



MAS' cyber security strategy for the financial sector

Tommy Tan
Director
Technology Risk Supervision Division

Cyber threats are...



... evolving,



persistent,



borderless,



disruptive

2013 – 2014



- ❑ US\$40M global ATM heist
- ❑ “Heartbleed” vulnerability on OpenSSL
- ❑ DD4BC emerges

2015 – 2016



- ❑ Armada Collective
- ❑ Dyre malware
- ❑ IoT Mirai Botnet (DYN DDoS attack, 1.2 Tbps)
- ❑ Hong Kong “pump & dump” trades

2017 – 2018



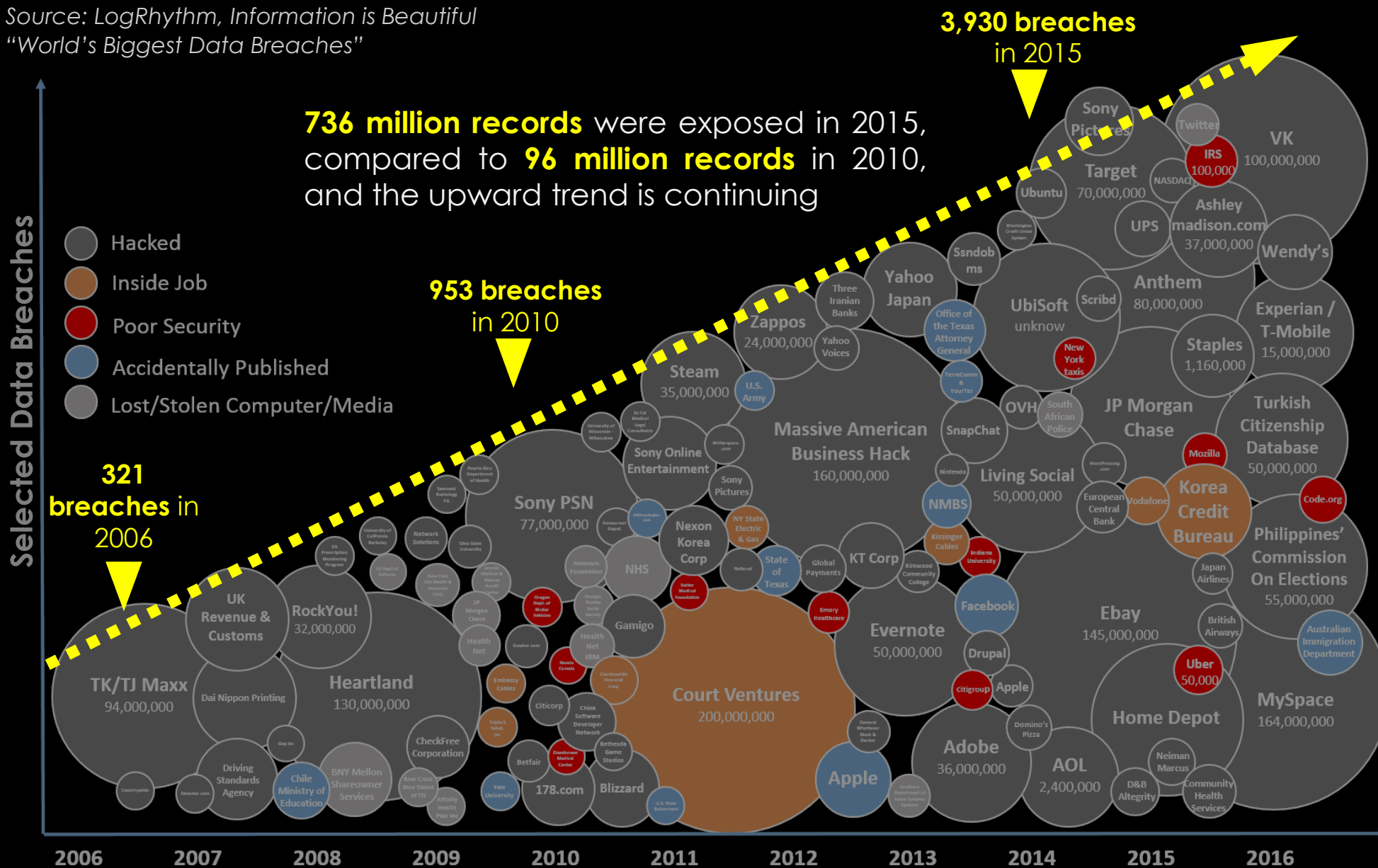
- ❑ Wannacry, NotPetya
- ❑ Brazilian bank DNS attack
- ❑ “Meltdown” & “Spectre” vulnerabilities in computer processors

“Robbing one person at a time using a knife or gun doesn’t scale well. But now one person can rob millions at the click of a button”

Marc Goodman of the Future Crimes Institute

Painting the cyber threat landscape...

Source: LogRhythm, Information is Beautiful
"World's Biggest Data Breaches"



A smart financial centre...



... has to be a
safe financial centre

... needs to address and
manage the risks from
persistent cyber threats



MAS adopts a 4-pronged cyber security strategy for the financial sector...



Regulation and guidance

Provide **guidance** to the financial sector in managing cyber risk



Supervision

Perform **supervision** to assess the quality of cyber risk management in FIs



Surveillance and information sharing

Maintain situational awareness through **surveillance, research, and info sharing**



Competency and capability development

Build **competencies** and **capabilities**, and **collaborate with industry** to uplift cyber resilience

... developed and refined based on inputs from the
MAS Cyber Security Advisory Panel (CSAP)

MAS adopts a 4-pronged cyber security strategy for the financial sector...



Ms. Valerie Abend
MD
Financial Services
Accenture Security



Mr. Keith Alexander
CEO
IronNet
Cybersecurity



Mr. Rohan Amin
MD & Group CISO
JPMorgan Chase & Co



Mr. Adrian Asher
Group CISO
London Stock
Exchange Group



Mr. Mikko Hypponen
Chief Research Officer
F-Secure



Mr. David Koh
Chief Executive
Cyber Security
Agency of Singapore



Mr. Vincent Loy
MD & Financial
Services Leader
Singapore Accenture



Mr. Kevin Mandia
CEO & Board Director
FireEye Inc



Ms. Cheri McGuire
Group CISO
Standard Chartered
Bank



Mr. Udi Mokady
CEO
CyberArk



Mr. Bruce Schneier
CTO
IBM Resilient

MAS Cyber Security Advisory Panel (CSAP)

MAS' cyber security strategy for the financial sector



Regulation and guidance

Provide **guidance** to the financial sector in managing cyber risk



Supervision

Perform **supervision** to assess the quality of cyber risk management in FIs



Surveillance and information sharing

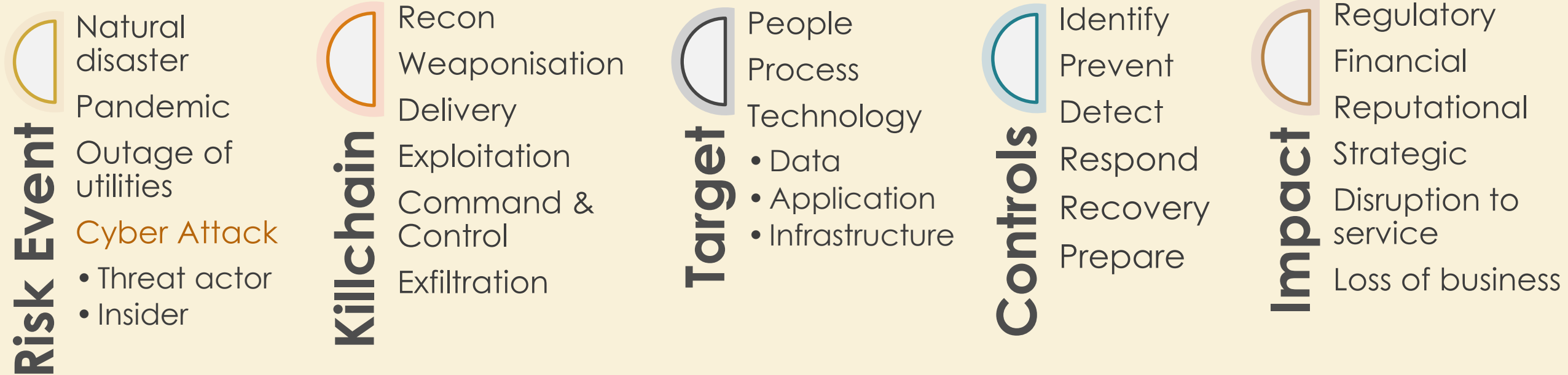
Maintain situational awareness through **surveillance, research, and info sharing**



Competency and capability development

Build **competencies and capabilities**, and **collaborate with industry** to uplift cyber resilience

Cyber risk management in a nutshell



Confidentiality, Integrity, Availability

MAS guides FIs using rules and guidelines

Rules...



Notice

Requirements that allow FIs to implement controls that are proportionate to risk and impact

... set out key objectives



Identify critical systems



Notify MAS of security incidents and outages of critical systems



Reduce unscheduled downtime



Enable rapid recovery



Protect customer information from unauthorised access or disclosure

Guidance...



Guidelines

Supervisory expectations applicable to all FIs in Singapore



Circulars / Advisories

Ad-hoc circulars and advisories

... set out supervisory expectations on good technology risk management (TRM) practices



IT management oversight



Operational controls on prevention, detection, response & recovery



IT audit

☐ Vulnerability assessment (VA) and penetration testing (PT)

☐ IT security risks posed by personal mobile devices

☐ Early detection of cyber intrusions

☐ Technology risk and cyber security training for board

Updating our rules...

... by issuing a new **Notice on Cyber Hygiene Practices**



To ensure all financial institutions put in place an effective set of cyber security controls to protect themselves against cyber attacks

And more updates..

... by reviewing the **TRM Guidelines**

to provide more specific cyber guidance and to include guidance on new technologies and emerging risks

Shaping international cyber security standards...



MAS' cyber security strategy for the financial sector



Regulation and guidance

Provide **guidance** to the financial sector in managing cyber risk



Supervision

Perform **supervision** to assess the quality of cyber risk management in FIs



Surveillance and information sharing

Maintain situational awareness through **surveillance, research, and info sharing**



Competency and capability development

Build **competencies and capabilities**, and **collaborate with industry** to uplift cyber resilience

Supervised Entities



Insurers



Capital Markets
Infrastructures



Banks



Capital Markets
Intermediaries

1,200+
FIs in
Singapore

Need for
Risk-Focused
Supervision



Stored Value Facilities



Money Changers &
Remittances



Credit Bureaus

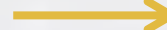
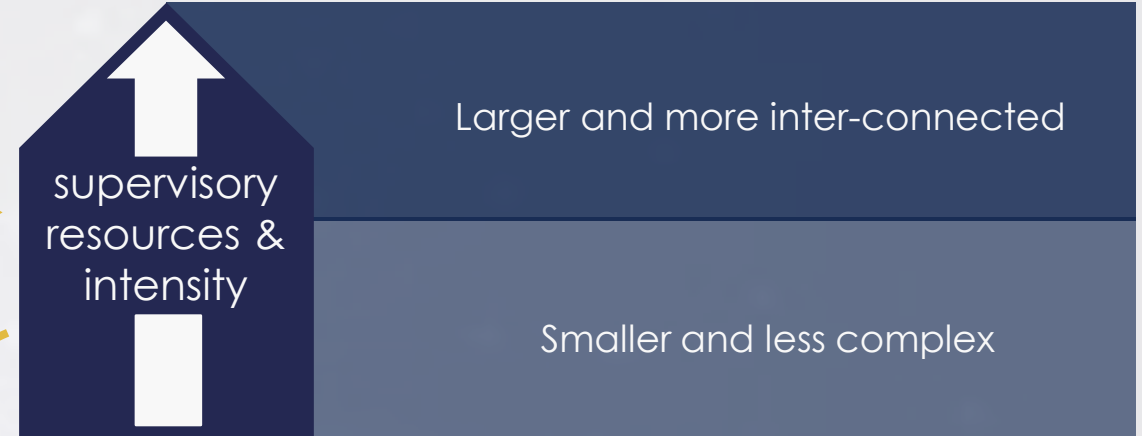


Other Financial Institutions

MAS' IT supervision approach...

... is risk focused

1,200+
Financial
Institutions



... and involves striking a balance

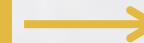
15
IT Supervision
Staff



On-site
Inspections



Off-site
Reviews



~5%
of all Financial
Institutions

On-site Inspections

- ❑ Focused on key FIs
- ❑ Scope can include review of IT operations, or thematic review on specific type of systems (e.g. wholesale payment systems, securities trading platforms, etc.)



Determine
FIs' cyber
security
posture



Adherence to
MAS
regulations
and guidelines



Develop
remedial
plan

Off-site Reviews

- ❑ Leverage Quantitative Risk Assessment Methodology (QRAM) to perform automated review based on scoring template

MAS' cyber security strategy for the financial sector



Regulation and guidance

Provide **guidance** to the financial sector in managing cyber risk



Supervision

Perform **supervision** to assess the quality of cyber risk management in FIs



Surveillance and information sharing

Maintain situational awareness through **surveillance, research, and info sharing**



Competency and capability development

Build **competencies and capabilities**, and **collaborate with industry** to uplift cyber resilience

Cyber surveillance and info-sharing are important in developing cyber situational awareness



Driving cross-border collaboration and cyber threat information-sharing



Model

- Bilateral, Multilateral



Parties

- FI2FI, FI2R, R2FI, R2R
FI denotes financial institution, R denotes regulator)



Principles

- Voluntary, Timeliness, Effectiveness, Confidentiality



Scope

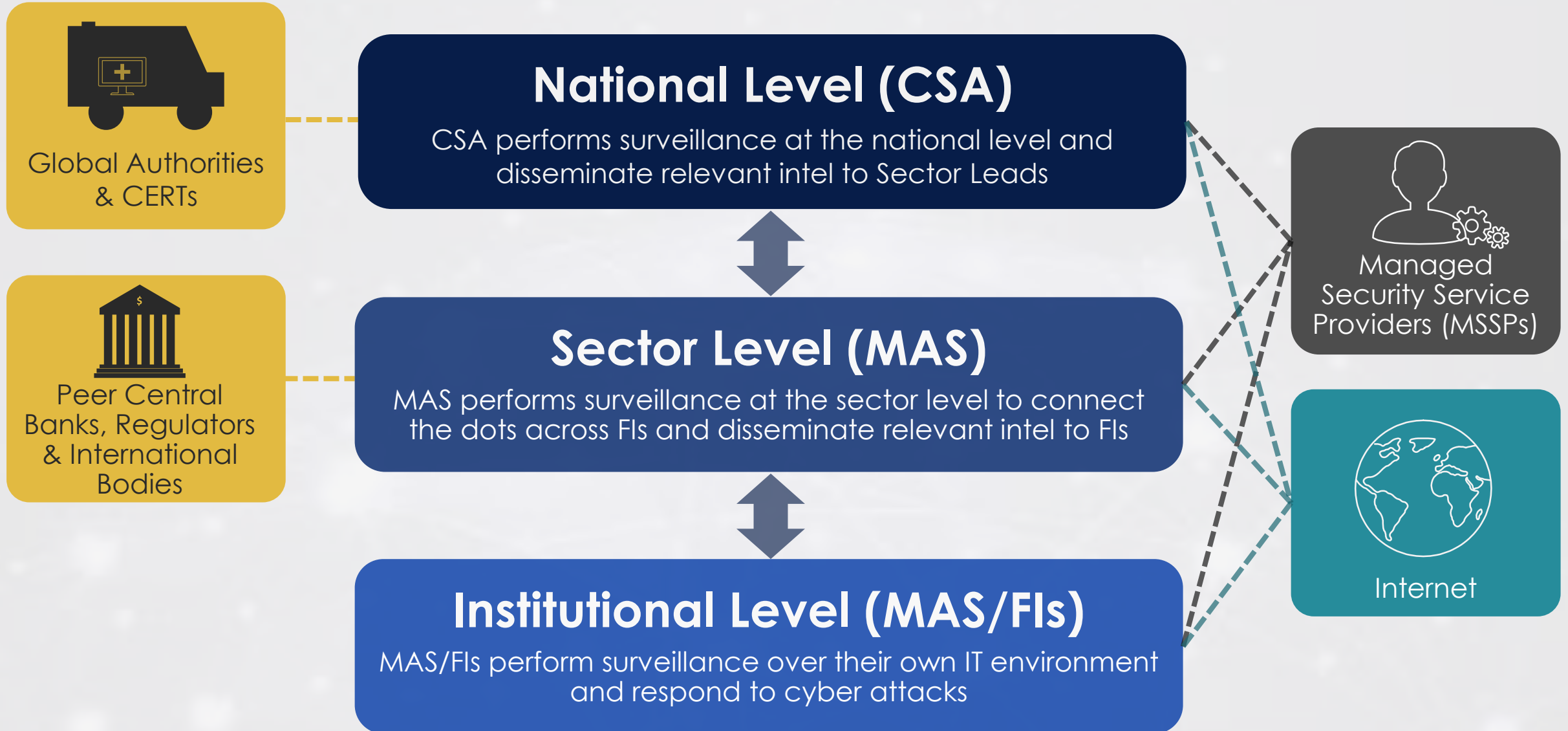
- Incident, information



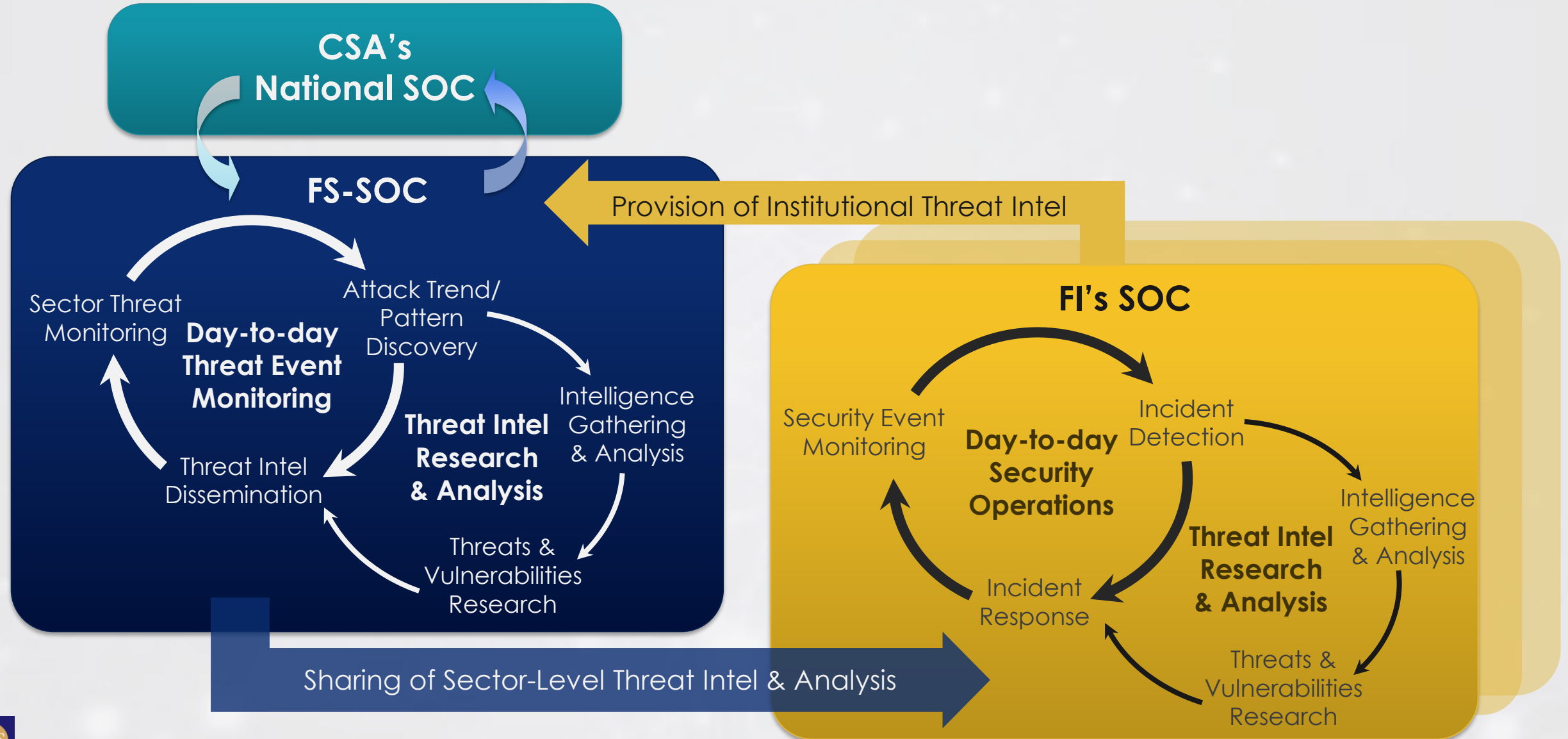
Procedure

- TLP, taxonomy, mode, frequency

MAS is sector lead in a tiered surveillance framework



MAS' FS-SOC works closely with FIs' SOC and CSA's National SOC to maintain cyber situational awareness



MAS' cyber security strategy for the financial sector



Regulation and guidance

Provide **guidance** to the financial sector in managing cyber risk



Supervision

Perform **supervision** to assess the quality of cyber risk management in FIs



Surveillance and information sharing

Maintain situational awareness through **surveillance, research, and info sharing**



Competency and capability development

Build **competencies** and **capabilities**, and **collaborate with industry** to uplift cyber resilience

MAS' efforts to bolster cyber security competencies and capabilities in the financial sector...

... include uplifting cyber security skillsets in the financial sector



Memorandum of Understanding
with Local Polytechnics



Technology Skills Accelerator (TeSA)
FinTech Collective



Financial Sector Technology &
Innovation (FSTI) Scheme



Singapore FinTech Festival's
Technology Risk Conference

MAS partnered with the industry to improve cyber security capabilities

2013



July 2013

- ❑ Standing Committee on Cyber Security ("SCCS") founded under ABS' guidance



2014

March 2014

- ❑ Study Trip to US

August 2014

- ❑ Provided cyber security guidance to Operation Raffles IV (IWE2014)

September 2014

- ❑ Inaugural Financial Sector – Information Security ("FS-IS") Forum launched
- ❑ Developed ABS-FITA Cyber Security Master Class program for SMU

October 2014

- ❑ 2nd ABS Technology Risk Seminar
- ❑ Developed Cyber Incident Management Framework (CIMF)



2015

February 2015

- ❑ 2nd FS-IS Forum
- ❑ Post-IWE2014 Improvement Work Streams Initiated

May 2015

- ❑ Published ABS Penetration Testing Guidelines
- ❑ Developed Focus Group on Talent Development of Infocomm Security Professionals

August 2015

- ❑ 3rd FS-IS Forum

September 2015

- ❑ Cloud Computing Taskforce formed

November 2015

- ❑ 3rd ABS Technology Risk Seminar

December 2015

- ❑ Drafted Cloud Computing WhitePaper



2016

March 2016

- ❑ Established working group in emerging technologies, methodologies and IOT

April 2016

- ❑ Study Trip to Israel
- ❑ Published ABS Cloud Computing Guidelines

July 2016

- ❑ Industry Briefing on ABS Cloud Computing Implementation Guide

November 2016

- ❑ 3rd ABS Technology Risk Conference (part of MAS Fintech Festival)
- ❑ Conducted cyber crisis table-top exercise (#OPSABSCISE) for SCCS member FIs



2017

March 2017

- ❑ #OPSABSCISE Post Mortem report published

April 2017

- ❑ Social Engineering Testing Working Group Formed

July 2017

- ❑ Provided joint consultation feedback to Singapore draft Cybersecurity Bill
- ❑ 4th FS-IS Forum

August 2017

- ❑ Participated in ABS Exercise Raffles V
- ❑ TRM Guidelines Review Working Group formed
- ❑ Conducted industry-wide social engineering assessment (SEEP-X)

MAS partnered with the industry to improve cyber security capabilities

2013



July 2013

- ❑ Standing Committee on Cyber Security ("SCCS") founded under ABS' guidance



2014

March 2014

- ❑ Study Trip to US

Operation Raffles IV (IWE2014)

September 2014

- ❑ Inaugural Financial Sector – Information Security ("FS-IS") Forum launched
- ❑ Developed ABS-FITA Cyber Security Master Class program for SMU

October 2014

- ❑ 2nd ABS Technology Risk Seminar
- ❑ Developed Cyber Incident Management Framework (CIMF)



2015

May 2015

- ❑ ABS Penetration Testing Guidelines

Guidelines

- ❑ Developed Focus Group on Talent Development of Infocomm Security Professionals

August 2015

- ❑ 3rd FS-IS Forum

September 2015

- ❑ Cloud Computing Taskforce formed

November 2015

- ❑ 3rd ABS Technology Risk Seminar

December 2015

- ❑ Drafted Cloud Computing WhitePaper



2016

July 2016

- ❑ ABS Cloud Computing Implementation Guide

July 2016

- ❑ Industry Briefing on ABS Cloud Computing Implementation Guide

November 2016

- ❑ 3rd ABS Technology Risk Conference (part of MAS Fintech Festival)
- ❑ Conducted cyber crisis table-top exercise (#OPSABSCISE) for SCCS member FIs



2017

August 2017

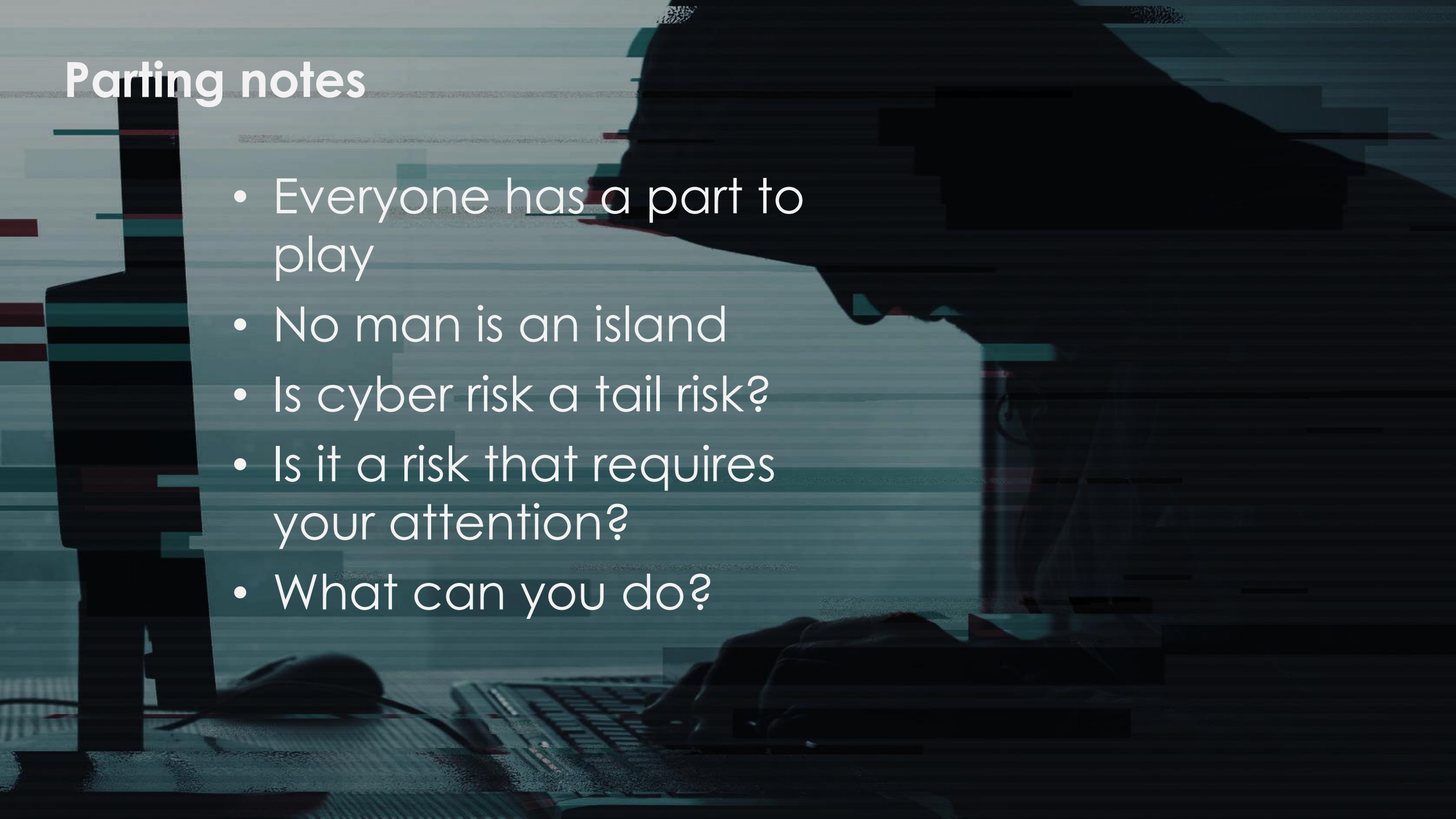
- ❑ Exercise Raffles V
- ❑ Industry-wide Social Engineering Exercise

4th FS-IS Forum

August 2017

- ❑ Participated in ABS Exercise Raffles V
- ❑ TRM Guidelines Review Working Group formed
- ❑ Conducted industry-wide social engineering assessment (SEEP-X)

Parting notes

A dark, moody photograph of a person sitting at a desk, their hands on a keyboard. The scene is dimly lit, with light coming from a screen or window, creating a silhouette effect. The person's head is bowed, and their hands are positioned over the keyboard. A mouse is visible on the desk to the left of the keyboard. The overall atmosphere is quiet and focused.

- Everyone has a part to play
- No man is an island
- Is cyber risk a tail risk?
- Is it a risk that requires your attention?
- What can you do?

Thank you!