DREW & NAPIER

DREWTECH SERIES

CHAPTER 8

New risks in new skins – Updates to the Guidelines on Risk Management – Technology Risk

3 March 2021

LEGAL UPDATE

In this Update

In recognition of the intensified risks to financial institutions associated with existing and emerging technological solutions, the Monetary Authority of Singapore has released its revised Guidelines on Risk Management Practices – Technology Risk earlier this year, providing the guidance for the new and ever evolving technology risks.

This article examines the recent changes as well as key points to note.

INTRODUCTION

Earlier this year, the Monetary Authority of Singapore ("**MAS**") released its revised Guidelines on Risk Management Practices – Technology Risk ("**TRM Guidelines**)'. The MAS's revisions to the TRM Guidelines seek to provide guidance for the new and ever emerging technology risks faced by financial institutions ("**FIs**") in the rapidly evolving technological landscape.

The revisions to the TRM Guidelines focus on four key areas:

(a) technology risk governance and oversight;

(b) software development and management;

(c) emerging technologies; and

(d) cyber resilience.

The revisions to the TRM Guidelines also incorporate circulars regarding technology risk issued by the MAS after the TRM Guidelines were released in 2013 (including those on vulnerability assessment and penetration testing (May 2014), IT security risks posed by personal mobile devices (September 2014), early detection of cyber intrusions and technology risk (August 2015) and cyber security training for FI's board of directors (August 2015)). The MAS's revisions represent the first major revision to the TRM Guidelines since the MAS consolidated and replaced its existing MAS Internet Banking and Technology Guidelines and past circulars on IT risk management into the first edition of the TRM Guidelines back in June 2013.

This article briefly examines the MAS's recent revisions to the TRM Guidelines and highlights points to note.

KEY CHANGES

The revisions to the TRM Guidelines focus on four key areas:

(a) technology risk governance and oversight;

(b) software development and management;

(c) emerging technologies; and

(d) cyber resilience.

In this section, we take a closer look into the changes in each area and highlight some key revisions.

Technology risk governance and oversight

Robust technology risk management starts at the top, and the revisions reflect the recognition that the board of directors and senior management of FIs play an integral role in the oversight and management of technological risk. The revisions are thus aimed at ensuring that the FI's board of directors and senior management are adequately equipped to handle technological risk, as well as reiterating the responsibility they have in determining the FI's risk culture and management framework.

The previous TRM Guidelines only provided generally that the board of directors should have oversight of technology risk and be involved in key technology decisions. In contrast, the revised TRM Guidelines set out specific roles which should be included in the FI's board of directors and senior management, such as a Chief Information Offer, Chief Technology Officer/Head of IT, and a Chief Information Security Officer/Head of Information Security. These individuals should have the requisite experience or expertise (although the TRM Guidelines do not define what this means).

The revised TRM Guidelines also sets out discrete responsibilities for the FI's board of directors and senior management. While these may arguably already have been implicit under the previous TRM Guidelines, the listing of specific and discrete responsibilities is welcome guidance and clarity on what is expected of FIs.

FIs should also note the express guidance on establishing information asset management practices and third-party management practices, which were not explicitly provided for in the previous TRM Guidelines. To this end, FIs should ensure that they have clear oversight of all information assets that support the FI's business, their risk classification, and the people that manage such assets. FIs should also ensure that third-parties which provide services to the FI employ a high standard of care and diligence in protecting confidentiality and ensuring system resilience. The importance of this was recently highlighted in the SolarWinds hack and the Singtel data breach, where secure systems were compromised not necessarily because of vulnerabilities in one's own systems but through those provided by a third party.

Software development and management

The revised TRM Guidelines also provides new guidance on the specific standards that FIs should adopt when developing and managing software applications. While FIs are taking development of their software in-house, there is still a reliance on open source and third-party software providers and their products. The revisions to the

TRM Guidelines address both in-house and outsourced software development by requiring that FIs adopt appropriate and industry standard security principles in its software development process, as well as keeping track of updates and reported vulnerabilities for third-party and open-source software code incorporated into the FI's software.

Emerging technologies

We live in an era of rapid technological advancement, and with new technology comes new technology risks. In such an ever-changing landscape, the revisions to the TRM Guidelines seek to provide guidelines on how to manage risk arising from new technologies by looking at the specific stress points associated with the use of new technologies. The TRM Guidelines now has specific sections addressing proper application programming interface ("**API**") development, virtualization technology and the Internet of Things. However, the basics remain the same – know what you have, know what you are connecting to, know who is connecting to you, and know what is going on.

APIs are essentially applications which allow software to "talk" and "interact" with each other. Thus, where new technologies are concerned, it is not uncommon for API's to be developed and used for the new technology to "talk" to and connect with the older technology. The revisions to the TRM Guidelines recognize that this may presents particular vulnerabilities, and provides that it is the FI's responsibility to manage the development and provisioning of APIs for secure delivery of new technologies. Thus, apart from screening third parties looking to connect to the FI's network through APIs, the FI should ensure that the API "keys" (credentials which validate the party using the API) and any transmission through the APIs are technologically secure. It is also important for FIs to test APIs thoroughly before deployment, lest an API function in an unintended manner which could lead to a security risk. Real-time monitoring of APIs should also be deployed to provide visibility and detect any suspicious activities.

The TRM Guidelines also now provide express guidance for virtualization security in recognition of the increased adoption by companies of virtualization technology. Virtualization is a technology where virtual machines (for example, an end user's desktop) is hosted on a central physical system, and the individual logs into the simulated (virtual) environment to access the system. One key benefit of virtualization is that an individual is no longer tied to his or her physical desktop (being able to log in to the virtual environment as long as he/she has an internet connection), the importance of which has been keenly brough to the fore during the COVID-19 pandemic. However, despite being a relatively "new" technology, the essentials remain the

same – ensure that access to the main operating system is strictly controlled, and that there are robust policies in place to track the creation, use and destruction of virtual images.

The TRM Guidelines also addresses one of the hottest buzzwords in town – the "Internet of Things" ("**IoT**"), the network of physical objects connected by the internet or the FI's network which exchanges information and data with each other. This is in particular relevant for insurance companies, which may seek to leverage the IoT to obtain more data from its customers and offer better/targeted discounts and promotions (one example being tying discounts and offers to how active its customer is). The TRM Guidelines provide that an FI should maintain an inventory of all its IoT devices, secure networks which host IoT devices or even segregate such networks from those which host core systems and confidential data, maintain proper access control, and monitor traffic to and from IoT devices.

Thus, while the revised TRM Guidelines provides welcome and specific guidance on how FIs should tackle new and emerging technologies, a closer look at the guidelines reveal that the basics remain the same – know what you have, know what you are connecting to, know who is connecting to you, and know what is going on.

Cyber resilience

It is now important for organizations to proactively ensure that their systems are cyber resilient. The SolarWinds attack briefly mentioned above affected even established cybersecurity companies. As the prevalence and intensity of such attacks escalate, organizations must increase their guard and maintain heightened standards against cyber risks. FIs are even more tempting targets for cyber rogues because of the valuable information they deal in.

In recognition of this, the TRM Guidelines require that FIs put in place measures to ensure their cyber resilience, i.e. the ability to withstand adverse conditions and continue operations with minimal disruption.

To this end, FIs should ensure that their systems have sufficient redundancy and resilience in place. This includes steps such as diversifying their networks and communication systems, putting in place environmental controls such as fire systems and humidity controls, and limiting physical access to data centers. All these should be performed under a framework which considers the threats and vulnerability of the organization's systems and takes into account weaknesses in the existing system architecture.

In preparation for an eventuality that the primary systems may go down, FIs should also put in place a disaster recovery plan with recovery time

objectives (the target time at which systems are restored) and recovery point objectives (the target age of the files that are restored). This framework should be reviewed at least annually, and backup systems tested periodically to ensure their availability in the event of a failover from the primary system.

While placed in a new context, these measures are not broadly different from existing paradigms for organizational resilience. At a high level of abstraction, the requirements are that there be a clear policy and procedure to be taken in the event of an adverse event, with measures to address identified risks and regular testing of these procedures, akin to a fire evacuation plan.

IMPLICATIONS MOVING FORWARD

KEYPOINT

The MAS TRM Guidelines represent a positive step to be taken in light of the growing reliance on technology, coupled with an increase in the brazenness and prevalence of cyberattacks.

Both as a matter of compliance with the TRM Guidelines, as well as a matter of sensible prudence, organisations would be well advised to carefully consider how they can best harden their infrastructure to deal with risks arising from the use of technology and exposure to possible attack vectors, while remaining supple and responsive to deal with any adverse conditions which impacts their operations.

UPDATES IN DREWTECH SERIES

1. Chapter 1: The Importance of an Exit Strategy in Technology Contracts <6 March 2019>
2. Chapter 2: Employees, Technology and A Legal Hangover – Bring Your Own Problems? <4 June 2019>
3. Chapter 3: I host, you post, I get sued? <24 September 2019>
4. Chapter 4: Diabolus ex machina <18 February 2020>
5. Chapter 5: Bringing hygiene online – the MAS notice on cyber hygiene <28 April 2020>
6. Chapter 6: Signing without signing – contactless contracts <16 July 2020>
7. Chapter 7: My Kingdom for a Horse – When your Systems are Held to Ransom <22 January 2021>

8. Chapter 8: New risks in new skins – Updates to the Guidelines on Risk Management Practices – Technology Risk <3 March 2021>

If you have any questions or comments on this article, please contact:

Rakesh Kirpalani
Director, Dispute Resolution &
Information Technology
Chief Technology Officer
T: +65 6531 2521
E: rakesh.kirpalani@drewnapier.com

Drew & Napier LLC
10 Collyer Quay
#10-01 Ocean Financial Centre
Singapore 049315

www.drewnapier.com

T : +65 6535 0733
T : +65 9726 0573 (After Hours)
F : +65 6535 4906

DREW & NAPIER