SECURITY BY DESIGN

National Cybersecurity & Infrastructure Protection for Thailand: Telecommunication Industry Focus

Edwin Lim
Director, Professional Services
Singapore Telecommunications Limited

10th August 2018

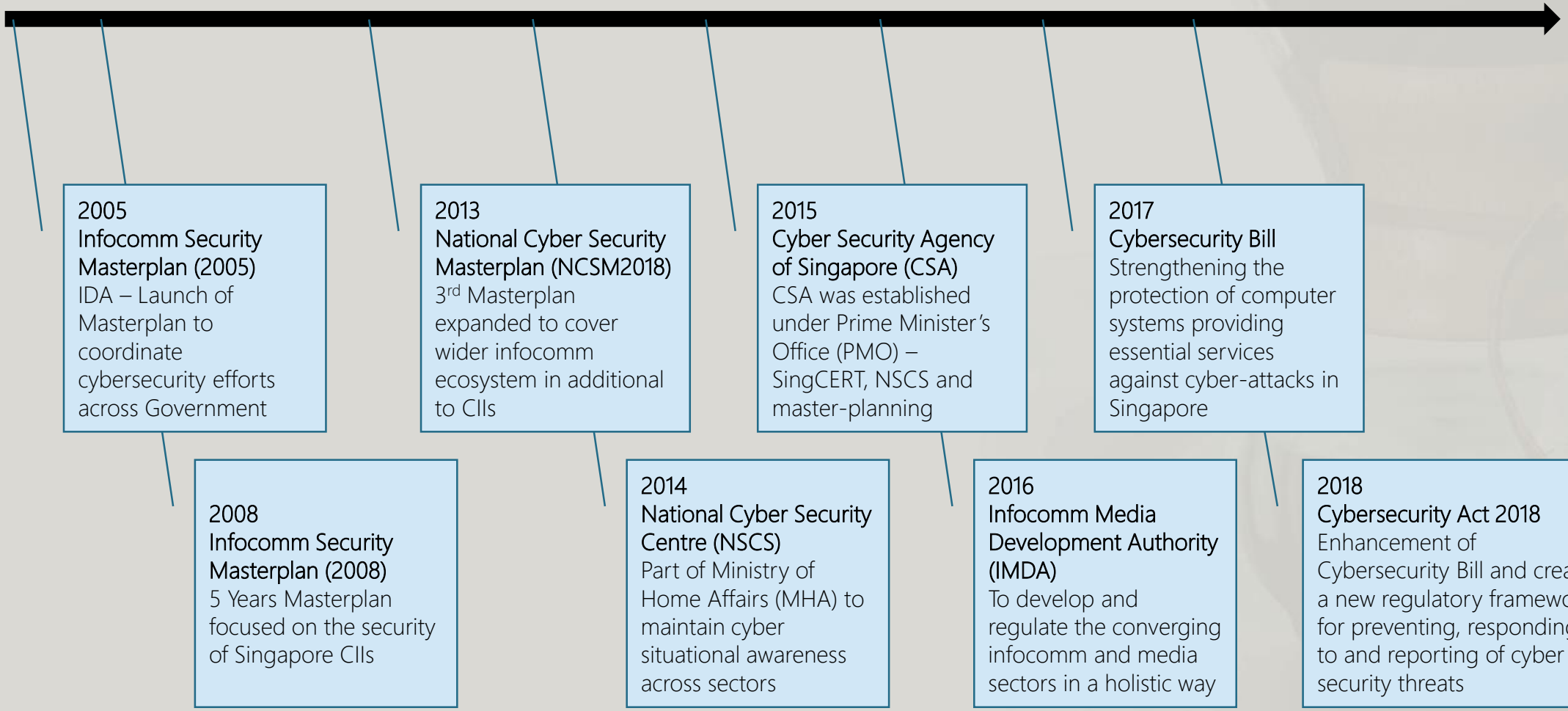
Agenda

- Sharing of Singapore Landscape
- Framework and Methodology
- Best Practices of Telecom CERT

Sharing of Singapore Landscape

Sharing of Singapore Landscape

"Cybersecurity Journey for Singapore Government"



Sharing of Singapore Landscape

SINGAPORE'S CYBERSECURITY STRATEGY AT A GLANCE

Singapore's Cybersecurity Strategy aims to create a resilient and trusted cyber environment. This will enable us to realise the benefits of technology and so secure a better future for Singaporeans.

Four pillars underpin our strategy. We will **strengthen the resilience of Critical Information Infrastructures** (CIIs). We will mobilise businesses and the community to **make cyberspace safer**, by countering cyber threats, combating cybercrime and protecting personal data.

We will **develop a vibrant cybersecurity ecosystem** comprising a skilled workforce, technologically-advanced companies and strong research collaborations, so that it can support Singapore's cybersecurity needs and be a source of new economic growth. Finally, given that cyber threats do not respect sovereign boundaries, we will step up efforts to **forge strong international partnerships**.

> "Cybersecurity is a team effort, everyone has a part to play, and everyone has to play their part. The Government will take the lead to spearhead initiatives to enhance Singapore's cybersecurity stance, and we will need everyone's cooperation to reap long term benefits for the cyber ecosystem. We aim to build a Smart Nation – one that will be enabled by trustworthy infrastructure and technology."
>
> **Minister-in-charge of Cybersecurity, Dr Yaacob Ibrahim,**
> GovernmentWare 2015

Building a Resilient Infrastructure

OUR STRATEGY:

To secure our digitally-enabled economy and society, the Government will work with key stakeholders – private sector operators and the cybersecurity community – to strengthen the resilience of our CIIs.

First, we will enhance our CII Protection Programme to establish robust and systematic cyber risk management processes across all critical sectors. Second, we will improve our sectors' response and recovery plans to breaches. We will mount multi-sector cybersecurity exercises to test cooperation across multiple sectors and address inter-dependencies during major cyber-attacks. We will also expand and beef up national resources such as the National Cyber Incident Response Team (NCIRT) and the National Cyber Security Centre (NCSC). Next, we will introduce the Cybersecurity Act to give the Cyber Security Agency of Singapore (CSA) greater powers to secure our CIIs. Finally, as threats to government networks will continue to grow, we will expand efforts to secure government systems and networks, so as to protect citizens' and official data.

Creating a Safer Cyberspace

OUR STRATEGY:

Cyber technology can enable and empower business and society, but only if it is safe and trustworthy. A safer cyberspace is the collective responsibility of the Government, businesses, individuals and the community.

First, to effectively deal with the threat of cybercrime, the Government will implement the recently launched National Cybercrime Action Plan. Second, we will enhance Singapore's standing as a trusted hub by fostering a trusted data ecosystem. We will work with global institutions, other governments, industry partners and Internet Service Providers to quickly identify and reduce malicious traffic on our Internet infrastructure. Finally, communities and business associations can play their part by fostering their members' understanding of cybersecurity issues and promoting the adoption of good practices.

Developing a Vibrant Cybersecurity Ecosystem

OUR STRATEGY:

Cybersecurity is both an imperative and an opportunity. With advanced infrastructure and a highly-skilled IT workforce, Singapore is well-positioned to build a vibrant cybersecurity ecosystem.

First, the Government will collaborate with industry partners and Institutes of Higher Learning (IHLs) to grow the cybersecurity workforce, including encouraging existing cybersecurity professionals to deepen their skills. Second, we will develop strong companies and nurture local start-ups to ensure that best-in-class solutions are available locally. There are also opportunities for cybersecurity companies to leverage Singapore's traditional strengths in areas such as financial and infocomm services to develop exportable solutions. Third, we will foster closer partnerships between academia and industry so as to harness cybersecurity R&D in a more targeted manner to deliver effective solutions. With skilled professionals, technologically-advanced companies and strong research collaborations, Singapore can be at the global forefront of cybersecurity innovation and create economic opportunities for Singaporeans and the industry.

Strengthening International Partnerships

OUR STRATEGY:

Cybersecurity is a global issue. Cyber threats do not respect sovereign boundaries; indeed, jurisdictional gaps are exploited to the cyber-attacker's advantage. Cyber-attacks disrupting one country can have serious spill-over effects on other countries as our inter-dependencies have increased through trade and global financial markets.

Singapore is committed to strong international collaboration in cybersecurity for our collective global security. Singapore will actively cooperate with the international community, particularly ASEAN, to address transnational cybersecurity and cybercrime issues. We will champion cyber capacity building initiatives, and facilitate exchanges on cyber norms and legislation. Through international consensus, agreement, and cooperation, we can make cyberspace a safer and more secure place for all.

Singtel

Sharing of Singapore Landscape

"Some of the National CERT / CIRT in Singapore"

SingCERT – Singapore Computer Emergency Response Team

Cyber Security Agency (CSA) Singapore

Responds to cyber security incidents for its Singapore constituent. It was set up to facilitate the detection, resolution and prevention of cyber security related incidents on the Internet

ISG-CERT – Infocommunications Singapore Computer Emergency Response Team

Infocomm Media Development Authority (IMDA) Singapore

Established in 1st April 2015 to provide IMDA with the capability to respond effectively to cyber threats within the Telecommunication and Media sector in Singapore.

NCIRT – National Cyber Incident Response Teams

Drawn from CSA, Government Technology Agency, Ministry of Home Affairs and Ministry of Defence

Part of Tier 1 & 2 under the national cyber response plan to deal with more complex and challenging attack scenarios

Singtel

Sharing of Singapore Landscape
"ISG-CERT for Telecommunication Sector"

ISG-CERT – Infocommunications Singapore Computer Emergency Response Team
Infocomm Media Development Authority (IMDA) Singapore

The ISG-CERT supports IMDA in overseeing and enhancing the cyber-security posture and preparedness of the Telecommunication and Media Sector. Internationally, as a full and active member of the Forum of Incident Response and Security Teams (FIRST), ISG-CERT cooperates and coordinates with regional and global trusted CERTs in responding to computer security incidents relating to the Telecommunication and Media Sector.

ISG-CERT provides the following to the constituents of the local Telecommunication and Media sector:

- Sharing of information through the issuance of actionable intelligence and advisories/alerts
- Promoting security awareness and enhance technical knowledge by conducting security courses, seminars and workshops
- Performing incident management, computer forensic analysis and malware analysis
- Coordinating with other CERTs and organisations to resolve security incidents

Sharing of Singapore Landscape
"Singapore Cybersecurity Act 2018"

Under this Bill, organisations with Critical Information Infrastructure ("CII") are now under scrutiny by the Commissioner of the Cyber Security Agency of Singapore ("CSA") with 11 sectors identified as likely to be under CSA remit: Energy, Water, Banking and Finance, Healthcare, Transport (which includes Land, Maritime, and Aviation), ***Infocommunications,*** Media, Security and Emergency Services, and Government organisations.

The Bill requires owners of the CII to comply with;

(1) codes of practice and performance standards,
(2) conduct cybersecurity audits and risk assessments, and
(3) participate in cybersecurity exercises. Non-compliance could see offenders hit with a maximum penalty of SGP $100,000, two years in jail or in the worst case both outcomes.

Apart from the above, CII owners will also be duty bound to inform the Commissioner of cybersecurity incidents that: occurs in respect of the CII;

- occurs in respect of any computer or computer system under the owner's control that is interconnected with or communicates with the CII; and
- are prescribed by notification or as specified by the Commissioner.
- Failure to do so may lead to mandatory investigations and remedial actions enforced upon the non-compliant organisation.

Singtel

Framework and Methodology

"Singapore Telecommunication Cybersecurity Code of Practice"

Telecommunication Cybersecurity Code of Practice

Infocomm Media Development Authority (IMDA) Singapore

The IMDA has formulated Codes of Practice to enhance the cyber security preparedness for designated licensees. The Codes are currently imposed on major Internet Service Providers ("ISP") in Singapore for mandatory compliance, and the coverage includes their network infrastructure providing Internet services. Besides security incident management requirements, the *Codes include requirements to prevent, protect, detect and respond to cyber security threats*. The Code was formulated using international standards and best practices including the ***ISO / IEC 27011 and IETF Best Current Practices.***

Singtel

Framework and Methodology

Framework and Methodology
"ISO/IEC 27011:2016"

Information technology -- Security techniques -- Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations

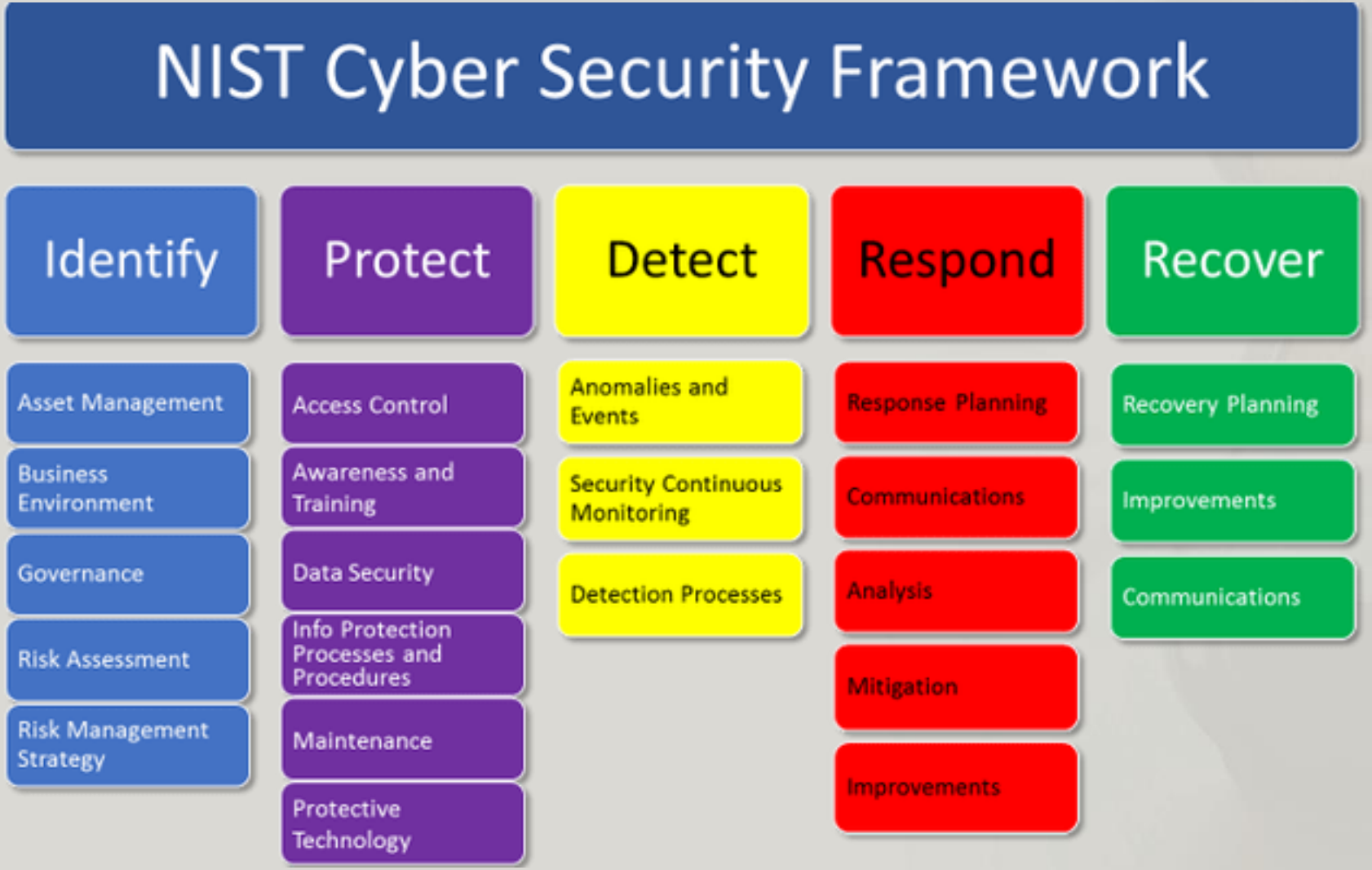
This ISMS implementation guide for the telecomms industry was developed jointly by ITU-T and ISO/IEC JTC1/SC 27, with the identical text being published as *both* ITU-T X.1051 *and* ISO/IEC 27011.

Establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security controls in telecommunications organizations based on ISO/IEC 27002; [and] Provides an implementation baseline of information security controls within telecommunications organizations to ensure the confidentiality, integrity and availability of telecommunications facilities, services and information handled, processed or stored by the facilities and services.

Human Resource Security	Asset Management	Access Control	Cryptography
Physical and Environment Security	Operations Security	Communications Security	System Acquisition, Development and Maintenance
Supplier Relationships	Information Security Incident Management	Information Security for Business Continuity Management	

Framework and Methodology

"NIST Cyber Security Framework"



US National Institute of Standards and Technology (NIST)

Singtel

Best Practices of Telecom CERT

Singtel

Best Practices of Telecom CERT

"Key Considerations"

- Stakeholders
- Regulatory / Legislation
- Scope of CERT
- Human Resources / Skill-sets / Trainings
- Services / Responsibilities
- Infrastructure and Technology
- Operational Policies and Procedures

Singtel

Best Practices of Telecom CERT

"StakeHolders"

Singtel

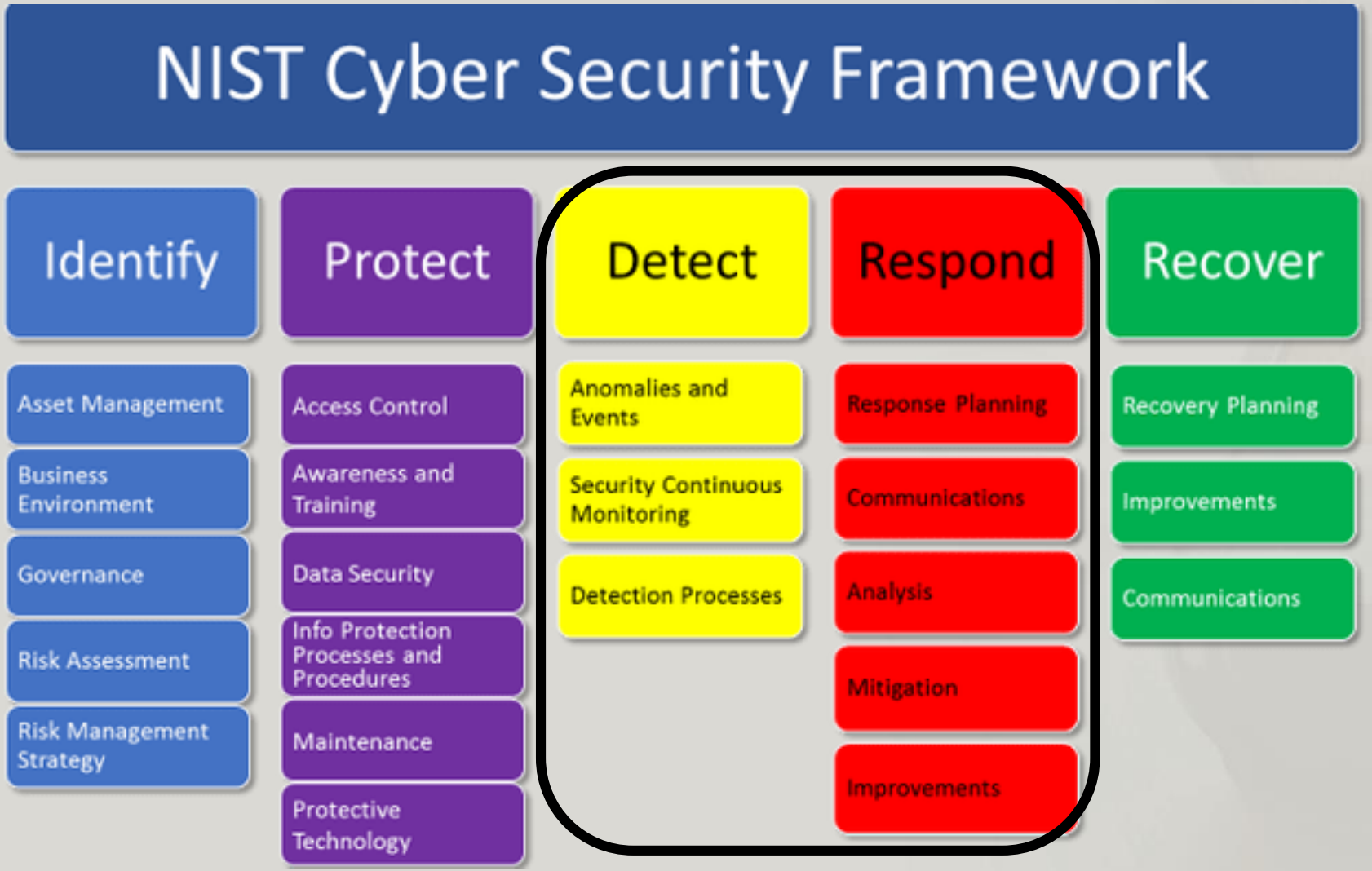
Best Practices of Telecom CERT

"Regulatory / Legislation"

- *Computer Crime Act B.E. 2550 (2007)*
- *Cybersecurity Bill*
- *Data Protection and Cyber Security Law*
- *Ministry of Digital Economy and Society (MDES)*
- *National Cybersecurity Committee (NCSC)*
- *Etc.*

Best Practices of Telecom CERT

"Scope of CERT"



Best Practices of Telecom CERT

"Human Resources / Skill-sets / Trainings"

Core Functions

- Incident Response Manager
- Security Analyst
- Threat Researchers

Support Functions

- Management
- Human Resources
- Auditors
- Legal Counsel
- Public Relations

Singtel

Best Practices of Telecom CERT

"Services / Responsibilities"

Reactive Services

- Alerts and Warnings
- Incident Handling
  - Incident Analysis
  - Incident Response On Site
  - Incident Response Support
  - Incident Response Coordination
- Vulnerability Handling
  - Vulnerability Analysis
  - Vulnerability Response
  - Vulnerability Response Coordination
- Artifact Handling
  - Artifact Analysis
  - Artifact Response
  - Artifact Response Coordination

Proactive Services

- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications & Infrastructure
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Security Quality Management

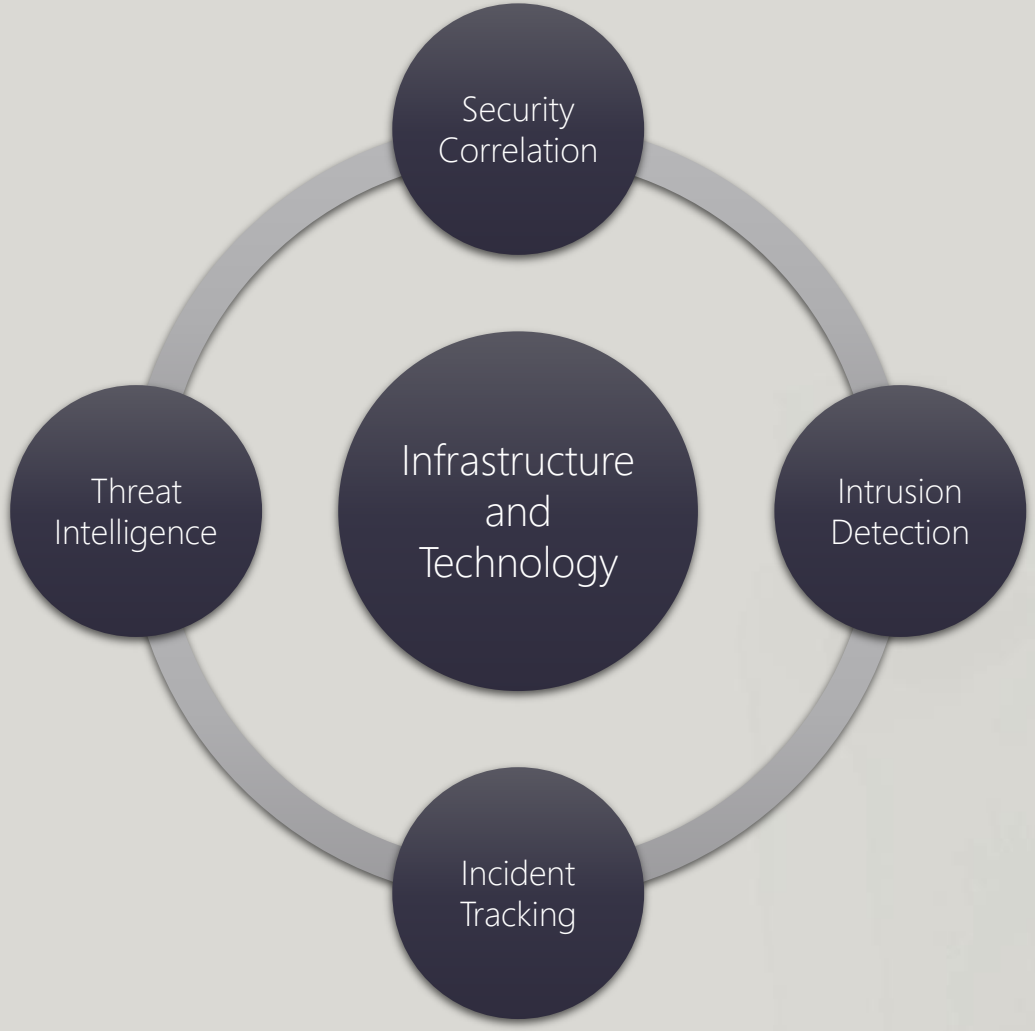
- Risk Analysis
- Business Continuity & Disaster Recovery Planning
- Security Consulting
- Awareness Building
- Education / Training
- Product Evaluation or Certification

Singtel

Best Practices of Telecom CERT

"Infrastructure and Technology"

Forensic Capabilities



Security Operations Center

Singtel

Best Practices of Telecom CERT

"Operational Policies and Procedures"

Examples of Policies

- *Security policy*
- *Open reporting environment policy*
- *Incident reporting policy*
- *Incident handling policy*
- *External communications policy*
- *Media relations policy*
- *Information disclosure policy*
- *Information distribution policy*
- *Human error policy*
- *Training and education policy*

Singtel

Best Practices of Telecom CERT

"Operational Policies and Procedures"

Examples of Procedures

- *Standard operating procedures (SOPs)*
- *Accepting and tracking incident reports*
- *Answering the hotline*
- *Incident and vulnerability handling*
- *Gathering, securing, and preserving evidence*
- *System and network monitoring and intrusion detection*
- *Backing up and storing incident data*
- *Notification processes (how information is packaged, distributed, archived, etc.)*
- *Training and mentoring*

Singtel

Best Practices of Telecom CERT

"Ecosystem / Partnership"

CERT Collaboration	• Partnership with other CERTs to deal with Incidents or sharing of information • Eg. ThaiCERT, SingCERT, FIRST, etc.
Regulator / Authority	• Legislative, Law Enforcement, Regulatory requirements • Eg. MDES, NBTC, CSA, etc.
Cybersecurity / Threat Intel Providers	• Threat Intelligence, Cybersecurity Practices, Incident Response • Eg. MSSPs, Threat Intelligence Feeds Providers, Cybersecurity Technology vendors, etc.

Singtel

References

- *Singapore's Cybersecurity Strategy – Cyber Security Agency Singapore (2016)*
- *The Singapore Cybersecurity Act 2018*
- *Infocomm Media Development Authority – Https://www.imda.gov.sg*
- *US National Institute of Standards and Technology – NIST Cybersecurity Framework*
- *Best Practices for Establishing a National CERT – The Organization of American States (OAS)*
- *AfNOG – Https://www.afnog.org*

Thank You

Edwin Lim
Director, Professional Services
APJ Consulting Services

Singapore Telecommunications Limited

Edwin.lim@singtel.com
+65 9662 4300