security Program for Power Reactors, Nuclear Energy institute	Control System cyber security
	NEI	NEI 08-09	Cyber Security Plan for Nuclear Power Reactors	Control System cyber security
	NEI	NEI 13-10	Cyber Security Control Assessments	Control System cyber security

Source: US DHS Cybersecurity Framework Implementation Guidance for Chemicals; Process Control System Cyber Security Standards – an Overview – Idaho National Laboratory; CISO Survey, Expert Interviews

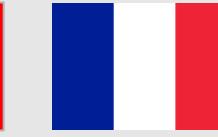
機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# B1: In addition, NCA should recommend a suite of sector-specific standards for the sectorial committee to choose from (3/3)

	<b>Organization</b>	<b>Number/Name</b>	<b>Description</b>	<b>Focus</b>
<b>6 Nuclear</b> 	RG	RG 1.152	Criteria for Use of Computers in Safe Systems of Nuclear Power Plants," U.S. Nuclear Regulatory Commission	Control System cyber security
	IEEE	IEEE standard 7-4.3.2-2003	Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers	Control System cyber security
	NIST	NIST SP 800-82	Guide to Industrial Control Systems Security, National Institute of Standards and Technology	Control System cyber security
<b>7 Healthcare</b> 	ISO	ISO 27799	Defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002 and is a companion to that international standard	Health informatics
	NIST	NIST SP 800-66	Federal guidance intended to help educate readers about information security terms used in the HIPAA security rule and improve understanding of the meaning of the security standards set out in the security rule	Information technology
	HITRUST	CSF	The HITRUST CSF was developed to address the multitude of security, privacy and regulatory challenges facing organizations. By including federal and state regulations, standards and frameworks, and incorporating a risk-based approach, the HITRUST CSF helps organizations address these challenges through a comprehensive and flexible framework of prescriptive and scalable security controls	Information Technology

## B: ‘Define’ component of CIIP includes 2 key steps

 Detailed next

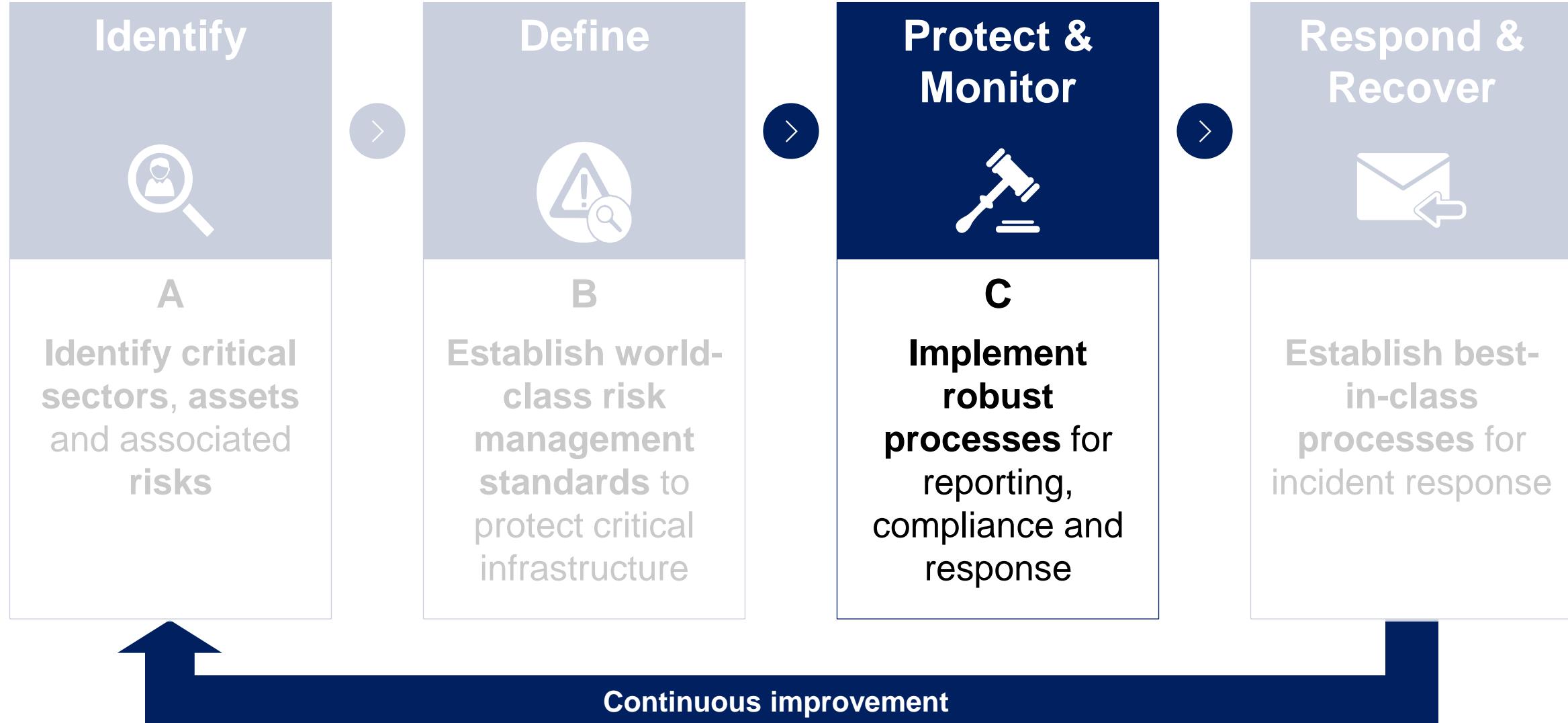
Key Steps	Methodology	Owner	Sources of insight
<b>1</b> Recommend general and sector-specific standards 	Recommend a suite of <b>general and sector-specific risk management standards</b> for cybersecurity controls organized by domains, from which entities in the critical sectors can choose from to protect their systems	NCA	        
<b>2</b> Customize domains and standards for each sector 	Based on sector specific requirements, each of the 9 sector committees to: <ul style="list-style-type: none"> <li>Decide whether to be prescriptive about specific general risk management standards for entities to use <b>or give entities the flexibility</b> to choose from the suite of recommended standards</li> <li>Choose and recommend sector-specific standards to address the unique needs of the sector</li> <li>Identify which domains are mandatory versus optional for entities to implement</li> </ul>	Sector Committee	     

## B2: Sector committees can customize the guidance based on the needs of their respective sectors

Area of guidance	Specific questions to be answered
<b>1</b> General standards	<ul style="list-style-type: none"> <li>From the list recommended by the NCA, which general standards to recommend the entities in the sector to follow?</li> <li>Are the recommended standards mandatory or optional?</li> </ul> 
<b>2</b> Sector-specific standards	<ul style="list-style-type: none"> <li>From the list recommended by the NCA, which sector-specific standards to recommend the entities in the sector to follow?</li> <li>Which additional sector-specific standards to include in the list of recommended standards?</li> <li>Are the recommended standards mandatory or optional?</li> </ul> 
<b>3</b> Domains/ Categories of controls	<ul style="list-style-type: none"> <li>Among the domains recommended by the NCA, which domains to prioritize for the entities in the sector to implement?</li> <li>Are the recommended domains mandatory or optional?</li> </ul> 

# Key components of the CIIP

Detailed next



# C: ‘Protect & Monitor’ component of CIIP program includes 2 key steps

Detailed next

Key Steps	Methodology	Owner	Sources of insight
1 Assess current state and define the plan to achieve the target state	Define the reporting template & frequency for sectorial entities based on the recommended standards to keep them accountable	NCA/Sector Committee	      
	Assess the current state of the organization against the standards or controls recommended by the Sector Committee and identify the gaps	Sectorial Entities	   
	Define the plan to bridge the gaps, and report the implementation status as per the template mandated by the regulator	Sectorial Entities	
2 Conduct periodic audits for compliance	Define the framework for audit and compliance	NCA	  
	Define the roles and responsibilities for auditing	Sector Committee	  
	Audit the sector entities for compliance	Accredited Auditors	

# C1: The proposed reporting mechanism is aligned with the best in class countries

対外厳秘



We benchmarked **6 countries** to understand the process of tracking the progress of CIIP program implementation



## Key learnings from best in class countries



**Define a reporting template** to enable sector regulators to track the progress of CIIP implementation across all sector entities



**Entrust the sector regulators to monitor the progress** for their respective sectors and hold the entities accountable



**Compile the reports from all sector regulators** who in turn compile it from their sectoral entities every quarter

# C1: Proposed reporting template for the entities is aligned with the approach of benchmark countries

 Detailed next



We **benchmarked**  
**4 countries** to  
understand the  
process of tracking  
the progress of CIIP  
program  
implementation



Completed: 0 Remaining: 3 % Completion: 0%													
Control #	Control Name	Control	Priority	Applicability		Status	Deadline	Ownership	Comment	Justification	Entry Complete		
<b>Family Name</b>													
<b>Sub-Family Name</b>													
Control Number	Priority 1 Control Name (can be management or Technical Control)	Control	Priority	Always Applicable	Applicable	Control Implementation: 0%	Control Completion Time:				Incomplete		
	Sub-control Number	Sub-control		Always Applicable	Applicable	Select	Select						
	Sub-control Number	Sub-control		Always Applicable	Applicable	Select	Select						
	Sub-control Number	Sub-control		Always Applicable	Applicable	Select	Select						
Control Number	Management Control Name	Control	Priority	Always Applicable	Applicable	Control Implementation: 0%	Control Completion Time:				Incomplete		
	Sub-control Number	Sub-control		Always Applicable	Applicable	Select	Select						
	Sub-control Number	Sub-control		Always Applicable	Applicable	Select	Select						
	Sub-control Number	Sub-control		Always Applicable	Applicable	Select	Select						
Control Number	Technical Control Name	Control	Priority	Based On Risk Assessment	Control Applicability	Control Implementation: 0%	Control Completion Time:				Incomplete		
	Sub-control Number	Sub-control		Based On Risk Assessment	Select	Select	Select						
	Sub-control Number	Sub-control		Based On Risk Assessment	Select	Select	Select						
	Sub-control Number	Sub-control		Based On Risk Assessment	Select	Select	Select						

# C1: Reporting template for the entities to report their progress on CIIP to the Sector Committee

											Completed: 0	Remaining: 3	% Completion: 0%
Control #	Control Name	Control	Priority	Applicability		Status	Deadline	Ownership	Comment	Justification	Entry Complete		
<b>Family Name</b>													
<b>Sub-Family Name</b>													
Control Number	Priority 1 Control Name (can be management or Technical Control)	Control	Priority	Always Applicable	Applicable	Control Implementation: 0%	Control Completion Time:				Incomplete		
	Sub-control Number	Sub-control		Always Applicable	Applicable	Select	Select						
	Sub-control Number	Sub-control		Always Applicable	Applicable	Select	Select						
	Sub-control Number	Sub-control		Always Applicable	Applicable	Select	Select						
Control Number	Management Control Name	Control	Priority	Always Applicable	Applicable	Control Implementation: 0%	Control Completion Time:				Incomplete		
	Sub-control Number	Sub-control		Always Applicable	Applicable	Select	Select						
	Sub-control Number	Sub-control		Always Applicable	Applicable	Select	Select						
	Sub-control Number	Sub-control		Always Applicable	Applicable	Select	Select						
Control Number	Technical Control Name	Control	Priority	Based On Risk Assessment	Control Applicability	Control Implementation: 0%	Control Completion Time:				Incomplete		
	Sub-control Number	Sub-control		Based On Risk Assessment	Select	Select	Select						
	Sub-control Number	Sub-control		Based On Risk Assessment	Select	Select	Select						
	Sub-control Number	Sub-control		Based On Risk Assessment	Select	Select	Select						

Source: Expert Interviews

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# C1: Example of the filled reporting template that the Sector Committee will receive from each of the sectorial entities reporting their progress every quarter

Completed: 103      Remaining: 188      % Completion: 55%										
Control #	Control Name	Control	Priority	Applicability	Status	Deadline	Ownership	Comment	Justification	Entry Complete
Protect										
<strong>ACCESS CONTROL</strong>										
<strong>REMOTE ACCESS IS MANAGED</strong>										
NIST SP 800-53 AC-17	REMOTE ACCESS	The organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing such connections.	P1	Always Applicable	Applicable	Control Implementation: 50% Control Completion By: Q3 2019				N/A -- All control applies  <span style="color: red;">Incomplete</span>
	AC-17 (1)	The information system monitors and controls remote access methods.		Always Applicable	Applicable	Implemented				N/A -- All control applies
	AC-17 (2)	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions		Always Applicable	Applicable	Implemented				N/A -- All control applies
	AC-17 (3)	The information system routes all remote accesses through [Assignment: organization-defined number] managed network access control points		Always Applicable	Applicable	Partially Implemented Q2 2019				N/A -- All control applies
	AC-17 (4)	The organization: (a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [Assignment: organization-defined needs]; and (b) Documents the rationale for such access in the security plan for the information system		Always Applicable	Applicable	Planned Q3 2019				N/A -- All control applies

# C: ‘Protect & Monitor’ component of CI cybersecurity program includes 2 key steps

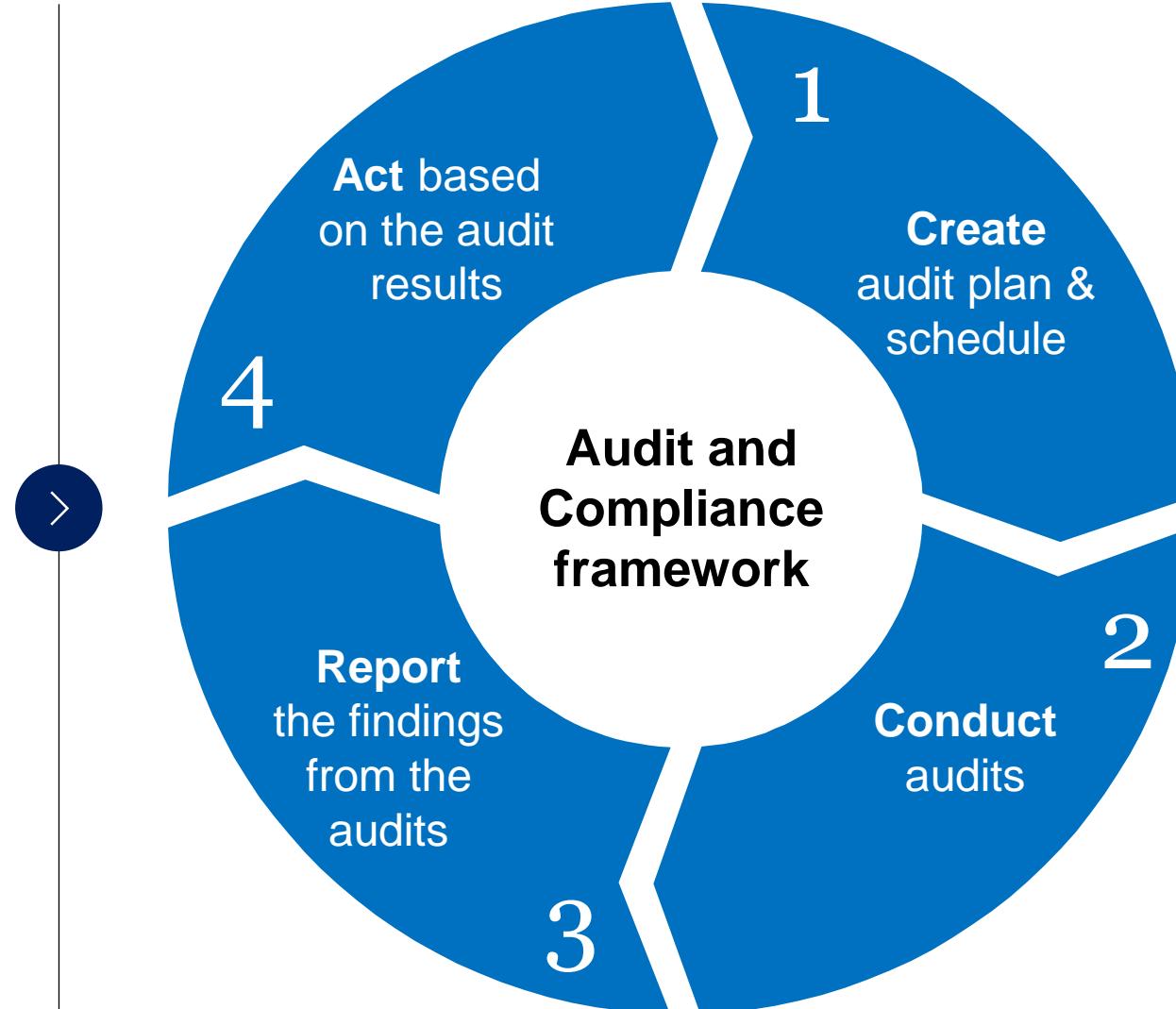
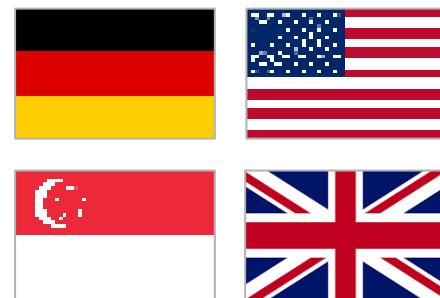
対外厳秘

Detailed next

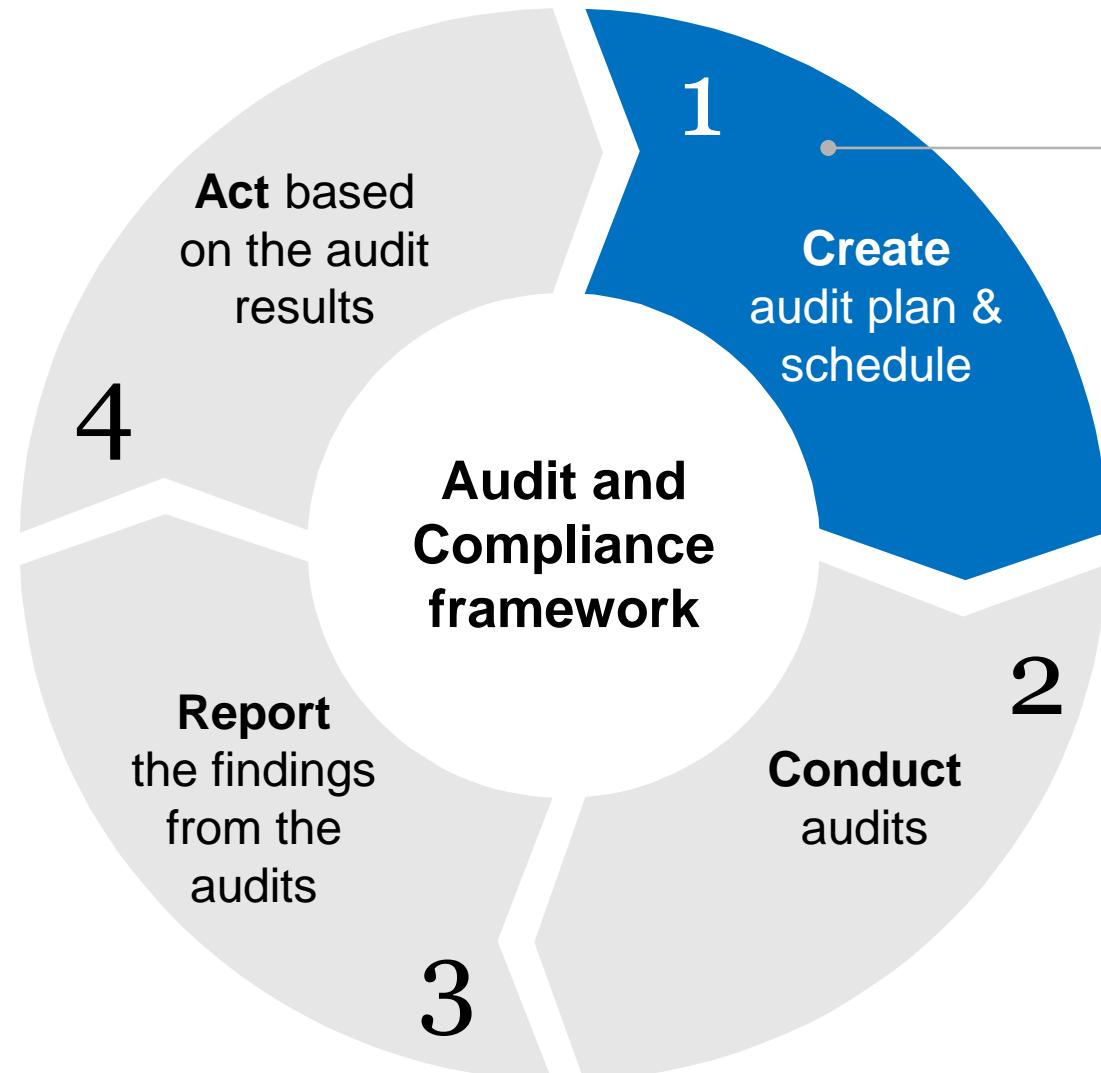
Key Steps	Methodology	Owner	Sources of insight
1 	<b>Define the reporting template &amp; frequency</b> for sectorial entities based on the recommended standards to keep them accountable	NCA/ Sector Committee	     
	<b>Assess the current state of the organization</b> against the standards or controls recommended by the Sector Committee and identify the gaps	Sectorial Entities	    
	<b>Define the plan to bridge the gaps, and report the implementation status as per the template</b> mandated by the regulator	Sectorial Entities	
2 	<b>Define the framework</b> for audit and compliance	NCA	  
	<b>Define the roles and responsibilities</b> for auditing	Sector Committee	  
	<b>Audit the sector entities</b> for compliance	Accredited Auditors	

# C3: Proposed framework for ensuring compliance through audits is aligned with that of the benchmark countries

  
We benchmarked  
4 countries to  
validate the  
proposed Audit  
and Compliance  
framework



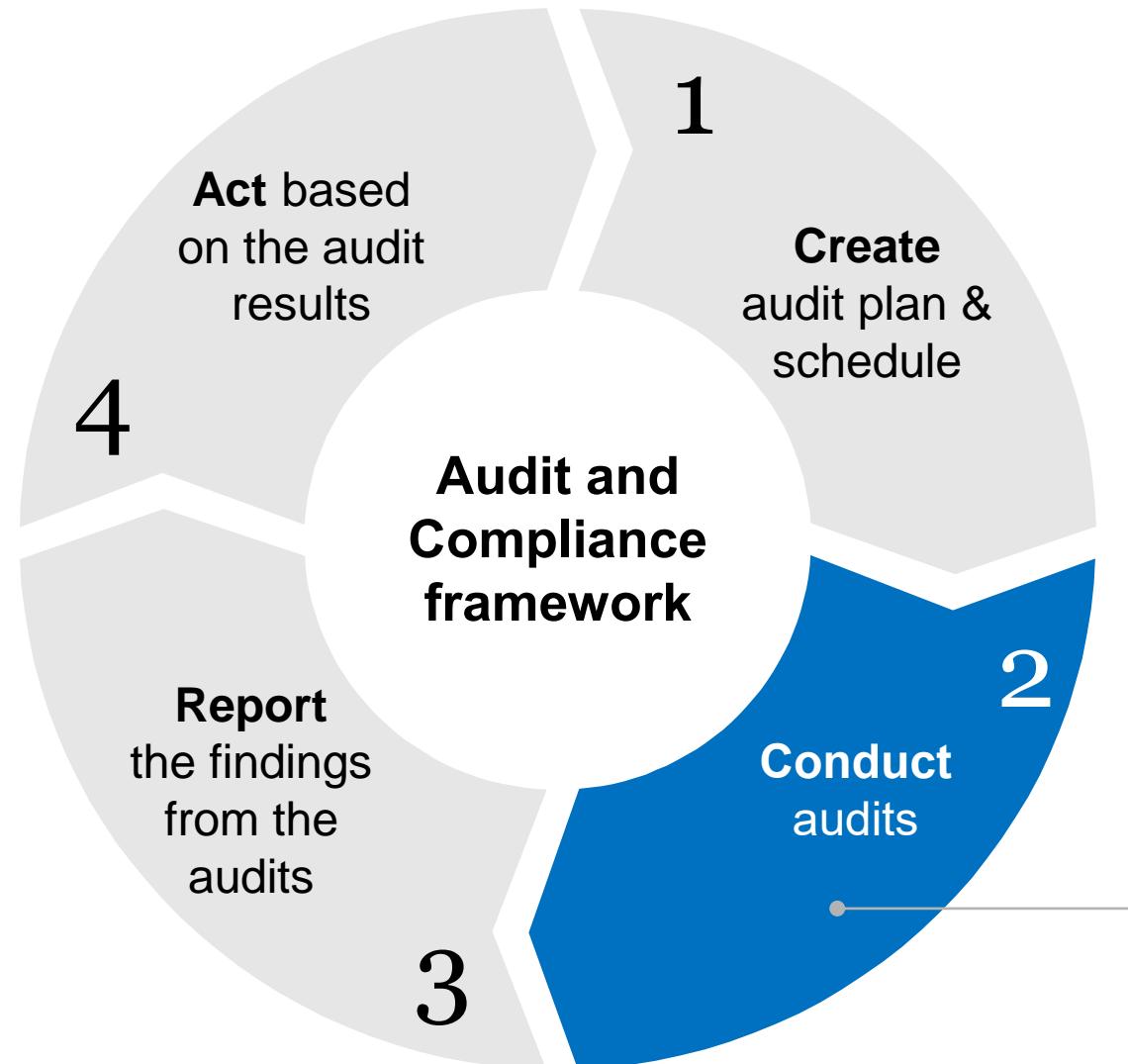
# C3: Proposed framework for ensuring compliance through audits is aligned with that of the benchmark countries



## Sector committees to:

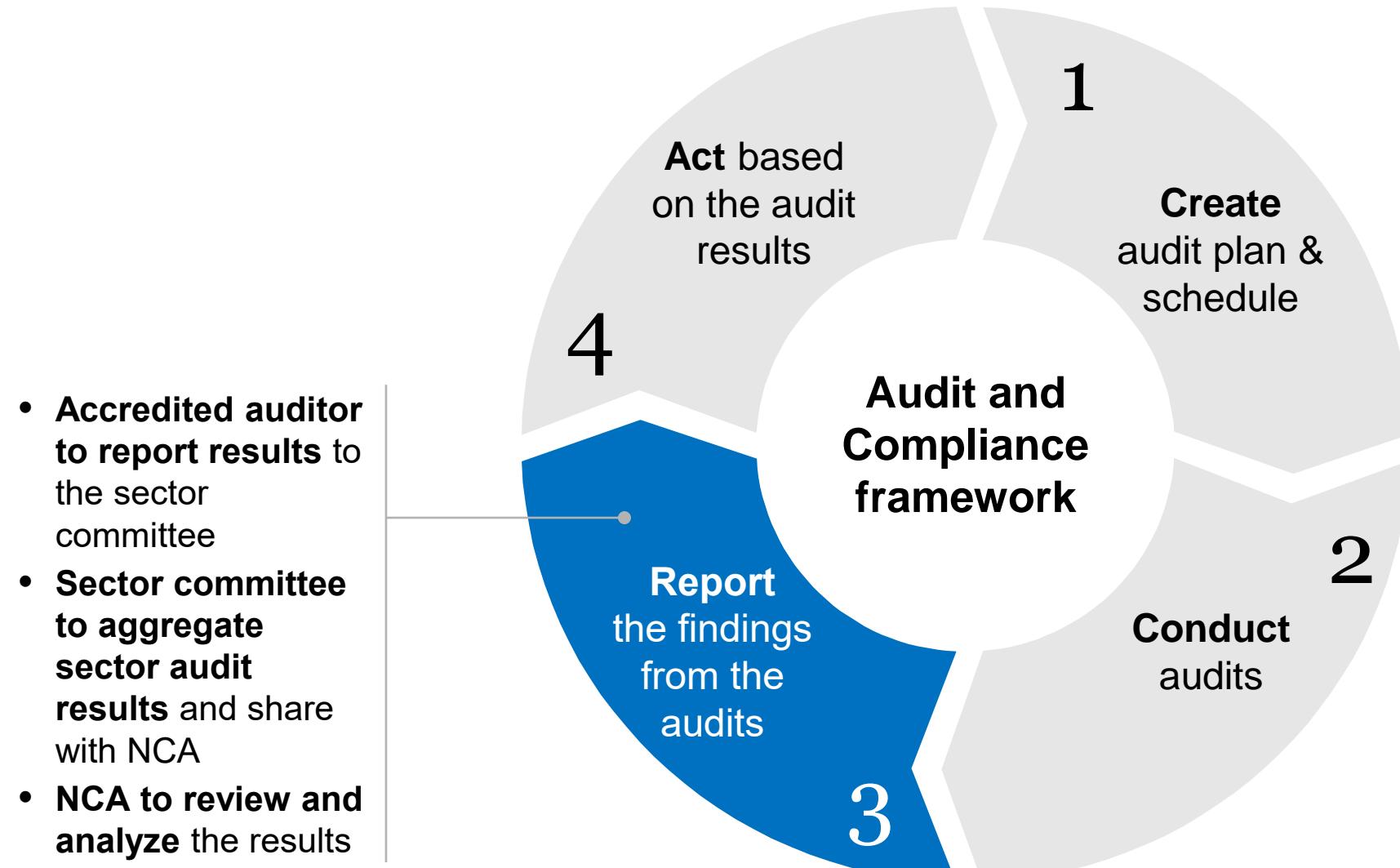
- **Prepare** sector-specific audit plan and schedule
- **Communicate** plan and schedule to the entities
- **Plan audits with accredited auditor** in liaison with the entities

# C3: Proposed framework for ensuring compliance through audits is aligned with that of the benchmark countries



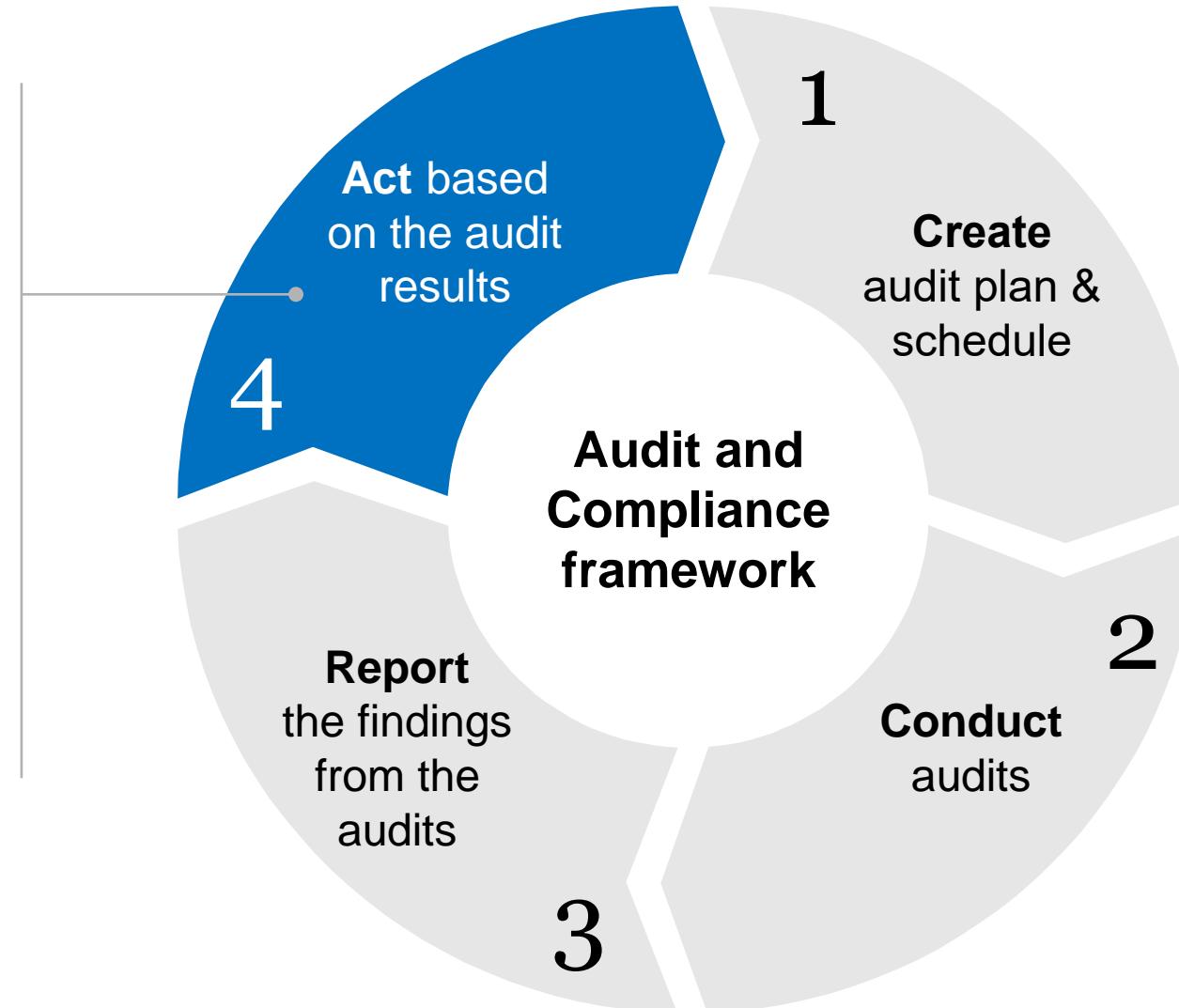
- Accredited auditor to audit the entities in coordination with the sector committees as per the schedule

# C3: Proposed framework for ensuring compliance through audits is aligned with that of the benchmark countries



## C3: Proposed framework for ensuring compliance through audits is aligned with that of the benchmark countries

- Sector committees to share the results with the entities
- NCA and/or sector committee to jointly enforce actions
- Entities to implement mitigation plans or recommendations from NCA/ Sector committees



# C3: Example of the audit report provided by the accredited partner 村外監査 to the sector committee

Control #	Control Name	Control	Priority	Implemented?
<b>ACCESS CONTROL</b>				
<b>REMOTE ACCESS IS MANAGED</b>				
<b>NIST SP 800-53 AC-17</b>	<b>REMOTE ACCESS</b>	The organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing such connections.	P1	<b>Yes</b>
	<b>AC-17 (1)</b>	The information system monitors and controls remote access methods.		<b>Yes</b>
	<b>AC-17 (2)</b>	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions		<b>Yes</b>
	<b>AC-17 (3)</b>	The information system routes all remote accesses through [Assignment: organization-defined number] managed network access control points		<b>Yes</b>
	<b>AC-17 (4)</b>	The organization: (a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [Assignment: organization-defined needs]; and (b) Documents the rationale for such access in the security plan for the information system		<b>Yes</b>

Source: Expert Interviews, Team analysis

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# B1: We propose to set a suite of general cybersecurity standards for sectorial committees to choose from (1/10)

Category	Subcategory	Suite of risk standards	Category	Subcategory	Suite of risk standards
<b>Asset Management:</b> The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy	Physical devices and systems within the organization are inventoried	<ul style="list-style-type: none"> <li>CIS CSC 1</li> <li>COBIT 5 BAI09.01, BAI09.02</li> <li>ISA 62443-2-1:2009 4.2.3.4</li> <li>ISA 62443-3-3:2013 SR 7.8</li> <li>ISO 27002 A.8.1.1, A.8.1.2</li> <li>NIST SP 800-53 Rev. 4 CM-8, PM-5</li> </ul>	<b>Business Environment:</b> The organization's role in the supply chain is identified and communicated	The organization's place in critical infrastructure and its industry sector is identified and communicated	<ul style="list-style-type: none"> <li>COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05</li> <li>ISO 27002 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2</li> <li>NIST SP 800-53 Rev. 4 CP-2, SA-12</li> </ul>
	Software platforms and applications within the organization are inventoried	<ul style="list-style-type: none"> <li>CIS CSC 2</li> <li>COBIT 5 BAI09.01, BAI09.02, BAI09.05</li> <li>ISA 62443-2-1:2009 4.2.3.4</li> <li>ISA 62443-3-3:2013 SR 7.8</li> <li>ISO 27002 A.8.1.1, A.8.1.2, A.12.5.1</li> <li>NIST SP 800-53 Rev. 4 CM-8, PM-5</li> </ul>		Priorities for organizational mission, objectives, and activities are established and communicated	<ul style="list-style-type: none"> <li>COBIT 5 APO02.06, APO03.01</li> <li>ISO 27002 Clause 4.1</li> <li>NIST SP 800-53 Rev. 4 PM-8</li> </ul>
	Organizational communication and data flows are mapped	<ul style="list-style-type: none"> <li>CIS CSC 12</li> <li>COBIT 5 DSS05.02</li> <li>ISA 62443-2-1:2009 4.2.3.4</li> <li>ISO 27002 A.13.2.1, A.13.2.2</li> <li>NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8</li> </ul>		Dependencies and critical functions for delivery of critical services are established	<ul style="list-style-type: none"> <li>COBIT 5 APO02.01, APO02.06, APO03.01</li> <li>ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6</li> <li>NIST SP 800-53 Rev. 4 PM-11, SA-14</li> </ul>
	External information systems are catalogued	<ul style="list-style-type: none"> <li>CIS CSC 12</li> <li>COBIT 5 APO02.02, APO10.04, DSS01.02</li> <li>ISO 27002 A.11.2.6</li> <li>NIST SP 800-53 Rev. 4 AC-20, SA-9</li> </ul>		Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	<ul style="list-style-type: none"> <li>COBIT 5 BAI03.02, DSS04.02</li> <li>ISO 27002 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1</li> <li>NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14</li> </ul>
	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	<ul style="list-style-type: none"> <li>CIS CSC 13, 14</li> <li>COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02</li> <li>ISA 62443-2-1:2009 4.2.3.6</li> <li>ISO 27002 A.8.2.1</li> <li>NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6</li> </ul>	<b>Governance:</b> The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Organizational cybersecurity policy is established and communicated	<ul style="list-style-type: none"> <li>CIS CSC 19</li> <li>COBIT 5 APO01.03, APO13.01, EDM01.01, EDM01.02</li> <li>ISA 62443-2-1:2009 4.3.2.6</li> <li>ISO 27002 A.5.1.1</li> <li>NIST SP 800-53 Rev. 4 -1 controls from all security control families</li> </ul>
	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	<ul style="list-style-type: none"> <li>CIS CSC 17, 19</li> <li>COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03</li> <li>ISA 62443-2-1:2009 4.3.2.3.3</li> <li>ISO 27002 A.6.1.1</li> <li>NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11</li> </ul>			

Source: Standards mapping from NIST CSF

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# B1: We propose to set a suite of general cybersecurity standards for sectorial committees to choose from (2/10)

Category	Subcategory	Suite of risk standards	Category	Subcategory	Suite of risk standards
<b>Governance:</b> The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	<ul style="list-style-type: none"> <li><b>CIS CSC 19</b></li> <li><b>COBIT 5</b> APO1.02, APO10.03, APO13.02, DSS05.04</li> <li><b>ISA 62443-2-1:2009</b> 4.3.2.3.3</li> <li><b>ISO 27002</b> A.6.1.1, A.7.2.1, A.15.1.1</li> <li><b>NIST SP 800-53 Rev. 4</b> PS-7, PM-1, PM-2</li> </ul>		Threats, both internal and external, are identified and documented	<ul style="list-style-type: none"> <li><b>CIS CSC 4</b></li> <li><b>COBIT 5</b> APO12.01, APO12.02, APO12.03, APO12.04</li> <li><b>ISA 62443-2-1:2009</b> 4.2.3, 4.2.3.9, 4.2.3.12</li> <li><b>ISO 27002</b> Clause 6.1.2</li> <li><b>NIST SP 800-53 Rev. 4</b> RA-3, SI-5, PM-12, M- 16</li> </ul>
	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	<ul style="list-style-type: none"> <li><b>CIS CSC 19</b></li> <li><b>COBIT 5</b> BAI02.01, MEA03.01, MEA03.04</li> <li><b>ISA 62443-2-1:2009</b> 4.4.3.7</li> <li><b>ISO 27002</b> A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5</li> <li><b>NIST SP 800-53 Rev. 4</b> -1 controls from all security control families</li> </ul>		Potential business impacts and likelihoods are identified	<ul style="list-style-type: none"> <li><b>CIS CSC 4</b></li> <li><b>COBIT 5</b> DSS04.02</li> <li><b>ISA 62443-2-1:2009</b> 4.2.3, 4.2.3.9, 4.2.3.12</li> <li><b>ISO 27002</b> A.16.1.6, Clause 6.1.2</li> <li><b>NIST SP 800-53 Rev. 4</b> RA-2, RA-3, SA-14, PM-9, PM-11</li> </ul>
	Governance and risk management processes address cybersecurity risks	<ul style="list-style-type: none"> <li><b>COBIT 5</b> EDM03.02, APO12.02, APO12.05, DSS04.02</li> <li><b>ISA 62443-2-1:2009</b> 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3</li> <li><b>ISO 27002</b> Clause 6</li> <li><b>NIST SP 800-53 Rev. 4</b> SA-2, PM-3, PM-7, PM- 9, PM-10, PM-11</li> </ul>		Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	<ul style="list-style-type: none"> <li><b>CIS CSC 4</b></li> <li><b>COBIT 5</b> APO12.02</li> <li><b>ISO 27002</b> A.12.6.1</li> <li><b>NIST SP 800-53 Rev. 4</b> RA-2, RA-3, PM-16</li> </ul>
<b>Risk Assessment:</b> The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Asset vulnerabilities are identified and documented	<ul style="list-style-type: none"> <li><b>CIS CSC 4</b></li> <li><b>COBIT 5</b> APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02</li> <li><b>ISA 62443-2-1:2009</b> 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12</li> <li><b>ISO 27002</b> A.12.6.1, A.18.2.3</li> <li><b>NIST SP 800-53 Rev. 4</b> CA-2, CA-7, CA-8, RA- 3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5</li> </ul>		Risk responses are identified and prioritized	<ul style="list-style-type: none"> <li><b>CIS CSC 4</b></li> <li><b>COBIT 5</b> APO12.05, APO13.02</li> <li><b>ISO 27002</b> Clause 6.1.3</li> <li><b>NIST SP 800-53 Rev. 4</b> PM-4, PM-9</li> </ul>
	Cyber threat intelligence is received from information sharing forums and sources	<ul style="list-style-type: none"> <li><b>CIS CSC 4</b></li> <li><b>COBIT 5</b> BAI08.01</li> <li><b>ISA 62443-2-1:2009</b> 4.2.3, 4.2.3.9, 4.2.3.12</li> <li><b>ISO 27002</b> A.6.1.4</li> <li><b>NIST SP 800-53 Rev. 4</b> SI-5, PM-15, PM-16</li> </ul>		Risk management processes are established, managed, and agreed to by organizational stakeholders	<ul style="list-style-type: none"> <li><b>CIS CSC 4</b></li> <li><b>COBIT 5</b> APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02</li> <li><b>ISA 62443-2-1:2009</b> 4.3.4.2</li> <li><b>ISO 27002</b> Clause 6.1.3, Clause 8.3, Clause 9.3</li> <li><b>NIST SP 800-53 Rev. 4</b> PM-9</li> </ul>
				Organizational risk tolerance is determined and clearly expressed	<ul style="list-style-type: none"> <li><b>COBIT 5</b> APO12.06</li> <li><b>ISA 62443-2-1:2009</b> 4.3.2.6.5</li> <li><b>ISO 27002</b> Clause 6.1.3, Clause 8.3</li> <li><b>NIST SP 800-53 Rev. 4</b> PM-9</li> </ul>
				The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	<ul style="list-style-type: none"> <li><b>COBIT 5</b> APO12.02</li> <li><b>ISO 27002</b> Clause 6.1.3, Clause 8.3 <b>NIST SP 800-53 Rev. 4</b> SA-14, PM-8, PM-9, PM- 11</li> </ul>

Source: Standards mapping from NIST CSF

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# B1: We propose to set a suite of general cybersecurity standards for sectorial committees to choose from (3/10)

Category	Subcategory	Suite of risk standards	Category	Subcategory	Suite of risk standards
Supply Chain Risk Management:  The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	<ul style="list-style-type: none"> <li><b>CIS CSC 4</b></li> <li><b>COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02</b></li> <li><b>ISA 62443-2-1:2009 4.3.4.2</b></li> <li><b>ISO 27002 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2</b></li> <li><b>NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9</b></li> </ul>	<b>Identity Management, Authentication and Access Control:</b> Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions	Response and recovery planning and testing are conducted with suppliers and third-party providers	<ul style="list-style-type: none"> <li><b>CIS CSC 19, 20</b></li> <li><b>COBIT 5 DSS04.04</b></li> <li><b>ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11</b></li> <li><b>ISA 62443-3-3:2013 SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4</b></li> <li><b>ISO 27002 A.17.1.3</b></li> <li><b>NIST SP 800-53 Rev. 4 CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9</b></li> </ul>
	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	<ul style="list-style-type: none"> <li><b>COBIT 5 APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03</b></li> <li><b>ISA 62443-2-1:2009 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14</b></li> <li><b>ISO 27002 A.15.2.1, A.15.2.2</b></li> <li><b>NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-12, SA-14, SA-15, PM-9</b></li> </ul>		Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	<ul style="list-style-type: none"> <li><b>CIS CSC 1, 5, 15, 16</b></li> <li><b>COBIT 5 DSS05.04, DSS06.03</b></li> <li><b>ISA 62443-2-1:2009 4.3.3.5.1</b></li> <li><b>ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9</b></li> <li><b>ISO 27002 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3</b></li> <li><b>NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11</b></li> </ul>
	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	<ul style="list-style-type: none"> <li><b>COBIT 5 APO10.01, APO10.02, APO10.03, APO10.04, APO10.05</b></li> <li><b>ISA 62443-2-1:2009 4.3.2.6.4, 4.3.2.6.7</b></li> <li><b>ISO 27002 A.15.1.1, A.15.1.2, A.15.1.3</b></li> <li><b>NIST SP 800-53 Rev. 4 SA-9, SA-11, SA-12, PM- 9</b></li> </ul>		Physical access to assets is managed and protected	<ul style="list-style-type: none"> <li><b>COBIT 5 DSS01.04, DSS05.05</b></li> <li><b>ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8</b></li> <li><b>ISO 27002 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8</b></li> <li><b>NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8</b></li> </ul>
	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	<ul style="list-style-type: none"> <li><b>COBIT 5 APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05</b></li> <li><b>ISA 62443-2-1:2009 4.3.2.6.7</b></li> <li><b>ISA 62443-3-3:2013 SR 6.1</b></li> <li><b>ISO 27002 A.15.2.1, A.15.2.2</b></li> <li><b>NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12</b></li> </ul>		Remote access is managed	<ul style="list-style-type: none"> <li><b>CIS CSC 12</b></li> <li><b>COBIT 5 APO13.01, DSS01.04, DSS05.03</b></li> <li><b>ISA 62443-2-1:2009 4.3.3.6.6</b></li> <li><b>ISA 62443-3-3:2013 SR 1.13, SR 2.6</b></li> <li><b>ISO 27002 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1</b></li> <li><b>NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15</b></li> </ul>

Source: Standards mapping from NIST CSF

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# B1: We propose to set a suite of general cybersecurity standards for sectorial committees to choose from (4/10)

Category	Subcategory	Suite of risk standards	Category	Subcategory	Suite of risk standards
Identity Management, Authentication and Access Control: Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	<ul style="list-style-type: none"> <li>CIS CSC 3, 5, 12, 14, 15, 16, 18</li> <li>COBIT 5 DSS05.04</li> <li>ISA 62443-2-1:2009 4.3.3.7.3</li> <li>ISA 62443-3-3:2013 SR 2.1</li> <li>ISO 27002 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5</li> <li>NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC- 5, AC-6, AC-14, AC-16, AC-24</li> </ul>	Awareness and Training :	All users are informed and trained	<ul style="list-style-type: none"> <li>CIS CSC 17, 18</li> <li>COBIT 5 APO07.03, BAI05.07</li> <li>ISA 62443-2-1:2009 4.3.2.4.2 ISO 27002 A.7.2.2, A.12.2.1 NIST SP 800-53 Rev. 4 AT-2, PM-13</li> </ul>
	Network integrity is protected (e.g., network segregation, network segmentation)	<ul style="list-style-type: none"> <li>CIS CSC 9, 14, 15, 18</li> <li>COBIT 5 DSS01.05, DSS05.02</li> <li>ISA 62443-2-1:2009 4.3.3.4</li> <li>ISA 62443-3-3:2013 SR 3.1, SR 3.8</li> <li>ISO 27002 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3</li> <li>NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7</li> </ul>	Privileged users understand their roles and responsibilities		<ul style="list-style-type: none"> <li>CIS CSC 5, 17, 18</li> <li>COBIT 5 APO07.02, DSS05.04, DSS06.03</li> <li>ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3</li> <li>ISO 27002 A.6.1.1, A.7.2.2</li> <li>NIST SP 800-53 Rev. 4 AT-3, PM-13</li> </ul>
	Identities are proofed and bound to credentials and asserted in interactions	<ul style="list-style-type: none"> <li>CIS CSC, 16</li> <li>COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03</li> <li>ISA 62443-2-1:2009 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4</li> <li>ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1</li> <li>ISO 27002, A.7.1.1, A.9.2.1</li> <li>NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC- 16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3</li> </ul>	Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities		<ul style="list-style-type: none"> <li>CIS CSC 17</li> <li>COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05</li> <li>ISA 62443-2-1:2009 4.3.2.4.2</li> <li>ISO 27002 A.6.1.1, A.7.2.1, A.7.2.2</li> <li>NIST SP 800-53 Rev. 4 PS-7, SA-9, SA-16</li> </ul>
	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	<ul style="list-style-type: none"> <li>CIS CSC 1, 12, 15, 16</li> <li>COBIT 5 DSS05.04, DSS05.10, DSS06.10</li> <li>ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9</li> <li>ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10</li> <li>ISO 27002 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4</li> <li>NIST SP 800-53 Rev. 4 AC-7, AC-8, AC-9, AC- 11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA- 9, IA-10, IA-11</li> </ul>	Senior executives understand their roles and responsibilities		<ul style="list-style-type: none"> <li>CIS CSC 17</li> <li>COBIT 5 EDM01.01, APO01.02, APO07.03</li> <li>ISA 62443-2-1:2009 4.3.2.4.2</li> <li>ISO 27002 A.6.1.1, A.7.2.2</li> <li>NIST SP 800-53 Rev. 4 AT-3, PM-13</li> </ul>
			Data Security:	Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	<ul style="list-style-type: none"> <li>CIS CSC 17</li> <li>COBIT 5 APO07.03</li> <li>ISA 62443-2-1:2009 4.3.2.4.2</li> <li>ISO 27002 A.6.1.1, A.7.2.2</li> <li>NIST SP 800-53 Rev. 4 AT-3, IR-2, PM-13</li> </ul>
			Data-at-rest is protected		<ul style="list-style-type: none"> <li>CIS CSC 13, 14</li> <li>COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06</li> <li>ISA 62443-3-3:2013 SR 3.4, SR 4.1</li> <li>ISO 27002 A.8.2.3</li> <li>NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28</li> </ul>

# B1: We propose to set a suite of general cybersecurity standards for sectorial committees to choose from (5/10)

Category	Subcategory	Suite of risk standards	Category	Subcategory	Suite of risk standards
<b>Data Security:</b> Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	Data-in-transit is protected	<ul style="list-style-type: none"> <li>CIS CSC 13, 14</li> <li>COBIT 5 APO01.06, DSS05.02, DSS06.06</li> <li>ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2</li> <li>ISO 27002 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3</li> <li>NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12</li> </ul>		The development and testing environment(s) are separate from the production environment	<ul style="list-style-type: none"> <li>CIS CSC 18, 20</li> <li>COBIT 5 BAI03.08, BAI07.04</li> <li>ISO 27002 A.12.1.4</li> <li>NIST SP 800-53 Rev. 4 CM-2</li> </ul>
	Assets are formally managed throughout removal, transfers, and disposition	<ul style="list-style-type: none"> <li>CIS CSC 1</li> <li>COBIT 5 BAI09.03</li> <li>ISA 62443-2-1:2009 4.3.3.3.9, 4.3.4.4.1</li> <li>ISA 62443-3-3:2013 SR 4.2</li> <li>ISO 27002 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7</li> <li>NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16</li> </ul>		Integrity checking mechanisms are used to verify hardware integrity	<ul style="list-style-type: none"> <li>COBIT 5 BAI03.05</li> <li>ISA 62443-2-1:2009 4.3.4.4.4</li> <li>ISO 27002 A.11.2.4</li> <li>NIST SP 800-53 Rev. 4 SA-10, SI-7</li> </ul>
	Adequate capacity to ensure availability is maintained	<ul style="list-style-type: none"> <li>CIS CSC 1, 2, 13</li> <li>COBIT 5 APO13.01, BAI04.04</li> <li>ISA 62443-3-3:2013 SR 7.1, SR 7.2</li> <li>ISO 27002 A.12.1.3, A.17.2.1</li> <li>NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5</li> </ul>	<b>Information Protection Processes and Procedures:</b> Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	A baseline configuration of information technology/ industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	<ul style="list-style-type: none"> <li>CIS CSC 3, 9, 11</li> <li>COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05</li> <li>ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3</li> <li>ISA 62443-3-3:2013 SR 7.6</li> <li>ISO 27002 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4</li> <li>NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10</li> </ul>
	Protections against data leaks are implemented	<ul style="list-style-type: none"> <li>CIS CSC 13</li> <li>COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02</li> <li>ISA 62443-3-3:2013 SR 5.2</li> <li>ISO 27002 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3</li> <li>NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE- 19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4</li> </ul>	A System Development Life Cycle to manage systems is implemented		<ul style="list-style-type: none"> <li>CIS CSC 18</li> <li>COBIT 5 APO13.01, BAI03.01, BAI03.02, BAI03.03</li> <li>ISA 62443-2-1:2009 4.3.4.3.3</li> <li>ISO 27002 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5</li> <li>NIST SP 800-53 Rev. 4 PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17</li> </ul>
	Integrity checking mechanisms are used to verify software, firmware, and information integrity	<ul style="list-style-type: none"> <li>CIS CSC 2, 3</li> <li>COBIT 5 APO01.06, BAI06.01, DSS06.02</li> <li>ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8</li> <li>ISO 27002 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4</li> <li>NIST SP 800-53 Rev. 4 SC-16, SI-7</li> </ul>	Configuration change control processes are in place		<ul style="list-style-type: none"> <li>CIS CSC 3, 11</li> <li>COBIT 5 BAI01.06, BAI06.01</li> <li>ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3</li> <li>ISA 62443-3-3:2013 SR 7.6</li> <li>ISO 27002 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4</li> <li>NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10</li> </ul>

Source: Standards mapping from NIST CSF

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# B1: We propose to set a suite of general cybersecurity standards for sectorial committees to choose from (6/10)

Category	Subcategory	Suite of risk standards	Category	Subcategory	Suite of risk standards
Information Protection Processes and Procedures:	Backups of information are conducted, maintained, and tested	<ul style="list-style-type: none"> <li>CIS CSC 10</li> <li>COBIT 5 APO13.01, DSS01.01, DSS04.07</li> <li>ISA 62443-2-1:2009 4.3.4.3.9</li> <li>ISA 62443-3-3:2013 SR 7.3, SR 7.4</li> <li>ISO 27002 A.12.3.1, A.17.1.2,</li> <li>A.17.1.3, A.18.1.3</li> <li>NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9</li> </ul>		Response and recovery plans are tested	<ul style="list-style-type: none"> <li>CIS CSC 19, 20</li> <li>COBIT 5 DSS04.04</li> <li>ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11</li> <li>ISA 62443-3-3:2013 SR 3.3</li> <li>ISO 27002 A.17.1.3</li> <li>NIST SP 800-53 Rev. 4 CP-4, IR-3, PM-14</li> </ul>
	Policy and regulations regarding the physical operating environment for organizational assets are met	<ul style="list-style-type: none"> <li>COBIT 5 DSS01.04, DSS05.05</li> <li>ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6</li> <li>ISO 27002 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3</li> <li>NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18</li> </ul>		Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	<ul style="list-style-type: none"> <li>CIS CSC 5, 16</li> <li>COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05</li> <li>ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3</li> <li>ISO 27002 A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4</li> <li>NIST SP 800-53 Rev. 4 PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21</li> </ul>
	Data is destroyed according to policy	<ul style="list-style-type: none"> <li>COBIT 5 BAI09.03, DSS05.06</li> <li>ISA 62443-2-1:2009 4.3.4.4.4</li> <li>ISA 62443-3-3:2013 SR 4.2</li> <li>ISO 27002 A.8.2.3, A.8.3.1, A.8.3.2,</li> <li>A.11.2.7</li> <li>NIST SP 800-53 Rev. 4 MP-6</li> </ul>		A vulnerability management plan is developed and implemented	<ul style="list-style-type: none"> <li>CIS CSC 4, 18, 20</li> <li>COBIT 5 BAI03.10, DSS05.01, DSS05.02</li> <li>ISO 27002 A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3</li> <li>NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2</li> </ul>
	Protection processes are improved	<ul style="list-style-type: none"> <li>COBIT 5 APO11.06, APO12.06, DSS04.05</li> <li>ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8</li> <li>ISO 27002 A.16.1.6, Clause 9, Clause 10</li> <li>NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6</li> </ul>	Maintenance:	Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures	<ul style="list-style-type: none"> <li>Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools</li> </ul>
	Effectiveness of protection technologies is shared	<ul style="list-style-type: none"> <li>COBIT 5 BAI08.04, DSS03.04</li> <li>ISO 27002 A.16.1.6</li> <li>NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4</li> </ul>		Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	<ul style="list-style-type: none"> <li>COBIT 5 BAI03.10, BAI09.02, BAI09.03, DSS01.05</li> <li>ISA 62443-2-1:2009 4.3.3.3.7</li> <li>ISO 27002 A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6</li> <li>NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5, MA-6</li> </ul>
	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	<ul style="list-style-type: none"> <li>CIS CSC 19</li> <li>COBIT 5 APO12.06, DSS04.03</li> <li>ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1</li> <li>ISO 27002 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3</li> <li>NIST SP 800-53 Rev. 4 CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17</li> </ul>			<ul style="list-style-type: none"> <li>CIS CSC 3, 5</li> <li>COBIT 5 DSS05.04</li> <li>ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8</li> <li>ISO 27002 A.11.2.4, A.15.1.1, A.15.2.1</li> <li>NIST SP 800-53 Rev. 4 MA-4</li> </ul>

Source: Standards mapping from NIST CSF

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# B1: We propose to set a suite of general cybersecurity standards for sectorial committees to choose from (7/10)

Category	Subcategory	Suite of risk standards	Category	Subcategory	Suite of risk standards
<b>Protective Technology:</b> Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	<ul style="list-style-type: none"> <li><b>CIS CSC 1, 3, 5, 6, 14, 15, 16</b></li> <li><b>COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01</b></li> <li><b>ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4</b></li> <li><b>ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12</b></li> <li><b>ISO 27002 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1</b></li> <li><b>NIST SP 800-53 Rev. 4 AU Family</b></li> </ul>	<b>Anomalies and Events :</b> Anomalous activity is detected and the potential impact of events is understood.	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	<ul style="list-style-type: none"> <li><b>COBIT 5 BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05</b></li> <li><b>ISA 62443-2-1:2009 4.3.2.5.2</b></li> <li><b>ISA 62443-3-3:2013 SR 7.1, SR 7.2</b></li> <li><b>ISO 27002 A.17.1.2, A.17.2.1</b></li> <li><b>NIST SP 800-53 Rev. 4 CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6</b></li> </ul>
	Removable media is protected and its use restricted according to policy	<ul style="list-style-type: none"> <li><b>CIS CSC 8, 13</b></li> <li><b>COBIT 5 APO13.01, DSS05.02, DSS05.06</b></li> <li><b>ISA 62443-3-3:2013 SR 2.3</b></li> <li><b>ISO 27002 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9</b></li> <li><b>NIST SP 800-53 Rev. 4 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8</b></li> </ul>	A baseline of network operations and expected data flows for users and systems is established and managed		<ul style="list-style-type: none"> <li><b>CIS CSC 1, 4, 6, 12, 13, 15, 16</b></li> <li><b>COBIT 5 DSS03.01</b></li> <li><b>ISA 62443-2-1:2009 4.4.3.3</b></li> <li><b>ISO 27002 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2</b></li> <li><b>NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4</b></li> </ul>
	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	<ul style="list-style-type: none"> <li><b>CIS CSC 3, 11, 14</b></li> <li><b>COBIT 5 DSS05.02, DSS05.05, DSS06.06</b></li> <li><b>ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4</b></li> <li><b>ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7</b></li> <li><b>ISO 27002 A.9.1.2</b></li> <li><b>NIST SP 800-53 Rev. 4 AC-3, CM-7</b></li> </ul>	Detected events are analyzed to understand attack targets and methods		<ul style="list-style-type: none"> <li><b>CIS CSC 3, 6, 13, 15</b></li> <li><b>COBIT 5 DSS05.07</b></li> <li><b>ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8</b></li> <li><b>ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2</b></li> <li><b>ISO 27002 A.12.4.1, A.16.1.1, A.16.1.4</b></li> <li><b>NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4</b></li> </ul>
	Communications and control networks are protected	<ul style="list-style-type: none"> <li><b>CIS CSC 8, 12, 15</b></li> <li><b>COBIT 5 DSS05.02, APO13.01</b></li> <li><b>ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6</b></li> <li><b>ISO 27002 A.13.1.1, A.13.2.1, A.14.1.3</b></li> <li><b>NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43</b></li> </ul>	Event data are collected and correlated from multiple sources and sensors		<ul style="list-style-type: none"> <li><b>CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16</b></li> <li><b>COBIT 5 BAI08.02</b></li> <li><b>ISA 62443-3-3:2013 SR 6.1</b></li> <li><b>ISO 27002 A.12.4.1, A.16.1.7</b></li> <li><b>NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4</b></li> </ul>
			Impact of events is determined		<ul style="list-style-type: none"> <li><b>CIS CSC 4, 6</b></li> <li><b>COBIT 5 APO12.06, DSS03.01</b></li> <li><b>ISO 27002 A.16.1.4</b></li> <li><b>NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4</b></li> </ul>
			Incident alert thresholds are established		<ul style="list-style-type: none"> <li><b>CIS CSC 6, 19</b></li> <li><b>COBIT 5 APO12.06, DSS03.01</b></li> <li><b>ISA 62443-2-1:2009 4.2.3.10</b></li> <li><b>ISO 27002 A.16.1.4</b></li> <li><b>NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8</b></li> </ul>

Source: Standards mapping from NIST CSF

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# B1: We propose to set a suite of general cybersecurity standards for sectorial committees to choose from (8/10)

Category	Subcategory	Suite of risk standards	Category	Subcategory	Suite of risk standards
Security Continuous Monitoring: The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures	The network is monitored to detect potential cybersecurity events	<ul style="list-style-type: none"> <li>CIS CSC 1, 7, 8, 12, 13, 15, 16</li> <li>COBIT 5 DSS01.03, DSS03.05, DSS05.07</li> <li>ISA 62443-3-3:2013 SR 6.2</li> <li>NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM- 3, SC-5, SC-7, SI-4</li> </ul>	Vulnerability scans are performed		<ul style="list-style-type: none"> <li>CIS CSC 4, 20</li> <li>COBIT 5 BAI03.10, DSS05.01</li> <li>ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7</li> <li>ISO 27002 A.12.6.1</li> <li>NIST SP 800-53 Rev. 4 RA-5</li> </ul>
	The physical environment is monitored to detect potential cybersecurity events	<ul style="list-style-type: none"> <li>COBIT 5 DSS01.04, DSS01.05</li> <li>ISA 62443-2-1:2009 4.3.3.3.8</li> <li>ISO 27002 A.11.1.1, A.11.1.2</li> <li>NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20</li> </ul>	Detection Processes:	Roles and responsibilities for detection are well defined to ensure accountability	<ul style="list-style-type: none"> <li>CIS CSC 19</li> <li>COBIT 5 APO01.02, DSS05.01, DSS06.03</li> <li>ISA 62443-2-1:2009 4.4.3.1</li> <li>ISO 27002 A.6.1.1, A.7.2.2</li> <li>NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14</li> </ul>
	Personnel activity is monitored to detect potential cybersecurity events	<ul style="list-style-type: none"> <li>CIS CSC 5, 7, 14, 16</li> <li>COBIT 5 DSS05.07</li> <li>ISA 62443-3-3:2013 SR 6.2</li> <li>ISO 27002 A.12.4.1, A.12.4.3</li> <li>NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11</li> </ul>		Detection activities comply with all applicable requirements	<ul style="list-style-type: none"> <li>COBIT 5 DSS06.01, MEA03.03, MEA03.04</li> <li>ISA 62443-2-1:2009 4.4.3.2</li> <li>ISO 27002 A.18.1.4, A.18.2.2, A.18.2.3</li> <li>NIST SP 800-53 Rev. 4 AC-25, CA-2, CA-7, SA-18, SI-4, PM-14</li> </ul>
	Malicious code is detected	<ul style="list-style-type: none"> <li>CIS CSC 4, 7, 8, 12</li> <li>COBIT 5 DSS05.01</li> <li>ISA 62443-2-1:2009 4.3.4.3.8</li> <li>ISA 62443-3-3:2013 SR 3.2</li> <li>ISO 27002 A.12.2.1</li> <li>NIST SP 800-53 Rev. 4 SI-3, SI-8</li> </ul>		Detection processes are tested	<ul style="list-style-type: none"> <li>COBIT 5 APO13.02, DSS05.02</li> <li>ISA 62443-2-1:2009 4.4.3.2</li> <li>ISA 62443-3-3:2013 SR 3.3</li> <li>ISO 27002 A.14.2.8</li> <li>NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, SI-3, SI-4, PM-14</li> </ul>
	Unauthorized mobile code is detected	<ul style="list-style-type: none"> <li>CIS CSC 7, 8</li> <li>COBIT 5 DSS05.01</li> <li>ISA 62443-3-3:2013 SR 2.4</li> <li>ISO 27002 A.12.5.1, A.12.6.2</li> <li>NIST SP 800-53 Rev. 4 SC-18, SI-4, SC-44</li> </ul>		Event detection information is communicated	<ul style="list-style-type: none"> <li>CIS CSC 19</li> <li>COBIT 5 APO08.04, APO12.06, DSS02.05</li> <li>ISA 62443-2-1:2009 4.3.4.5.9</li> <li>ISA 62443-3-3:2013 SR 6.1</li> <li>ISO 27002 A.16.1.2, A.16.1.3</li> <li>NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA- 5, SI-4</li> </ul>
	External service provider activity is monitored to detect potential cybersecurity events	<ul style="list-style-type: none"> <li>COBIT 5 APO07.06, APO10.05</li> <li>ISO 27002 A.14.2.7, A.15.2.1</li> <li>NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4</li> </ul>		Detection processes are continuously improved	<ul style="list-style-type: none"> <li>COBIT 5 APO11.06, APO12.06, DSS04.05</li> <li>ISA 62443-2-1:2009 4.4.3.4</li> <li>ISO 27002 A.16.1.6</li> <li>NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA- 5, SI-4, PM-14</li> </ul>
	Monitoring for unauthorized personnel, connections, devices, and software is performed	<ul style="list-style-type: none"> <li>CIS CSC 1, 2, 3, 5, 9, 12, 13, 15, 16</li> <li>COBIT 5 DSS05.02, DSS05.05</li> <li>ISO 27002 A.12.4.1, A.14.2.7, A.15.2.1</li> <li>NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4</li> </ul>			

Source: Standards mapping from NIST CSF

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# B1: We propose to set a suite of general cybersecurity standards for sectorial committees to choose from (9/10)

Category	Subcategory	Suite of risk standards	Category	Subcategory	Suite of risk standards
<b>Response Planning:</b> Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents	Response plan is executed during or after an incident	<ul style="list-style-type: none"> <li>CIS CSC 19</li> <li>COBIT 5 APO12.06, BAI01.10</li> <li>ISA 62443-2-1:2009 4.3.4.5.1</li> <li>ISO 27002 A.16.1.5</li> <li>NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8</li> </ul>	<b>Analysis:</b> Analysis is conducted to ensure effective response and support recovery activities.	Notifications from detection systems are investigated	<ul style="list-style-type: none"> <li>CIS CSC 4, 6, 8, 19</li> <li>COBIT 5 DSS02.04, DSS02.07</li> <li>ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8</li> <li>ISA 62443-3-3:2013 SR 6.1</li> <li>ISO 27002 A.12.4.1, A.12.4.3, A.16.1.5</li> <li>NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4</li> </ul>
<b>Communications:</b> Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Personnel know their roles and order of operations when a response is needed	<ul style="list-style-type: none"> <li>CIS CSC 19</li> <li>COBIT 5 EDM03.02, APO1.02, APO12.03</li> <li>ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4</li> <li>ISO 27002 A.6.1.1, A.7.2.2, A.16.1.1</li> <li>NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8</li> </ul>	The impact of the incident is understood	Forensics are performed	<ul style="list-style-type: none"> <li>COBIT 5 DSS02.02</li> <li>ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8</li> <li>ISO 27002 A.16.1.4, A.16.1.6</li> <li>NIST SP 800-53 Rev. 4 CP-2, IR-4</li> </ul>
	Incidents are reported consistent with established criteria	<ul style="list-style-type: none"> <li>CIS CSC 19</li> <li>COBIT 5 DSS01.03</li> <li>ISA 62443-2-1:2009 4.3.4.5.5</li> <li>ISO 27002 A.6.1.3, A.16.1.2</li> <li>NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8</li> </ul>	Incidents are categorized consistent with response plans	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	<ul style="list-style-type: none"> <li>COBIT 5 APO12.06, DSS03.02, DSS05.07</li> <li>ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1</li> <li>ISO 27002 A.16.1.7</li> <li>NIST SP 800-53 Rev. 4 AU-7, IR-4</li> </ul>
	Information is shared consistent with response plans	<ul style="list-style-type: none"> <li>CIS CSC 19</li> <li>COBIT 5 DSS03.04</li> <li>ISA 62443-2-1:2009 4.3.4.5.2</li> <li>ISO 27002 A.16.1.2, Clause 7.4, Clause 16.1.2</li> <li>NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4</li> </ul>			<ul style="list-style-type: none"> <li>CIS CSC 19</li> <li>COBIT 5 DSS02.02</li> <li>ISA 62443-2-1:2009 4.3.4.5.6</li> <li>ISO 27002 A.16.1.4</li> <li>NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8</li> </ul>
	Coordination with stakeholders occurs consistent with response plans	<ul style="list-style-type: none"> <li>CIS CSC 19</li> <li>COBIT 5 DSS03.04</li> <li>ISA 62443-2-1:2009 4.3.4.5.5</li> <li>ISO 27002 Clause 7.4</li> <li>NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8</li> </ul>			<ul style="list-style-type: none"> <li>CIS CSC 4, 19</li> <li>COBIT 5 EDM03.02, DSS05.07</li> <li>NIST SP 800-53 Rev. 4 SI-5, PM-15</li> </ul>
	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	<ul style="list-style-type: none"> <li>CIS CSC 19</li> <li>COBIT 5 BAI08.04</li> <li>ISO 27002 A.6.1.4</li> <li>NIST SP 800-53 Rev. 4 SI-5, PM-15</li> </ul>			

Source: Standards mapping from NIST CSF

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

# B1: We propose to set a suite of general cybersecurity standards for sectorial committees to choose from (10/10)

Category	Subcategory	Suite of risk standards	Category	Subcategory	Suite of risk standards
<b>Mitigation:</b> Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Incidents are contained	<ul style="list-style-type: none"> <li>CIS CSC 19</li> <li>COBIT 5 APO12.06</li> <li>ISA 62443-2-1:2009 4.3.4.5.6</li> <li>ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4</li> <li>ISO 27002 A.12.2.1, A.16.1.5</li> <li>NIST SP 800-53 Rev. 4 IR-4</li> </ul>	<b>Improvements:</b> Recovery planning and processes are improved by incorporating lessons learned into future activities.	Recovery plans incorporate lessons learned	<ul style="list-style-type: none"> <li>COBIT 5 APO12.06, BAI05.07, DSS04.08</li> <li>ISA 62443-2-1:2009 4.4.3.4</li> <li>ISO 27002 A.16.1.6, Clause 10</li> <li>NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8</li> </ul>
	Incidents are mitigated	<ul style="list-style-type: none"> <li>CIS CSC 4, 19</li> <li>COBIT 5 APO12.06</li> <li>ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10</li> <li>ISO 27002 A.12.2.1, A.16.1.5</li> <li>NIST SP 800-53 Rev. 4 IR-4</li> </ul>		Recovery strategies are updated	<ul style="list-style-type: none"> <li>COBIT 5 APO12.06, BAI07.08</li> <li>ISO 27002 A.16.1.6, Clause 10</li> <li>NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8</li> </ul>
	Newly identified vulnerabilities are mitigated or documented as accepted risks	<ul style="list-style-type: none"> <li>CIS CSC 4</li> <li>COBIT 5 APO12.06</li> <li>ISO 27002 A.12.6.1</li> <li>NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5</li> </ul>		Communications: Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors)	<ul style="list-style-type: none"> <li>COBIT 5 EDM03.02</li> <li>ISO 27002 A.6.1.4, Clause 7.4</li> </ul>
<b>Improvements:</b> Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities	Response plans incorporate lessons learned	<ul style="list-style-type: none"> <li>COBIT 5 BAI01.13</li> <li>ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4</li> <li>ISO 27002 A.16.1.6, Clause 10</li> <li>NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8</li> </ul>	<b>Reputation:</b> Reputation is repaired after an incident	Public relations are managed	<ul style="list-style-type: none"> <li>COBIT 5 MEA03.02</li> <li>ISO 27002 Clause 7.4</li> </ul>
	Response strategies are updated	<ul style="list-style-type: none"> <li>COBIT 5 BAI01.13, DSS04.08</li> <li>ISO 27002 A.16.1.6, Clause 10</li> <li>NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8</li> </ul>		Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	<ul style="list-style-type: none"> <li>COBIT 5 APO12.06</li> <li>ISO 27002 Clause 7.4</li> <li>NIST SP 800-53 Rev. 4 CP-2, IR-4</li> </ul>
<b>Recovery Planning :</b> Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents	Recovery plan is executed during or after a cybersecurity incident	<ul style="list-style-type: none"> <li>CIS CSC 10</li> <li>COBIT 5 APO12.06, DSS02.05, DSS03.04</li> <li>ISO 27002 A.16.1.5</li> <li>NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8</li> </ul>			

Source: Standards mapping from NIST CSF

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

---

# Questions?

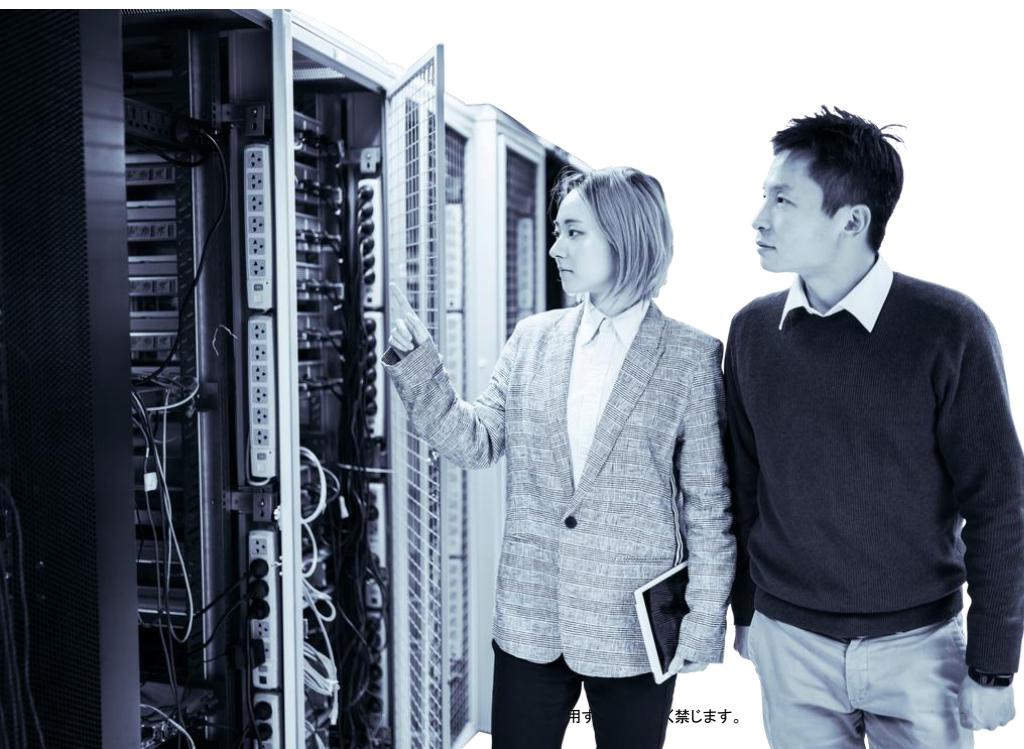
---



## Workshop Topics (40 minutes)

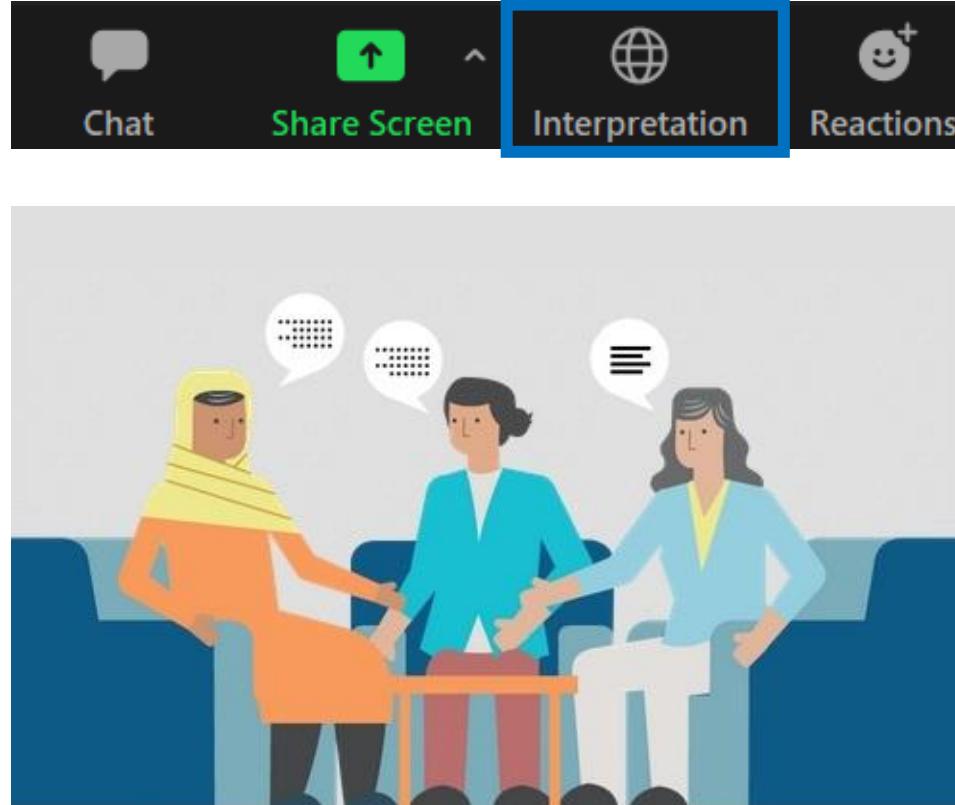
---



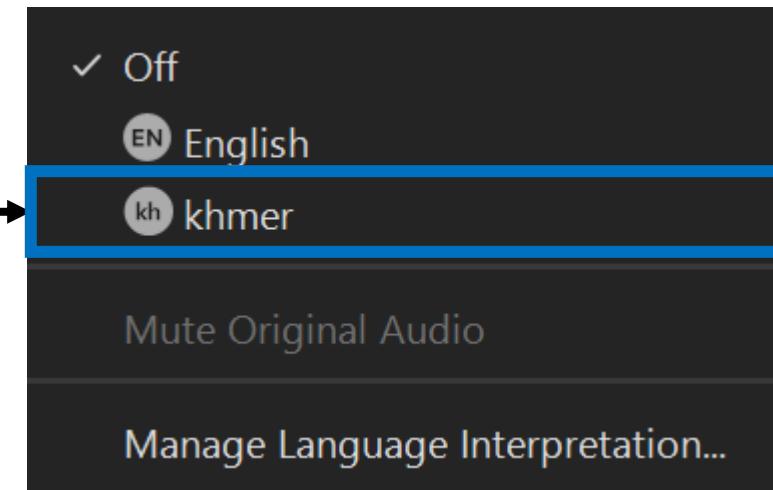
- 
1. Overview of Cyber Security Trend
  2. Definition of Cyber threat and national Incident response framework
  3. Cyber Security Regulation framework
  4. Partnership(Public, Private, Academia, International)
  5. Professional training and certification
  6. Public awareness and alerts
  7. Cyber Security for SME
  8. Critical Infrastructure Industry protection
  - 9. CERT/ Resilience**
  10. Wrap up / Cyber security assessment

# Khmer simultaneous Interpretation available

Select “Interpretation” on the bottom



Select “Khmer”



- Presentation is simultaneously translated into Khmer
- You can post question in Khmer



## Timeline

## Overview

100 minuets

## Workshop & QA

20 minuets

# Cambodia need to design Cyber security strategy with suggested strategy element

Cybersecurity strategy element	Insights from benchmarking cybersecurity strategy	#
A Governance 	<ul style="list-style-type: none"> <li>Top-performing nations are moving towards <b>centralized governance bodies</b> reporting directly to executive branches of government and serving as <b>E2E owners of cybersecurity strategy implementation</b></li> </ul>	• #2
B Legal and regulations 	<ul style="list-style-type: none"> <li><b>Comprehensive legislative frameworks</b> cover mandatory IT security standards, regulations, and best practices, and are enforced through audits and law enforcement</li> <li><b>Specific legislations to address emerging technologies</b> are evolving at fast pace in countries with advanced cybersecurity legislations</li> </ul>	• #3
E Partnerships 	<ul style="list-style-type: none"> <li><b>Regional and international partnerships</b> are actively used to foster sharing of best practices and enhancing operational and technical capabilities through joint drills &amp; audits</li> </ul>	• #4
C Talent and people 	<ul style="list-style-type: none"> <li><b>Public awareness and training</b> programs, which draw on <b>international standards and offerings</b>, form the basis for cybersecurity talent development</li> </ul>	• #5~7
F Critical infrastructure 	<ul style="list-style-type: none"> <li>CII protection programs, executed by national cybersecurity agencies, focus <b>selectively on critical assets</b> in critical sectors with timely involvement of relevant authorities</li> </ul>	• #8
D Incident response 	<ul style="list-style-type: none"> <li>National cybersecurity agencies, through <b>specialized incident response teams</b>, lead integrated response efforts with close coordination with impacted assets</li> </ul>	• #9

# CERT



## History of CERT

In 1988, following an internet worm incident, the Defence Advanced Research Agency (DARPA) in the US tasked the Software Engineering Institute (SEI) of Carnegie Mellon University to set up a center to coordinate with security and computer experts to respond to and help prevent future incidents. This became the first Computer Emergency Response Team (CERT) Coordination Center.

The SEI at Carnegie Mellon trademarked and owns the 'CERT' name. They encourage other organizations to use CSIRT (Computer Security Incident Response Team), or prefix/suffix with an additional term (e.g., US-CERT)

## Mission

To respond quickly to and recover from cyber attacks, and improve the resilience of the country against cyber threats

## Scope of work

During a cyber incident: incident handling (issuing alerts, warnings, announcements, coordinating with necessary stakeholders) analysis and reporting

Steady state: Awareness building, sharing standards and best practices

## Typical Governance model

2 key models:

1. Led by an existing ministry in the government (such as the telecom ministry)
2. Set up an independent 'cyber security center' which is responsible for the CERT and the entire cybersecurity strategy

# There are a variety of emergency response teams to support different constituents (1/2)

対外厳秘

**National CERT**

<b>Scope of work</b>	<ul style="list-style-type: none"> <li>National and international PoC for cyber incidents</li> <li>Identify and manage cyber threats, and respond to, recover from and prevent future cyber incidents</li> <li>Support continuity of services and minimize theft of information and disruption of services</li> <li>Develop tools and knowledge to detect, manage and prevent cyber incidents</li> <li>Share security related, security best practices and guidance available through publications, websites, etc.</li> <li>Develop education, awareness and training materials for different audiences</li> </ul>
<b>Ministries involved</b>	Ministry of communications, Ministry of Information Technology, Prime Minister's Office, Ministry of Home Affairs
<b>Types of CERT</b>	National, governmental, de facto national
<b>Example</b>	JPCERT/CC CamCERT/MNCERT Singapore's SingCERT

**Regional CERT**

<ul style="list-style-type: none"> <li>Improving cooperation, strengthening relationships between and enhancing resilience of CSIRTs in and of member states</li> <li>Assisting countries in setting up their CSIRTs</li> <li>Developing standards and supporting education &amp; outreach programs in ICT security in member countries</li> <li>Promoting good practices, policy frameworks and legal guardrails among member countries</li> <li>Promoting R&amp;D on ICT security</li> </ul>
--

**Sectoral CERT**

<ul style="list-style-type: none"> <li>PoC for security incident-related information and reporting for the sector</li> <li>Strengthen the IT security competence</li> <li>Ongoing security incident management</li> <li>Relevant training</li> <li>Participation in international cyber security exercises</li> <li>Collaborate on creation of security standards for the relevant sector</li> </ul>
--

# There are a variety of emergency response teams to support different constituents (2/2)



## Organizational CERT



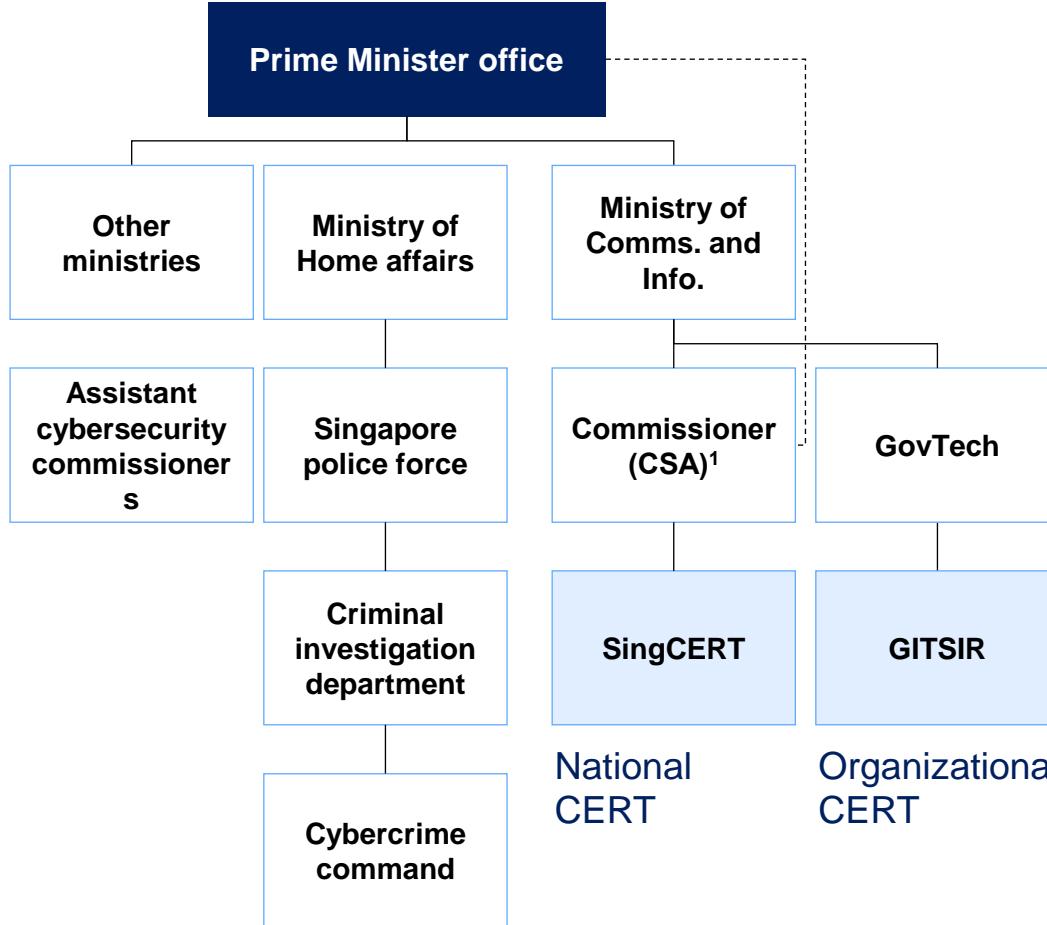
## Commercial (Vendor) CERT

<b>Scope of work</b>	<p>Key PoC for all security incidents in government</p> <p>Coordinate with external entities (other government agencies, external organisations, Internet Service Providers, law enforcement, etc.)</p> <p>Provide technical support to investigate, resolve and recover from security incidents</p> <p>Improve incident response capabilities of government offices</p>	<p>Security communication services</p> <p>Proactive services</p> <p>Incident response services</p> <p>Threat intelligence information services</p> <p>Security quality management services</p> <p>Vulnerability management services</p> <p>Threat hunting services</p>
<b>Ministries involved</b>	<p>For government: Ministry of Information Technology, Ministry of communications</p> <p>For private: None</p>	None
<b>Types of CERT</b>	Governmental, military, commercial and non-commercial organizations	Commercially offered CERT services
<b>Example</b>	<p>Singapore's Government IT Security Incident Response (GITSIR)</p> <p>Estonia EDF CIRC</p> <p>Corporate CERT</p>	<p>IBM CERT</p> <p>Cisco CERT</p> <p>Verizon's CERT services</p>

# CERT : In Singapore, Both national CERT and organizational CERT are located under Ministry of Commision and Information



## Singapore's cybersecurity governance structure



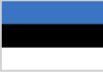
## Key Governance elements

- |  |   |  |
|--|---|--|
|  | <b>Authority of central coordination body</b> | <ul style="list-style-type: none"> <li>The Cybersecurity Agency of Singapore (CSA) is the regulator for the sector and reports nominally to the Prime Minister Office</li> <li>CSA is responsible for delivering Singapore's cybersecurity strategy</li> </ul> |
|  | <b>Sectoral governance</b>                    | <ul style="list-style-type: none"> <li>Assistant Commissioner public officers from Ministries or regulators will be "Sector Leads" in the respective sector, i.e., lead government agency in charge of each CII sector</li> </ul>                              |
|  | <b>KPIs monitoring</b>                        | <ul style="list-style-type: none"> <li>CSA publishes the "Singapore Cyber Landscape" in which he reports on threats and KPIs against the national cybersecurity strategy pillars</li> </ul>  |
|  | <b>National incidence response</b>            | <ul style="list-style-type: none"> <li>The Commissioner of Cybersecurity is responsible for investigating cybersecurity threats and incidents</li> </ul>   |

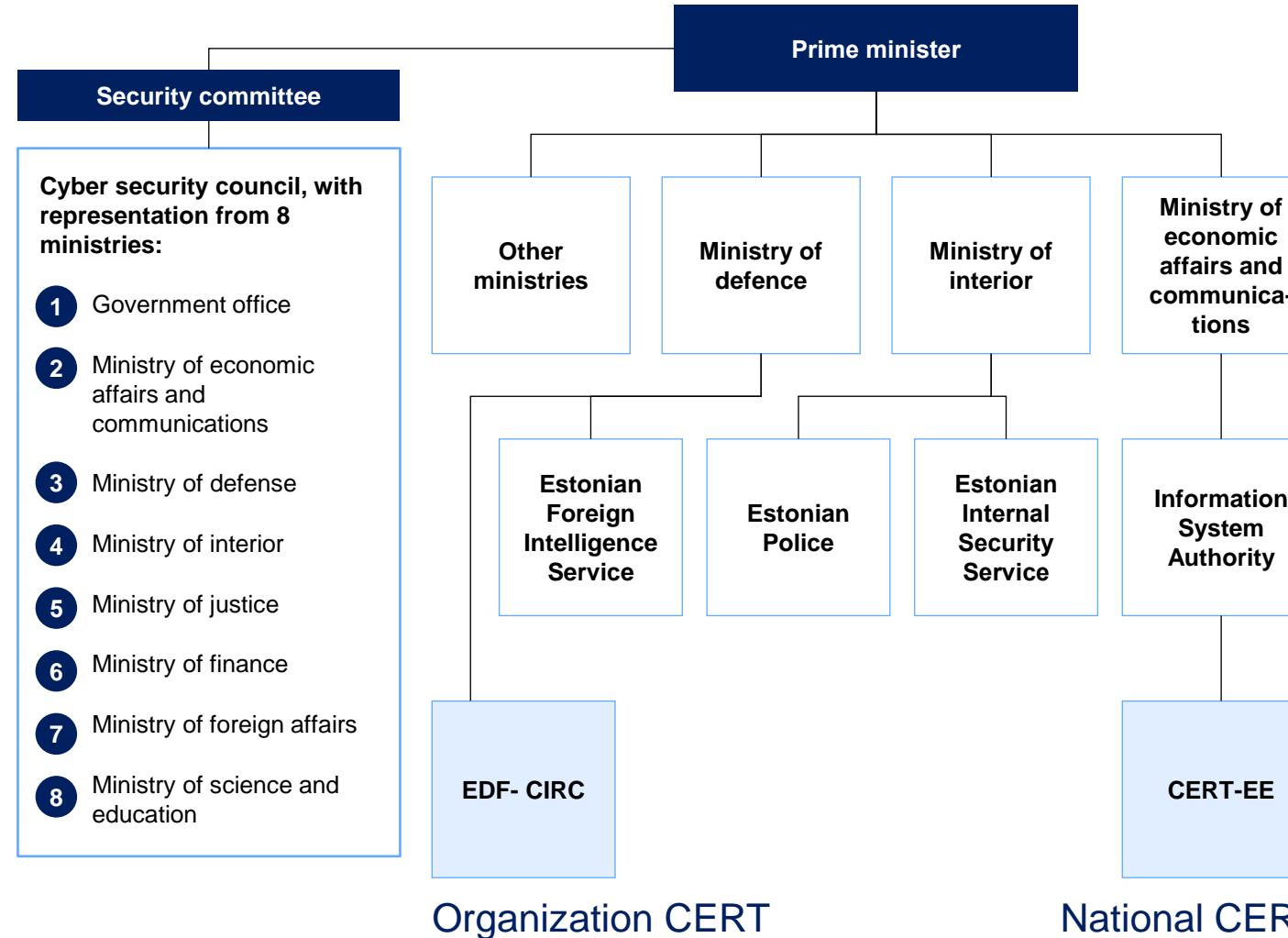
1. Today Cyber security Commissioner is also the CEO of the Cyber Security Agency

# CERT : Estonia allocate Organization CERT under Ministry of defence for mostly defence purpose

対外厳密



## Estonia's governance structure



## Key governance drivers

<b>Authority and mandate of central coordination body</b>	New cybersecurity bill (2018) specifies the duties of the national supervisory body, the Information System Authority (RIA), in coordinating the ensuring of cybersecurity
<b>Sectoral governance</b>	Sector regulators and ministers are responsible for the development/adaption of regulations to their sectors
<b>KPI monitoring</b>	The RIA monitors and publishes reports on the status of cybersecurity in Estonia
<b>National incidence response</b>	Estonia has two cybersecurity response teams, one to handle incidents involving the military and one non-military entities

# Sector CERT : USA's “Office of Cybersecurity, Energy Security and Emergency Response”



## Overview



To enhance the security of U.S. critical energy infrastructure to all hazards, mitigate the impacts of disruptive events and risk to the sector overall through **preparedness and innovation**, and respond to and facilitate recovery from energy disruptions in collaboration with other Federal agencies, the private sector, and State, local, tribal, and territory governments.

## Key goals



- Advance cyber discovery, vulnerability assessment, and rapid risk mitigation
- Pursue game-changing R&D and technology transition
- Build capacity in the energy sector to understand risks, assess priorities, and identify cost effective security and resilience improvements
- Enhance sector-wide situational awareness to inform decision-making in the energy sector
- Coordinate effective and efficient emergency response and recovery efforts

## Key partners



- Electricity Subsector Coordinating Council (ESCC)
- Electricity Information Sharing and Analysis Center (E-ISAC)
- Oil and Natural Gas Subsector Coordinating Council
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- National Cybersecurity and Communications Integration Center (NCCIC)
- NIST Smart Grid Interoperability Panel (SGIP)
- DARPA
- Department of Defense

## 2020 Impact

Initiated the **Energy Sector Pathfinder** in partnership with industry and DOD, DHS and FBI, to increase cybersecurity coordination between government and industry

Launched the **Securing Energy Infrastructure Executive Task Force** to convene key stakeholders from all levels of government, industry, academia, and the National Labs to jointly address priority technical vulnerabilities in energy systems.

Identified use cases and developed tools to **enhance detection of malicious cyber activity in OT networks** and expanded tools to include application in the wind industry

145 cybersecurity experts from 75 electricity, oil, and gas sector companies participated in **updating and validating the Cybersecurity Capability Maturity Model (C2M2)**

# Commercial CERT - CISCO covers the whole spectrum of solutions across Cybersecurity value chain

対外厳秘



## Basic Information

**Founded :** December 1984

**Headquarters :** San Jose, California, USA

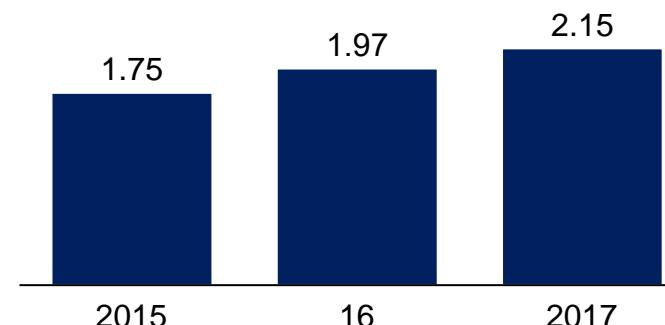
**Employees :** 72790

**Revenues :** USD 2.1 bn+ (FY2017, security business only)

**CEO :** Chuck Robbins

## Company Performance

### Security Revenues, USD billion



1. ...

## Solution Overview

### Hardware

- Content Management, Data Centre
- Network Security
- Firewall, VPN, Threat management, Adaptive Security Management applications, Integrated Router Security

### Software

- Integrated Cyber defence
- Advanced Malware
- Network Visibility and Segmentation
- Endpoint Security
- Web Security
- Messaging Security (Encryption)
- Network Security
- Cloud Security

### Services

- Implementation Services
- Managed Security Services – Threat Monitoring
- Consulting and advisory Services
- Technical support, optimisation and education Services

## Strengths

Worldwide and world class security team

On-going research and new technology development

Open Platform

Integrated portfolio

Scale and capabilities to tackle high volume complex threats

## Presence and key clients

Present globally, share of revenues for FY 2017, across all segments: Americas (59%), EMEA (25%) and Asia-Pacific Japan (16%)

Serves clients across all verticals and sectors

# Japan is member of steering committee of APCERT



## APCERT – Governance structure

Chair

Malaysia;  
Cyber Security Malaysia



Deputy  
Chair

China  
National Computer network Emergency Response technical Team / Coordination Center of China



Steering  
Committee

Malaysia;  
CyberSecurity  
Malaysia



China  
National  
Computer  
network  
Emergency  
Response  
technical Team /  
Coordination  
Center of China



Australia:  
Australian Cyber  
Security Centre



Japan:  
Japan Computer  
Emergency  
Response Team  
/ Coordination  
Center



Korea:  
Korea Internet  
Security Center



Sri Lanka:  
Sri Lanka  
Computer  
Emergency  
Readiness  
Team  
Coordination  
Centre



Taipei  
Taiwan National  
Computer  
Emergency  
Response Team



# Korean government play a leading role in 2016 to form CS consortium, CAMP(Cybersecurity Alliance for Mutual Progress)

## Overview



CAMP is initiated by the **Korean government** with the purposes of achieving sustainable benefits and serving as a platform where members prepare themselves with collective actions to keep cyberspace safe. CAMP was **officially launched on July 11, 2016 in Korea with 40 organizations from 29 countries**

## Mission & Vision

CAMP will serve as a **network platform to lift up the overall level of cybersecurity** of the members. The members will share development experiences and trends of cybersecurity to catalyze mutual growth as well as contribute to development of global cybersecurity for large.



### Building a Global Human Network

To make cybersecurity society available for actively interacting each other



### Sharing Information on Cybersecurity issues

Such as up-to-date industrial news and policy trends on cybersecurity



### Responding Collectively on Cyber Matter

Against the major cyber matter and enhance political leveraging power at the global scale

## ASEAN members



Cambodia: Ministry of Posts and Telecommunications(MPTC)



Mongolia: Communications and Information Technology Authority(CITA)



Laos: Lao CERT



Thailand: Electronics Government Agency (EGA)



Philippines: Department of Information and Communications Technology (DICT)

Malaysia: CyberSecurity Malaysia

Sri Lanka:Sri Lanka CERT|CC

Vietnam:Vietnam Computer Emergency Response Teams(VNCERT)

Indonesia: National Cyber and Crypto Agency(BSSN)

**(Total 61 organizations from 46 countries)**

# Singapore CRA leading ASEAN CERTs by setting up ASEAN-Singapore Cybersecurity Center of Excellence(ASCCE) in 2016

## Overview



**The ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE)**, an extension of the ASEAN Cyber Capacity programs (ACCP) which was launched in 2016, aims to build a **more secure and resilient cyberspace** through capacity building programs for ASEAN senior policy and technical officials with decision-making responsibilities.

## Focus

## Programs

The ASCCE will undertake a modular, multi-disciplinary and multi-stakeholder approach to deliver these programs. **With a five year funding commitment of S\$30 million(US\$22 million)**

Conduct **research and provide trainings** in areas **technical training** as well as **trainings and exercises** spanning **international law, cyber strategy, legislation, cyber norms and other cybersecurity policy issues**.

Provide **CERT-related technical training** as well as **trainings and exercises** facilitate the exchange of open-source cyber threat and attack-related information and best practices;

Conduct **virtual cyber defence trainings and exercises**.

## International partners

Nation : Australia, Canada, the European Union, Japan, New Zealand, Republic of Korea, U.K. and U.S.A.  
Organization : International Advisory Panel (IAP), International Programme Committee (IPC),

## ASEAN Cyber Capacity Programme (ACCP)

ACCP aims to build cyber capacity in ASEAN Member States. It will enhance regional ability to respond to the evolving cyber threat landscape and to build a secure and resilient ASEAN cyberspace. Focus areas under the programme includes **cyber policy, legislation, strategy development as well as incident response**. Events under the ACCP will include **workshops, seminars and conferences**.  
Trainers of the programme are selected from **the INTERPOL Global Centre for Innovation** in Singapore, ASEAN Dialogue Partners, academics from institutes as the **Centre of Excellence for National Security (CENS)** at the S.Rajaratnam School of International Studies (RSIS), the **Cyber Security Agency of Singapore(CSA)**

# Thailand and Philippines are members of The Global Forum on Cyber Expertise (GFCE) launched by the Dutch Government in 2015

## Overview



The GFCE was **established during the 2015 Global Conference on Cyber Space** in the Hague to strengthen cyber capacity building and coordinate existing international efforts more effectively. The GFCE was **launched by the Dutch Government** along with 41 ministers and other high-level representatives from **business and international organizations**. In 2017, at the Global Conference on Cyber Space in New Delhi, the GFCE positioned itself as the **coordinating platform for cyber capacity building** by developing the Global Agenda for Cyber Capacity Building.

## Mission & Vision

To strengthen cyber capacity and expertise globally through international collaboration and cooperation.

**GFCE Working Groups:** The Working Groups aim to **strengthen international cooperation and coordination** on their respective theme by developing a common focus, enabling efficient use of available resources, and avoiding duplication of efforts.

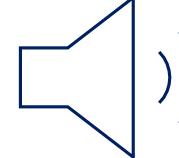
A

**Policy & Strategy**



B

**Incident Management & Infrastructure Protection**



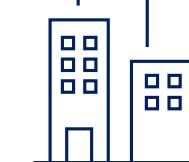
C

**Cybercrime**



D

**Culture & Skills**



## Members

GFCE Members consist of countries, intergovernmental organizations (IGOs), international organizations and private companies with the commitment and resources to contribute to cyber capacity building.

## Partners

GFCE Partners are organizations with specific cyber expertise that have been endorsed by at least one GFCE Member. Partners include but are not limited to nongovernmental organizations (NGOs), academia, the tech community and private organizations.

# ENISTA CERT capacity framework



**1**  
**Mandate & Strategy**

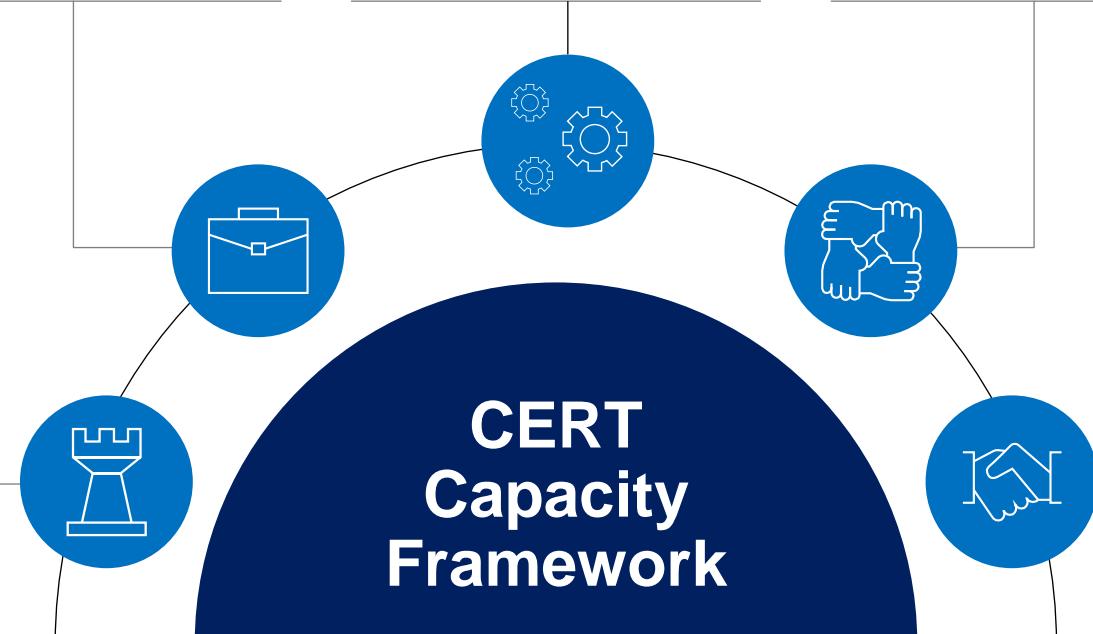
**2**  
**Service Portfolio**

**3**  
**Operation**

**4**  
**Cooperation**

**5**  
**Capacity, skills and trust building**

**CERT  
Capacity  
Framework**



# 1 Mandate & Strategy



## Mandate



Host organisation



Constituency

## Details

The official, legal framework within which the national / governmental CERT must work sometimes depends on the host organisation in which the CERT is located. In other cases, the official, legal framework should be defined by the official mandate given by the government.

The constituency of a CERT is an established term for the customer base for its services. So, in theory, the constituency of a national / governmental CERT consists of all entities with the state's borders. This is due to the fact that any domestic entity is a potential customer of the national / governmental CERT. The constituency of a national/governmental CERT can typically be broken down into subgroups, according to the services the CERT delivers to the entities in the group or based on the responsibilities the CERT carries with regards to the group. Typically, the following constituency subgroups can be distinguished:

- Government and public bodies
- Critical information infrastructure organisations
- Other stakeholders within the state's borders

# 2 Service Portfolio (1/6)



## Services portfolio



### Proactive services

Aimed at improving the infrastructure and security processes of the constituency before any incident or event occurs or is detected. The main goals are to avoid incidents and reduce their impact and scope when they do occur.



### Reactive services

Aimed at responding to requests for assistance, reports of incidents from the CERT constituency, and tackling threats or attacks against the CERT's systems



### Other security quality management services

Are the common services designed to improve the overall security of an organisation. By leveraging the unique experiences gained in providing reactive and proactive services to its high-value constituency, a national/governmental CERT finds itself in a special position to apply those experiences to these quality management services. These services are designed to incorporate feedback and lessons learned based on knowledge gained in responding to incidents, vulnerabilities and attacks.

# 2 Service Portfolio (2/6) National CERT Core Capability



## Services portfolio



### Incident handling

The only certainty within cyber-security is the fact that 100% security does not exist. Security incidents will happen, no matter what. Without an effective incident handling capability, attacks and intrusions on critical national information infrastructure could cripple the state for the duration of the attack. Consequently, handling cyber-security incidents on a national (and cross-border) scale, and incidents related to critical information infrastructure, are a priority for a national/governmental CERT. Incidents related to critical information infrastructure can pose a direct threat to society (economic, governmental, infrastructural or ecologic threats) and the lives of a state's citizens (eg, in the case of an incident at a nuclear power plant). These incidents should therefore receive priority over all ongoing activities and be contained and mitigated as quickly as possible.



### National point of contact for incident reporting and information dissemination

Probably the second most important task performed by a national/governmental CERT is its role as the national point of contact for reports on incidents and the dissemination of security-related information. This is one of the responsibilities that must be officially mandated by a government to its national/governmental CERT in order to achieve clear and flexible national and international collaboration. Foreign CERT teams must clearly know whom to contact with regards to the sharing of security-related information and the reporting of incidents. Additionally, the national/governmental CERT is best positioned to further disseminate such information (alerts, warnings, announcements, vulnerabilities, etc) among the other CERTs in the country and the information security communities. In addition, the national/governmental CERT will also represent the country in international CERT communities by virtue of this official mandate.



### Critical information infrastructure protection

The role of a national/governmental CERT in national CIIP is not fixed. Several services could be provided in addition to the incident handling service. Examples include risk analysis, security consulting, security assessment, intrusion detection services and many other services. The exact role of the national/governmental CERT will depend heavily on the national strategy for CIIP.

## 2 Service Portfolio (3/6)



### CII Protection

Announcements informing constituents about new developments with medium- to long-term impact, such as newly found vulnerabilities

Security-related information sharing that provides constituents with a comprehensive and easy-to-find collection of useful information and guidelines for improving security

Alerts and warnings involving the dissemination of information that describes an intruder attack, security vulnerability, intrusion alert, computer virus or hoax, etc, and providing a short-term recommended course of action for dealing with the resulting problem

Awareness building that provides information and guidance for conforming better to accepted security practices and organisational security policies

## 2 Service Portfolio (4/6)



### Proactive services

Technology watch, announcements, and the dissemination and sharing of security-related information could provide early warnings of threats or vulnerabilities and help the constituency protect its systems before it is too late

Security assessments could aid the constituency in mitigating existing vulnerabilities in their infrastructure

Providing guidelines on security configuration could assist the constituency in hardening their systems in order to minimize the attack surface and reduce the residual risk

Providing intrusion detection services could help the constituency to detect ongoing attacks or intrusions, and to initiate the incident handling process as soon as possible

# 2 Service Portfolio (5/6)



## Reactive services



Issuing alerts and warnings



Vulnerability handling



Artifact handling

## Details

Alerts and warnings can be based on inter-CERT communications, incidents that happened in the constituency and/or detected vulnerabilities.

In order to provide high-quality vulnerability alerts, counter-measures and expert incident handling, the national/governmental CERT needs to receive information about and to be able to analyse system vulnerabilities.

To be able to provide high-quality alerts on new malware and other artifacts and to provide expert incident handling, the national/governmental CERT needs to receive information about and to be able to analyse system artifacts.

## 2 Service Portfolio (6/6)



### Security quality management services



Awareness building



Education and training



Business continuity management and disaster recovery planning



Risk management

### Details

The national/governmental CERT has an important role in advancing security knowledge and awareness, both within government and critical information infrastructure organisations, as well as with the general public. Most CERTs publicise awareness materials with regards to, for example, password best practices and phishing protection. As humans are often considered one of the weakest links in cyber-security, awareness building is a very important objective.

During workshops, courses, tutorials or exercises, national/governmental CERTs may provide their constituents with information and training on various topics, such as good practices in incident or vulnerability management. More and more national/governmental CERTs will organize national exercises to train their staff and key constituents, often in collaboration with a military CERT.

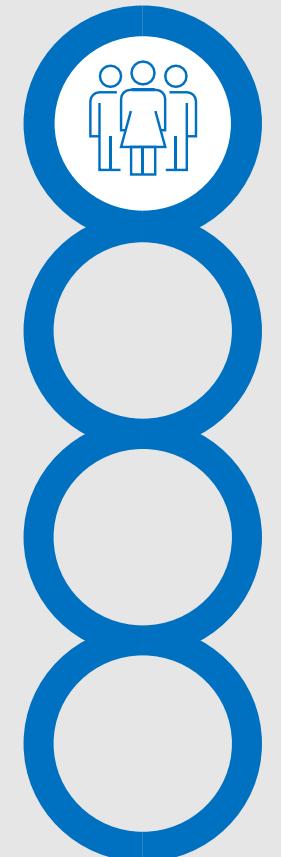
BCM/DRP is, without a doubt, key aspect of any plan for critical information infrastructure protection. National/governmental CERT experts should be involved in the cyber-security aspects of the business continuity and disaster recovery management processes for their constituents (for, in particular, the critical information infrastructure).

Traditional static risk analysis is now evolving towards a more dynamic process. Using their knowledge of the environments and information collected via the reactive (incident, vulnerability and artifact handling) and proactive (intrusion detection service and security assessments) services, a national/governmental CERT can build a snapshot of the situational awareness in its constituency. This snapshot of overall risk will support decision-making in situations where a significant incident or crisis has arisen.

# 3 Operation (1/4)



## Operation area



Human resources

Infrastructure

Service delivery

Business continuity

## Details

### Team

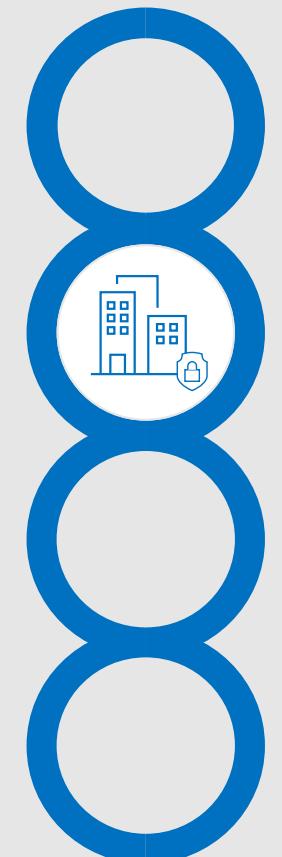
- Team leader/manager/coordinator who:
  - Provides strategic direction
  - Is the authoritative representative of the national/governmental CERT
  - Supervises or leads the team
- Incident handlers who:
  - Provide incident handling capability by monitoring, analyzing and responding to incidents
  - Undertake technology watch, the dissemination of information and other tasks when no incidents are ongoing
- Technical experts who can take on a number of roles, such as:
  - Vulnerability handling
  - Technical writing
  - Training
  - Platform specific support
- Support staff who:
  - Carry out administrative tasks
  - Monitor reports on events and incidents
  - Undertake technology watch and the dissemination of information

Operation mode

# 3 Operation (2/4)



## Operation area



Human resources

### Infrastructure

Service delivery

Business continuity

## Details

The role national/governmental CERTs play in crisis situations (e.g., large-scale cyber-attacks)

The confidentiality of the information processed and stored by a national/governmental CERT (records of incidents, CII vulnerabilities, etc.)

The criticality of the infrastructure that a national/governmental CERT helps to protect (energy, healthcare, communication networks, etc.)

Communication services

Logical security

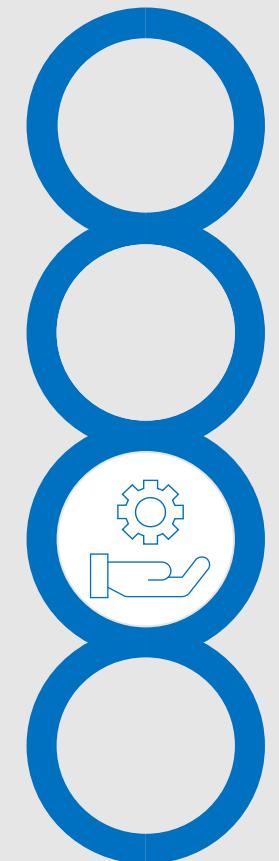
- An internal information security management framework and policy – in order to provide the security strategy and authorization to implement controls over the:
  - Information classification scheme, shared with the
  - Constituency and partners in cooperation
  - Password policy
  - Access management policy
- Integrity controls (e.g., hash comparison) to prevent unauthorized changes
- Confidentiality controls such as encryption.

Physical security

# 3 Operation (3/4)



## Operation area



Human resources

Infrastructure

**Service delivery**

Business continuity

## Details

Response times for service events (e.g, incident, vulnerability report) and/or priority scheme

Level of information provided for service events (short-term)

Time-to-live for service events

Level of information provided on the longer term (reports, summaries, announcements)

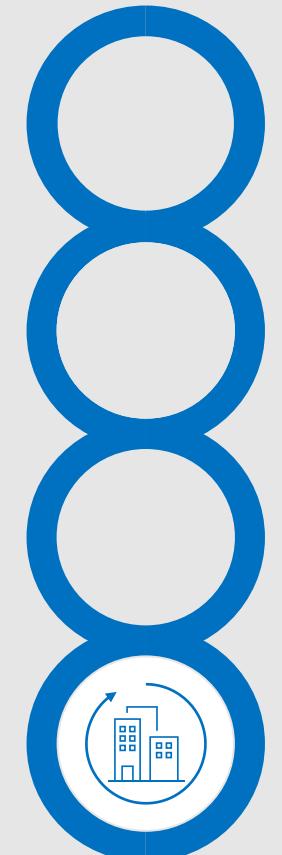
Follow-up time on vulnerability reports for all nonurgent vulnerabilities: the national/governmental CERT will follow-up with a constituent within two working days of the initial report

Follow up on high-priority incidents: every high priority incident will be acknowledged within two hours. Analysis will start within the first hour of receipt of such a report.

# 3 Operation (4/4)



## Operation area



Human resources

Infrastructure

Service delivery

**Business continuity**

## Details

A national/governmental CERT is involved in the mitigation of targeted attacks against the infrastructure of its country. Therefore, the resilience of the team's infrastructure in the face of attacks needs to be ensured, as well as its possession of a solid plan for service continuity. Having and demonstrating this ability also directly reflects on the perceived competence and level of trust its constituency has in a team.

Managing incoming requests and the ability to correctly distribute them between staff (even across work-shifts) is one of these aspects. A second is the 24/7/365 operational mode which allows constituents to call in reports anytime (see paragraph 5.1). A third aspect is the ability to cope with the unavailability of critical communication channels and operational elements such as e-mail or information servers (WWW, FTP, etc). This could lead to an inability to provide specific services in a timely fashion and failure to meet contractual requirements and/or services as specified in service level agreements. This needs to be avoided as far as possible by a redundant and resilient infrastructure and a variety of communication channels as discussed previously.

# 4 Cooperation (1/4)



## Cooperation

An effective coordinated response is not possible when an incident report is passed on to a neighboring national/governmental CERT and that CERT does not act upon it by taking the necessary measures

If procedures differ too much between various national/governmental CERTs, cooperation will prove to be problematic in practice

### Cooperation area



Bi/multilateral cooperation

### Details

Bi/multilateral cooperation is a model of cooperation between two or more teams or organizations that is based on lateral agreements, i.e., agreements between the parties without a group or association being formed. The agreement could be informal (i.e., solely based on trust) or it could be formalized by a mandate, a nondisclosure agreement (NDA), a memorandum of understanding (MoU) or a contract.



Association or community

An association or community is a model of cooperation between many teams or organizations which have common interests and objectives. The framework for this kind of cooperation might be set by a common geographical area, common sets of services, similar constituencies or sectors of operations, etc.

# 4 Cooperation (2/4)



## Cooperation area



National cooperation

## Details

Constituency

Internet service providers/telecommunication network operators

Other CII operators

Law enforcement

- The incident data collected by national/governmental CERTs may contain information on criminal activities on the internet
- As part of their day-to-day job, incident handlers of national/governmental CERTs gather a vast knowledge base on the activities, tools and techniques of cybercriminals
- National/governmental CERTs cooperate daily with many organizations at the national and cross-border level. As a result, national/governmental CERTs are well connected in the cyber-security community.
- Some national/governmental CERTs offer specific services and therefore many have in-depth knowledge in computer forensics and artifact analysis

Policymakers

Other CERTs

Military and intelligence

# 4 Cooperation (3/4)



## Cooperation area



### Cross-border cooperation

## Details

Initiatives in cooperation

Trusted Introducer (TI)

European Network and Information Security Agency (ENISA)

### FIRST

- FIRST is an international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programs;
- FIRST members develop and share technical information, tools, methodologies, processes and best practices;
- FIRST encourages and promotes the development of quality security products, policies & services;
- FIRST develops and promulgates computer security best practices;
- FIRST promotes the creation and expansion of Incident Response teams and membership from organizations from around the world;
- FIRST members use their combined knowledge, skills and experience to promote a safer and more secure global electronic environment.

### IMPACT

Sector working groups

# 4 Cooperation (4/4)



## Cooperation area



Crucial  
elements for  
cooperation

## Details

### Trust

- Trust building
- Trust models

### Quality of information

### Sustainable reaction

- Sufficiently high quality and timely information
- Communication and collaborative links with trusted partners
- Common terminology and schemes in use

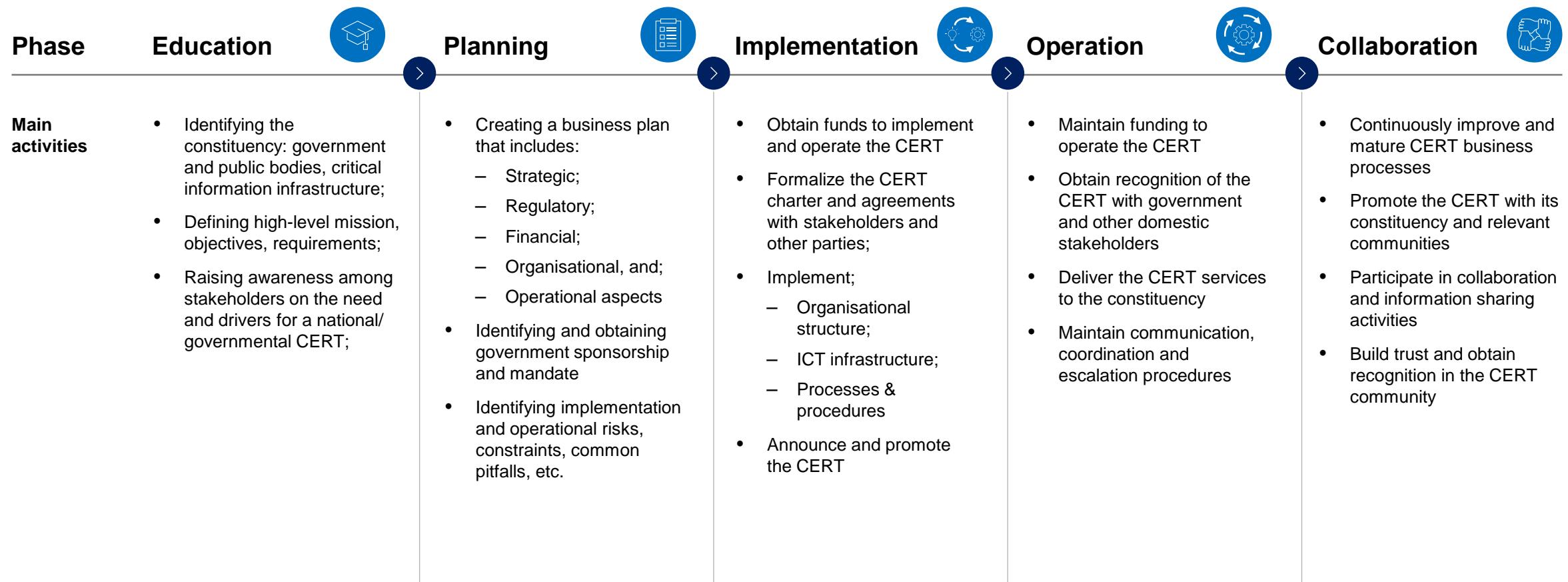
### Common terminology and schemes

- Incident reporting forms and incident exchange formats
- Information classification schemes
- System and application naming conventions
- Frameworks and taxonomies for cyber-security metrics
- Procedures to handle critical incidents and the associated expectations with regards to priority, feedback, etc.



# 5 Capacity, skills and trust building (Implementation roadmap)

## National/governmental CERT implementation roadmap

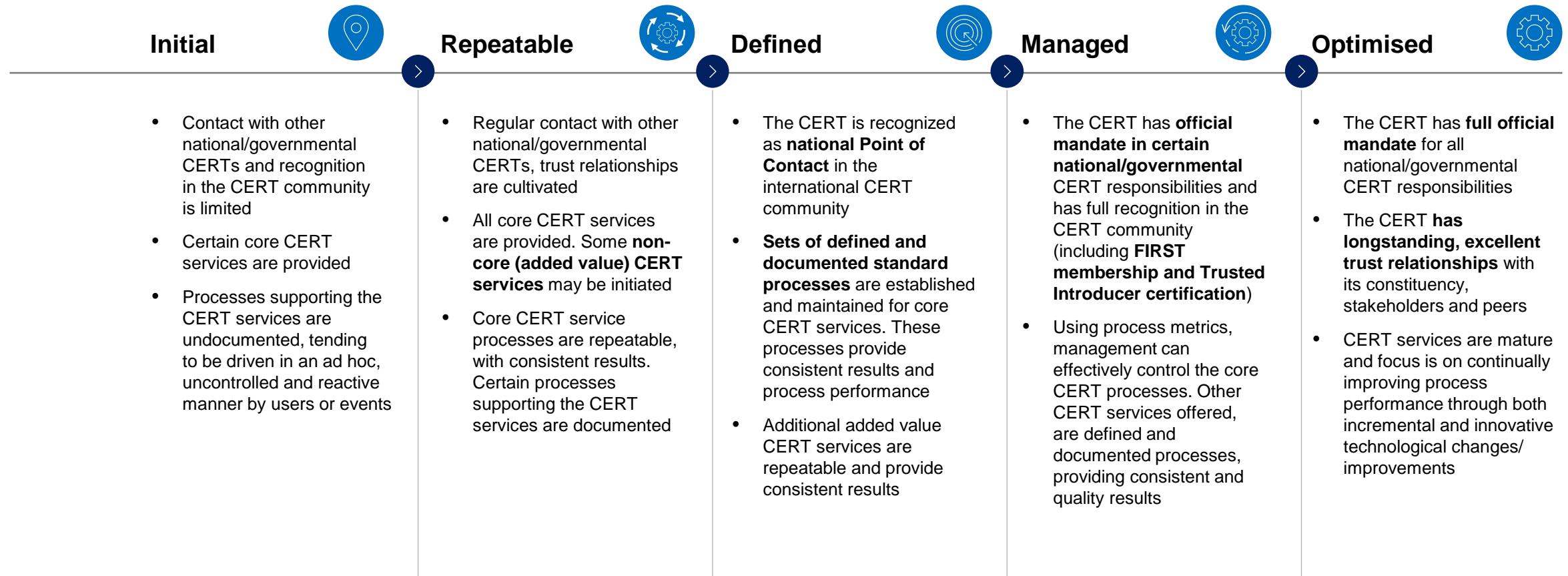


# JICA could consider to strengthen national CERT based on ENISA CERT capability maturity model

対外厳秘



## ENISA CERT capability maturity model *enisa*



資料: ENISA- Baseline Capabilities of National / Governmental CERTs

機密・専有情報: 個別の明示的な承諾を得ることなく、この資料を使用することを固く禁じます。

---

# Questions?

---

