Deloitte.

Monetary Authority of Singapore (MAS) Notice on Cyber Hygiene Assessment - How we can help you

April 2020

Singapore Cyber Threat Environment

What are you up against?

ASEAN average cost of data breach

$2.6m

- **Overall Cyber Crime Rate**

Cyber crimes account for **18.6%** of crime in Singapore

- **Phishing**

Top targets of phishing attacks:

1. Banking and Financial Services
2. Technology
3. File Hosting Provider

- **Malware**

21 Cases of Ransomware reported

300 Command and Control servers observed

2900 Botnet drones observed daily on average

- **Website Defacement**

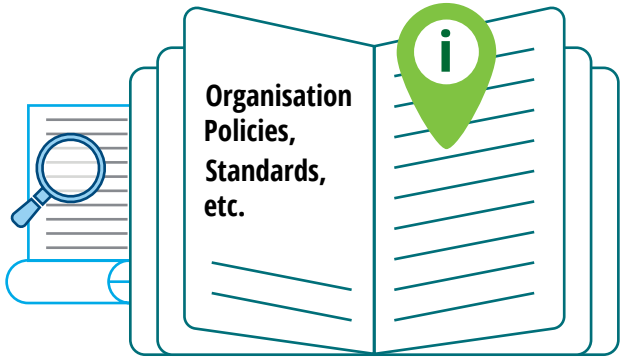
605 Singapore-linked website defacements were detected

Source: IBM Security, Ponemon Institute

Introduction

Singapore Financial Institutions Technology and Cyber Regulatory Landscape

The regulatory landscape for Financial Institutions, specifically for Technology and Cyber has been rapidly evolving in the past 2 years. Given updated requirements, organisations are looking to leverage industry standards to set the base benchmark and tweaked to meet other regulatory requirements. The common industry standards used are NIST Cyber Security Framework, Centre for Internet Security (CIS) Top 20 Controls and ISO 27001.



- Technology Policies
- Cyber Risk Management Framework
- Existing IT Controls in key focus areas
- Governance and Reporting
- Third-Party Management Framework

STANDARDS AND REQUIREMENTS

- NIST Cyber Security Framework
- CIS Top 20 Controls
- MAS Cyber Hygiene
- Guidelines on Outsourcing dated 5 October 2018
- Technology Risk Management Guidelines – dated June 2013
- Personal Data Protection Act 2012

MAS Notice on Cyber Hygiene

On 6 August 2019 the Monetary Authority of Singapore (MAS) issued a set of legally binding requirements to raise the cyber security standards and strengthen cyber resilience of the financial sector. The Notice on Cyber Hygiene sets out the measures that financial institutions must take to mitigate the growing risk of cyber threats. The "Notice" prescribes six cyber hygiene practices applicable to banks, insurers, capital markets services license holders, designated payment system operators, and settlement institutions.

1

4.1 Administrative Accounts

A relevant entity must ensure that every administrative account is secured to prevent any unauthorized access or usage.

2

4.2 Security Patches

A relevant entity must ensure that security patches are applied within a defined timeframe and mitigating controls are in place for systems that cannot be patched.

3

4.3 Security Standards

A relevant entity must ensure that there is a written set of security standards for systems and that systems are tested to ensure compliance to the security standards.

4

4.4 Network Perimeter Defence

A relevant entity must ensure the implementation of controls at the network perimeter to restrict all unauthorized network traffic.

5

4.5 Malware Protection

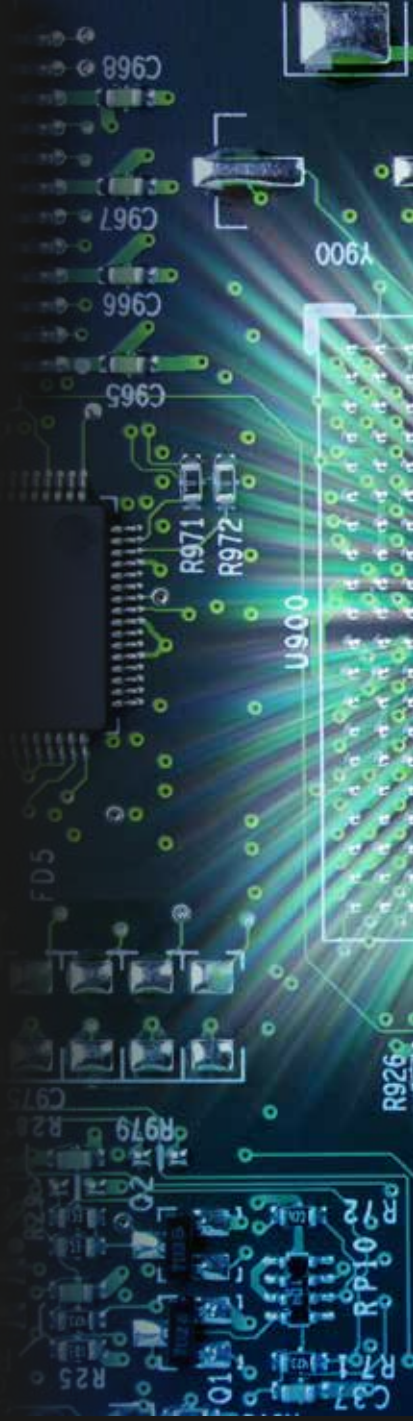
A relevant entity must ensure that one or more malware protection measures are implemented on every system, to mitigate the risk of malware infection, where applicable.

6

4.6 Multi-factor Authentication

A relevant entity must ensure that multi-factor authentication is implemented for all administrative accounts and all accounts on any system used to access critical information from the internet.

*The effective date of 6 August 2020, does not apply to cyber hygiene practice 4.6 Multi-Factor Authentication for the period between 6 August 2020 and 5 February 2021 (dates are inclusive).



Our Offering

How can Deloitte be of assistance?

The Deloitte Cyber Hygiene Assessment offering includes a two-part assessment encompassing **core compliance assessment and a technical compliance assessment** against the six defined cybersecurity practices with mitigating recommendations to accompany each identified gap or finding. We have structured our approach to assess the design and operating effectiveness of the cybersecurity countermeasures implemented throughout our client's network environment.

Based on the client's need, Deloitte offers the following types of services:

Core Compliance Assessment | **Technical Compliance Assessments (Optional)**

Phase 1: Assessment & Analysis

Objective: Understand the current state of compliance

Key Activities

- Interview business and technical stakeholders and review relevant documentation to understand existing cyber capabilities
- Document current state of people, process and technology controls in relevant capability areas
- Validate clients understanding of compliance in relevant capability areas.

Phase 2: Discussion & Confirmation

Objective: Define the target state of compliance against the six defined requirements

Key Activities

- Determine target state of cyber capabilities to comply with regulatory and industry best practices for Cyber Hygiene requirements
- Discuss identified observations and confirm factual accuracy

Phase 3: Recommendations & Reporting

Objective: Identify specific recommendations to address gaps in existing processes

Key Activities

- Define recommendations and prioritize based on the gaps

Phase 4: (Optional)

Objective: Perform technical assessment

Key Activities

- Assess current technical controls
- Define technical recommendations and prioritize based on gaps

Deliverables

- Current state analysis
- Target state analysis and confirmed observations
- Confirm observations
- Technical assessment report and recommendations

*The estimated effort to complete depends on the scope and complexity of the client's environment.

Contact us

Thio Tse Gan
Cyber Risk Leader
Southeast Asia Risk Advisory
tgthio@deloitte.com

Eric Lee
Executive Director, Cyber Risk
Southeast Asia Risk Advisory
ewklee@deloitte.com

Hisashi Ohta
Director, Cyber Risk
Southeast Asia Risk Advisory
hohta@deloitte.com

Siah Weng Yew
Executive Director, Cyber Risk
Southeast Asia Risk Advisory
wysiah@deloitte.com

Amol Ashok Dabholkar
Director, Cyber Risk
Southeast Asia Risk Advisory
adabholkar@deloitte.com

Sigit Kwa
Director, Cyber Risk
Southeast Asia Risk Advisory
skwa@deloitte.com

Edna Yap
Executive Director, Cyber Risk
Southeast Asia Risk Advisory
edyap@deloitte.com

Andrew Koay
Director, Cyber Risk
Southeast Asia Risk Advisory
akoay@deloitte.com

Stanley Yong
Director, Cyber Risk
Southeast Asia Risk Advisory
styong@deloitte.com