



Circular No. SRD TR 02/2009

18 August 2009

The Principal Officers of All Insurers
The Chief Executive Officers of All Holders of a Capital Markets Services Licence

Dear Sir / Madam

TECHNOLOGY RISK MANAGEMENT

Financial institutions in the capital market and the insurance industry are progressively deploying more advanced technology and online systems, such as online trading platforms and insurance portals for policyholders, to offer a greater range of products and services to their customers. Ongoing technology innovations and developments have provided participants in the financial industry opportunities to expand their market reach and geographical coverage. As financial institutions rely increasingly on information systems technology and the internet to operate their trading activities and commercial functions, their acuity and capacity in understanding technology and operational risks associated with computer systems and networks should correspondingly be more responsive and perceptive.

2 The Board and senior management of financial institutions are responsible and accountable for managing and controlling technology risks as well as implementing security measures to protect their computer systems and operations. They serve a central role in ensuring the adequacy and effectiveness of their risk management processes and security controls.

3 Financial institutions should adopt risk management principles and security practices which will assist them in:

- a) establishing a sound and robust technology risk management framework;
- b) strengthening system security, reliability, availability and recoverability; and
- c) deploying strong cryptography and authentication mechanisms to protect customer data and transactions.

4 A serious security breach or failure in online systems has severe reputational repercussions on customer confidence in the financial institution concerned as well as market consequences, including financial losses and regulatory strictures. In addition, unauthorized transactions executed from compromised online trading accounts could also have far reaching impact on the fair and orderly functioning of markets.

5 The key measures that should be taken for enhancing the security of online systems and IT operations are delineated in the Appendix. For further guidance, financial institutions should also refer to the MAS Internet Banking and Technology Risk Management Guidelines, obtainable from the MAS website.

6 The objective of this advisory is to nurture the adoption of sound control processes in managing technology risks and the implementation of security practices. MAS will incorporate these recommendations into supervisory expectations for the purpose of assessing the adequacy of technology risk management and security measures adopted by financial institutions.

7 Should you have any questions or comments, please contact Mr Tony Chew, Director, Technology Risk Supervision at 62299109 or tonychew@mas.gov.sg.

Yours sincerely

(via MASNET)

CHUA KIM LENG
EXECUTIVE DIRECTOR
SPECIALIST RISK SUPERVISION DEPARTMENT
PRUDENTIAL SUPERVISION GROUP

TECHNOLOGY RISK MANAGEMENT (TRM) GUIDELINE FOR INSURERS AND HOLDERS OF A CAPITAL MARKETS SERVICES LICENCE

Network Security

1 Given the proliferation and propagation of security breaches and hacking attempts on online systems, financial institutions should be vigilant and take the following precautionary measures in respect of network security:

- conduct systems penetration testing and network vulnerability assessment regularly and take prompt action to improve security.
- apply latest vendor-supplied systems upgrades and software patches to enhance security.
- remove all unnecessary services and functions on website servers which could pose security risks.
- ensure all changes to system/firewall configurations and security parameters are evaluated, documented, tested and approved.
- review contracts with security product vendors to ascertain the adequacy and effectiveness of their products, services and procedures.
- monitor, report and respond to suspicious network traffic.
- maintain up-to-date incident response procedures, contingency planning and recovery preparedness.
- implement end-to-end encryption security pertaining to customer passwords and other sensitive data.

System Security

2 The principles of system security encompass the authenticity, reliability, integrity, accuracy and completeness of systems functions, operations and the data processed, stored or transmitted. A high level of system security should be achieved consistent with the nature, scale and complexity of the institution's operations and systems environment.

3 System defects and deficiencies should be detected early at the system design stage or during testing. Financial institutions should establish a robust software development lifecycle framework that includes the following functions and processes:

- A steering committee consisting of various management, development and user stakeholders should be established to provide oversight and to monitor the progress of major projects.

- User functional requirements, systems design and technical specifications should be documented and approved at appropriate management levels.
- Security requirements relating to system access control, authentication, transaction authorisation, data integrity, system activity logging, audit trail, security event tracking and exception handling should be clearly specified.
- A system validation methodology to ensure comprehensive test coverage of business logic, security controls and system performance under various stress-load scenarios and recovery conditions should be established.
- Separate physical or logical environments should be maintained for unit, integration, system and user acceptance testing (UAT).
- Access to the UAT environment by vendor and developers should be strictly controlled and monitored.
- UAT sign-offs should be obtained from project and user management and properly documented.
- Systems changes and updates to the production environment should be strictly validated, approved and documented.

Password Protection

4 The protection of customer passwords is of paramount importance for online systems. Financial institutions should implement the following specific control measures to safeguard customer passwords:

- deploy hardware security modules or similar tamper-resistant devices to perform encryption and decryption of passwords.
- implement dual control and segregation of duties in the generation of passwords, printing of password mailers and activation of online accounts.
- print password mailers in a secure location where physical access is restricted and monitored.
- ensure all mailer spoilages are destroyed immediately and a new password is generated for each reprint.
- destroy all stationery which may contain any password imprint during mailer printing.
- strengthen the password dissemination process and ensure that clear-text passwords would not be exposed or compromised.
- ensure that passwords are not processed, transmitted or stored in cleartext or as hash values in the systems or networks.
- require customers and system users to change issued or new passwords immediately upon first login.

Two Factor Authentication

5 Strong authentication can be achieved through the use of two factor authentication (2FA). Financial institutions are encouraged to adopt 2FA for login to online systems, such as online trading platforms and insurance portals for policyholders, and for transaction authorization. Any two of the following factors would constitute 2FA:

- What you know (eg. password)
- What you have (eg. one-time-password token)
- Who you are (eg. biometrics)

6 Back-office staff, trading representatives and insurance advisors who are able to access multiple customer accounts and critical back-office¹ functions are deemed to be privileged users. Consequently, financial institutions should consider implementing 2FA for privileged users who perform high risk transactions such as funds transfer, payment and settlement.

Data Loss Prevention (DLP)

7 The continuing progression and growing diversity of distributed processing, remote systems access, telecommuting² arrangements and the use of endpoint devices³ with data storage capabilities by trading representatives, insurance advisors, mobile sales force and financial advisors, have increased security risks associated with data confidentiality and accessibility.

8 Conventional logical access controls which largely focus on managing access rights to system resources and data have been rendered inadequate to prevent the theft or loss of confidential data with the advent of a growing miscellany of endpoint devices. Financial institutions should develop a comprehensive DLP strategy to protect confidential data, taking into consideration the following specifications:

- Data in Motion – data that traverses a network or transported between sites.
- Data at Rest – data in computer storage which includes files stored on servers, databases, backup media and storage area network (SAN) etc.
- Data at Endpoint – data which resides in notebooks, personal computers, portable storage devices etc.

9 For effective protection of data, financial institutions are expected to have in place data security classification policies which address network, host-based and end-point security. In particular, sensitive data such as clients' policy information, health information, investment portfolios and personal particulars stored in endpoint devices should be protected by strong encryption⁴.

¹ Back-office functions include customer account maintenance, password reset, password printing, accounting, settlement, account enquiry, rate maintenance, credit approval etc.

² Telecommuting or working off-premises is a work arrangement which accords employees the flexibility in working location and hours.

³ Endpoint devices include laptops, notebooks, thumb-drives, flash memory cards, mobile phones, ipod, PDA, Blackberry, CD/DVD/BlueRay and any portable optical or magnetic disks.

⁴ Appropriate controls for handling of sensitive data printed on hard copies should also be implemented.

Outsourcing and White Labeling

10 An increasing number of financial institutions have outsourced the management⁵ and operation of online systems to third-party service providers or intra-group entities. A popular outsourcing model is the adoption of white-label solutions where the system, owned and operated by a vendor, is offered to customers under the name of the financial institution.

11 As spelt out in MAS Guidelines on Outsourcing, financial institutions are expected to be cognizant of the risks associated with different types of outsourcing models. It is imperative that prior to entering into an outsourcing relationship, thorough due diligence is exercised to ensure that the service provider is able to deliver the level of performance and service required. The performance of service providers should be closely monitored against clearly defined service levels and security standards.

12 MAS supervisory power and its ability to carry out its supervisory functions should not be hindered in any way by any outsourcing arrangements between financial institutions and their service providers. Every financial institution should ensure that its outsourcing contract contains specific provisions that enable MAS to obtain whatever information, reports, documentation, systems access, functions, data and facilities from its service providers that are required for MAS to fulfil its regulatory functions and objectives.

Disclosure of Security Incidents

13 Financial institutions should have an open policy of disclosure of security incidents and intrusions affecting their customers. Public announcement of such events, including mitigating measures taken, should be made in the most timely and prudent manner, taking into account the need to maintain customer confidence. Hacking, system security incidents and intrusion offences must be promptly reported to MAS as well as the police so that appropriate action can be taken.

⁵ Functions that are commonly outsourced include server hosting, application development, system maintenance, disaster recovery etc.