Circular No. SRD TR 01/2014

21 May 2014

The Chief Executive Officers of All Financial Institutions
The Chief Executives of All Insurers

Dear Sir / Madam

SYSTEM VULNERABILITY ASSESSMENTS AND PENETRATION TESTING

Financial institutions ("FIs") are increasingly relying on the internet to manage their operations, and to deliver greater convenience and efficiency to customers. Greater internet usage has however heightened FIs' exposure to cyber-attacks. This makes FIs today more vulnerable to security breaches such as unauthorised system access, data theft, system outages and website defacement.

2 Under the MAS Technology Risk Management Guidelines, FIs are expected to implement robust security measures to ensure that their systems and data are well protected against any breach or loss. These measures would include -

(a) *Vulnerability Assessments*: FIs should continuously monitor for emergent security exploits, and perform regular vulnerability assessments of their IT systems against common and emergent threats[1];

(b) *Penetration Testing*: FIs should perform penetration tests at least annually on their internet facing systems; and

(c) *Timely Remediation:* FIs should establish a process to effectively remedy issues identified from the vulnerability assessments and penetration testing in a timely manner.

3 As vulnerability assessments and penetration testing would only enable FIs to identify security deficiencies in their IT systems at a particular point in time, FIs should institute a robust regime of prompt system patching and hardening, as well as adopt secure software coding practice.

[1] Common security vulnerabilities include injections, security mis-configurations, sensitive data exposure, components with known vulnerabilities, and cross-site scripting / cross-site request forgery. FIs could refer to resources such as the Open Web Application Security Project (OWASP) to stay updated of common and emergent security vulnerabilities.

4 FIs are reminded that the above would similarly apply to outsourced activities. Outsourcing should not result in any weakening or degradation of the FIs' controls over the outsourced activity. Where an outsourcing arrangement involves the handling of sensitive customer data by the service provider, FIs shall ensure that the data is accorded the same level of protection as if it is processed in-house. Where applicable, stringent requirements for regular vulnerability assessments and penetration testing must be applied to the service providers' environment.

5 Should you have any questions or comments, please contact your respective MAS Review Officers.

Yours faithfully

(via MASNET)

HO HERN SHIN
EXECUTIVE DIRECTOR & HEAD
SPECIALIST RISK DEPARTMENT