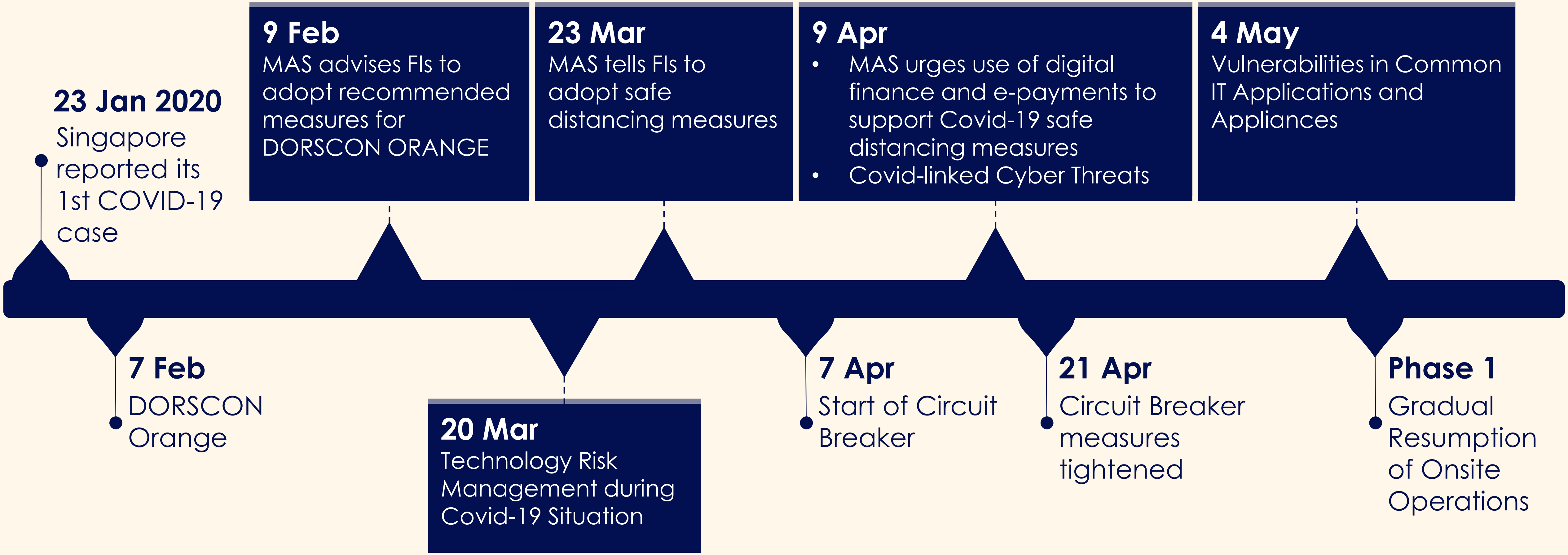
MAS Monetary Authority of Singapore

# Cybersecurity Risk Supervision during COVID-19

Tan Yeow Seng
Executive Director (Technology and Cyber Risk Department) &
Chief Cyber Security Officer
Monetary Authority of Singapore

# COVID-19 Pandemic Timeline – Singapore

## MAS’ Guidance to the Industry in response to the COVID-19 Pandemic



**23 Jan 2020**
Singapore reported its 1st COVID-19 case

**7 Feb**
DORSCON Orange

**9 Feb**
MAS advises FIs to adopt recommended measures for DORSCON ORANGE

**20 Mar**
Technology Risk Management during Covid-19 Situation

**23 Mar**
MAS tells FIs to adopt safe distancing measures

**7 Apr**
Start of Circuit Breaker

**9 Apr**
- MAS urges use of digital finance and e-payments to support Covid-19 safe distancing measures
- Covid-linked Cyber Threats

**21 Apr**
Circuit Breaker measures tightened

**4 May**
Vulnerabilities in Common IT Applications and Appliances

**Phase 1**
Gradual Resumption of Onsite Operations

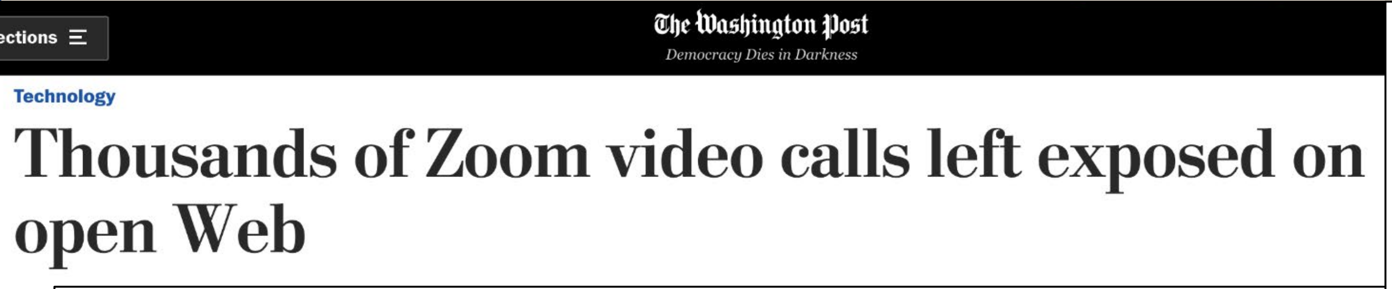
# Cyber Attacks Riding on COVID-19 Bandwagon

Cyber threats arising from **work from home** arrangement

Cyber threats targeting **FIs and customers**

Vulnerabilities in Remote Access and Collaboration Tools (e.g. VPN, Video-conferencing)

Social Engineering (e.g. Business Email Compromise, Phishing)



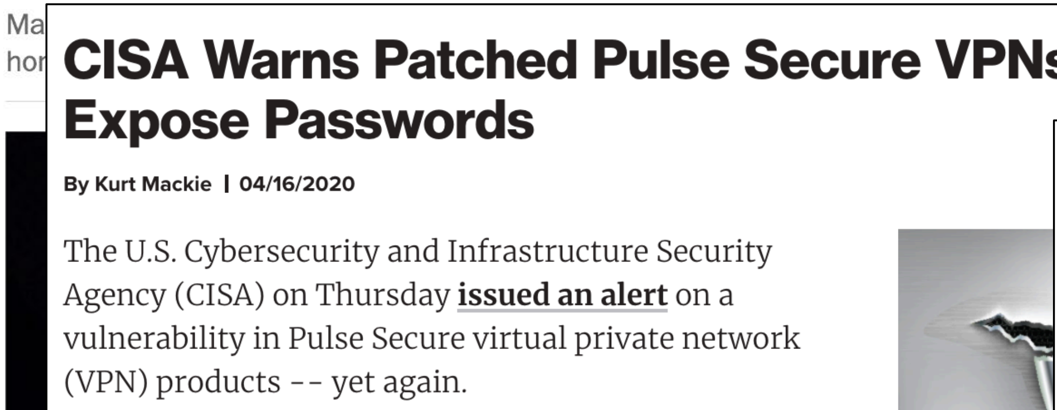
ections

The Washington Post
*Democracy Dies in Darkness*

Technology

# Thousands of Zoom video calls left exposed on open Web

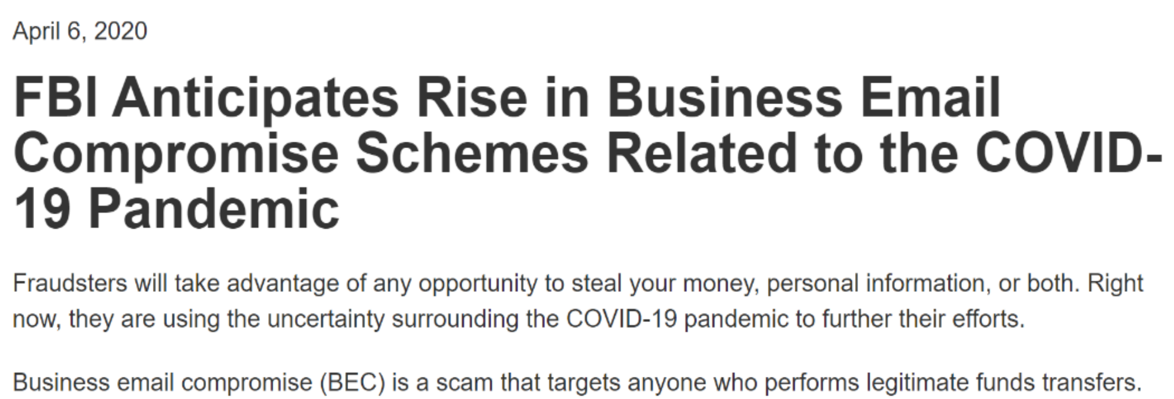
Ma
hor



## CISA Warns Patched Pulse Secure VPNs Could Still Expose Passwords

**By Kurt Mackie | 04/16/2020**

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Thursday **issued an alert** on a vulnerability in Pulse Secure virtual private network (VPN) products -- yet again.

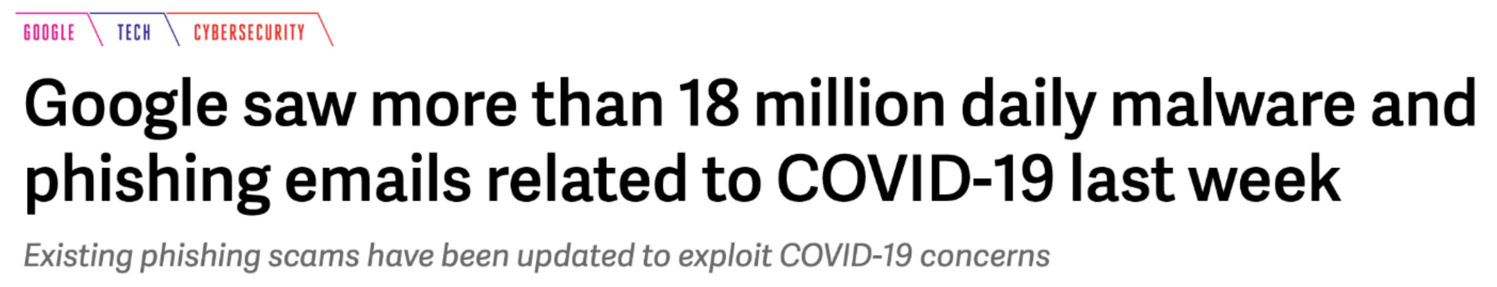


April 6, 2020

## FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic

Fraudsters will take advantage of any opportunity to steal your money, personal information, or both. Right now, they are using the uncertainty surrounding the COVID-19 pandemic to further their efforts.

Business email compromise (BEC) is a scam that targets anyone who performs legitimate funds transfers.

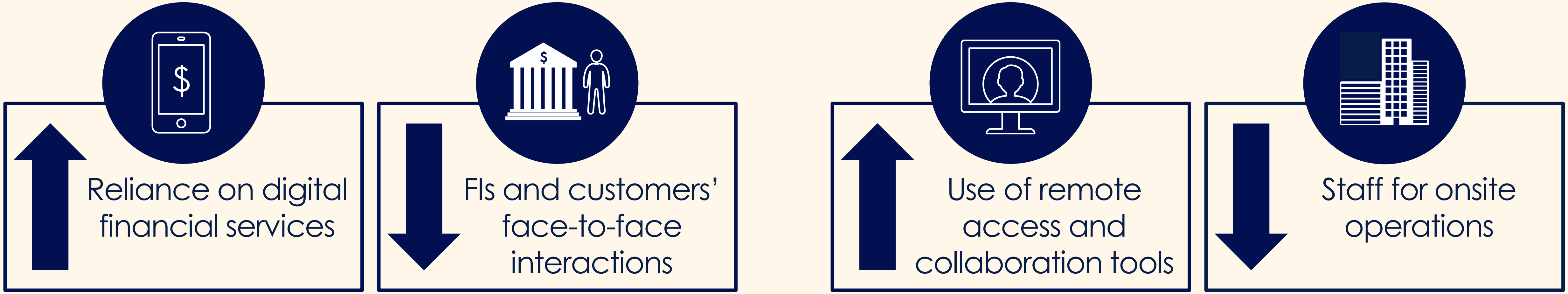


GOOGLE TECH CYBERSECURITY

## Google saw more than 18 million daily malware and phishing emails related to COVID-19 last week

*Existing phishing scams have been updated to exploit COVID-19 concerns*

# Key Shifts in FIs' Operating Environment



## Digitalisation of Financial Services

↑ Reliance on digital financial services

↓ FIs and customers' face-to-face interactions

## Work from home

↑ Use of remote access and collaboration tools

↓ Staff for onsite operations

**FIs need to ensure sustainability of new business operating model and acceleration of digitalisation**

↑

- ❖ **Reliance on Technology**
- ❖ **IT and Cyber Resilience**

# MAS’ Cybersecurity Strategy for Financial Sector

**OBJECTIVES**
Desired outcomes

- Continuous delivery of financial services
- Sustainability of IT operations
- Cyber Resilience

**STRATEGY**
Enhance operational, IT and cyber resilience

### Supervision

Continuous monitoring – cyber resilience

### Regulation and Guidance

Provide guidance to the financial sector on cyber risk management

### Surveillance & Info-sharing

Heightened cyber threat intelligence monitoring and surveillance, and information-sharing

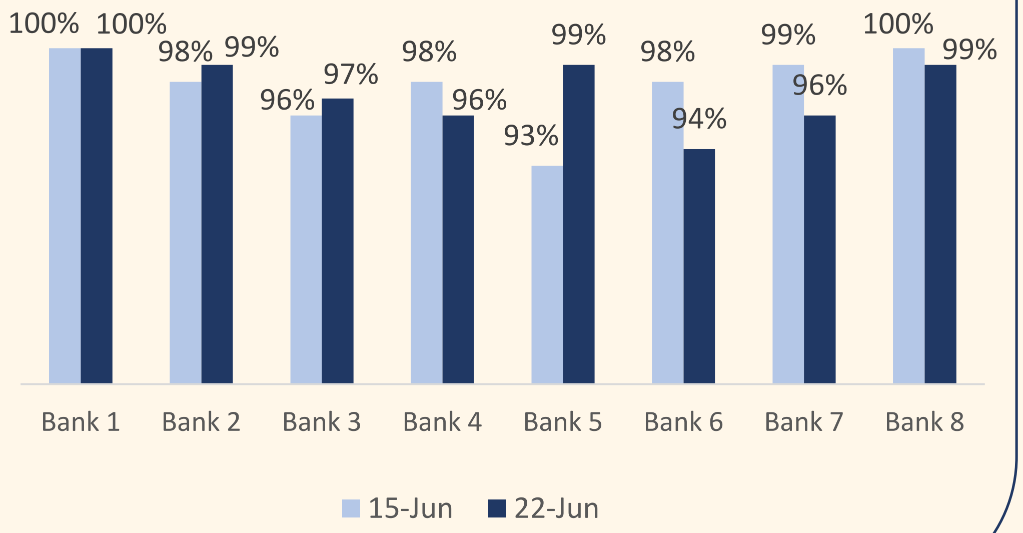
### Strategic Engagement

Strengthen collaboration with agencies, global regulators and industry

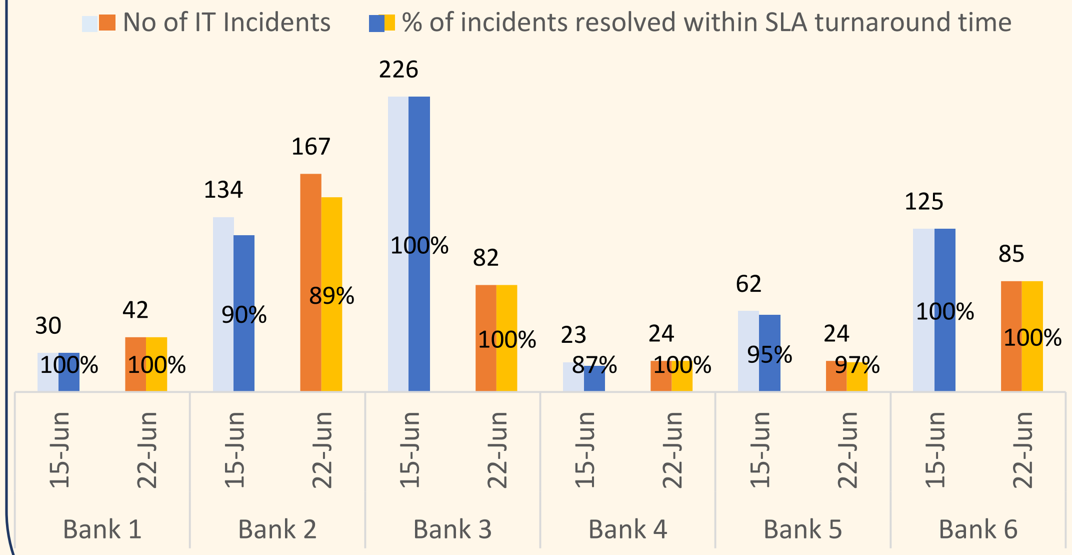
# Active Monitoring by MAS

**Focus supervision** on FIs with **systemic impact**

## Status of Security Patching and Anti-Malware Updates for Laptops/Desktops used for Telecommuting



## Number of IT Incidents and Incident Resolution



# MAS issued advisories to industry in response to COVID-19

### Technology Risk Management during COVID-19

- Implement sound internal controls during split operations and telecommuting
- Apply above measures to outsourced IT services
- Raise staff security and customer awareness of cyber threats

### COVID-linked Cyber Threats

- Remain vigilant to cyber threats
- Implement cybersecurity best practices to safeguard IT assets & sensitive data
- Conduct security assessments on remote working technologies

### Vulnerabilities in Common IT Applications and Appliances

- Implement measures to address risks from these applications & appliances

# MAS plays an active role to shape international cybersecurity standards for financial sector

## Financial Stability Board (FSB)

**Chair**
Cyber Incident Response & Recovery Working Group (CIRR)

**Member**
Cyber Lexicon Working Group (CLWG)

## Banking

Basel Committee on Banking Supervision (BCBS)

**Co-Chair**
Task Force on Financial Technology (TFFT)

**Member**
Operational Resilience Working Group (ORG)

## Payments & Market Infrastructures

Committee on Payments and Market Infrastructures (CPMI)

**Co-Chair (2015-17) / Member**
Working Group on Cyber Resilience (WGCR)

## Securities

International Organization of Securities Commissions (IOSCO)

**Member**
Cyber Task Force (CTF)

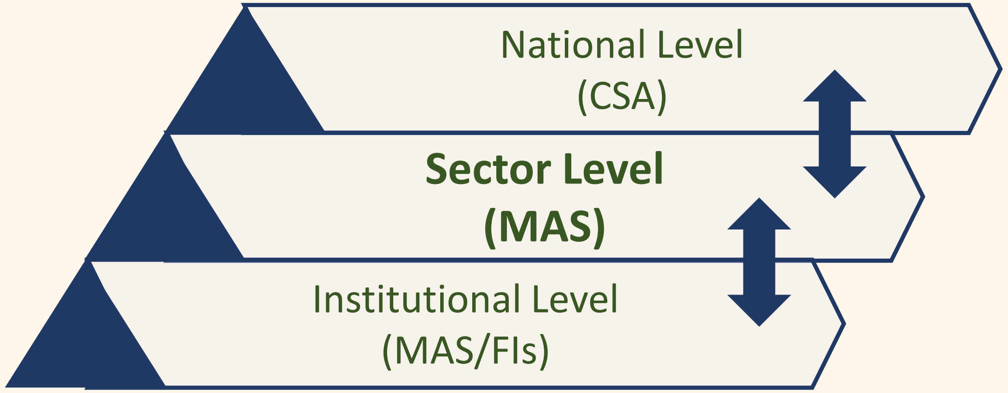
## Insurance

International Association of Insurance Supervisors (IAIS)

**Member**
Financial Crime Task Force (FCTF)

# Heightened cyber threat intel monitoring

- Plugged into the **tiered national surveillance framework..**

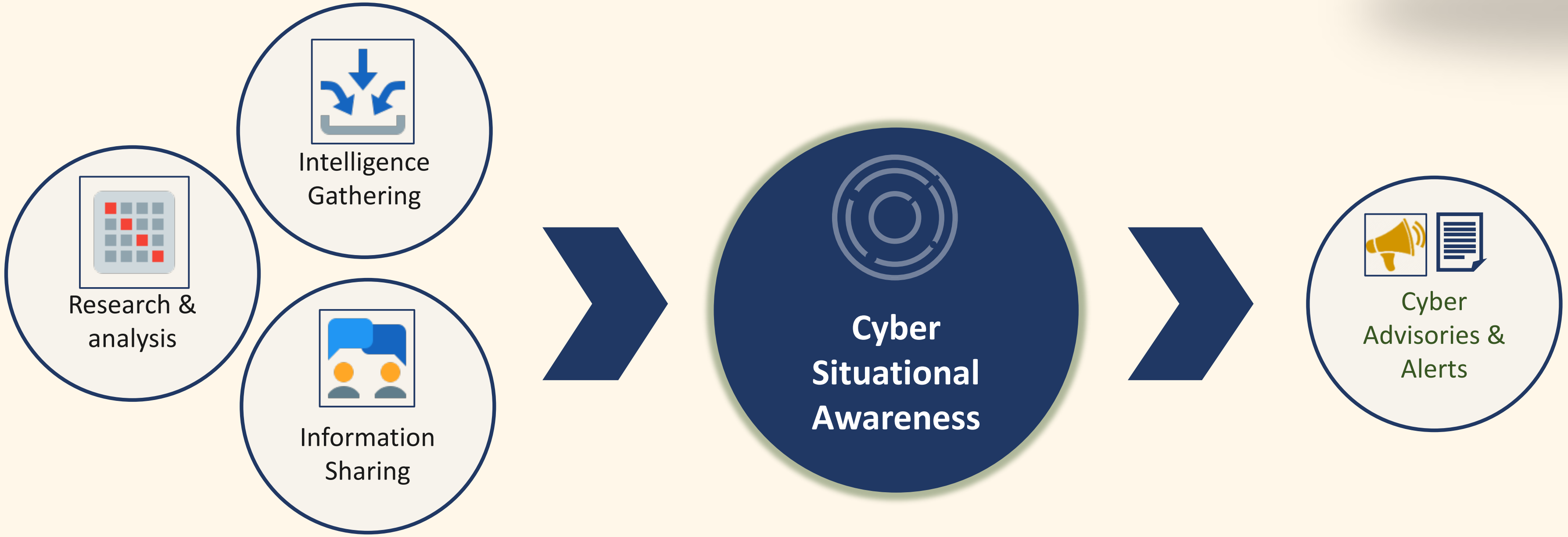


National Level
(CSA)

**Sector Level
(MAS)**

Institutional Level
(MAS/FIs)

- Shared relevant intelligence with FIs and peers through **alerts and advisories**



Research & analysis

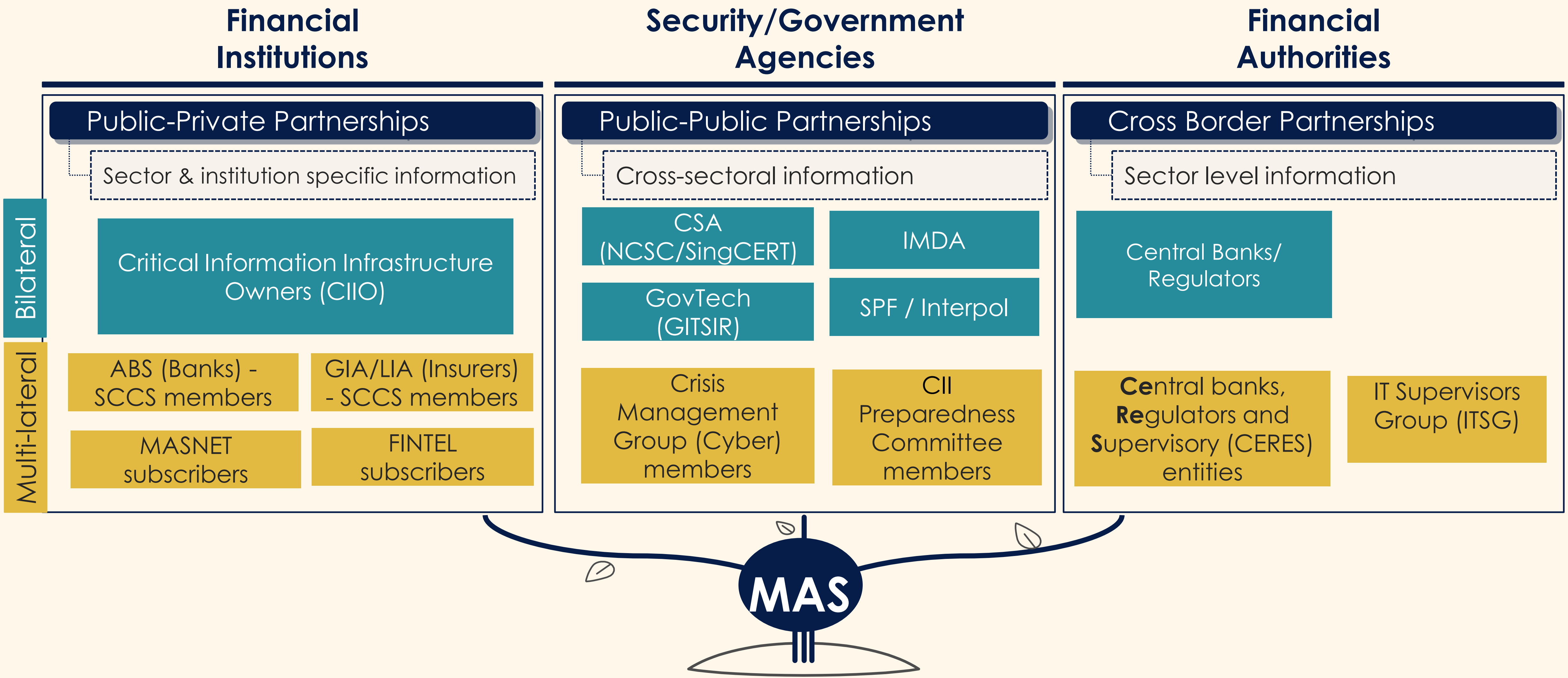
Intelligence Gathering

Information Sharing

**Cyber Situational Awareness**

Cyber Advisories & Alerts

# Strengthen Collaboration with Industry, Agencies and Global Regulators



Bilateral

Multi-lateral

## Financial Institutions

### Public-Private Partnerships

Sector & institution specific information

- Critical Information Infrastructure Owners (CIIO)
- ABS (Banks) - SCCS members
- GIA/LIA (Insurers) - SCCS members
- MASNET subscribers
- FINTEL subscribers

## Security/Government Agencies

### Public-Public Partnerships

Cross-sectoral information

- CSA (NCSC/SingCERT)
- IMDA
- GovTech (GITSIR)
- SPF / Interpol
- Crisis Management Group (Cyber) members
- CII Preparedness Committee members

## Financial Authorities

### Cross Border Partnerships

Sector level information

- Central Banks/ Regulators
- **Ce**ntral banks, **Re**gulators and **S**upervisory (CERES) entities
- IT Supervisors Group (ITSG)

MAS

ADAPT

TRANSFORM

ENHANCE

# Supervisory Engagement with Key FIs

Review FIs' IT and cyber resilience posture and technology risks related to COVID-19

- Availability of internet-facing online services
- Remote access and collaboration tools used to support telecommuting
- Changes in technology and cyber risk activities due to COVID-19
- Remote privileged access to production systems

# Metric-driven Supervision

## Technology Risk Unified Supervision Tool (TRUST)

- FIs’ Information Repository
- Inspection Management System
- Data Processing and Reporting

**Straight-through data collection** process with data warehouse and data visualisation tools.

# Continuous Monitoring of FIs' Resilience Posture

Enhance **key indicators** for continuous monitoring and analysis on FIs' **IT and cyber resilience** posture

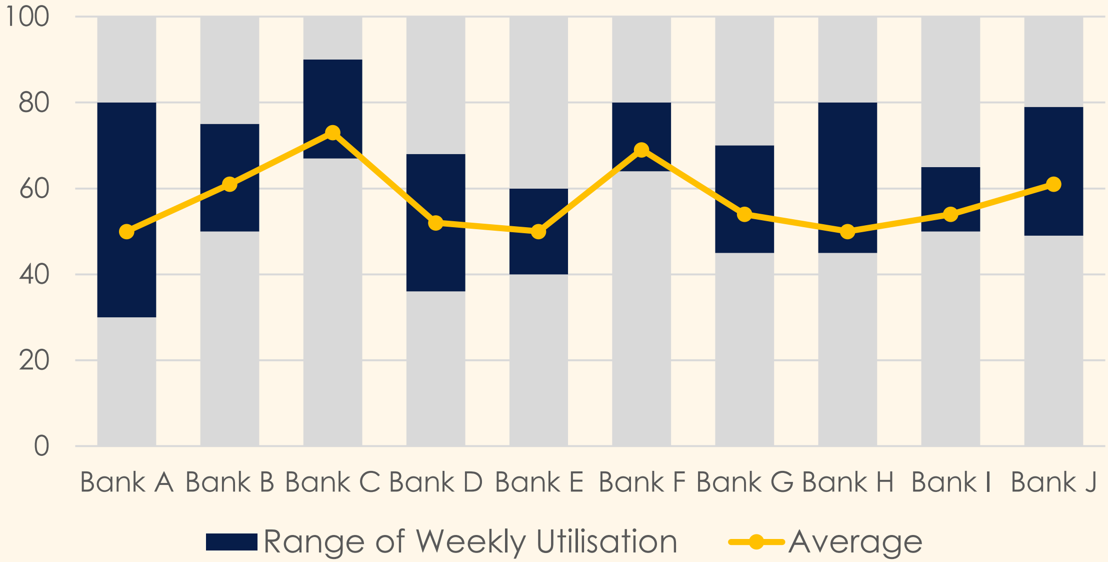
**Examples:**

- System and application capacity
- System patch management
- Technology refresh of critical systems
- System conformance to security baselines
- Privileged access to production systems
- Ops disruption, IT and cyber incidents

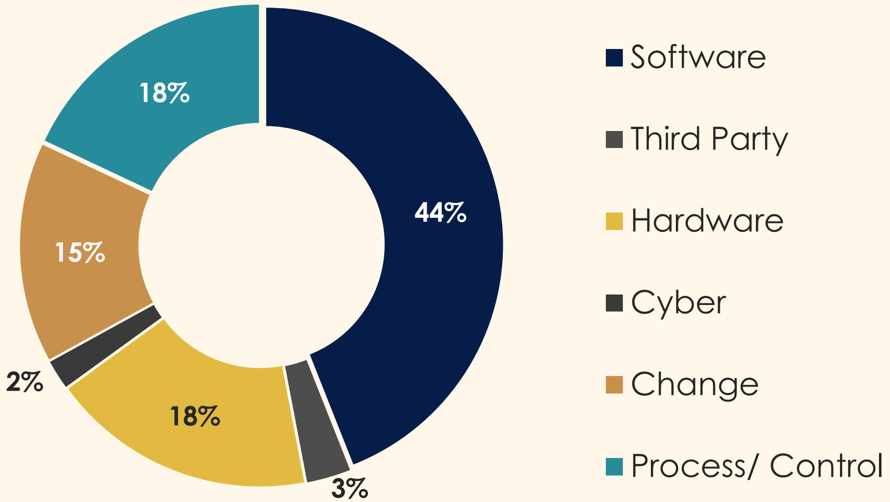
# Technology Vital Signs

**Dashboard** to perform trend analysis of FIs' **key risk indicators**

## Critical System Capacity



## Root Cause Analysis of Ops Disruption, IT and Cyber Incidents



Identify **institutional and systemic risks** and enhance FIs' IT resilience posture by sharing **common issues observed** and provide **recommendations** to the industry

“We need to ready ourselves for **a new way of living for the foreseeable future.**

Our lives and approach to stopping transmission must continue to adapt and evolve”

**Dr Takeshi Kasai, the WHO’s regional director for the Western Pacific**

Thank you