Monetary Authority of Singapore

FIGI Symposium:
Cyber Resilience from the MAS' Perspective

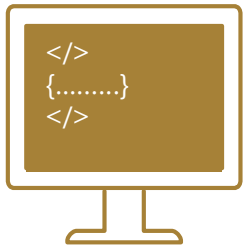
Tan Yeow Seng
Executive Director (Technology and Cyber Risk Supervision Department) &
Chief Cyber Security Officer
Monetary Authority of Singapore

The Cyber Threat Landscape

presents significant risks in an increasingly inter-connected digital world

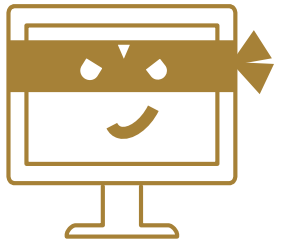
Managing IT and Cyber Risk in the Digital Age

A **Smart Financial Centre** has to be a **Safe Financial Centre**



Adoption of **new software and infrastructure** to support a digital economy

Increased **partnership** with fintech companies, and **complex linkages**



Persistent cyber threats to data security and operational continuity

The Cyber Threat Landscape

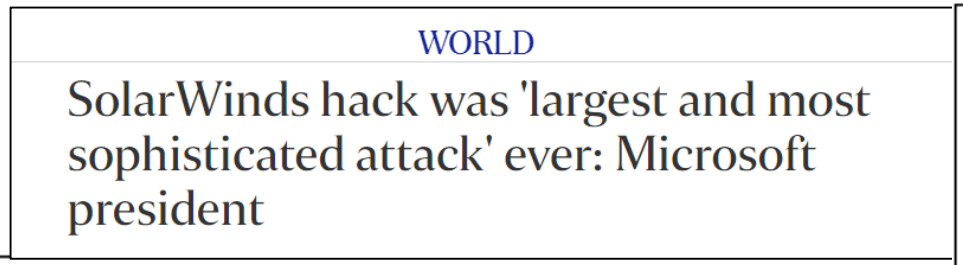
requires constant vigilance to guard against opportunistic threat actors

Cyber attacks riding on the 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)

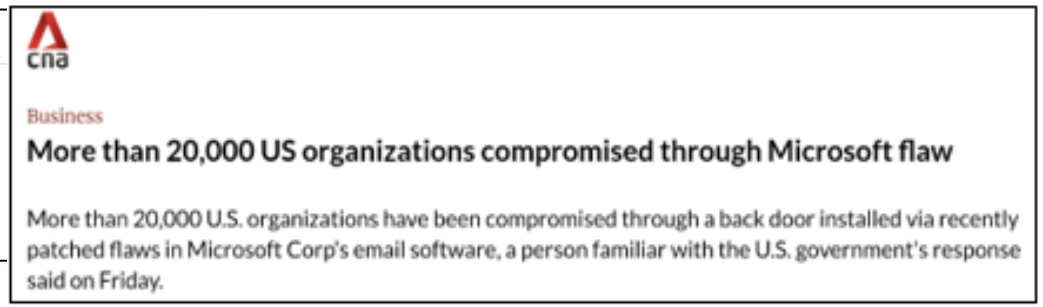
Supply chain attacks and Exploitation of zero-day vulnerabilities

Compromise of victims' **trusted suppliers**	Exploitations of zero-day vulnerabilities in **widely used applications**



WORLD

SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president



cna

Business

More than 20,000 US organizations compromised through Microsoft flaw

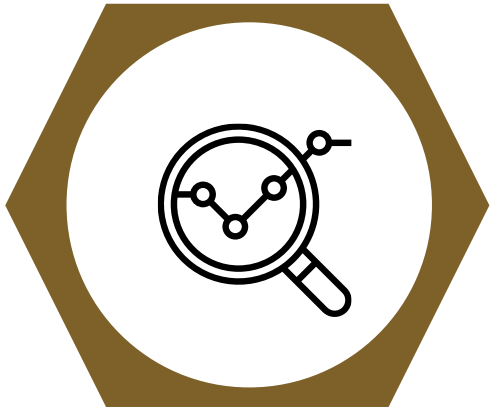
More than 20,000 U.S. organizations have been compromised through a back door installed via recently patched flaws in Microsoft Corp's email software, a person familiar with the U.S. government's response said on Friday.

Roles and Responsibilities of MAS

MAS' Cybersecurity Strategy is shaped by the multiple roles that MAS plays

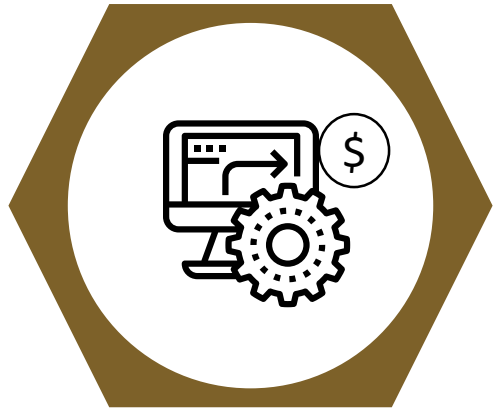
MAS' roles…

Central Banking



Financial sector regulation

Singapore financial sector development



Real-Time Gross Settlement system (RTGS) operator

MAS' Internal Cybersecurity Strategy

developed with reference to international standards on building cyber resilience

CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures

FSB Effective Practices for Cyber Incident Response and Recovery

- Governance
- Planning & Preparation
- Analysis
- Mitigation
- Restoration & Recovery
- Coordination & Communication
- Improvement

Cybersecurity Strategy for Financial Sector

was developed in consultation with our Cyber Security Advisory Panel

MISSION

To promote a Sound and Progressive Financial Sector in Singapore

OBJECTIVES

Desired outcomes

- Stable financial system
- Safe & sound intermediaries
- Safe & efficient infrastructure

STRATEGY

To enhance cybersecurity resilience of financial sector

Regulation & Guidance

Regulate and **provide guidance** to the financial sector in managing cyber risk

Supervision

Supervise FIs to assess the quality of their cyber risk management and address any gaps noted

Surveillance & Info-sharing

Conduct cyber **surveillance and research,** and engage in **information-sharing** to maintain cyber situational awareness

Capability Development

Partner the industry to **uplift and assess** the sector's cyber **capabilities** to maintain cyber resilience

Cybersecurity Strategy for Financial Sector

Our rules and guidance to the industry

Regulation and Guidance | Supervision | Surveillance and Information-sharing | Capability Development

Rules set out key tech and cyber risk management objectives

Notices

Specify requirements that allow FIs to implement controls that are proportionate to risk

- Notice on Technology Risk Management
- Notice on Cyber Hygiene

Guidance set out supervisory expectations on good technology risk management and business continuity management practices

Guidelines

Supervisory expectations applicable to all FIs in Singapore

- Technology Risk Management Guidelines
- Business Continuity Management Guidelines

Circulars/ Advisories

Ad-hoc circulars and advisories

- IT security risks posed by emerging threats
- Awareness on cyber attacks

Cybersecurity Strategy for Financial Sector

We play an active role to shape international cybersecurity standards

Regulation and Guidance | Supervision | Surveillance and Information-sharing | Capability Development

Financial Stability Board (FSB)

Chair (2019-2020)
Cyber Incident Response & Recovery Working Group (CIRR)

Member
Cyber Lexicon Working Group (CLWG)

Member
Cyber Incident Reporting Working Group (CIR)

Banking

Basel Committee on Banking Supervision (BCBS)

Co-Chair
Financial Technology Expert Group (FTG)

Member
Operational Resilience Working Group (ORG)

Securities

International Organization of Securities Commissions (IOSCO)

Member
Cyber Task Force (CTF)

Payments & Market Infrastructures

Committee on Payments and Market Infrastructures (CPMI)

Co-Chair (2015 – 2017) / Member
Working Group on Cyber Resilience (WGCR)

Insurance

International Association of Insurance Supervisors (IAIS)

Member
Financial Crime Task Force (FCTF)

Cybersecurity Strategy for Financial Sector

Our IT supervisory approach is risk focused and involves striking a balance

Regulation and Guidance | **Supervision** | Surveillance and Information-sharing | Capability Development

Risk focused IT supervision…

> 1,600
Financial Institutions

Impact
&
Risk

… with the following objectives

Focus supervisory resources on FIs with **systemic impact**

Greater supervisory attention on FIs assessed to have **weaker risk management** processes & controls

On-site Inspections

- ❑ Focus on **key FIs**
- ❑ **Thematic reviews** on specific systems or type of FIs

Off-site Reviews

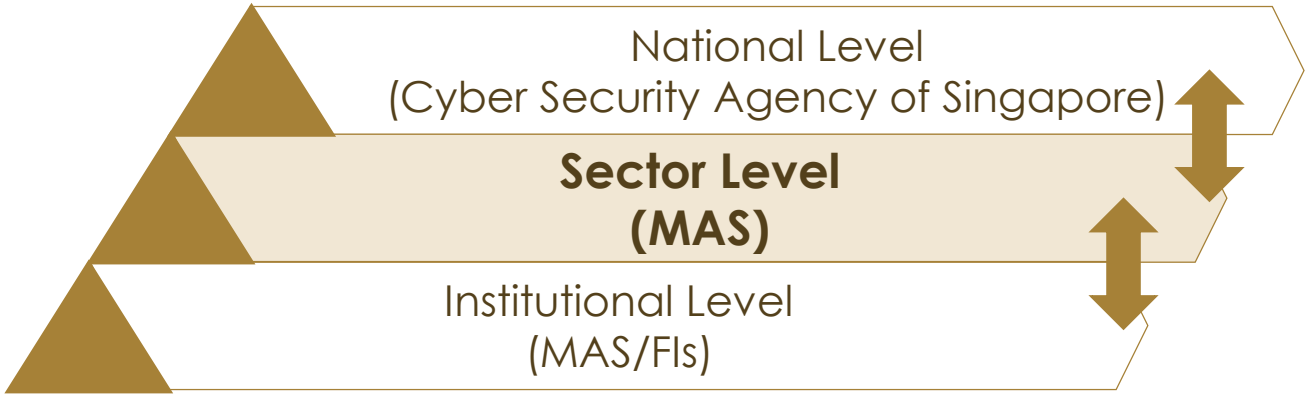
- ❑ Leverage **Quantitative Risk Assessment Methodology (QRAM)** to perform automated review based on scoring template

Cybersecurity Strategy for Financial Sector

Enhancing cyber situational awareness

Regulation and Guidance | Supervision | **Surveillance and Information-sharing** | Capability Development

MAS is plugged into the tiered national surveillance framework



MAS shares relevant intelligence with FIs and peers via alerts and advisories, FINTEL, etc.

- Intelligence gathering
- Research & analysis
- Information sharing

→ **Cyber Situational Awareness** →

- Cyber advisories & alerts
- Cyber policy-making

Cybersecurity Strategy for Financial Sector

We are involved in many bilateral and multi-lateral information sharing arrangements

Regulation and Guidance | Supervision | **Surveillance and Information-sharing** | Capability Development

	Security/Government Agencies	Financial Authorities	Financial Institutions
	Public-Public Partnerships	Cross Border Partnerships	Public-Private Partnerships
	Cross-sectoral information	Sector level information	Sector & institution specific info
Bilateral	Cyber Security Agency; Infocomm & Media Development Authority; Government Technology Agency; Law Enforcement Agencies	Peer Regulators	Critical Information Infrastructure Owners (CIIO)
Multi-lateral	Crisis Management Group (Cyber) members; CII Preparedness Committee members	Central banks, Regulators and Supervisory (CERES) entities; IT Supervisors Group (ITSG)	ABS (Banks) - SCCS members; GIA/LIA (Insurers) - SCCS members; MASNET subscribers; FINTEL subscribers

MAS

Cybersecurity Strategy for Financial Sector

We collaborate with the industry to uplift competencies

Regulation and Guidance | Supervision | Surveillance and Information-sharing | **Capability Development**

Standing Committee on Cyber Security ("SCCS") founded under ABS' guidance in July 2013

Insurers' SCCS founded in 2015 by the General Insurance Association and Life Insurance Association

2014
- ❑ Study Trip to US
- ❑ Provided cyber security guidance to Operation Raffles IV (IWE2014)
- ❑ Inaugural Financial Sector – Information Security ("FS-IS") Forum launched
- ❑ Developed ABS-FITA Cyber Security Master Class program for SMU
- ❑ 2nd ABS Technology Risk Seminar
- ❑ Developed Cyber Incident Management Framework (CIMF)

2015
- ❑ 2nd FS-IS Forum
- ❑ Post-IWE2014 Improvement Work Streams initiated
- ❑ Published ABS Penetration Testing Guidelines
- ❑ Developed Focus Group on Talent Development of Infocomm Security Professionals
- ❑ 3rd FS-IS Forum
- ❑ Cloud Computing Taskforce formed
- ❑ 3rd ABS Technology Risk Seminar
- ❑ Drafted Cloud Computing White Paper

2016
- ❑ Established working group in emerging technologies, methodologies and IOT
- ❑ Published ABS Cloud Computing Guidelines
- ❑ Industry Briefing on ABS Cloud Computing Implementation Guide
- ❑ 3rd ABS Technology Risk Conference (part of MAS Fintech Festival)
- ❑ Conducted cyber crisis table-top exercise (#OPSABSCISE) for SCCS member FIs

2017
- ❑ #OPSABSCISE Post Mortem report published
- ❑ Social Engineering Testing Working Group Formed
- ❑ Provided joint consultation feedback to Singapore draft Cybersecurity Bill
- ❑ 4th FS-IS Forum
- ❑ Participated in ABS Exercise Raffles V
- ❑ TRM Guidelines Review Working Group formed
- ❑ Conducted industry-wide social engineering assessment (SEEP-X)

2018
- ❑ ASEAN and ABA workshops
- ❑ Project Pegasus
- ❑ Adversarial Attack Simulation Working Group
- ❑ UK study trip with MAS and CSA
- ❑ Meeting with Korea FSI
- ❑ FS-IS forum
- ❑ 2019 Exercise Raffles (ER) VI Planning started
- ❑ Cloud Implementation Guide Revised

2019 - 2020

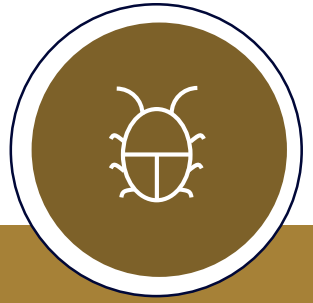
2019 - 2021
- ❑ Industry Wide Cyber Exercise
- ❑ Third party source code
- ❑ Red teaming

MAS' Latest Cyber Initiatives

Revised Technology Risk Management Guidelines

Paper on Remote working risks due to COVID-19

Cyber Threat Intelligence & Management System



Insurers Bug Bounty Programme (BBP)

Close supervision on Cloud concentration risk

Advisory on Cloud Risk Management

Thank you

SG SINGAPORE