KPMG

cutting through complexity

Cyber Risks in Emerging Markets

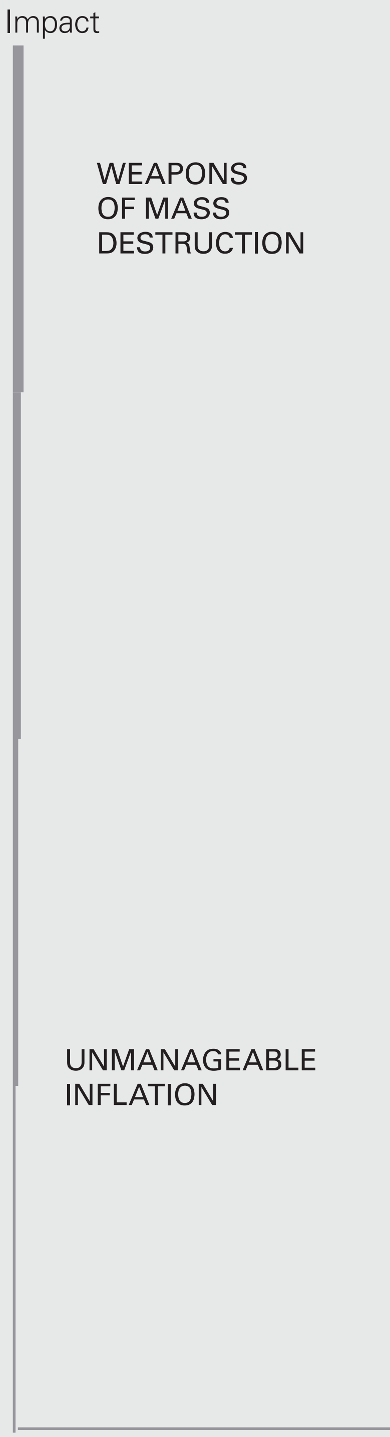
Highlights

While developed markets may today bear the brunt of cyber breaches, emerging markets are no less vulnerable. Their risks arise from weak processes and governance, the complexity of global supply chains, the need to remain low cost to attract investment, and the rapid adoption of technology without adequate cyber defences.

Improving cybersecurity will require:

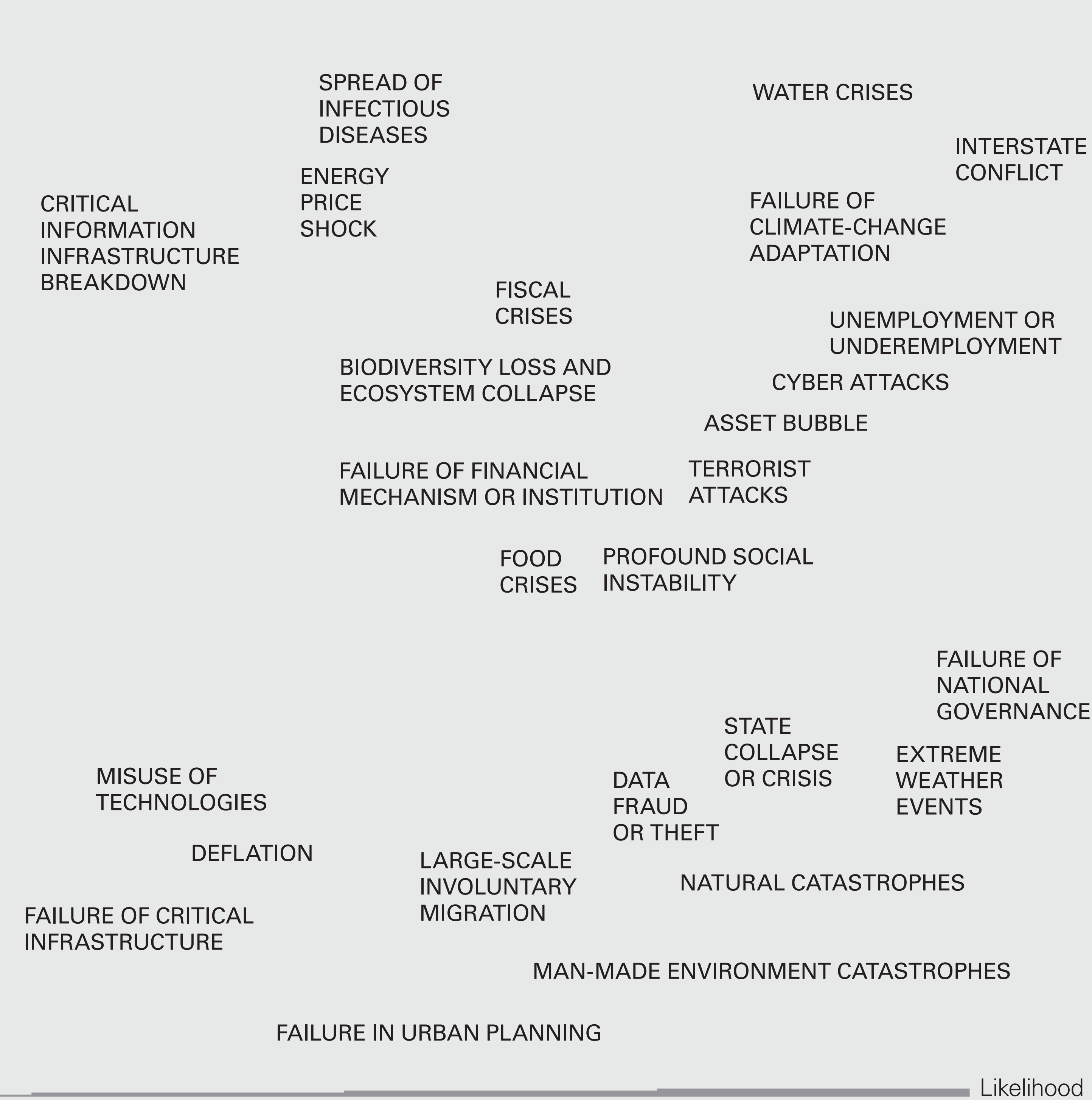
- PUTTING IN PLACE A SET OF BASIC CYBER PRECAUTIONS
- TESTING FOR VULNERABILITIES IN SOFTWARE DESIGN AND OPERATIONS
- IDENTIFYING AND MONITORING CRITICAL DIGITAL ASSETS, BUILDING DEFENCE AROUND THEM
- PREPARING AN INCIDENT RESPONSE PLAN
- EXPANDING CROSS-INDUSTRY COOPERATION

Global Risks Landscape



SOURCE: World Economic Forum, Global Risks 2015

2015



World Economic Forum (WEF) forecasts that delays in adopting cyber security capabilities could result in $3 trillion loss in economic value by 2020.

SOURCE: World Economic Forum, Risk and Responsibility in a Hyperconnected World

Foreword

Defending the cyber frontier

Over the last three years, Indonesia has suffered 36.6 million cyber attacks.[1] In Malaysia, cyber crime was estimated to have shaved off over $560 million from its GDP in 2013.[2]

In the World Economic Forum Global Risks 2015 report, cyber attacks were ranked alongside unemployment and climate change as one of the top 10 most significant long term risks worldwide.

This reflects the joint threats posed by increasingly sophisticated cyber attacks and the rise of hyper-connectivity. More systems are now being hooked up to the Internet and ever more sensitive personal data is being stored by companies in these systems.

Beyond cyber attacks lies the threat of a breakdown in critical information infrastructure and data fraud, two other emerging technology risks.

Governments have increasingly woken up to the seriousness of the cyber threat. To keep on top of the risks, more regulators have hardened their stance on cyber security. Within the developed world, the fines payable for not protecting clients' data are hefty in regulated industries such as financial services and healthcare.

Beyond the direct costs of business interruption and restoring crucial proprietary electronic information, weak cyber defences can therefore lead to reputational loss and remediation expenses.

With many countries in the ASEAN region hosting a growing share of global supply chains, multinational companies cannot simply address cyber security risks only in their own organisations.

A small chink in their cyber security armour can occur anywhere along their supply chain spanning developed and emerging markets, subsidiaries and third-party vendors. This weak link in the chain can open their entire supply chain to attack.

Besides considering the usual cost, efficiency, responsiveness and quality considerations in building a global supply chain, cyber security is practically a 'hygiene' factor. Companies ignore strengthening cyber security in their global supply chains at their own risk.

We hope that this publication will contribute to the broader discussion of cyber security, and welcome your comments.

Ho Wah Lee
Head, Emerging Markets
Head, Advisory
KPMG in Indonesia

[1] Government to set up national cyber agency. The Jakarta Post, 7 Jan 2015

[2] Center for Strategic and International Studies (2015). Net Losses: Estimating the global cost of cybercrime

THE WEAK LINK OF EMERGING MARKETS

New entrants pose new risks

Information technology has enabled supply chains to evolve into interdependent material, financial and information flows.

While increasing efficiency, the very complexity and synergies of supply chains expose them to cyber risk. A successful breach of any one component could endanger the operation and security of other flows and result in system-wide failure.[3]

[3] World Economic Forum (2013). Building resilience in supply chains.

Cyber attacks are therefore increasingly moving from targeting individual organisations to chained attacks: access to third-party information or systems is an increasingly significant motivation behind data breaches.

As organisations increasingly operate in chains and with their systems integrating, it therefore becomes possible to attack one organisation to access the digital assets of another.

Once inside the system, attackers look for the most vulnerable point to attack – this can be an offshore subsidiary that isn’t up to the group’s global standards, or third-party suppliers in emerging markets.

The extent to which global value chains are integrated across borders today means that weakness in cyber security in emerging markets can easily be passed on to mature ones via the supply chain.

Compounding this problem is the often widespread adoption of generic cloud, mobile and social technologies among smaller and medium-sized companies in emerging markets, even as these often serve larger companies in global supply chains.

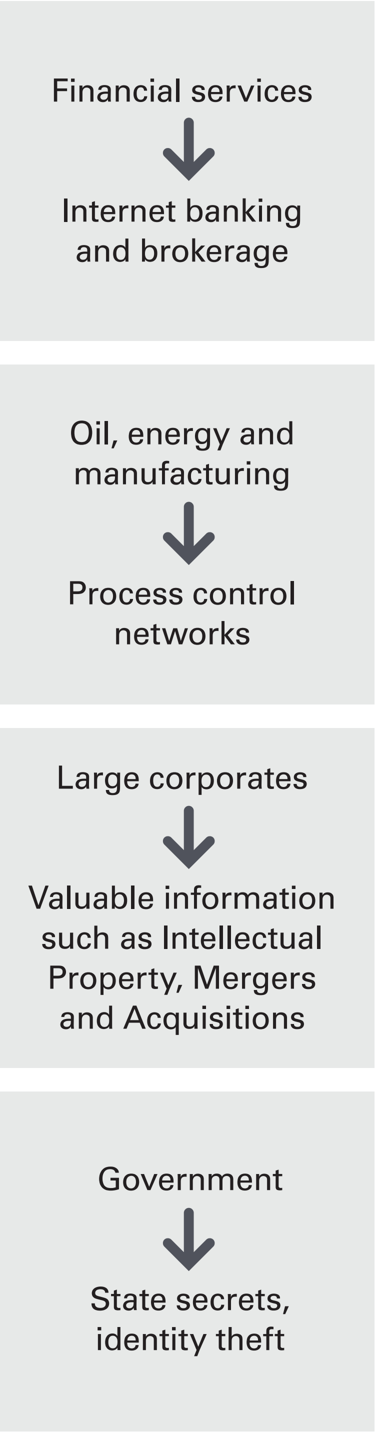
More likely to be cost conscious, less risk conscious, these smaller local companies may be using freeware or inexpensive public services such as Gmail and Dropbox in the course of business.

This suggests lower standards of technology governance overall among supply chain partners in emerging countries, which can put the sensitive customer data of global companies at risk.

This paper considers the weak link of emerging markets in cyber security. The risks to emerging markets arise from four areas: the complexity of supply chains; the need to remain low cost to attract investment; the rapid spread of technology without adequate availability or awareness of training on technological risks; and weak regulations.

What attackers are after

Examples of value to attackers



Financial services

↓

Internet banking and brokerage

Oil, energy and manufacturing

↓

Process control networks

Large corporates

↓

Valuable information such as Intellectual Property, Mergers and Acquisitions

Government

↓

State secrets, identity theft

Emerging markets are not immune to cyber threats. In fact, their growing role in global supply chains could increase their attractiveness to cyber attackers particularly if their governance is weak while handling sensitive customer data for global companies.

Lyon Poh
Partner, Cyber Security
KPMG in Singapore

Ripe target
The story of the hackers that hit the bull's eye at Target is instructive of how the use of poorly governed technologies offers vulnerabilities to cyber attackers. Cyber attackers broke in via the computers of a heating, ventilation and air-conditioning firm that was a supplier to the giant retailer and had access to login details for the retailer's systems.

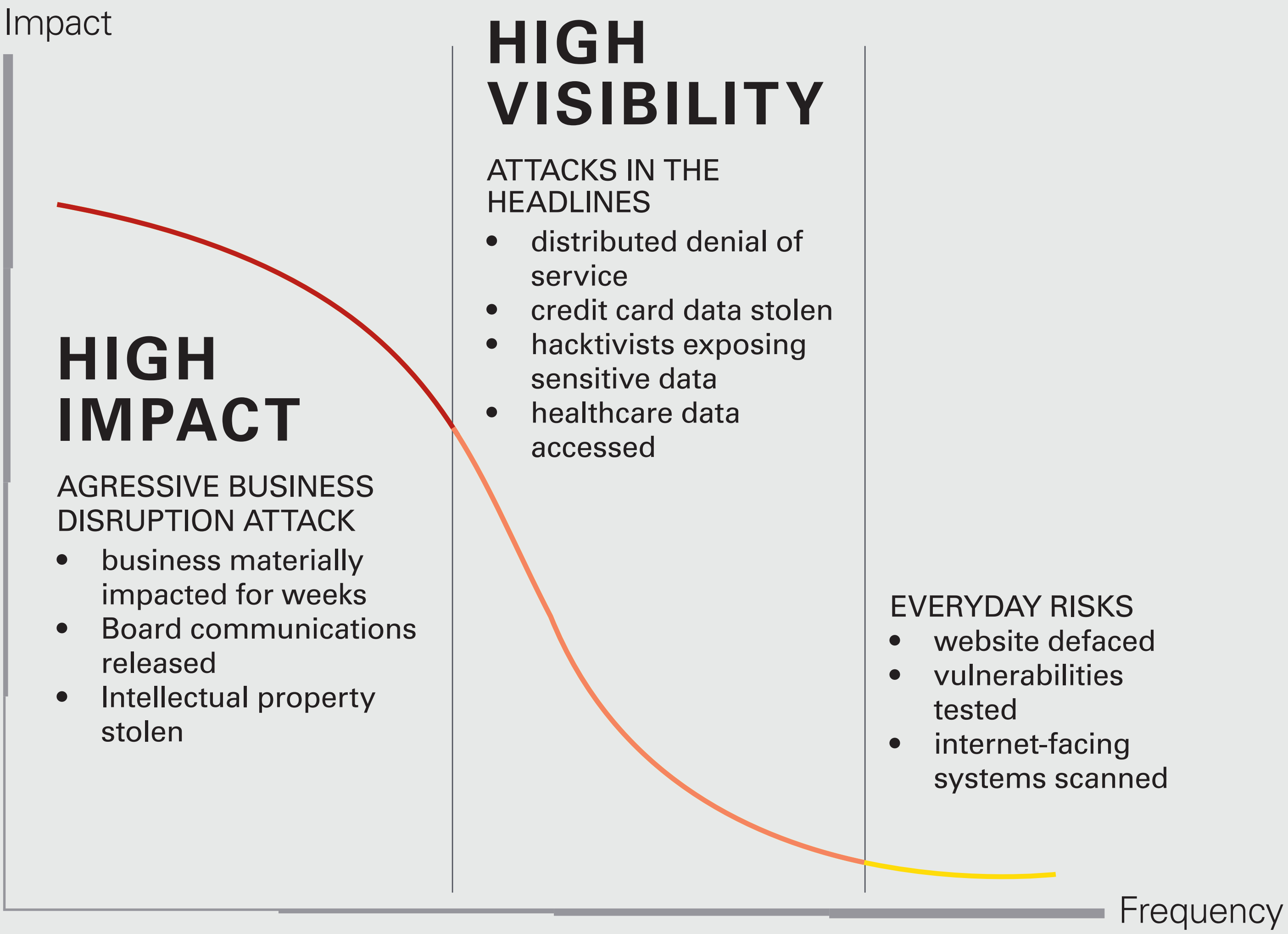
Once inside, the hackers were able to install malware on Target's point-of-sale system that captured credit- and debit-card details at tills before the data were encrypted. The scam affected some 40 million customers.

In Singapore, bank statements of 647 private bank clients were picked off a Fuji Xerox server in December 2013. The theft was only uncovered when the criminal was arrested for other offenses.

Both cases highlight the need to think carefully about how data is transmitted, stored and accessed. They also demonstrate the importance of more stringent oversight on third-party service providers, particularly if these are cross-border.

Most attacks in the news headlines take aim at credit card data, such as Target and JPMorgan Chase. Aggressive security attacks, on the other hand, materially impact internal business operations and interrupt revenue streams with the express purpose of causing widespread business damage. This was the case for Sony Pictures Entertainment. The attack brought down all the computer systems and employees had to resort to using pen, paper and landline telephones for days.

Frequency of attacks relative to impact



HIGH IMPACT

AGRESSIVE BUSINESS DISRUPTION ATTACK

- business materially impacted for weeks
- Board communications released
- Intellectual property stolen

HIGH VISIBILITY

ATTACKS IN THE HEADLINES

- distributed denial of service
- credit card data stolen
- hacktivists exposing sensitive data
- healthcare data accessed

EVERYDAY RISKS

- website defaced
- vulnerabilities tested
- internet-facing systems scanned

SOURCE: Gartner

Hitting the Target

The greatest source of risk in cyberspace comes from groups with the resources and commitment to relentlessly target a company or government agency until they succeed in breaking in and extracting value. These attackers are known as Advanced Persistent Threat (APT).

Target's data breach in December 2013 was a case in point. The attackers exploited a vulnerability in Target's own networks to implant malware that spread to the point-of-sale, the machines where people swipe their credit cards at stores. Infecting the point-of-sale helped evade Target's defenses and internal controls. The malware was written to avoid detection by Target's defenses. Credit card data is encrypted after the card is swiped, so the malware was designed to capture the credit card data in the second between swipe and encrypting and then forwarded on to the attackers. The attack combined programming skill and knowledge of business processes to take down an otherwise well-defended company.

By the numbers

$600,000

Approximate price tag for an IT incident

776,000

Average number of people (eg. individuals, patients, employees, affected by an IT incident)

4 MILLION

Average number of financial accounts (eg. credit cards) affected by an IT Incident

SOURCE: KPMG Technology Risk Radar, Second edition

A world of insecurity

Information security spending

2014

71

BILLION USD

2015 FORECAST

77

BILLION USD

1

billion breached records in 2014

SOURCE: Gartner; Risk Based Security; Ponemon Institute

Financial costs of investing in cyber security
Larger organisations understand the risks involved. Last year, organisations around the world spent $71 billion on information security. But such spending may be beyond the reach of small-medium enterprises (SMEs), which form a key component of global supply chains. Cost considerations are paramount on SME agendas, and the need to be cost-effective means that investments to harden cyber security are often pushed back. This is compounded by many SMEs being unaware of the risks associated with having a presence in cyberspace and often lacking knowledge of threats from cyber-attacks or the training to deal with them.

Complexity of global supply chains adds to cyber risk
Further, most SMEs may not know the intricacy of global supply chains they are a part of and thus are unaware of potential losses as a result of breaches which involve them. Since publicised attacks have so far tended to be big global names in developed markets with high financial stakes, it becomes easy to underestimate the risks to SMEs in emerging markets. Ralph Sherbahn of XL Group, a cyber-insurer, says what has tended to make emerging markets sit up is when they hear about losses hitting their own industry segment. The news of the Russian cybercrime-ring Anuak and Carbanak stealing $1bn from banks across 30 countries, for instance, has been a major source of interest in cyber insurance among Asian banks.

Drivers for cyber risks in emerging markets

- Cost considerations of investing in cyber security
- Lack of awareness of risks that come with having a cyber presence
- Lack of understanding of the full complexity of global supply chains
- Immature legal frameworks to penalize perpetrators
- Rapid spread of technology without attendant defence mechanisms

Mature security programmes
Multinationals aware of these risks set in place stringent security frameworks for third-parties. They typically require suppliers to attest compliance to the framework via a yearly self-assessment exercise, an expectation which is formally inked into service-level agreements.

Some go a step further by requiring third parties to provide timely or real-time monitoring information on elements such as who has access to data or the number of incidents. Such measures, while costly, go some way in establishing a common governance framework to manage cyber risk, and how to respond when something goes wrong. This increases in importance when operations cross borders, where the language and understanding of cyber risks might differ and could lead to misunderstandings if not specified appropriately.

Put in place a more mature security framework to address third-party risks

Include cyber security in your supplier contracts and service-level agreements

Establish a common framework for cyber risk, to ensure shared understandings and norms

Require continuous monitoring of networks

Limit access to sensitive business data

Conduct regular audit of suppliers

As systems become more tightly integrated, dependency increases, and the potential impact of a cyber attack rises. But it can also offer opportunities to provide more sophisticated cyber defences, with fewer but better managed network connections, and a scale of operations which allows for dedicated incident response and monitoring services.

Malcolm Marshall
Global Head, Information Protection and Business Resilience

The cyber factor
Beyond organisational programmes, strong regulations drive companies' planning around cyber risks. But a scan of cyber laws suggests unevenness in enforcement. The US' data-breach laws require firms to report any loss of sensitive customer information while in the European Union, a draft Data Protection regulation is due to be finalised in 2015. Outside these two jurisdictions, stringent legal requirements don't yet exist, least of all in emerging markets. One reason could be cost – slapping on high regulatory penalties could drive away large multinationals, and defeat the purpose of their outsourcing or offshoring processes in the first place.

Yet with the world waking up to the reality of the cyber threat and pricing in its associated risks, the cyber factor may become increasingly important when businesses decide where to outsource or offshore. Emerging markets that get this factor right and can meet rising standards of due care may prove more attractive, and win more business. In fact, being newer entrants to the global supply chain, emerging markets can by design take security into account from early on when planning their IT systems and processes. This is in sharp contrast to developed markets that have to rethink and retool older, legacy systems for security monitoring.

In this, developed markets have an added incentive to ensure everyone's cyber hygiene standards come up to par, as more trade agreements including the proposed ASEAN Economic Community (AEC) bind regional economies and their systems more closely together. The chain will be as strong as its weakest link.

The winds are already changing. In Singapore, the Monetary Authority of Singapore (MAS) has significantly tightened the screw on banks in terms of the IT controls they are expected to put in place to protect customer information, and in requirements to report incidents. Other regulators in the immediate region are expected to follow suit. Companies operating in ASEAN can expect stiffer regulations on cyber security, and should prepare to assess their vulnerabilities and raise their cyber defences.

Some of Monetary Authority of Singapore (MAS) requirements:

- Maintain **high availability and resiliency** of critical systems
- Establish **Recovery Time Objective (RTO)** of not more than 4 hours for critical systems
- Ensure maximum **unscheduled system downtime** does not exceed 4 hours within 12 months
- Notify MAS within an hour upon discovery of **IT security incidents & system malfunctions**
- Submit a **root cause and impact analysis report to MAS** within 14 days from the discovery of a Relevant Incident
- **Implement IT controls** to protect customer information from unauthorised access or disclosure

What we can do to help ourselves

Cyber risks in emerging market can be largely mitigated by following a number of 'hygiene' practices. Far from being defenceless against hackers, companies can take a few steps to help themselves.

6 building blocks for cybersecurity

Put in place cyber hygiene	Have a senior leader or board member advocate and oversee the cause	Build detect and respond mechanisms
Share information with industry peers	Acknowledge good practices	Build up threat intelligence

Cyber hygiene is the starting point

No company can address cyber threats without first putting in place basic protections. At least 80 percent of the targeted breaches we see can be prevented by just six measures:

- patch widely used software such as Microsoft Office, web browsers and PDF viewers on a regular basis, and do the same for operating systems
- monitor networks constantly
- restrict access to sensitive data
- educating employees and raising security awareness
- perform regular vulnerabilities checks

Get a leadership sponsor

Cyber security starts with senior leadership prepared to invest the time to understand why cyber security matters to their business – which assets to protect, and the consequences of not doing so. From this flows a security culture embedded in the business, and an investment of business time in educating staff to understand why it matters and what they can do to help the business remain secure.

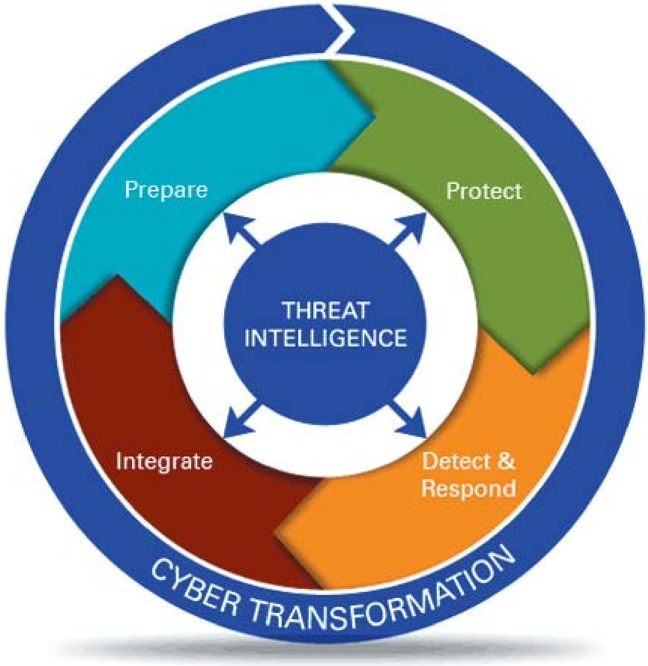
Detect and respond

Monitor your networks and be prepared to respond quickly when incidents occur. Identify your most sensitive data, take additional protection measures such as segregating your internal networks, encrypting data at rest, maintaining backups and having fallback arrangements.

Share information with industry peers

Companies often know only a piece of the cyber security puzzle. Cross-industry sharing about where attacks have come from and the technology used can go a long way in shoring up everyone's defences. In developed markets, this is being done systematically in some industries via Information Sharing & Analysis Centers (ISACs) in the United States. Such knowledge sharing – between the public and private sector, cross-border – is vital too, in emerging markets, where the next frontier in the fight against cybercrime might well be.

KPMG Cyber Security Framework



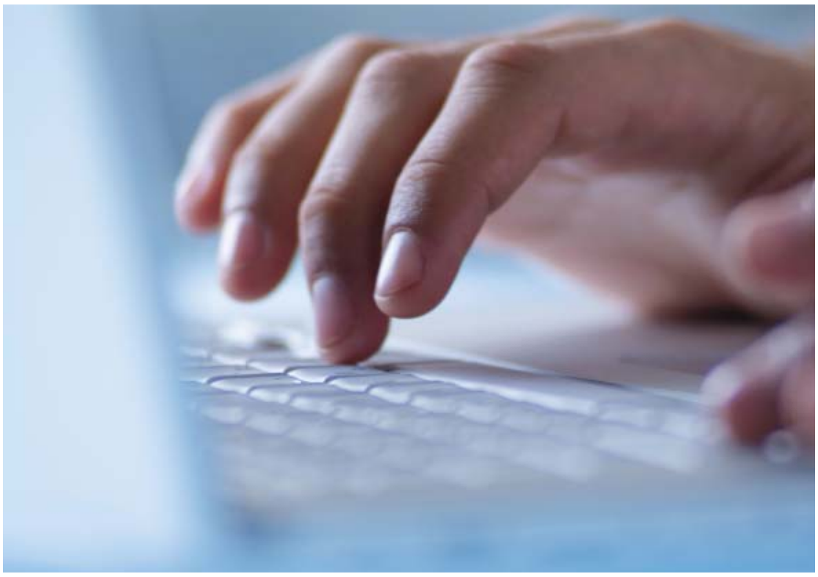
Acknowledge good practices

While stronger regulations are necessary, they run the risk of regulatory over-reach. A lighter touch being proposed involves issuing standards to encourage improved security. In June 2014, Britain introduced a scheme called "cyber-essentials" under which firms can apply for a certificate to show that they comply with certain minimum standards. Applicants undergo an external audit, and if successful, are awarded a badge which they can use on marketing materials. Extending such schemes to outsourcing firms in emerging markets may provide a strong incentive for them to accelerate their cyber defences.

Build up threat intelligence

This involves knowing what cyber threats your organisation face, what risks they pose to your valuable information assets, what responses you should take and how effective they have been.

Conclusion



Many modern businesses outsource their data to third-parties which aggregate, store, process, and broker the information. Such sensitive data is not just about customers, but also includes business structure, financial health, strategy, and exposure to risk. They thus become very dependent on how these third-parties handle risks.

Yet these third-parties often rely on outsourced IT services, lacking the inhouse security expertise of a major corporate; their cultures may also be more entrepreneurial and less compliance-oriented.

The rise of more integrated supply and value chains, the digitisation of the financial system, and the rising capabilities of hackers make it important for companies to approach cyber security as a critical component of business operations.

While developed markets with their promise of higher returns have so far borne the economic brunt of publicised cyber attacks, hackers will increasingly exploit the vulnerabilities in emerging markets as a backdoor into bigger markets.

Regulatory frameworks in emerging markets are often immature, compounding the risks companies face. At the same time, the technology is evolving and spreading faster than there can be a growth in adequate programmes to manage associated risks.

The strengths of emerging markets ironically means that while being late-joiners to global supply chains allows them to quickly adopt most current and affordable systems, this is also its Achilles heel. As they need to remain low cost to attract foreign investment, this sometimes compromises the robustness of their cyber governance procedures.

Nevertheless, there are still some basic 'hygiene' practices that should not be neglected. These include educating employees about social engineering risks, requiring suppliers to cooperate in the implementation of cyber security measures and regular audits can help ensure that they meet cyber hygiene standards.

Constant network monitoring and scans can also help keep networks in good working order. In the same spirit of low cost software that these outsourced companies for operations, there are similarly also low cost cloud-based alternatives for network and port scanning which should at a minimum be deployed.

Cyber security as competitive advantage

As more global companies outsource their IT and other processes, they increase their dependence on how these outsourcing companies handle cyber and other risks.

Given the huge role of technology in the modern business world, cyber risks are real for any business. The cyber factor is likely to be increasingly important when companies decide where to outsource or offshore.

Those suppliers handling confidential third-party data in emerging markets that are able to demonstrate strong security posture around that data are likely to be more attractive and potentially able to win more business.

If well-managed, cyber security can become a strategic edge and competitive advantage for outsourced vendors in emerging markets.

Contact us

Tham Sai Choy
Chairman, KPMG's Asia Pacific Region
Managing Partner,
KPMG in Singapore & Brunei
T: +65 6213 2500
E: saichoytham@kpmg.com.sg

Ho Wah Lee
Head, Emerging Markets
Head, Advisory
KPMG in Indonesia
T: +62 21 5799 6339
E: wahlee.ho@kpmg.co.id

Bob Yap
Head, Advisory
KPMG in Singapore
T: +65 6213 2677
E: byap@kpmg.com.sg

Lyon Poh
Partner, Cyber Security, ASEAN
KPMG in Singapore
T: +65 6411 8899
E: lpoh@kpmg.com.sg

Dani Michaux
Lead, Information Protection
& Business Resilience, ASEAN
KPMG in Malaysia
T: + 60 377 213 388
E: danimichaux@kpmg.com.my

KPMG ASEAN
E: asean@kpmg.com.sg
www.ASEANconnections.com