Cybersecurity Risk Supervision during COVID-19

Tan Yeow Seng
Executive Director (Technology and Cyber Risk Department) & Chief Cyber Security Officer
Monetary Authority of Singapore
**MAS’ Guidance to the Industry in response to the COVID-19 Pandemic**

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

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

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

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

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

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

**7 Apr**
Start of Circuit Breaker

**21 Apr**
Circuit Breaker measures tightened

**21 Apr**
Phase 1 Gradual Resumption of Onsite Operations
# Cyber Attacks Riding on COVID-19 Bandwagon

## Cyber threats arising from work from home arrangement
- Vulnerabilities in Remote Access and Collaboration Tools (e.g. VPN, Video-conferencing)

## Cyber threats targeting FIs and customers
- Social Engineering (e.g. Business Email Compromise, Phishing)

---

**Thousands of Zoom video calls left exposed on open Web**

CISA Warns Patched Pulse Secure VPNs Could Still Expose Passwords


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

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

- Reliance on Technology
- IT and Cyber Resilience

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.
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

<table>
<thead>
<tr>
<th>Bank</th>
<th>15-Jun</th>
<th>22-Jun</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank 1</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>Bank 2</td>
<td>98%</td>
<td>99%</td>
</tr>
<tr>
<td>Bank 3</td>
<td>96%</td>
<td>97%</td>
</tr>
<tr>
<td>Bank 4</td>
<td>98%</td>
<td>96%</td>
</tr>
<tr>
<td>Bank 5</td>
<td>99%</td>
<td>93%</td>
</tr>
<tr>
<td>Bank 6</td>
<td>98%</td>
<td>94%</td>
</tr>
<tr>
<td>Bank 7</td>
<td>99%</td>
<td>96%</td>
</tr>
<tr>
<td>Bank 8</td>
<td>100%</td>
<td>99%</td>
</tr>
</tbody>
</table>

Number of IT Incidents and Incident Resolution

<table>
<thead>
<tr>
<th>Bank</th>
<th>No of IT Incidents</th>
<th>% of incidents resolved within SLA turnaround time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank 1</td>
<td>30</td>
<td>100%</td>
</tr>
<tr>
<td>Bank 2</td>
<td>42</td>
<td>100%</td>
</tr>
<tr>
<td>Bank 3</td>
<td>134</td>
<td>90%</td>
</tr>
<tr>
<td>Bank 4</td>
<td>167</td>
<td>89%</td>
</tr>
<tr>
<td>Bank 5</td>
<td>226</td>
<td>100%</td>
</tr>
<tr>
<td>Bank 6</td>
<td>226</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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)

Securities
International Organization of Securities Commissions (IOSCO)
Co-Chair (2015-17) / Member
Working Group on Cyber Resilience (WGCR)

Insurance
International Association of Insurance Supervisors (IAIS)
Member
Financial Crime Task Force (FCTF)

Operational Resilience Working Group (ORG)

Cyber Task Force (CTF)
Heightened cyber threat intel monitoring

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

- Shared relevant intelligence with FIs and peers through **alerts and advisories**.
Strengthen Collaboration with Industry, Agencies and Global Regulators

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

- **Public-Public Partnerships**
  - Cross-sectoral information
  - CSA (NCSC/SingCERT)
  - GovTech (GITSIR)
  - SPF / Interpol
  - MASNET subscribers
  - FINTEL subscribers
  - ABS (Banks) - SCCS members
  - GIA/LIA (Insurers) - SCCS members
  - Crisis Management Group (Cyber) members
  - Central banks, Regulators and Supervisory (CERES) entities
  - IT Supervisors Group (ITSG)

Security/Government Agencies

- **Public-Public Partnerships**
  - Cross-sectoral information
  - CSA (NCSC/SingCERT)
  - GovTech (GITSIR)
  - SPF / Interpol
  - Crisis Management Group (Cyber) members
  - Central banks, Regulators and Supervisory (CERES) entities
  - IT Supervisors Group (ITSG)

- **Critical Information Infrastructure Owners (CIIO)**

Financial Authorities

- **Cross Border Partnerships**
  - Sector level information
  - IMDA
  - Central Banks/Regulators
  -中国国际信息安全基础设施委员会（CII）

- **Preparedness Committee members**

- **ABS (Banks) - SCCS members**

- **FINTEL subscribers**

- **Multi-lateral**

- **Bilateral**

- **Financial Institutions**

- **Security/Government Agencies**

- **Financial Authorities**

- **MAS**
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)

Technology Risk Supervision (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