PwC Straight Away
Notice on Cyber Hygiene

19 August 2019

Overview of the Notice on Cyber Hygiene

On 6 August 2019, the Monetary Authority of Singapore ("MAS") issued a Notice on Cyber Hygiene ("Notice") to strengthen cyber resilience in the financial industry. The requirements are legally binding, and include key elements in the existing MAS Technology Risk Management ("TRM") Guidelines and measures that financial institutions ("FIs") must take to guard against increasing risk of cyber threats.

The legally binding requirements will come into effect on 6 August 2020, giving FIs about 12 months to implement the necessary measures.

A concession is made for a period of 6 months from 6 August 2020 to 5 February 2021 (both dates inclusive) on implementation of multi-factor authentication if FIs meet all the following:

i) Risk assessment: identify all risks or potential risks posed by FIs' non-compliance to implement multi-factor authentication;
ii) Controls: implement controls to reduce risks identified above; and
iii) Appointed committee or member of the senior management: agree with the risk assessment and satisfied with the implemented controls being adequate to reduce the risks.

6 Cyber Security Measures

There are six (6) legally binding cyber security measures:

1. **Secure the use of every administrative account** in respect of any operating system, database, application, security appliance or network device through preventive controls. These controls should prevent the unauthorised access to or use of such account.
2. **Address system vulnerabilities in a timely manner** by applying available security patches to every system (including both hardware and software) in a risk-commensurate timeframe. Mitigating controls must be implemented where no security patch is available.
3. **Establish a written set of security standards for every system** and **ensure compliance to the security standards**. Mitigating controls should be implemented where the system is unable to conform to the security standards.
4. **Implement controls at its network perimeter** to restrict all unauthorised network traffic.
5. **Implement malware protection measures on every system** to mitigate the risk of malware infection, where available and can be implemented.
6. Strengthen user authentication through **implementation of multi-factor authentication** for all administrative accounts in respect of any operating system, database, application, security appliance or network device that is a critical system, and all accounts on any system used to access customer information through the internet.

Contact us

If you have any queries, please do not hesitate to call your usual PwC contacts or any of the following PwC subject matter experts:

Tan Shong Ye
Digital Trust Leader
shong.ye.tan@sg.pwc.com

Kyra Mattar
Digital Trust, Financial Services
kyra.mattar@sg.pwc.com

Jimmy Sng
Digital Trust, Cyber Security
jimmy.sng@sg.pwc.com

pwc

What do FIs need to consider

Whilst the requirements are largely similar to the MAS Cyber Hygiene Consultation Paper previously issued in September 2018 and are already embedded in good cyber security practices, these requirements are legally binding in the Notice. Existing policies and procedures would need to be considered in conjunction with FIs' systems and data. FIs should consider:

- System landscape – The extent of the system landscape to which the requirements will apply. The requirements for security patches, security standards and malware protection measures will apply to every system for administrative accounts will apply to any operating system, database, application, security appliance or network device.

- Critical systems – FIs need to define its critical systems which would require multi-factor authentication for all administrative accounts. Most FIs would have already defined 'critical systems' based on the previous Technology Risk Management Notice.

- Customer Information – FIs need to determine customer information applicable to the related entity. **"Customer information"** means any information relating to, or any particulars of, any customer of the relevant entity, where a named customer or group of named customers can be identified, or is capable of being identified, from such information. FIs will be required to have multi-factor authentication to access "customer information" through the internet.

- Third parties – FIs should determine key requirements to be placed on third parties where FIs have direct or indirect control of the systems managed by third parties.

Who is impacted?

The requirements would be applicable to a "relevant entity" that is licensed, approved, registered or regulated by the MAS, including banks, merchant banks, insurers and insurance agents, insurance brokers, credit card or charge card licensees, financial holding companies, finance companies, financial advisers, capital market entities, trust companies, and operators of designated payment systems.

FIs need not comply with the requirements to the extent where FIs cannot exercise direct or indirect control (through the system provider) over the system, and it is not reasonable to procure an alternative system provider over whom FIs are able to exercise control.

Next Steps

The above are just some of the many areas that FIs need to consider. We would recommend that FIs assess their current measures against the requirements and their pragmatic ability to implement the measures in the next 12 months to meet the legally binding requirements.