KPMG
cutting through complexity

Cyber Security Standards Compliance: *A Vital Measure to Critical Infrastructure Protection*

kpmg.com/my

Contents

FOREWORD

The usage of technology in today's world is inevitable. Whether it is making reservations on our smart phones, or checking emails, or checking in for flights, usage of technology is present. Further, the globalization phenomenon we see today means we are living in a world where almost everything is interconnected to one another. Governments, businesses and societies around the world are relying more and more on technology and the Internet in their daily lives. Whilst its benefits cannot be questioned, unfortunately the increase of our reliance on technology implies that we are at higher risk of attack and breaches – *cyber-attacks*. Companies are being hacked causing millions of individuals to be victims of stolen identity and information. Governments worldwide are also facing the increasing threats of cyber-attacks. Successful attacks put prosperity of economies and the well-being of societies at risk. Consequently, governments are putting measures in place in hope of having a resilient, healthy and secure cyberspace. Nonetheless, even with these efforts, cyber security continues to dominate headlines in the wrong way. Responding to this current scenario, current trends of governments protecting their critical infrastructures is the implementation of cyber security standards to their critical sectors.

The objective of this paper is to provide an overview of the various approaches that countries are taking with regard to the implementation of cyber security standards. Further, the paper discusses the benefits of the implementation of cyber security standards to organizations as well as nations as a whole. Aligned with our strategic growth areas, we are in view that efforts in protecting organizations' critical assets for a healthy cyberspace is paramount. We hope this Thought Leadership provides you the overview of the subject discussed and look forward to discussing your questions or issues.

Muazzam Mohamed
Executive Director
Management Consulting

Chief Information Officer
KPMG in Malaysia

Cyber-attacks – A global risk

As we begin 2015, there are no signs of cyber threats and attacks on organizations worldwide easing. Whether targeted to government entities or private corporations, the threats from cyber adversaries continue to grow in scale and sophistication globally. Public and private organizations in various sectors worldwide now openly acknowledge that cyber threats are one of the most common and high impact risks they face. Dealing with cyber threats is becoming a complex challenge due to the evolving cyber security landscape. Organizations today face not only common and known cyber threats, but new and emerging ones where targeted and large scale attacks can impact not only the organizations but may potentially lead to the adverse impact on nations' critical infrastructures.

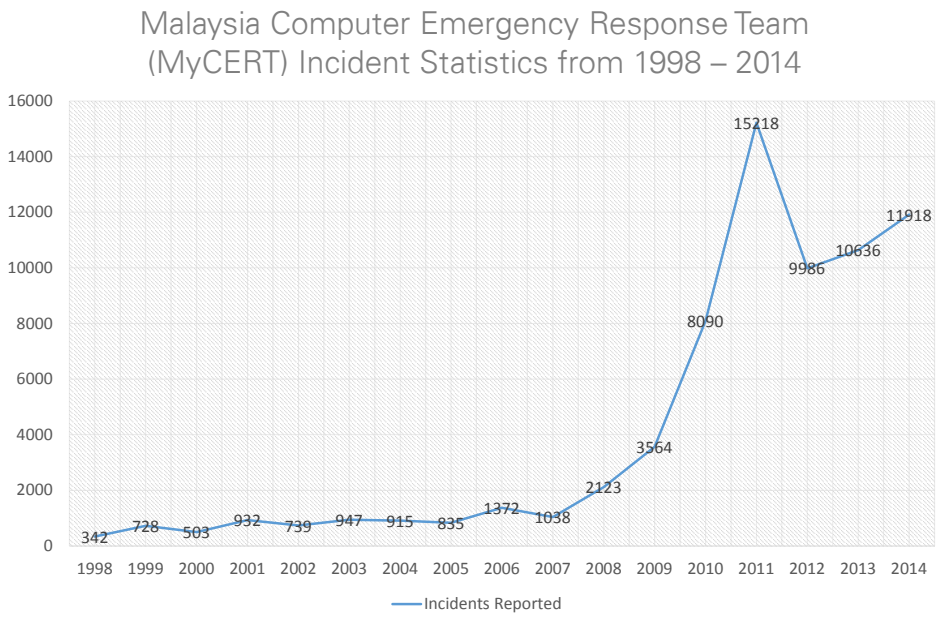
Cyber-attacks on critical sectors.

The recent cyber-attack against an American entertainment subsidiary of Japanese multimedia conglomerate in 2014 has not only affected the company, but also the nation's security as a whole. Apart from releasing confidential data, the hackers had also sent threatening messages if their demands were not met[1]. The Financial sector has also become a regular target. The malware attack in 2013 in South Korea has resulted in the malfunction of 48,000 personal computers and servers, disrupting work at banks and television broadcasters in the country[2]. In 2012, a virus attack known as Shamoon on Saudi Arabia's leading Oil & Gas company had damaged approximately 30,000 computers resulting in the disruption of oil and gas flow to the local and international markets[3]. Global technology companies have had their fair share of experiencing cyber-attacks in recent years as well. These companies were hacked, resulting in exposed proprietary information and sensitive communications that was then used to target major corporations.

The Global Risk 2014 by World Economic Forum (WEF) highlights that dependency on technology by economies and societies is inevitable[4]. The reliance and dependence on information data and systems have resulted in higher occurrence of cyber-attacks and their effects more impactful. It further underlines this point as 'cyber-attacks' is listed in the top 5 global risks in terms of likelihood:

Top 5 Global Risks in Terms of Likelihood	
1st	Income disparity
2nd	Extreme weather events
3rd	Unemployment and underemployment
4th	Climate change
5th	Cyber-attack

Malaysia too has had its fair share or weathering cyber security attacks. According to Malaysia Computer Emergency Response Team (MyCERT), cyber incidents reported to the agency have substantially increased over the past decade; from 342 cases in the year 1998 to 11,918[5] in 2014.

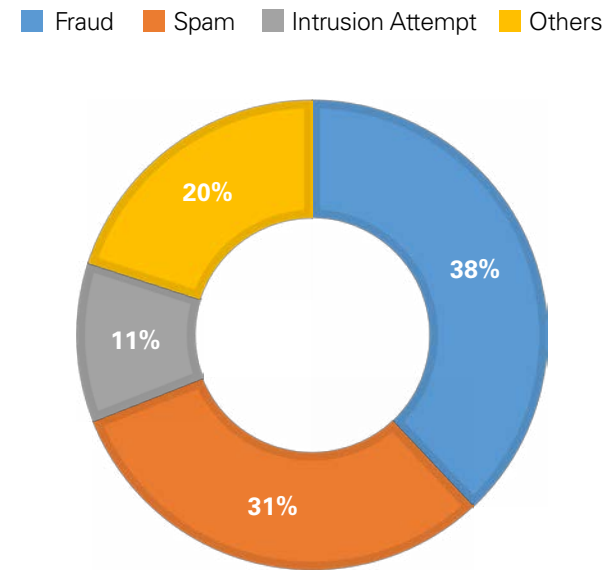


Source: MyCERT Incident Statistics as of December 2014.

The number of incidents as a percentage of total case reported in 2014 are stated below:

- Fraud, 38%;
- Spam, 31%; and
- Intrusion attempt, 11%.

CYBER INCIDENTS REPORTED



Source: MyCERT Incident Statistics as of December 2014.

Similar with many other countries, critical infrastructure in Malaysia are owned by both the public and private sectors - *estimated to be valued at USD3.8 trillion*[6]. In Malaysia, known cyber-attacks have amounted to a total loss of USD286 million* in the first six months of 2013, compared with USD314 million* in the previous year[7].

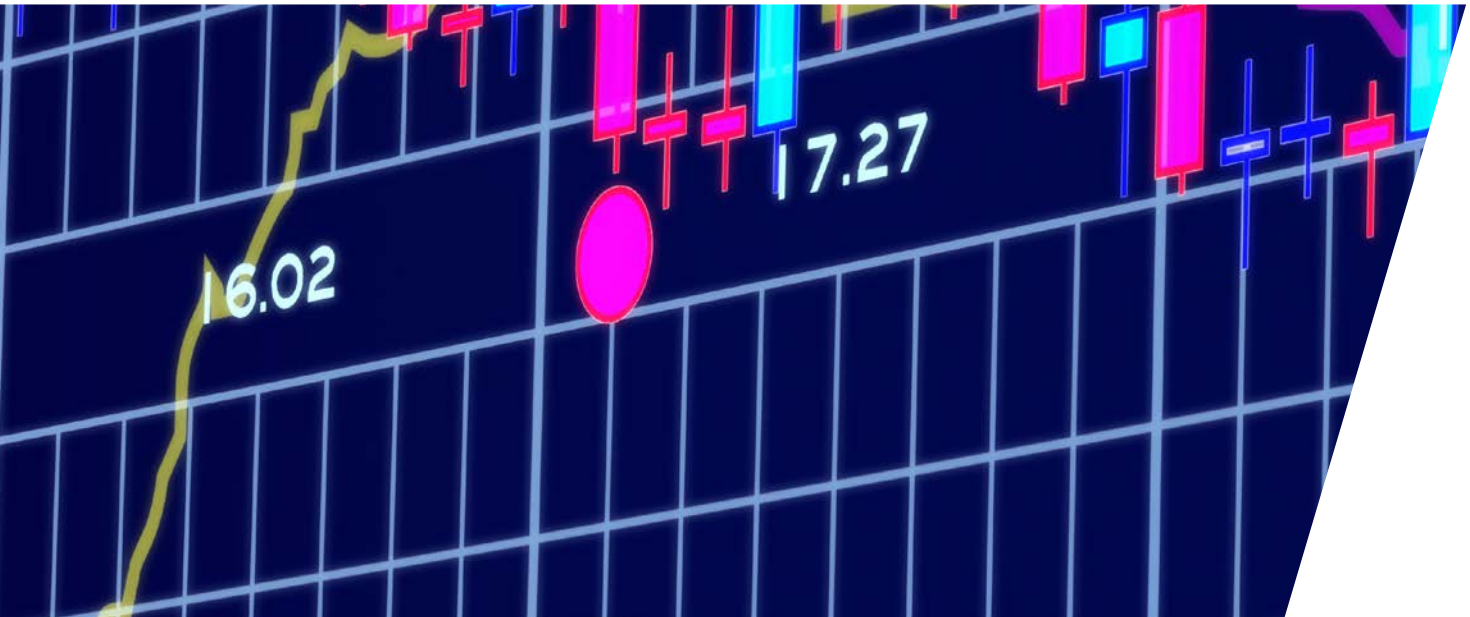
* Conversion rates used throughout the publication taken from Oanda as on 31 December 2014: US$/ RM - 3.49806

Global cost of cybercrime.

From a global standpoint, a recent publication by McAfee estimated the annual cost of cybercrime to the global economy is more than USD400 billion[8]. Facing the brunt of these losses are the 4 largest economies in the world; the United States of America (USA), China, Japan, and Germany with an accumulative figure reaching USD200 billion. The financial loss on the global economy is only expected to rise as reliance on technology in the cyberspace increases. Consequently, governments worldwide are realizing that cyber threats can not only disrupt critical infrastructure networks, but also potentially escalate to the level of a national security threat.

Dealing with cyber threats and attacks is no longer just about being aware or vigilant – but it's about being resilient. Governments around the world are putting measures in place to enhance resiliency in weathering the cyber threats and attacks. Whilst the global community have undertaken actions and steps in mitigating these cyber threats, it is important to ensure the critical infrastructure remains resilient to withstand cyber-attacks. The term 'resiliency' can have many definitions, but generally it is the capability to prepare, protect, respond and recover from threats and hazards.

> **"Dealing with cyber threats and attacks is no longer just about being aware or vigilant – but it's about being resilient."**



“The cyber security standards may support the capabilities of preparing, protecting, responding and recovering from cyber-attacks.”

How do countries or organizations remain resilient?

The implementation of cyber security standards is by no means a silver bullet in critical infrastructure protection. However, its implementation can establish a set of controls that contribute and build better resiliency. The cyber security standards may support the capabilities of preparing, protecting, responding and recovering from cyber-attacks. Some of the common cyber security-related standards being implemented globally include the following (not exhaustive):

ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cyber security

ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements

ISO 22301 Societal security – Business continuity management systems — Requirements

ISO/IEC 15408 Information technology – Security techniques – Evaluation criteria for IT security

ISO/IEC 27035 Information technology – Security techniques – Information security incident management

ISO/IEC 27005 Information technology – Security techniques – Information security risk management

FIPS 140-1: Security Requirements for Cryptographic Modules

FIPS 186-3: Digital Signature Standard

The implementation and compliance with cyber security standards may enable the principles and better practices in cyber security management be applied in improving the security and resilience of critical infrastructures.

Remain resilient through cyber security standards compliance

Countries take different approaches towards implementing cyber security standards in the efforts of protecting their critical infrastructures. Some countries implement cyber security standards through mandatory requirements, whilst others provide guidelines and frameworks. The subsequent discussion highlights observations on the many approaches certain countries take.

> **“Some countries implement cyber security standards through mandatory requirements, whilst others provide guidelines and frameworks.”**

United Kingdom (UK). The UK government recognizes that the Internet has become increasingly important to its economy and society. In 2010, the UK had one of the largest Internet-based economies, valued at USD188 billion*[9]. Due to the high reliance on Internet, as well as the country's Cyber Security Strategy 2010's vision which is "...to derive huge economic and social value from a vibrant, resilient and secure cyberspace..."[10], it is vital that the country's basic infrastructure be protected. The UK government has enforced compliance to the Network Interoperability Consultative Committee (NICC) Minimum Security Standards (ND 1643) through the Communications Act 2003 to the Communications Sector. In addition, one of the strategic priorities outlined in the UK's Cyber Security Strategy is to reduce vulnerabilities in the country's government systems and critical infrastructure. For this reason, the UK has developed the cyber security and information assurance standards – Information Assurance Maturity Model (IAMM). IAMM was developed by incorporating the requirements from the Security Policy Framework (SPF) which is mandated to government agencies. SPF recognizes and has aligned its principles to the ISO/IEC 27001 and the Business Continuity Management (BCM) standards (BS 25999/ISO 22301). The UK's priorities for action is to model the best practice on cyber security in the government systems which will set standard for suppliers to government to raise the bar on cyber security requirement. On the flipside, the UK government also takes the approach of voluntary standards implementation. The application of standards is promoted through the establishment of national-level certification schemes for the following standards such as the ISO/IEC 15408, ISO/IEC 27001, ISO/IEC 20000, BS 25999 and ISO 22301.

* Conversion rates taken from Oanda as on 31 December 2014: US$/ GBP 0.64374

"...UK's priorities for action is to model the best practice on cyber security in the government systems..."

Australia. Australia's cyber security standards compliance implementation is supported by the country's Cyber Security Strategy 2009. The Strategy highlighted on the need for a consistent and integrated framework of policies, procedures and standards to protect its government's systems, as well as the other interconnected systems[11]. In realizing this, one of the measures that the country has undertaken is the development and enforcement of the Protective Security Policy Framework (PSPF) to the government agencies through a Directive by the Attorney-General Department (AGD). PSPF which is mapped to the ISO/IEC AS/NZ 27001 has 33 mandatory requirements and is developed to protect the government's people, information and assets. The Australian government takes the lead-by-example approach whereby it enforces standards to government agencies to encourage and create market demand for good security practices and more secure services and products to be made available to the public. In addition, the Australian government has enforced the ISO/IEC 15408 for procurement of products with security functions in the Government Sector. This is in line with the priority outlined in the Cyber Security Strategy 2009 which is to establish minimum security standards in the government for a more centralized approach for ICT products and services procurement and management. Standards that are implemented voluntarily and adopted by critical infrastructure organizations in Australia are the American National Standard Institute/International Society of Automation (ANSI/ISA)-99 Industrial Automation and Control Systems Security and ISO27799 Health Informatics - Information security management in health using ISO/IEC 27002.

"The Australian government takes the lead-by-example approach whereby it enforces standards to government agencies to encourage and create market demand for good security practices and more secure services and products to be made available to the public."

United States of America (USA). Over the decade, the country has weathered constant cyber security attacks and acknowledges the inevitable increase of threats to critical infrastructure and federal operations information systems. The country has developed various national strategies on cyber security. The Comprehensive National Cybersecurity Initiative (CNCI) will evolve to become the key element of a broader updated national USA cyber security strategy. The CNCI consists of various initiatives designed to help secure the country in the cyber space[12]. Furthermore, it has specific strategies for each of its critical sectors which not only covers physical security, but also cyber and human security. The government has mandated the compliance with cyber security standards through related legislations to certain sectors; Energy, Dams and Government. The standards mandated to the Energy and Dams sectors are the Reliability Standards Critical Infrastructure Protection (CIP) 002-009 through the Code of Laws of the United States of America (U.S.C) Title 16 – Conservation, Section 824o – Electric Reliability (16 U.S.C 824o). The standard is mandated to ensure a secure electronic information exchange to support the reliability of the bulk power system and to assist in preventing unauthorized access to the sectors' critical assets. The standards mandated for the Government Sector is the Federal Information Processing Standards (FIPS) through Federal Information Security Management Act 2002 (FISMA). Other standards in the critical sectors are ISO 27799, ISO/IEC 27010 Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications as well as ISO/IEC 27011 Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 for Telecommunications and ISO/IEC TR 27015 Information technology -- Security techniques -- Information security management guidelines for financial services for Financial Services. Notwithstanding, the government promotes the application of cyber security standards via establishment of national-level certification schemes for the following standards such as ISO/IEC 27001, ISO/IEC 27005, ISO/IEC 27006, ISO/IEC 20000, and ISO 22301.

"The government has mandated the compliance with cyber security standards through related legislations to certain sectors ..."

South Korea: Being one of the most connected countries in the world, the South Korean government realizes that as it continues to embark on information technology initiatives for the nation, the risks of cyber-attacks will also increase. A report by the Ministry of Strategy and Finance states that there is a "high concern over the potential damages to Korea's main national information communication infrastructures caused by cyber-attacks"[13]. The government has put equal importance of cyber security and information through its Long Term Comprehensive Plan for information security for the protection of its critical information infrastructure.
The Communications Sector complies with the ISO/IEC 27001 under the Act on Promotion of Information and Communications Network Utilization and Information Protection 2005 to ensure reliability and trust of the information communication network[13]. Its purpose is focused on promotion of the use of information and communication networks as well as protection of user's personal information. In order to ensure compliance, the government conducts Information security management system (ISMS) Compliance Information Security Checks on the mandated organizations. Additionally, to promote the usage of the standard to the industry, the government provides incentives such as discounts, eligibility criteria and evaluation points in bids for government projects. Other standards that are implemented voluntarily by the industry in South Korea include ISO/IEC 20000 and ISO/IEC 15408. The government also provides incentives for the ISO/IEC 15408 scheme to reduce economic burden to the smaller companies.

"The Communications Sector complies with the ISO/IEC 27001 under the Act on Promotion of Information and Communications Network Utilization and Information Protection 2005 to ensure reliability and trust of the information communication network."

Malaysia. Cyber security standards compliance implementation in Malaysia is supported by the country's National Cyber Security Policy (NCSP). The NCSP aims to strengthen the nation's critical national information infrastructure and facilitate the country's drive towards Vision 2020 as part of the country's strategy towards attaining a developed nation status by the year 2020.

The country has identified the ISO/IEC 27001 as the baseline standard for information security and has enforced it to its critical sectors through a Directive. There are also Directives by the government that outline requirements in implementing the ISO/IEC 27001 or equivalent to reduce the risks of cyber security incidents. The Government, Financial Services as well as Information and Communication Sectors comply with various cyber security standards and guidelines. These are made mandatory through enabling provisions in the Electronic Government Activities Act 2007, the Financial Services Act 2013 and the Communication and Multimedia Act 1998 respectively. In addition, there are specific sectors that comply with other cyber security-related industry standards. For example, the Banking & Finance Sector complies with Payment Card Industry Data Security Standard (PCI-DSS), Public Key Infrastructure (PKI) Standards and Europay-Mastercard-Visa (EMV) Standard. The Transportation Sector which includes sub-sectors Aviation, Maritime, and Land complies with cyber security-related international regulations and standards such as standards by International Air Transport Association (IATA) and International Civil Aviation Organization. Notwithstanding, the government promotes the application of cyber security standards via establishment of national-level certification schemes such as the Malaysia Common Criteria Evaluation and Certification Scheme (MyCC Scheme) that evaluates and certifies the security functionality within technology products against ISO/IEC 15408 standard and ISMS Audit and Certification Scheme based on the ISO 27001:2005 standards to ensure and achieve continual improvement in the management of information security.

"The country has identified the ISO/IEC 27001 as the baseline standard for information security and has enforced it to its critical sectors through a Directive."

Conclusion

As the global community rely and depend more on technology, it is inevitable the threats from cyber adversaries continue to grow. The evolving cyber landscape opens the possibility for large scale cyber-attacks that may have an adverse impact on nations' critical infrastructures. The wider adoption and implementation of cyber security standards is argued to contribute to and build better resiliency of nations' critical infrastructures. This can bring about higher success of a country's cyber security strategy in withstanding the cyber threats which no longer observe national borders. As a result, this is able to link the global community in a common defense and better collaboration and capability to respond for improved cyber resiliency globally.

Analysis on how compliance with cyber security standards improve critical infrastructure protection

The different approaches that countries take to cyber security standard compliance shows that cyber security standards whether implemented mandatorily or voluntarily is a measure to enhance the protection of the critical infrastructure. Enforcing cyber security standards compliance may bring about positive outcome to the overall cyber security management of a country, and not just the organizations implementing them.

The benefits of cyber security standards compliance are summarized below:

- Provide a baseline requirement;
- Establish a consistent and iterative approach to manage cyber security;
- Enhance integration and interoperability;
- Drive the development and creation of market demands;
- Acknowledge the global nature of cyber security risks in addition to the ecosystem's local risks; and
- Encourage and promote international cooperation.

Baseline. The enforcement of cyber security standards may provide a baseline requirement for the critical infrastructure organizations to manage cyber security risks and protect their critical assets. It provides a common language that may contribute in achieving a consistent approach to manage cyber security in the critical infrastructure organizations. Various countries have enforced cyber security standards to the organizations in their critical sectors. In the USA, the UK and Australia, it is observed that standards such as FIPS, SPF and PSPF respectively have been enforced to the Government Sector to protect the government's information and information systems. In addition, the UK and South Korea have enforced standards to their Communications Sector to ensure the reliability of the sector's services.

Consistency. The implementation of cyber security standards may help establish a consistent approach to identify, assess and monitor the cyber security posture of the critical infrastructure. In the UK, the IAMM is the tool used to assess the compliance with the mandatory requirements of the SPF for the Government Sector. South Korea has developed its own National Information Security Index to measure the country's level of preparedness for information security in the country and the threat index used in measuring the scope of damages caused by cyber threats.

Integration and Interoperability. As the reliance on technology and interconnectivity between sectors have increased, the critical infrastructure sectors may be more vulnerable to potential cyber risks and threats. The enforcement of cyber security standards that are technology neutral and evolves with technology advances may be able to enhance integration and interoperability between the critical sectors. This in turn contributes to the improvement of the overall security and resilience of the country's critical infrastructure. The Australian government in its Cyber Security Strategy 2009 highlighted the need for a consistent and integrated framework, procedures and technical standards to ensure the protection of its government systems as well as interconnected systems.

Market Demands. The enforcement of cyber security standards compliance may also drive the development and creation of market demands for effective products, services and practices. As the demand increases, there may be an increase in the market competition for the suppliers which may promote faster and better distribution of secure technologies and practices. This may allow the critical infrastructure organizations to realize the benefits of implementing cyber security standards. Many countries have established certification schemes to promote the usage of cyber security standards to the industry. Whilst there are countries that enforce these schemes, such as the USA and Australia which enforce the ISO/IEC 15408 for government procurement, there are countries that encourage the implementation of these standards by providing incentives. For example, South Korea provides incentives to the industry to implement the ISO/IEC 27001 and ISO/IEC 15408. A study by McAfee shows that there is an 8.7% increase globally for cyber security products since 2011 to 2013, which is from USD53 billion to USD58 billion[14]. In addition, the business demand for cyber security products for the same period has increased by 14.7%, whilst consumer demand has increased by 10.7%. The report indicated that the increase is contributed by the growing awareness of cyber security risks in the industry.

Acknowledgment of Global Risks. Generally, internationally-accepted cyber security standards are developed by industry experts. These standards have usually taken into consideration the global risks that are commonly faced by the industries in which by enforcing cyber security standards compliance, organizations may acknowledge the global nature of cyber security risks in addition to their ecosystem's local risks. Observations suggest that countries have implemented international cyber security standards to assist in the protection of their critical assets. For example, the UK's communication providers implement the ND 1643 based on a requirement from the Communications Act 2003 to form a baseline for the security and integrity of network interconnections. This standard is in line with the Electronic Communications Framework by the European Commission. In Australia, the Generic SCADA Risk Management Framework for Australian Critical infrastructure has adopted the ANSI/ISA-99 Industry Automation and Control System Security that is developed by the American National Standard Institute.

International Cooperation. The enforcement of cyber security standards may encourage and promote international cooperation in strengthening critical infrastructure protection as countries that implement cyber security standards may be able to contribute in international fora on standards. Forum of Incident Response and Security Teams (FIRST) is an international platform for information exchange and cooperation on incident response and cyber security vulnerabilities between government, commercial and academic sectors. One of FIRST's global initiatives includes efforts on cyber security-related standards for ISO and International Telecommunication Union (ITU). Amongst the standards that FIRST are currently working on include the ISO 27032 – Guidelines for Cyber Security and ISO 27035 – Information Security Incident Management[15]. The World Trustmark Alliance is an international platform to discuss issues and standards concerning e-commerce transactions and dispute resolutions for cross-border transactions.

"...cyber security standards compliance may also drive the development and creation of market demands for effective products, services and practices."

Acknowledgment

We would like to thank the following people for their valuable contribution to this report:

Rozana Rusli
Executive Director, Management Consulting, KPMG in Malaysia

Shahrul Kamal Kamaruddin
Assistant Manager, Management Consulting, KPMG in Malaysia

Najlaa' Fadzli
Assistant Manager, Management Consulting, KPMG in Malaysia

Endnotes

1 "Sony cyber-attack: North Korea calls US sanctions hostile." BBC 4 January 2015. Web. 5 January 2015.

2 "South Korea blames North for bank and TV cyber-attacks." BBC 10 April 2013. Web. 16 January 2014.

3 "Saudi Aramco says most damage from computer attack fixed." BBC 26 August 2012. Web. 16 January 2014.

4 "Global Risks 2014, Ninth Edition." World Economic Forum, 2014.

5 MyCERT. MyCERT Incident Statistics as of October 2014. November 2014.

6 Malaysia. Performance Management & Delivery Unit (PEMANDU). "Accelerating the growth of local cyber security industry by securing Malaysia's Critical National Information Infrastructure based on international cyber security safety standards." n.d. Document.

7 BAE to make Malaysia hub for security solutions." Business Times. 2013.

8 McAfee - Center for Strategic and International Studies. "Net Losses: Estimating the Global Cost of Cybercrime." 2014.

9 BBC, "UK is the 'most Internet-based major economy'", 19 March 2012.

10 HM Government, "The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world", November 2011.

11 Australian Government. "Cyber Security Strategy." 2009.

12 The White House. Foreign Policy - The Comprehensive National Cybersecurity Initiative. 2013

13 Ministry of Strategy and Finance. "2011 Modularization of Korea's Development Experience: Information Security Activities in Korea." 2012.

14 McAfee - Center for Strategic and International Studies. "Net Losses: Estimating the Global Cost of Cybercrime." 2014.

15 FIRST. Standardization Efforts. n.d. March 2014.

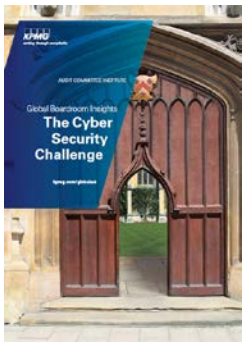
Thought Leaderships

Cyber security: It's not just about technology

As cyber security is an important concern for every organization, this whitepaper provides insights on the common cyber security mistakes made by organizations.

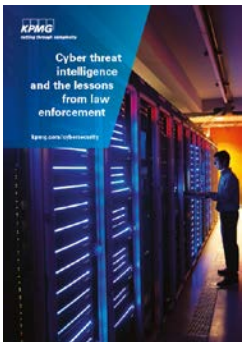
Cyber security: Are consumer companies up to the challenge?

This report discusses the outcome of a webcast survey that was conducted by KPMG on consumer companies. The survey, "Cyber security: It's not just about technology" focused on assessing and effectively managing cyber risk.



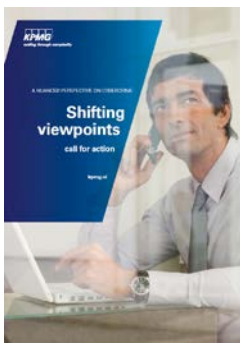
Global Boardroom Insights - The Cyber Security Challenge

Key elements of effective cyber risk oversight and governance are explored in this edition of KPMG Global Boardroom Insights. The paper provides insights from various professionals from the industry on cyber security challenges.



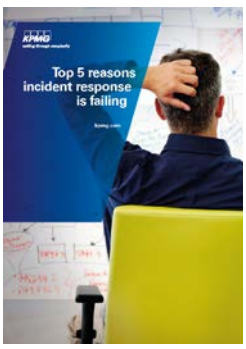
Cyber threat intelligence and the lessons from law enforcement

This report provides the cyber intelligence principles and processes that will help organizations manage cyber threat proactively and minimize risk to customers, shareholders and employees.



A Nuanced Perspective on Cybercrime: Shifting viewpoints call for action

This whitepaper on cybercrime is based on a survey and interviews amongst Dutch organizations. It provides an overview of the cybercrime landscape and actions to be undertaken.



Top 5 reasons incident response is failing

This report identifies the five reasons that represent the top failures of the incident response function.

Cybercrime Survey Report 2014

This report discusses the outcome of a cybercrime survey that was conducted by KPMG in India. The survey provides a summary on the complexity of cybercrime and the measures that organizations should take to mitigate such crime, while creating awareness on what one should do to prevent such attacks.

kpmg.com/my

Contact Us

Muazzam Mohamed
Executive Director
Management Consulting

Chief Information Officer
KPMG in Malaysia
Phone: +60 (3) 7721 7086
Email: mmohamed@kpmg.com.my

Dani Michaux
Executive Director
Management Consulting
KPMG in Malaysia
Phone: +60 (3) 7721 7742
Email: danimichaux@kpmg.com.my