

## Foreword

### Cybersecurity at the fore



Cybersecurity continues to be a source of concern for financial institutions. Financial institutions are attractive targets for hackers who are systematically looking for vulnerabilities and the most lucrative payoffs. Events of the past year underscore the need for organisations to improve their cyber-defence capabilities. The costs of cyber-attacks are substantial. Affected organisations suffer loss of reputation, and more tangibly, share prices could suffer as worried customers move their business elsewhere.

In response, financial institutions have been beefing up their cybersecurity

defences. Many understand the need to set aside a budget for this purpose. The challenge for organisations is to determine the appropriate level of cybersecurity needed and the amount of resources to be dedicated. The return of investment on cybersecurity is in the form of loss avoided and not necessarily profit gained. These and other considerations on developing a cybersecurity framework are discussed in this issue.

#### **Leong Kok Keong**

Partner, Head of Financial Services  
KPMG in Singapore

## Contents



### **Return on Cybersecurity defences**

Discuss factors to consider when deciding how to make the most of your cybersecurity investment.



### **Regulatory, tax and accounting updates**

Highlights recent updates to regulatory, tax and accounting changes that may have an impact on your business.



### **Global topics**

Showcases some of the latest reports, whitepapers and publications on the financial services sector from KPMG.



# Return on Cybersecurity defences

**Boards, audit committees and corporate leaders are rightly starting to ask what value has been gained from cybersecurity investment, which continues to expand at an exponential rate. Already in excess of \$80USD billion in 2016, it may double to \$170USD billion by 2020.<sup>1</sup> This problem is particularly acute for financial services, as it has been the focus of cybersecurity crime. Bloomberg<sup>2</sup> has recently noted that although billions have been spent, actual return on investment continues to be subjective. Although proof of value is required for comparable investment in almost all other disciplines, cybersecurity has too often not been required to demonstrate results. Too much cybersecurity investment is undirected or made in response to a breach or regulation. Cybersecurity is now a significant investment for most financial services organisations and assurance is required that this effort is effective in reducing risk.**

By: Luke Forsyth & Daryl Pereira

## 1. The value of information

### Not all information is the same

Information has different values, too many organisations try to provide the same level of protection for all information infrastructure. Next week's financial results announcement has a different value compared to last year's Christmas party invitation. Managing cyber-risk requires making an accurate assessment of the value of information. The CEO needs different information, controls and equipment to those provided for a graduate trainee. Although financial services information

has comparatively calculable value in comparison to many other industries, this value is often considered implicit and not given the specific valuation that may be found in other industries such as energy or pharmaceuticals.

### Information Asset Valuation

Like many other fields of risk management, cybersecurity is enabled by realistic asset values. Many other assets with non-obvious value, such as organisational reputation or personnel injury, have successfully had a realistic financial value assessment. Information is a comparatively easy asset to value,

using methods such as the cost of its creation or its impact on the revenue it enables. The valuation of financial services information can also provide a wider benefit in providing greater granularity of "intangible" asset valuation.

### Make use of the regulation

Regulation can be regarded as a cost or impediment. In most jurisdictions, cybersecurity regulation and industry standards actually prove to be quite practical and useful. Rather than viewed as a box-ticking exercise, some organisations leverage the regulations to gain their full operational value. An

<sup>1</sup> Forbes, "Worldwide Cybersecurity Spending Increasing To \$170 Billion By 2020", 9 Mar 2016.

<sup>2</sup> Bloomberg, "Training companies to handle a hack", 23 Nov 2016.

example has been privacy and data governance regulation motivating efficiency and cost savings in data storage. Regulators are increasingly looking beyond a compliance focus towards a risk management centric approach to cybersecurity.

## 2. Understanding the threat

### The increasing sophistication of hacking

Hacking has now become a professional activity performed or sponsored by nation-states and organised crime. Even so-called “hacktivism” is in many known examples performed with the assistance or at least passive consent of nation-states or organised crime. High value or high profile hacking events are preceded by research into the cybersecurity technologies in use by the target organisation, as well as any weaknesses in personnel management. The efficiency of organised cyber-crime leads to the targeting of financial services, where criminal proceeds are most immediate and easily translated into transferrable reward.

### Social media, bribery and blackmail

The attack may also be advanced by information gleaned from social media and the employment of blackmail and bribery. In some cases, hacking teams have been discovered to have undertaken significant planning and rehearsal prior to executing their actual attack. Social and technical research has for some attacks been found to have commenced three years before the final attack is executed or discovered. Research into the personal financial circumstances of staff members of financial services firms has also been employed as leverage for staff collusion. A particularly acute risk is the association between illicit gambling, higher risk lending and cyber-crime organisations.

### Threats are not universal and the hackers read the financial news

Political, environmental and a range of other factors contribute to the cybersecurity threats to an organisation, as well as the finances and public profile of the organisation. For example, organisations known to

be undertaking fundraising, initiating new supply or delivery agreements, restructuring or technical transformation are at significantly greater risk of a cybersecurity attack. Each organisation has its own threats and this should then inform in which controls and technologies to invest. A comparatively small effort in threat analysis can significantly improve the selection and effectiveness of cybersecurity controls. Boards and executives considering an IPO, divestment or acquisition should be advised of the criminal and competitive risk of cybersecurity disruption targeted at this market activity.

### Cybersecurity is expensive and makes it harder to get work done

Cybersecurity technologies slow down networks and computers by placing additional resource demands on these technologies. As an example, placing security software on a phone significantly reduces its battery life and operating speed. It is not efficient for every organisation to have every available cybersecurity control or technology. Nor is it efficient for controls to be applied universally within an organisation. Onerous or unwieldy cybersecurity procedures have been leveraged for customer churn between retail banks. Unfortunately, vendors of cybersecurity products and services do not give sufficient attention to the performance impact of the cybersecurity technologies.

## 3. Designing the defenses

### Protecting the crown jewels

Once the information has been valued, then the location of information needs to be governed by this value. This may mean not allowing some information on portable devices or implementing a tiered email system. For example, at a retail and commercial bank, some emails are no longer available on phones. Move the most valuable information to the safest locations so that the availability of information is based on its value.

### Concentrate the investment on where the valuable information is

Many organisations apply their cybersecurity investment universally.

One characteristic of modern hacking is the efficiency of the criminals own cost-benefit processes, they have proven very adept at targeting high value or high profile information. Concentrate cybersecurity investment on the high value information. It is not only a sound return on investment policy but is also likely to be where the attacks will be concentrated.

## 4. Measuring the results

### The problem of measuring what hasn't happened

A common claim for a lack of available cybersecurity data for return on investment measurement is that implemented technologies have worked so well that there is very little evidence available. We know that most organisations of any substantial size, value or profile will be targeted. An early stage action in sophisticated hacking is to reduce the efficiency of cybersecurity early warning technologies. A lack of cybersecurity data is an indicator of hacking activity. This has been recently enabled by advances in big-data analytics and cyber forensics.

### Insider threat

Insider threat describes when staff make mistakes or betray the trust of their employer. It is estimated to be the root cause of at least 60% of cybersecurity incidents, with estimates range as high as 90%. It is the subject of a surprisingly low level of return on investment measurement. Analysis of the skills and behaviours of executives, IT personnel and frontline staff can be incredibly valuable in gaining early warning to limit the impact of an incident. Too many cybersecurity incident response efforts stop at diagnosis and do not look at opportunities for improvement. This is another field where big-data analytics and forensic analysis is creating a paradigm shift.

### Fraud and event analytics

Cybersecurity is an operational risk that shares many of the same probability characteristics as other types of fraud or operational events. The data sets and algorithmic tools employed in these other



risk management disciplines can assist in the measurement of cybersecurity control effectiveness.

**It is worth the effort to look for the evidence**

Some of the most valuable data to support the measurement of cybersecurity risk management does require some effort. This is particularly true of evidence of advanced hacking, but the data can be located. This analysis effort is still significantly less onerous and less expensive than the cost of implementing the relevant controls or the potential costs of a cybersecurity breach.

**Conclusion**

Gaining effective cybersecurity management information and return on investment analysis requires both effective planning and effective analysis. What is required is:

- 1 Valuation of the value and location of the information assets.

- 2 A realistic appreciation of the cybersecurity threats to the organisation.

- 3 Make the cybersecurity investment based on the information value and assessed threat.

- 4 Actively seeking information for how effective the controls are.

Too many financial services companies are making significant investments in cybersecurity without analysing the results. This is both bad investment practice but also ineffective cybersecurity. Boards and executives of financial services firms need to know that, as the main target of cyber-crime, are they reducing risk and gaining value from their investment. It really is the case that good investment management also leads to good cybersecurity.

# Regulatory and tax updates



## Regulatory Updates

### Financial Institutions

#### New Guidelines on Outsourcing Risk Management

On 27 July 2016, MAS cancelled Circular SRD TR01/2011 on Information Technology Outsourcing. This circular will be superseded by the Guidelines on Outsourcing dated 27 July 2016. The new Guidelines provide expanded guidance on risk management practices of outsourcing arrangements. The key changes include, but are not limited

to a new section on cloud computing, removal of the expectations for FIs to pre-notify MAS of material outsourcing arrangements, and revision of the definition of material outsourcing arrangements to include arrangements that involve customer information.

## Commercial Banks

### MAS Notice 609 - Auditors' Reports and Additional Information to Be Submitted With Annual Accounts

On 30 June 2016, MAS revised Notice 609 to include changes on the requirements for submission of the Reports of the Auditor of the Bank. The key changes relate to banks where an auditor of a bank incorporated in Singapore shall perform a limited assurance engagement in accordance with the SSAE 3000 (Revised), issued by the Institute of Singapore Chartered Accountants in respect of the reporting schedules submitted by the bank, under Part XII of MAS Notice on Risk Based Capital Adequacy Requirements for Banks incorporated in Singapore. These changes shall take effect in respect of the Reporting Schedules, which relate to a Reporting Date that falls on or after 31 December 2016.

### Commercial Banks, Merchant Banks, Finance Companies and Insurance Companies

### MAS Notice 645, 1115, 831 and 128 on Computation of Total Debt Servicing Ratio (TDSR) for Property Loans, and its Guidelines

On 1 September 2016, MAS announced that it has revised refinancing rules under the TDSR framework to help borrowers to refinance their existing property loans at lower interest rates and manage their debt obligations. From 1 September 2016, owner-occupied properties bought after the introduction of TDSR is exempted from the TDSR framework if the borrower wishes to refinance his housing loan. As for investment property, borrower is allowed to refinance his

property loan above the TDSR threshold if he fulfills the 2 conditions set by MAS, which are: a) able to repay at least 3 percent of the outstanding balance over a period of not more than 3 years to his financial institution under a debt reduction plan; and b) able to meet his financial institution's credit assessment.

With the revision of this framework, the Notice and Guidelines have been amended to include the definition of 'Debt Reduction Plan' and 'Outstanding Relevant Credit Facility and Arrangement'. In addition, amendments were also made with regards to conditions for computation of total debt servicing ratio, conditions for monthly repayment instalments for credit facilities, and the documentary evidence to be obtained from Borrower to determine whether the Borrower is an occupant of a property.

### MAS Notice 632A, 1106A, 825A and 115A on Residential Property Loans – Fact Sheet

On 29 September 2016, Form 1 and Form 2 of the existing Notice are amended by inserting and deleting some subparagraphs, which some additional information have been included in the forms:

- i) Under section D, checking with the FI on whether a Mortgagee Interest Policy (MIP) is required if the property is a private apartment or condominium;
- ii) Under section F, acknowledgement includes clauses on MIP where some FIs may require the borrower to take up a MIP if the borrower's private apartment or condominium is mortgaged to the FI. In addition, borrower should approach the FI for further information on financing rules if the borrower wishes to refinance the property loan.

The revised Notices took effect on 1 November 2016.

### Securities, Futures and Funds Management

### Guidelines on Criteria for the Grant of a Capital Markets Services Licence other than for Fund Management and Real Estate Investment Trust (REIT) Management SFA04-G01

On 1 November 2016, following the release of the Notice and Guidelines to CMSL holders for REIT Management SFA04-G07, Guidelines SFA04-G01 have been amended to remove the requirements for REIT management. Amendments also include the minimum Professional Indemnity Insurance (PII) requirements for CMSL holders for dealing in securities and base capital requirements for "Other" companies in the regulated activity of dealing in securities and trading in futures contract. Guidance has been provided on the definition of "Restricted Broker" and "Other" companies.

### Guidelines on Licensing, Registration and Conduct of Business for Fund Management Companies SFA04-G05

On 21 June 2016, MAS released the revised Guidelines on Licensing, Registration and Conduct of Business for Fund Management Companies; The Guidelines have been amended to provide further guidance on the minimum PII coverage. For example, the minimum PII amount applicable to a FMC should apply to each of the following baseline items:

- i) breach of professional duty by FI or its representatives;
- ii) infidelity or dishonesty of the licensee, its employees, agents or contractors; and
- iii) loss of documents evidencing title of assets belonging to customers.

### Notice on Financial Market Infrastructure standards – SFA 02A/03-N01 & SFA 03AA – N02

On 16 June 2016, MAS issued a revised Notice on Financial Market Infrastructure (FMI) standards that apply to licensed trade repositories and approved clearing houses for central securities depositories. This Notice sets out the remaining

principles in the Principles for Financial Market Infrastructures (PFMI) that an FMI has to comply with. In addition, MAS issued a new Notice for regulated central securities depositories (CSD) pursuant to section 81SV of the Securities and Futures Act (Cap. 289) (SFA). This Notice sets out the principles in the PFMI that a regulated CSD has to comply with.

MAS administers the SFA in respect of the supervision and oversight of trade repositories, clearing houses and central securities depositories in accordance with the PFMI, as set out under the Monograph on Supervision of Financial Market Infrastructures.

### Consultation Papers

#### Consultation Paper on Enhancements to Regulatory Requirements on Protection of Customer's Moneys and Assets

The Consultation Paper takes into consideration the international standards circulated by the International Organization of Securities Commission and Financial Stability Board. Some of the proposed amendments are:

- i) To expand the definition of customer's moneys to include contractual rights arising from transactions entered into on behalf of a customer;
- ii) To conduct due diligence for the selection and appointment of third party custodians;
- iii) To perform periodic reviews on such third party custodians;
- iv) To maintain information systems and controls that can promptly produce information pertaining to customers moneys and assets; and
- v) To increase disclosure to customers on the segregation, risks and consequences of the customer's money and assets.

#### MAS Proposes Further Revisions to Risk Based Capital Framework for Insurers

MAS published its third consultation paper on proposed revisions to the Risk-Based Capital (RBC) framework for insurers, taking into account feedback obtained from the industry. It will also conduct a second quantitative study to assess the impact of the revised proposals.

The latest consultation paper sets out the revised proposal with revisions such as:

- i) Capital requirements for equity investment, credit spread, counterparty default and operational risk have been re-calibrated downwards to more accurately reflect the risks they pose to insurers;
- ii) The discounting of life insurance liabilities has been adjusted to reduce the impact of short-term volatility on insurers' capital adequacy. This will enable insurers to continue providing sustainable long-term insurance solutions to policyholders.

#### Consultation Paper on New Regulatory Framework and Governance Model for Payments

In order to improve Singapore's payments landscape, MAS has issued a consultation paper on proposed amendments to the payments regulatory framework, and the setting up of a National Payments Council. The amendments aim to monitor all payment services under a single framework as well as to strengthen standards of consumer protection, anti-money laundering, and cyber security in relation to payment activities. The establishment of National Payment Council would govern scheme rules for payment systems in Singapore and will coordinate key initiatives such as promoting interoperability and adopting common standards among its members.

## Tax Updates

#### Goods and Services Tax ("GST") remission on expenses for prescribed funds managed by prescribed fund managers in Singapore

Under the GST remission scheme, funds that meet all qualifying conditions will be able to recover GST incurred on all business expenses (except disallowed expenses under GST Regulations 26 and 27) based on a fixed recovery rate determined annually, without having to register for GST. Currently, the GST remission is available to qualifying funds up till 31 March 2019.

The fixed recovery rate for expenses incurred during the period from 1 January 2017 to 31 December 2017 is 88%.

## Accounting Updates

In October 2016, FRS 102 was amended to clarify the accounting for share-based payments. The amendments will improve consistency in the following three accounting areas:

- Measurement of cash-settled share-based payments;
- Classification of share-based payments settled net of tax withholdings; and
- Accounting for a modification of a share-based payment from cash settled to equity-settled.

Once a company applies the amendments, the timing and amount of expense recognised for new and outstanding awards could change. The amendments are effective for annual periods beginning on or after 1 January 2018. Early adoption is permitted.

# Global topics



## Frontiers in Finance: December 2016

The December 2016 issue of Frontiers in Finance shows how the financial services industry is facing challenges right across the horizon.



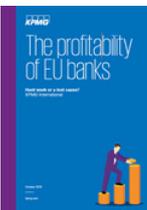
## Stress Testing - A benchmarking analysis of systemically important financial institutions

A benchmarking assessment of 19 systemically important banks, covering how they currently approach and use stress testing within their businesses, the costs, challenges and future development, and the value they and the regulators derive from it.



## 2016 Top Risks – Banking

The document highlights KPMG's view of top risks by value driver faced by corporates in the banking sector.



## The profitability of EU Banks: Hard Work or a Lost Cause?

A paper analysing the key drivers of bank profitability both theoretically and empirically, using the same data set as the KPMG Peer Bank metrics.



## Fintech 100: Leading Global Fintech Innovators 2016

Our third annual report, based on a collaborative research effort between KPMG and fintech investment firm, H2 Ventures, listing the leading 50 'Established' fintech companies across the globe, and the most intriguing 50 'Emerging Stars'.



## The Panama Papers: A KPMG Survey of Initial Responses by Financial Institutions

Panama Papers reflect Mossack Fonseca involvement in creation of secret shell companies and offshore accounts, often for prominent persons, and in connection with alleged illegal activities. KPMG Surveyed Financial Institutions to respond.



## Meet EVA: Your Enlightened Virtual Assistant and the future face of the Invisible Bank

A KPMG UK report setting out a vision for retail banking in 2030 as a disaggregated industry – with three distinct components, platform, product, and process layers - showing examples of how consumers could interact with a personal digital assistant.



## IFRS Newsletter - The Bank Statement Q3 2016 (October 2016)

A quarterly publication which provides updates on IFRS developments directly impacting banks, considers accounting issues affecting the sector, and discusses the potential accounting implications of regulatory developments.



## Money Issuance: Alternative Monetary Systems (Report)

A KPMG report, commissioned by the Icelandic Prime Minister's Office, providing an overview of the developments in public and political discussions on alternative monetary systems.



## Raising the Bar: Aligning and enhancing regulatory reporting for greater strategic advantage

An Americas FS Regulatory CoE client report highlighting key regulatory reporting challenges, strategies to address these, and how KPMG can help.



## Banking on an Agile IT Risk Management: How the financial services sector manages and secures technology risk in disruptive times

A survey based report looking at the key issues confronting financial services IT organisations and the tactics they use to manage risk proactively.



## Missing Link: Navigating the Disruption Risks of Blockchain

This paper addresses the key risk considerations to both providers and users in the blockchain ecosystem; tips for navigating the coming disruption responsibly; and a risk-based case study of trading over-the-counter derivatives using blockchain.

# Contributors to this issue



**Leong Kok Keong**

Head of Financial Services

**T:** +65 6213 2008

**E:** kokkeongleong@kpmg.com.sg



**Alan Lau**

Head of Financial Services Tax

**T:** +65 6213 2027

**E:** alanlau@kpmg.com.sg



**Gary Chia**

Head of Financial Services  
Regulatory & Compliance

**T:** +65 6411 8288

**E:** garydanielchia@kpmg.com.sg



**Yvonne Chiu**

Partner  
Chief Editor

**T:** +65 6213 2323

**E:** yvonnechiu@kpmg.com.sg



**Reinhard Klemmer**

Head of Accounting Advisory  
Services

**T:** +65 6213 2333

**E:** rklemmer2@kpmg.com.sg



**Luke Forsyth**

Principal, Cybersecurity

**T:** +65 6213 3618

**E:** lukeforsyth@kpmg.com.sg

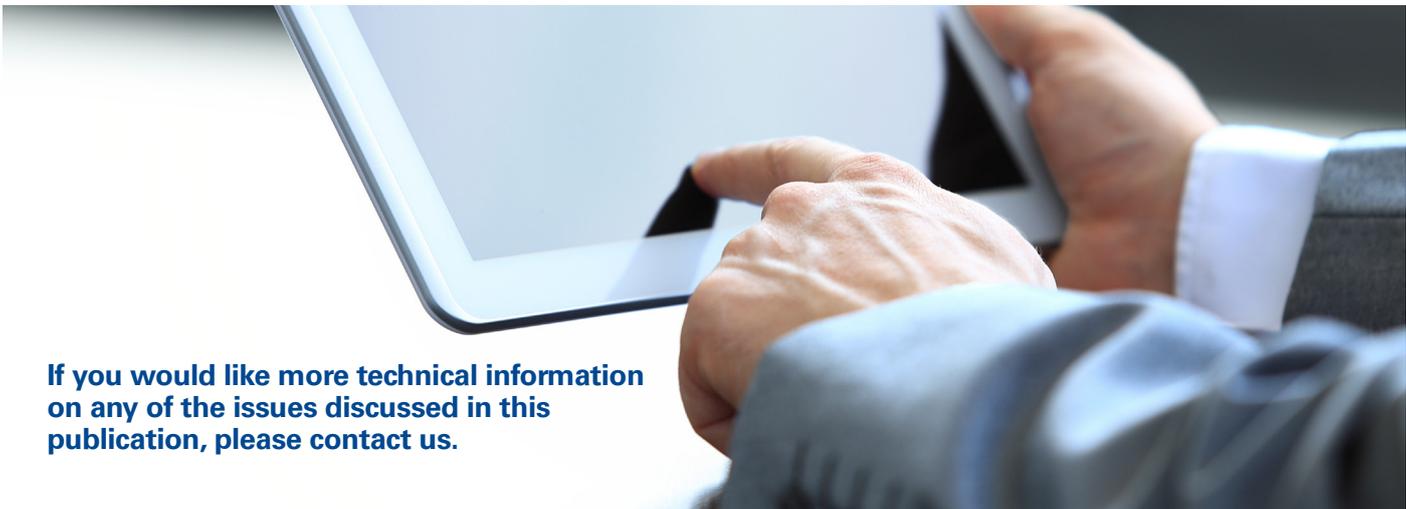


**Daryl Pereira**

Partner, Cybersecurity

**T:** +65 6411 8116

**E:** darylperreira@kpmg.com.sg



**If you would like more technical information on any of the issues discussed in this publication, please contact us.**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2017 KPMG Services Pte. Ltd. (Registration No: 200003956G), a Singapore incorporated company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Singapore.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.