KPMG
cutting through complexity

Financial Services Briefings

Issue 13 April 2014
MICA (P) 029/02/2014

Foreword

Many think that cyber attacks will never happen to their organisation.

Truth is there are almost daily occurrences of cyber attacks from individual, opportunistic hackers, to professional and organised groups with strategies to systematically steal intellectual property and disrupting businesses.

The risk posed by cyber attacks is ever present, compounded by the fact that dealing with cyber threats is a complex challenge.

Investors and regulators are increasingly challenging boards and management to step up their oversight of cyber security and calling for greater transparency around major breaches and the impact on businesses.

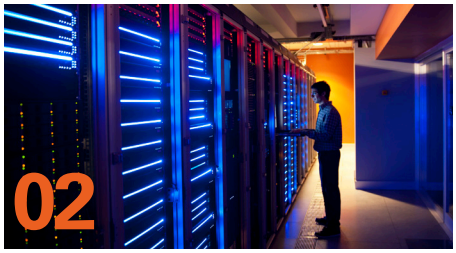
The critical challenge of protecting information systems and assets – financial information, customer data, intellectual property – and the reputational and regulatory implications of failing to do so continue to raise the stakes on cyber security and governance.

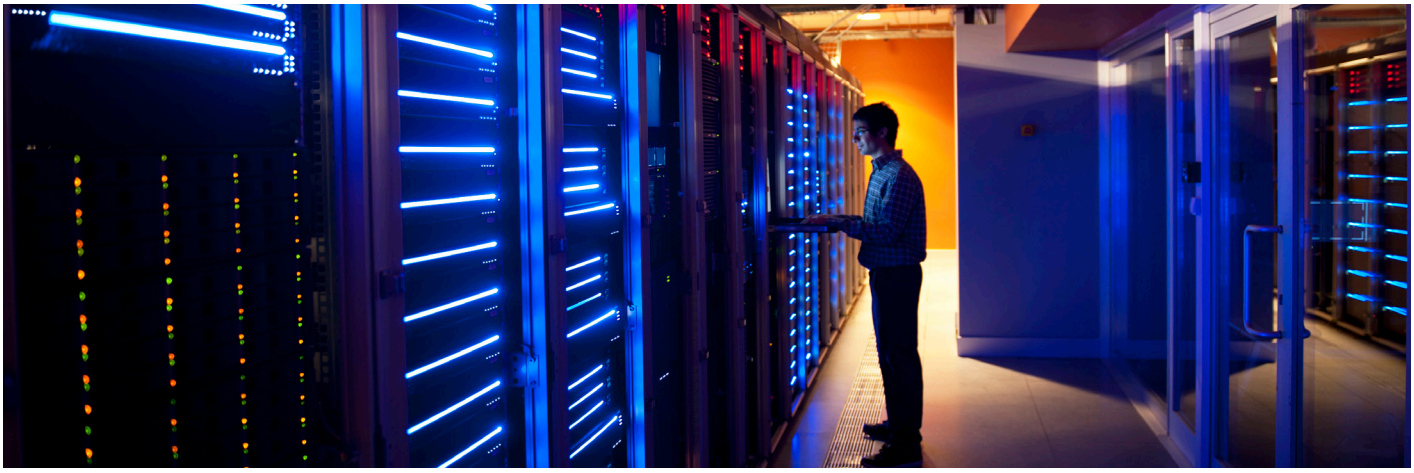
Read on to find out why large global organisations should move from a reactive to proactive operating mode in dealing with cyber threats. This calls for transformative change.

In addition to technological vulnerability, organisations must also look into core people processes, culture and behaviours so that cyber security becomes an organisation-wide approach.

Leong Kok Keong
Partner
Head of Financial Services KPMG LLP

Contents





Cyber security: the need to move from prevention to intelligence and detection

By: Lyon Poh

In the past decade, the emphasis placed on cyber security has grown rapidly. Just in the last few months, the world has seen at least three massive cyber security breaches.

Target, one of the world's largest retailers, confirmed a data breach of 40 million credit and debit card accounts last December.

In February, a Distributed Denial of Service attack designed to knock a company's systems off the internet, broke the 400 Gbps mark. This cyber tsunami smashed the previous record of 300 Gbps.

A month later, an internet security firm stumbled upon 360 million accounts and 1.25 billion email addresses up for sale in the black market.

These cyber attacks all point to a fact which could not be ignored: it is not a question of whether systems will be compromised, but when.

Cyber risk more prominent on board agendas

Cyber security breaches could threaten entire systems and in some instances, have resulted in extensive damage of physical infrastructure across critical national and corporate systems.

The World Economic Forum (WEF) has also identified cyber attacks as one of the top global risks since 2012.

In a report released earlier this year, the WEF noted that major technology trends could create between US$9.6 trillion and US$21.6 trillion in value for the global economy.

Conversely, failure to defend against cyber attacks will lead to new regulations and corporate policies, which will cost the global economy some US$3 trillion by 2020.

It is no wonder that organisations today are finding themselves under heightened scrutiny. They are increasingly subjected to legislative, corporate and regulatory requirements which demand evidence that confidential information is being protected and managed appropriately.

Cyber risk has also risen in prominence on the board agenda. Investors, governments and regulators are increasingly challenging board members to actively demonstrate diligence in this area.

Regulators expect personal information to be protected and systems to be resilient to both accidents and deliberate attacks.

The Monetary Authority of Singapore (MAS) requires financial institutions under the Technology Risk Management (TRM) to ensure monitoring and swift detection of IT incidents. Financial institutions are also expected to report discovery of any IT security incidents within one hour to MAS.

The existing cyber security landscape

KPMG's analysis of the current technology and security landscape reveals several megatrends.

For one, organisations are increasingly losing control over the computing environment.

Consumerisation of information technology (IT) and the rapid adoption of disruptive technologies increase the attack breadth and thus, strains existing defences.

Changing work patterns including remote access, big data, cloud computing and mobile technology among others all increase organisations' exposure to cyber threats.

Cybersecurity systems are also in a state of continuous compromise. The rise of sophisticated, determined and well-funded attackers performing

advanced attacks capable of bypassing traditional protection mechanisms have further increased security challenges. In some instances, threats persist undetected for extended periods.

With the pressure to optimise capital and operational spend on already constrained IT and security budgets, organisations are forced to make assumptions that existing security measures are sufficient to mitigate against today's advanced security threats.

This has challenged the ability of many organisations in acquiring, retaining and enhancing relevant talent in their workforce.

Understanding the Cyber Adversary
Cyber criminals are, of course, also aware of these vulnerabilities. The motives of cyber criminals are various, from pure financial gain, to espionage or terrorism.

Understanding the adversary, or the person or organisation sponsoring or conducting the attacks, is the first step essential for effective defence.

Adversaries can be divided into four categories:

- an individual hacker, generally acting alone and motivated by being able to show what he or she could do;
- the activist, focused on raising the profile of an ideology or political viewpoint, often by creating fear and disruption;
- organised crime, focused solely on financial gain through a variety of mechanisms from phishing to selling stolen company data; and
- governments, focused on improving their geopolitical position and/or commercial interests.
- Attacks by these different adversaries have a number of different characteristics, such as the type of target, the attack methods and scale of impact.

Understanding the adversary will go a long way towards establishing intelligence, a vital component to effective cyber security.

Why intelligence is key

Threat intelligence is growing in importance because solely relying on defence is no longer viable. The determined adversary will get through eventually.

Intelligence will help organisations know and understand the larger cyber environment. This is so that they could quickly identify when an attack has taken place or when an attack is imminent.

An intelligence capability enables organisations to identify potential threats and vulnerabilities in order to minimise the 'threat attack window' and limit the amount of time an adversary gains access to the network before they are discovered.

Organisations that take this approach understand that threat intelligence is the 'mechanism' that drives cyber security investment and operational risk management.

Prevent, detect, respond

Having a strong intelligence capability will allow organisations to effectively prevent, detect and respond to threats.

- Prevention – This begins with governance and organisation. It is about technical measures, including placing responsibility for dealing with cyber attacks within the organisation and awareness training for key staff.
- Detection – Through monitoring critical events and incidents, an organisation can strengthen its technological detection measures. Monitoring and data mining together form an excellent instrument to detect strange patterns in data traffic, find the location on which the attacks focus and observe system performance.
- Response – This refers to activating a plan as soon as an attack occurs. During an attack, the organisation should be able to directly deactivate all technology affected. When developing a response and recovery plan, an organisation should perceive information security as a continuous process and not as a one-off solution.

Managing cyber threats as part of risk management

Cyber threats should be considered a part of the company's risk management process.

Companies should start with identifying the critical information assets they wish to protect against cyber attack – the crown jewels of the firm – whether financial data, operational data, employee data, customer data or intellectual property.

More importantly, companies should focus on the perspective of the attackers and understand through a robust intelligence framework, what the threats are after and the value of assets to cybercriminals.

Companies should also determine their cyber risk tolerance and implement controls to prepare, protect, detect and respond to a cyber attack – including the management of the consequences of a cyber security incident.

Finally, organisations should monitor cyber security control effectiveness and institute a programme of continuous improvement, or where needed, transformation, to match the changing cyber threat – with appropriate performance indicators.

Transformative change for cyber security

Dealing with cyber threats today is complex and challenging. As the threat landscape evolves, a shift of focus from relying solely on preventive defence to a more detective and responsive approach is vital.

Also, intelligence and the insight that it brings is at the heart of next generation information security.

In many large global organisations, moving from a reactive to proactive operating mode requires transformative change. Technological vulnerabilities are just part of the solution. Organisations must also look into core people processes, culture and behaviours so that cyber security becomes a company-wide approach.

Regulatory and tax updates

Regulatory Updates

Commercial Banks / Merchant Banks/ Finance Companies / Insurance

Notice on Bridging Loan for the purchase of immovable property

MAS Notices 116, 633, 826, and 1107 dated 1 April 2013 are replaced with the Notices dated 29 November 2013 (collectively known as the "revised Notices"). Key revisions in the revised Notices include lending requirements on joint borrowers, where a bank in Singapore shall not grant any bridging loan to the joint borrowers that is not fully secured, unless every joint borrower has an annual income of at least $20,000 at the time of application for the bridging loan. The revised Notices are effective from 1 December 2013.

Notice on Unsecured credits facilities to individuals

MAS Notices 118, 635, 827 and 1109 dated 25 February 2009 were cancelled with effect from 1 December 2013 and replaced with the Notices dated 29 November 2013 (collectively known as "the revised Notices"). The key amendments in the revised Notices include:

- the addition of the fiancé or fiancée of the borrower, as the case may be, as a permissible joint borrower of a renovation loan, subject to certain conditions;
- obtaining an indication from the borrower of his preferred credit limit in a signed document for any request of unsecured non-card credit facility by the borrower on or after 1 June 2014; and
- disallowing any amount relating to the use of any unsecured non-card credit facility to be drawn down by a borrower, on or after 1 June 2015, if he has any amount outstanding on any credit or charge card issued, or unsecured non-card credit facility past due for 60 consecutive days or more; or if his cumulative total outstanding unsecured amount exceeds his annual income for 3 consecutive months.

Notice on Residential Property Loan

MAS Notices 115, 632, 825 and 1106 (collectively, the "Notices") dated 27 August 2013 were updated on 10 February 2014. The updates pertain to the lending requirements for refinancing facilities, where new Paragraphs 23A, 24A and 24B stipulate the conditions that are to be met before a refinancing facility may be granted.

Notice on Computation of Total Debt Servicing Ratio for Property Loans

MAS Notices 128, 645, 831 and 1115 (collectively, the "Notices") dated 28 June 2013 were revised on 10 February 2014. The revisions mainly relate to definitions, in particular, a "relevant credit facility" is amended to include any hire-purchase arrangement as set out in a hire-purchase agreement. A hire-purchase agreement means an agreement under which a motor vehicle is bailed to the hirer in return for periodical payments and the property in the motor vehicle will pass to the hirer if the terms of the agreement are met. Another key revision pertains to the purchase of Executive Condominium ("EC"), whereby, subject to certain conditions, financial institutions may not grant any credit facility / refinancing facility for the purchase of an EC, if the aggregate monthly repayment instalments for thecredit facility / refinancing facility and any other outstanding relevant credit facilities exceed 30percent percent of the borrower's gross monthly income.

Consultation Paper on the MAS's Guidelines on the Application of Total Debt Servicing Ratio ("TDSR") for Property Loans under MAS Notices 128, 645, 831 and 1115

The Guidelines dated June 2013 were revised on 10 February 2014, where revisions were made to segregate the Guidelines between owner-occupied and non owner-occupied properties to provide more clarity on the conditions to be met before any refinancing facility may be granted in excess of the TDSR threshold of 60percent.

Consultation Paper on the Review of the Banking Act (BA)

MAS issued a consultation paper dated 28 November 2013 on the proposed changes to the Banking Act to ensure that it remains current and reflects MAS' requirements and expectations. The proposed changes are also intended to strengthen MAS' supervisory oversight over banks and codify MAS' expectations as to the risk management practices that banks should implement. Key changes proposed are:

- banks are required to notify MAS as soon as they are made aware of any material adverse developments affecting the bank (including its head office and branches, or any entity in its group)
- banks are required to notify MAS as soon as they become aware of any material information which may negatively affect the fitness and propriety of any bank officer whose appointment was approved by MAS
- replace current grounds of removal of any director / executive officer under Section 54(2) with a single criterion of the director / executive officer ceasing to be fit and proper, and include "interest of the Singapore financial system" as an additional premise for such removals
- include a safe harbour provision into the Banking Act to protect bank auditors which disclose information to MAS in good faith and in the course of their duties from being held liable for breach of confidentiality or defamation; and
- prescribe the failure of bank auditors to discharge their statutory duties as an offence.

Consultation Paper on Related Party Transactions (RPT) Requirements for Banks

The consultation paper issued on 5 December 2013 sets out the proposed changes to MAS' requirements on

banks' transactions with related parties (RPTs) as prescribed under MAS Notice 643 and in the Banking Act. The proposed changes are intended to address the industry feedback that MAS has received, as well as to ensure oversight and controls over RPTs and to minimise the risk of abuses arising from conflicts of interest. Key proposed changes include:

- exempting nominal RPTs below SGD 100,000 from the scope of MAS Notice 643
- changes to definition of related parties, such as "director group", "senior management group" and "substantial shareholders' group"
- exempting intra-group transactions from the requirement to obtain prior Board approval
- extending director's declaration requirement under Section 28 (1) of the Banking Act from only credit facilities and exposures, to also include non-exposure transactions
- specifying materiality thresholds on an aggregated basis for all exposures transactions, and per transaction basis for non-exposure transactions.

Commercial Banks (Banks)

Banking (Credit Card and Charge Card) Regulations 2013 ("Regulations")

These Regulations supersede the Banking (Credit Card and Charge Card) Regulations 2004, and set out the requirements that banks have to comply with when issuing credit cards and charge cards. These requirements include but are not limited to:

- minimum requirements for issuance of credit cards, charge cards and supplementary cards
- requirements for issuance of new credit card or charge card
- requirements for increase in credit limit
- checks on income or total net personal assets
- credit checks with credit bureau
- requirements for dealing with cardholders with outstanding amounts
- disclosure requirements for card issuers.

These Regulations came into effect on 1 December 2013.

Finance Companies

Risk Based Capital Adequacy Requirements for finance companies incorporated in Singapore

MAS Notice 832 ("the Notice") which takes effect from 1 January 2015 establishes the minimum capital adequacy ratios for a Finance Company and the methodology a Finance company shall use for calculating these ratios. In addition to complying with the minimum regulatory capital requirements in the Notice, a Finance Company shall also consider whether it has adequate capital to cover its exposure to all risks.

A Finance Company shall, at all times, maintain a total capital adequacy ratio of at least 10percent, at both the Solo and Group levels.

Financial Advisors

Minimum Entry and Examination Requirements for Representatives of Licensed Financial Advisers and Exempt Financial Advisers

MAS Notice FAA-N13 was amended on 22 November 2013 to reflect the higher minimum academic requirements that an appointed representative of a financial adviser must meet. The Notice takes effect from 1 February 2014.

Securities, Futures and Fund Management

Consultation Paper on the Review of Securities Market Structure and Practices

On 1 February 2014, MAS and SGX jointly issued a consultation paper to introduce improvements to various market functions and trading practices in the securities market in Singapore.

MAS and SGX have identified three main areas of possible enhancements, namely: promoting orderly trading and responsible investing; improving transparency of intervention measures; and strengthening the process for admitting new listings and enforcing against listing rule breaches. The consultation paper discusses broad proposals addressing each of the identified areas in turn. The consultation closes on 2 May 2014.

Tax Updates

Budget 2014

The Budget 2014 Statement was tabled in the Parliament on 21 February 2014 by Deputy Prime Minister and Minister for Finance, Mr Tharman Shanmugaratnam. The Budget 2014 builds on economic and social strategies in recent years to restructure our economy and build a fair and equitable society. Several existing incentivised schemes for businesses were enhanced and extended to encourage businesses and industries to grow.

The following highlights are relevant to the Singapore financial services sector:

1. **Treating Basel III Additional Tier 1 Instruments as Debt for Tax Purposes**

   Additional Tier 1 instruments are a new type of capital instrument under the Basel III global capital standards. Under Monetary Authority of Singapore (MAS) Notice 637, Singapore-incorporated banks are required to meet the following requirements:

   - minimum capital adequacy ratios that are 2% higher than the Basel III minimum requirements from 1 January 2015; and
   - Basel III minimum capital adequacy requirements from 1 January 2013, two years ahead of the Basel Committee on Banking Supervision's 2015 timeline.

   Currently, the tax treatment of such Additional Tier 1 instruments has not been publicly clarified.

   To provide tax certainty and maintain a level-playing field for Singapore-incorporated banks which issue Basel III Additional Tier 1 instruments, such instruments (other than shares), will be treated as debt for tax purposes. Hence, distributions on such instruments will be deductible for issuers and taxable in the hands of investors, subject to existing rules.

   The tax treatment will apply to distributions accrued in the basis

period for Year of Assessment 2015 and thereafter, in respect of such instruments issued by Singapore-incorporated banks (excluding their foreign branches) that are subject to MAS Notice 637.

Further details will be released by the MAS by end May 2014.

2. Extending and refining Tax Incentive Schemes for qualifying funds

Recovery of Goods and Service Tax (GST) for qualifying funds

Funds managed by Singapore-based fund managers ("qualifying funds") currently enjoy the following tax concessions, subject to conditions:

- a.tax exemption on specified income derived from designated investments
- withholding tax exemption on interest and other qualifying payments made to all non-resident persons (excluding permanent establishments in Singapore); and
- under the GST Remission scheme, qualifying funds are allowed to claim GST incurred on expenses at an annual fixed rate set by the MAS, without having to register for GST.

Qualifying funds comprise the following:

- trust funds with resident trustee ("section 13C scheme")
- trust funds with non-resident trustee and non-resident corporate funds ("section 13CA scheme")
- resident corporate funds ("section 13R scheme")
- enhanced-tier funds ("section 13X scheme")

The sections 13CA and 13R schemes impose conditions on investor ownership levels on the last day of the qualifying fund's basis period for the relevant YA. The investor ownership levels are computed based on the historical value of the qualifying fund's issued securities.

The tax exemption schemes and GST remission scheme for qualifying funds will lapse after 31 March 2014.

To anchor and continue to grow Singapore's asset management industry, the sections 13CA, 13R and 13X schemes will be extended for five years till 31 March 2019. The section 13C scheme will be allowed to lapse after 31 March 2014.

The sections 13CA, 13R and 13X schemes will be refined as follows:

- from 1 April 2014, the section 13CA scheme will be expanded to include trust funds with resident trustees , which are presently covered under the section 13C scheme
- from 1 April 2014, the investor ownership levels for the sections 13CA and 13R schemes will be computed based on the prevailing market value of the issued securities on that day instead of the historical value; and
- the list of designated investments will be expanded to include loans to qualifying offshore trusts, interest in certain limited liability companies and bankers acceptance and this will apply to income derived on or after 21 February 2014 from such investments.

Other existing conditions of the sections 13CA, 13R and 13X schemes remain unchanged. Further details will be released by the MAS by end May 2014.

The GST Remission will also be extended for five years until 31 March 2019. The MAS will release further details of the change by end March 2014.

3. Refining the Designated Unit Trust (DUT) Scheme

Specified income derived by a unit trust with the DUT status is not taxed at the trustee level, but is taxed upon distribution in the hands of certain investors. Qualifying foreign investors and individuals (unless such income is derived through a partnership in Singapore or is derived from the carrying on of a trade, business or profession) are exempted from tax on any distribution made by a DUT.

The DUT scheme is available to both retail unit trusts and certain other types of unit trusts, which are targeted at more sophisticated and institutional investors (non-retail unit trusts). A retail unit trust refers to a unit trust authorised under section 286 of the Securities and Futures Act and is open to the public for subscription, as well as a unit trust included under the CPF-Investment Scheme.

The DUT will be streamlined as follows:

- From 21 February 2014, the DUT scheme will be limited to unit trusts offered to retail investors. Non-retail unit trusts may consider other fund schemes
- Existing non-retail unit trusts being granted the DUT scheme prior to 21 February 2014 may continue to enjoy the benefits provided under the scheme; and
- From 1 September 2014, unit trusts do not have to apply for the DUT scheme to enjoy the benefits of the scheme, subject to fulfilment of conditions.

A review date of 31 March 2019 will be legislated to ensure that the relevance of the scheme is periodically reviewed.

Further details will be released by the MAS by end May 2014.

Global topics

The Social Banker v2.0 - Social Media Lessons from Banking Insiders (January 2014)

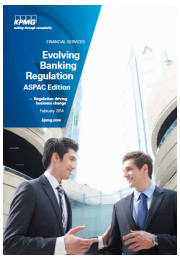
A compendium of articles from the Social Banker v2.0 series looking at how social media is being adopted within the banking sector and explores some of the new approaches that are emerging from the social sphere.

IFRS Newsletter - The Bank Statement Q4 2013 (January 2014)

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

Banking Outlook 2014 - An Industry at a Pivot Point (January 2014)

A KPMG US paper addressing the top issues facing banks and our views on what they can do now to grow revenue in this challenging environment. It also identifies a number of other areas including the challenges facing banks stemming from technology issues.



Evolving Banking Regulation – ASPAC edition (February 2014)

Insights into regulatory change in the Banking sector, based on discussion with clients, assessment of key regulatory developments and through links with policy bodies in the region.

Global Anti-Money Laundering Survey 2014 (January 2014)

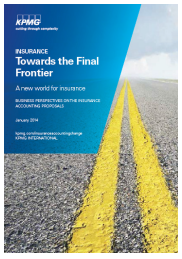
Thought Leadership Survey on how global organisations are preventing, detecting, and responding to Anti-Money Laundering (AML) compliance risks; in-depth analysis of the AML landscape and emerging areas of risk.

Operational Risk Management Excellence – Get to Strong Survey (March 2014)

A survey of leading US financial institutions, in conjunction with the Risk Management Association (RMA), on the evolution of their operational risk frameworks. It highlights next steps in the evolution of the operational risk management.

Analysis of FATCA Regulations for Foreign Financial Institutions - Withholding, Information Reporting (February 2014)

KPMG's observations following the U.S. Treasury and Internal Revenue Service (IRS) publication (20 February 2014) of a regulation package containing substantive changes to the final regulations under the Foreign Account Tax Compliance Act (FATCA).



Towards the Final Frontier - Business Perspectives on the Insurance Accounting Proposals (January 2014)

In this publication we examine the most important implications for insurers to consider regarding the accounting proposals from the IASB and FASB -impacts on relevant systems, processes, product strategy and design and the organisation's people.

FATCA: Key Action Steps Required by Funds for FATCA Compliance (March 2014)

The Foreign Account Tax Compliance Act (FATCA) is a complex reporting and withholding regime enacted with a goal of achieving greater tax transparency by enforcing disclosure by certain non-US entities of US persons' offshore accounts, investments, and income.

Contributors to this issue

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

Andrew Tinney
Head of Financial Services Advisory
T: +65 6411 8026
E: andrewtinney@kpmg.com.sg

Alan Lau
Head of Financial Services Tax
T: +65 6213 2027
E: alanlau@kpmg.com.sg

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

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

Lyon Poh
IT Assurance
T: +65 6411 8899
E: lpoh@kpmg.com.sg

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