KPMG
cutting through complexity

Financial Services Briefings

Issue 05 February 2012
MICA (P) 160/02/2011

Foreword

Every business, regardless of maturity or industry, faces threats of cyber risks.

Past experiences have shown that Singapore is not immune to cyber attacks. Cyber criminals have moved beyond hacking to launching the theft of intellectual property or confidential data. Future cyber crime attacks are also likely to become more complex and difficult to detect and prevent as attackers become increasingly sophisticated in infiltrating computer networks.

It is the responsibility of every business to understand and address the risks they face. Singapore is in the process of setting up a National Cyber Security Centre in the coming months to boost its capacity to counter cyber security threats. To be led by the Singapore Infocomm Techology Security Authority (SITSA), the National Cyber Security Centre will also be the key contact point in Singapore's collaboration with international partners in combating cyber threats.

In this issue, we discuss this area of growing interest – the Advanced and Persistent Threats (APTs). This form of cyber attack focuses on the unique vulnerabilities of the target and is coordinated by an organisation to attack a specific target. We talk about how these risks can be mitigated and why it is important to do so right now.

As in the past issues, we highlight pertinent accounting, regulatory and tax changes of relevance to the financial services industry.

Leong Kok Keong
Partner, Head of Financial Services
KPMG LLP

Contents

Advanced Persistent Threats: Understanding the New Realities of Cyber Risk

This article is contributed by Victor Keong, Partner, Management Consulting at KPMG in Singapore.

Lightning-quick change is an accepted fact of life in the cyber world, where the constant development of new hardware and software sees the latest technologies rapidly eclipsing their predecessors.

Unfortunately, the same is true when it comes to computer-related threats. Well-funded criminal elements ensure a steady supply of sophisticated and evolving cyber attacks intended to stay one step ahead of the defences. Barely a week goes by in recent years without news of a major cyber security breach grabbing headlines around the world.

One area of growing interest—and concern—in this arena is Advanced and Persistent Threats (APTs). An APT is a cyber attack funded and coordinated by an organisation to attack a specific target, such as a pre-identified individual or organisation with the intention of stealing confidential data or intellectual property. In a research paper titled 'Operations Shady Rat' published by McAfee in 2011, 70 global organisations were found to be victims of APT, of which 12 were large financial services institutions.

Targeted attacks

While attacks from harmful computer viruses or other forms of malware are commonplace in the cyber world, these tend to be opportunistic in nature. They tend to spread widely without a specific target in mind, attacking any and all vulnerable systems to which they can gain access.

In contrast, APTs are designed with a specific target in mind, often involving extensive research and planning to tailor the attack to the unique vulnerabilities of the target. In September 2011, such targeted attacks against financial institutions in Singapore led to the Association of Banks issuing a specific press release to warn online banking customers to be mindful of such targeted attacks.

As their name suggests, APTs are advanced. They typically attack via 'zero-day' vulnerabilities, which are those inherent in software or systems and unknown to their developers. APTs gain a head-start by embedding themselves within their target system before the system owners become aware of any threat.

As most of today's antivirus solutions are signature-based with some heuristic or self-adaptive capabilities, they are often unable to detect APTs given that the latter have unknown signatures.

APTs are also polymorphic in nature, changing their behaviour once inside their target in order to evade detection. Using command-and-control servers based outside their targets, hackers are able to direct the actions of the APT, such as seeking out further

vulnerabilities to exploit it from within the organisation.

Another unique characteristic of APTs is that they are persistent. As they are designed to target a specific objective rather than achieve an opportunistic short-term gain, APTs will sometimes lie dormant for extended periods of time. They are then activated, as the hackers behind them put in place other elements required for a coordinated attack.

Furthermore, hackers will often install more than one variant of the APT within the target, making the threat resistant to complete removal even if one of its elements are detected and removed.

Weak defences

Even when they are aware of the risks posed by APTs, organisations face several challenges in combating them. Typically, end-users are the weakest link in the defences. While often there are legitimate reasons for employees to access the Internet in the course of their work, it takes only a momentary lapse in judgement—such as downloading free software or opening an attachment from an unknown sender—for one employee out of thousands to compromise an organisation's systems.

While APTs typically attack via previously unknown vulnerabilities, an organisation can remain at risk even after the vulnerability in a program or application is identified. This is because it takes time for a software vendor to develop, distribute and apply a patch.

Even when a security patch is made available, many organisations will first conduct quality assurance tests to ensure that the functionality of their systems will not be adversely affected by the patch. This further extends the period of vulnerability.

Monitoring and detection are critical tasks in the ongoing battle against APTs. Real-time automated monitoring of networks and hosts can help organisations identify threats at the earliest possible stage.

One of the first high-profile APT attacks was Operation Aurora, which took place in the second half of 2009. Targeting at least 34 companies in the technology, financial and defence sectors, including Google and Adobe, the attack showed that even companies with highly advanced cyber defences were vulnerable to cyber threats.

The public admission by RSA, maker of the highly secure two-factor tokens used by many of us to authenticate ourselves into sensitive systems being a victim of APT in March 2011 has shown that no one is immune to APT.

Another example was an attack launched against the French government's finance ministry in 2011 by hackers targeting information related to the Group of 20 (G20) nations. The attack compromised 100 computers in the ministry's central services and resulted in 10,000 computers being taken offline.

Reducing the risks

The existence of such sophisticated threats begs the question: What can be done to protect us against APTs? While their very nature ensures that APTs will continue to pose a serious and enduring problem, there are steps that can be taken to minimise and mitigate the risks that they pose.

Monitoring and detection are critical tasks in the ongoing battle against APTs. Real-time automated monitoring of networks and hosts can help organisations identify threats at the earliest possible stage.

Early detection of APTs also provides an organisation the best possible chance of taking action against the

threat while minimising negative fallout. Typically, the longer an APT has had to burrow into an organisation's systems, the firmer its foothold will be and thus the harder it will be to remove.

Analysis and response are another key step in defending against APTs. Once a threat has been identified within an organisation, a swift response comprising investigation, analysis and remediation is essential. These activities generally require experienced professionals with a highly sophisticated understanding of both the organisational and threat environments.

Finally, post-incident reporting and forensic investigation play an important role in dealing with the fallout from APTs and minimising their ability to cause further harm.

Forensic investigations are used to identify, recover and preserve evidence from an APT attack for analysis.

Forensic investigations are used to identify, recover and preserve evidence from an APT attack for analysis. This can help an organisation learn about its vulnerabilities and the modes of attack used against it. For example, network data can be captured, retrieved and stored to understand the events and activities leading up to and following an infection. Disk imaging can also be performed on hosts to support these investigations.

Finally, the intelligence gathered through such forensic activities can be used to enhance an organisation's cyber defences against future attacks.

Organisations must employ constant vigilance with the appropriate tools, and deploy a skilled team capable of adapting and responding to an evolving threat environment.

Regulatory, accounting and tax updates

Regulatory Updates

Changes in the regulations concerning Banks & Merchant Banks

Residential Property Loans – Fact Sheet

The new Monetary Authority of Singapore (MAS) Notice 632A (corresponding Notices 825A (to finance companies), 1106A (to merchant banks) and 115A (to direct insurers) is issued to introduce the inclusion of a Fact Sheet as part of the documentation in the process of providing residential property loans to customers. Refer to Form 1 of the Notice for a template of the Fact Sheet.

A Fact Sheet is to be given to the customer in the following circumstances:

1. when discussions are initiated on the key features of the credit facility for the purchase of Residential Property
2. when there are changes to the key features of the proposed credit facility for the purchase of Residential Property; and
3. when the customer wishes to re-finance or restructure an existing credit facility for the purchase of Residential Property.

In addition, at the time of or prior to the issue of the Letter of Offer for the credit facility, a written self-declaration shall be obtained from the customer acknowledging that he has received a Fact Sheet which contains the key features of the credit facility as contained in the Letter of Offer.

A copy of the Fact Sheet with the signed customer declaration shall be kept by the lender in its records. Refer to Form 1 of the Notice for a template of the declaration.

This Notice shall take effect on 1 March 2012.

Revised Regime for Fund Management companies : Draft Legislation and further proposed enhancements

Following its public consultation in April 2010 to enhance the regulatory regime for fund management (FMCs), the MAS has issued another consultation paper on 27 September 2011(recent consultation paper) on draft legislation to implement the revised regime for FMCs as well as to propose other

measures. In addition, the MAS is now proposing further enhancements to the business conduct requirements in line with international best practices for all FMCs. Pursuant to these proposed business conduct changes, FMCs will need to have in place a formalised risk management framework; the framework will be implemented over the FMC's fund management operations, suited to the size and scale of their operations, to identify, address and monitor the risks associated with the assets that they manage.

Registered FMCs will need to subject their operations to an independent audit every year, and certain representatives of Licensed Retail FMCs will have to comply with new examination requirements. In addition, two administrative measures have been proposed: (i) an online licensing and regulatory filing submission system for all FMCs, and (ii) the imposition of annual administrative fees for Registered FMCs.

Implementation timeframe

The MAS intends to issue the legislative amendments and implement the new regime in early 2012. There will be a six-month transitional period before the amendments take effect.

Accounting Updates

New Financial Reporting Standard (FRS) - FRS 110 *Consolidated Financial Statements*

The International Accounting Standard Board (IASB) issued the new consolidation standard International Financial Reporting Standard (IFRS) - IFRS 10 *Consolidated Financial Statements* in May 2011. In Singapore, the Accounting Standard Council (ASC) issued an identical FRS 110 in September 2011. The new standard replaces the current IAS/ FRS 27 *Consolidated and Separate Financial Statements* and SIC/ INT FRS 12 *Consolidation – Special Purpose Entities* and applies to all investees.

Registered FMCs will need to subject their operations to an independent audit every year, and certain representatives of Licensed Retail FMCs will have to comply with new examination requirements.

The IASB published IFRS 10 to address observed divergence in practice when entities applied the current IAS 27 and SIC 12, which could lead to different consolidation conclusions. Another criticism of IAS 27 and SIC 12 was that the requirements led to a focus on 'bright lines' and provided structuring opportunities, rather than focusing on the nature of a reporting entity's relationship with the investee.

Instead of having different consolidation models – IAS 27 that focuses on control and SIC 12 that focuses on risks and rewards – for different investees, IFRS 10 introduces a single consolidation model that is based on the principle of control to be applied consistently to all investees.

IFRS 10 builds on the concepts and principles in IAS 27 and SIC 12, and includes detailed explanations of the control principle. It also includes extensive application guidance that details factors that an entity considers in situations in which control is difficult to assess. The IASB believed that by doing so, IFRS 10 will lead to more appropriate and consistent accounting in those situations.

FRS 110 is effective for annual periods beginning on or after 1 January 2013.

Exposure draft (ED) - ED/2011/6 Revenue from Contracts with Customers

On 14 November 2011, the IASB issued the ED/2011/6 Revenue from Contracts with Customers. This ED sets out a revised version of the proposals included in the ED of the same name published in 2010.

The ED proposes a single principles-based revenue model that would apply to all contracts with customers. The ED retains the 5-step approach to revenue recognition and the focus on the transfer of control of goods and services to customers. Revenue is recognised as performance obligations are satisfied, which may occur over time or at a point in time.

The effective date of the new standard will not be earlier than 1 January 2015. The ED proposes retrospective application with limited reliefs and permits early adoption. In Singapore, the ASC has issued the equivalent proposals. The comment period will close on 13 February 2012.

Amendments to IFRS 7 Financial Instruments: Disclosures – Offsetting Financial Assets and Financial Liabilities

On 16 December 2011, the IASB issued the Amendments to IFRS 7. The amendments calls for additional disclosures in respect of:

- financial instrument that are set off in the statement of financial position; and
- financial instruments that are subject to an enforceable master netting arrangement or similar agreement, irrespective of whether they are set off in the statement of financial position.

The amendments are effective for annual periods beginning on or after 1 January 2013. The required disclosures should be provided retrospectively.

Amendments to IAS 32 Financial Instruments: Presentation – Offsetting Financial Assets and Financial Liabilities

On 16 December 2011, the IASB issued the Amendment to IAS 32. Under IAS 32, financial assets and financial liabilities can be offset in the statement of financial position only when certain criteria are met. The amendments provide further guidance on the application of these criteria, without changing the existing principles of IAS 32 on offsetting.

The amendments are effective for annual periods beginning on or after 1 January 2014 and are to be applied retrospectively.

Amendments to IFRS 9 and IFRS 7 Financial Instruments – Mandatory Effective Date and Transition Disclosures

On 16 December 2011, the IASB issued the Amendments to IFRS 9 and IFRS 7. The amendments modified the requirements on disclosures and restatement of comparative financial information upon an entity's transition from IAS 39 to IFRS 9.

In addition, the effective date for IFRS 9 Financial Instruments has been deferred to 1 January 2015. Early application continues to be permitted.

Tax Updates

Goods and Services Tax (GST) Remission on Expenses for Prescribed Funds Managed by Prescribed Fund Managers in Singapore

The Minister for Finance introduced a GST remission scheme under which funds that meet the qualifying conditions will be able to recover GST incurred on all expenses (except disallowed expenses under the GST Regulations 26 and 27) from 22 January 2009 to 31 March 2014 based on a fixed recovery rate, without requiring the funds to register for GST.

In this regard, the fixed recovery rate for expenses incurred during the period from 1 January 2012 to 31 December 2012 is 90 percent.

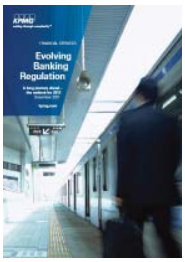
Global topics

The New World for Insurance – Preparation and readiness for accounting change, an industry survey

This publication is highlighting what insurers around the world are doing to start preparing for the forthcoming financial reporting changes.

IFRS for Investment Funds - Issue 2 (December 2011)

This publication addresses practical application issues that investment funds may encounter when applying IFRS 8 Segment Reporting. It discusses the key requirements and includes interpretative guidance and illustrative examples.



Evolving Banking Regulation – A long journey ahead… (December 2011)

The journey towards the re-shaped financial sector continues, with the implementation of current regulation and major new proposals. Our report provides a comprehensive analysis of how the current regulatory reform is changing the way banks work.

The Social Banker: a weekly series

With one in ten of the world's population already on Facebook the impact of social media is hard for banks to ignore. KPMG responds with a 12 week article series written by industry experts and our own SMEs who are providing their unique insights.

Frontiers in Tax November 2011

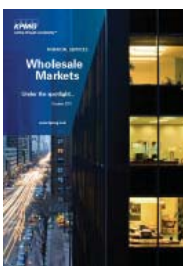
In the latest edition of frontiers in tax KPMG's Global Financial Services Tax practice focuses on some of the many regulatory issues facing financial institutions today.

Hong Kong Banking Survey 2011

The survey details the financial performance of banks during 2010, a period characterised by sustained loan growth, rising asset prices, low levels of bad debts and significant increases in the sale of investment products.

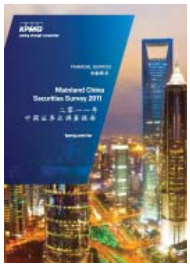
New valuation and pricing approaches for derivatives in the wake of the financial crisis (October 2011)

The survey shows that all banks have dealt with Collateral Support Annex discounting approaches for some time and have a well-defined idea regarding its implementation.



Wholesale Markets - Under the spotlight (October 2011)

Proposed rules over derivatives are game changing. This report explores the key challenges and critical areas of focus for financial institutions. It also looks at how the industry should start to position itself ahead of final rules.



Mainland China Securities Survey 2011

This is KPMG China's 5th annual survey of securities brokerage firms in mainland China. The publication outlines the opportunities and challenges facing securities brokers in the mainland, with a focus on the mainland China's securities market outlook.

To obtain any of the reports, please send a request to sg-marketing@kpmg.com.sg.

Contributors to this issue

Leong Kok Keong
Partner, Head of
Financial Services
T: +65 6213 2008
E: kokkeongleong@kpmg.com.sg

Ho Wah Lee
Partner,
Head of Advisory
T: +65 6411 8008
E: wahleeho@kpmg.com.sg

Tay Hong Beng
Partner,
Head of Tax
T: +65 6213 2565
E: hongbengtay@kpmg.com.sg

Yvonne Chiu
Partner,
Chief Editor
T: +65 6213 2323
E: yvonnechiu@kpmg.com.sg

Victor Keong
Partner,
Management Consulting
T: +65 6411 8282
E: vkeong@kpmg.com.sg

Gary Chia
Partner,
Risk & Compliance
T: +65 6411 8288
E: garydanielchia@kpmg.com.sg

Alan Lau
Partner, Financial
Services - Tax
T: +65 6213 2027
E: alanlau@kpmg.com.sg

Reinhard Klemmer
Partner, Accounting
Advisory Services
T: +65 6213 2333
E: rklemmer2@kpmg.com.sg