Baker McKenzie Wong & Leow.

Financial Services Regulatory
TMT
Singapore

Client Alert

September 2018

For more information, please contact:

Stephanie Magnus
+65 6434 2672
Stephanie.Magnus@bakermckenzie.com

Ken Chia
+65 6434 2558
Ken.Chia@bakermckenzie.com

Liew, Ying Yi
+65 6434 2531
YingYi.Liew@bakermckenzie.com

Alex Toh
+65 6434 2783
Alex.Toh@bakermckenzie.com

MAS consults on draft notice on cyber security measures for the financial sector

The Monetary Authority of Singapore (**MAS**) released a consultation paper on 6 September 2018 proposing a new Notice On Cyber Hygiene (**Notice**) which will set out cyber security measures (outlined below) for prescribed financial institutions regulated by the MAS (**FIs**). The Notice seeks to outline a "clear and common cyber security waterline for the financial industry".

Most of these FIs are already subject to an existing Notice on Technology Risk Management (**TRM Notice**) and Technology Risk Management Guidelines, among others, which imposes obligations in relation to managing technology risks. This proposed Notice goes further to impose more prescriptive legally binding obligations in relation to cyber security measures.

Will this affect you?

The MAS proposes to apply this Notice not just to entities licensed, approved, registered or regulated by MAS but also to some other entities that MAS will be regulating in the future. As an example, the MAS specifically referenced persons who will be licensed under the proposed Payment Services Bill including, for account issuance, domestic money transfer, merchant acquisition and virtual currency services.

Notably, this Notice will apply to a broader scope of FIs than the TRM Notice currently applies to, e.g. stored value facility holders and registered fund management companies. This means that even if these FIs are not currently expected to assess and identify which of its systems are critical systems, they may be required to do so in order to comply with certain requirements under this Notice.

Where FIs have outsourcing arrangements relating to their IT systems, these FIs may seek to impose these standards on their outsourced service providers as well.

How will this affect you?

The Notice sets out the following non-exhaustive list of proposed cyber hygiene measures:

Cyber Hygiene Requirements	Proposed Cyber Hygiene Measures
Secure Administrative Accounts to prevent unauthorized access or	• Keep a record all administrative accounts in its system. • Implement strong password controls such as

use	changing the default password, enforcing minimum password length and password complexity. • Grant access to administrative accounts only to authorised staff. • Validate on a regular basis that only authorised persons have access to administrative accounts.
Timely application of Security Patches to be address vulnerabilities	• Perform regular checks for available security patches. • Establish a framework to assess the criticality of any available patch and the timeframe within which the patch must be implemented. • The framework should include controls to reduce any risk in the event that a patch cannot be applied.
Written Security Standards	• Establish, document and keep up-to-date security standards. • Ensure every system complies with the security standards established by the relevant entity. • Take steps to reduce any risk, including approving deviations from the security standards, if the system cannot fully conform with the security standards.
Implement Firewalls	• Implement one or more firewalls at the network perimeter in order to segment the internal network from the public internet. • Configure any implemented firewalls and regularly review the firewall rules to only allow authorised network traffic to pass through.
Implement Anti-virus measures	• Update any anti-virus software and signatures promptly.
Implement Multi-factor Authentication	• Implement multi-factor authentication for all administrative accounts on its critical systems and all accounts on any system used by the FI to access confidential information through the internet. An example

	cited was an account belonging to Human Resource Department that can be used to remotely access staff information through the internet.

MAS accepts that differences in the scale, complexity and nature of business of different FIs, may result in implementation differences between the various FIs.

Most FIs are likely to have IT security policies or procedures in place which may already cover some or all of these matters. They should review existing policies to confirm that their standards are in line with the MAS' expectations as outlined in the proposed Notice. They should also ensure that they are indeed carrying out ongoing validation checks or audits to confirm that these prescribed standards are met on an ongoing basis.

Implementation Timeline

MAS has proposed that the Notice would be effective 12 months from its date of issuance.

MAS is seeking public feedback on the proposed Notice. The consultation period will end on 5 October 2018.

If you have any questions or any feedback you would like to provide in relation to the consultation paper, please do not hesitate to contact us.

www.bakermckenzie.com

Baker McKenzie Wong & Leow
8 Marina Boulevard
#05-01 Marina Bay Financial
Centre Tower 1
Singapore 018981

Tel: +65 6338 1888
Fax: +65 6337 5100