KPMG

CYBERSPACE - Is your organisation secure?

Do you know that on 31 October 2016, the Securities Commission Malaysia ("SC") issued their "Guidelines on Management of Cyber Risk" pursuant to section 377 of the Capital Market and Services Act 2007 ("CMSA")?

Does your organisation have the following?

- Defined roles and responsibilities of the Board of Directors and management in the oversight and management of cyber risk;
- Appropriate cyber risk policies and procedures;
- Awareness of the requirement to manage cyber risks; and
- Robust reporting requirements.

> Nearly a third of CEOs in KPMG's latest global survey identified cyber security as the issue having the biggest impact on their companies today—and only 49% say they are fully prepared for a cyber-event.
>
> Organisations need to develop a proactive and predictive approach to cyber security instead of relying too heavily on reactive technologies such as firewalls and other intrusion-prevention tools. Constantly testing for vulnerabilities is one way to stay ahead. Understanding the threat landscape and enhancing your security intelligence is another. What you can't prevent, you should try to detect. And what you can't detect, you should be prepared to respond quickly.
>
> Investors and regulators are increasingly challenging boards to step up their oversight of cyber security and calling for greater transparency around major breaches and the impact they have on the business. Given this environment, it is not surprising that cyber risk is now near the top of board and audit committee agendas.
>
> As such, corporate boards must address cyber security issues on their front lines as it is not just an Information Technology (IT) issue. In fact, cyber risks are an enterprise-wide risk management issue.

Datuk Johan Idris
Managing Partner

> In Asia only 32% of CEOs reported that their organisations are fully prepared on the cyber front. Organisations are aggressively adopting new technologies, including fintech, AI, industry 4.0 and smart cities in the race to keep and extend their market share. While disruption and digital strategies are on the forefront of the agenda of many organisations, cyber threats are still being neglected.
>
> Organisations sleep walk thinking that the risks of the business remain the same even in a technology driven world. Often the risk management teams of organisation fail to imagine the extent of sophistication and the damage a cyber attack can have over the new technology world.
>
> Understanding cyber risks and the extent of potential damage, and understanding what is really key and core to the business is a mandatory step to be taken for anyone willing to address cyber issues. Embedding cyber resiliency within your business and ability to continue your business with minimal disruption in the event of cyber attacks are becoming key in this dynamic, fast phased technology adopting environment.

Dani Michaux
Head of IT Advisory, ASEAN and ASPAC Cyber Security Lead

Cyber Maturity Assessment

MANAGEMENT OF CYBER RISK

- Cyber risk policies and procedures
- Cyber risk measures
- Prevention
- Detection
- Recovery

How robust is your governance and policies?

KPMG's Cyber Maturity Assessment aims to assist an entity to ascertain the robustness of their process in the following areas:

- Roles and responsibilities of the board of directors and management in oversight of cyber risk;
- Cyber risk policies and procedures that should be developed and implemented;
- Requirements for managing cyber risk; and
- Reporting of cyber risk.

KPMG will perform a Cyber Maturity Assessment via documentation and evidence reviews, interviews of key personnel in all key areas and will identify areas of non–compliance in both the design and effectiveness of:

- Roles and responsibilities of the board of directors;
- Roles and responsibilities of the management;
- Cyber risk policies and procedures, including overall cyber security strategy, organisational responsibilities, cyber breach management processes, third party cyber risk management, communications strategies, etc.;
- Cyber risk measures, overall cyber risk management framework, including third parties;
- Prevention techniques, ongoing regular assessments and compliance programmes, and cyber technology deployments;
- Ongoing awareness programmes for board members, senior management, operational staff and third parties, and preparedness assessments;
- Detection techniques, including ongoing monitoring techniques for timely detection of breaches, and escalation and reporting procedures; and
- Recovery techniques, including cyber incident playbooks and alignment with business continuity processes.

The Securities Commission's Guideline on Management of Cyber Risk (SC-GL/2-2016) will be used as a benchmark for capital market entities.

Each area will be rated based on the three (3) levels of compliance - fully compliant, partially compliant and non-compliant.

Compromise Assessment

MANAGEMENT OF CYBER RISK

- Cyber Incident
- Cyber Threat
- Detection
- Response

How secure is your business?

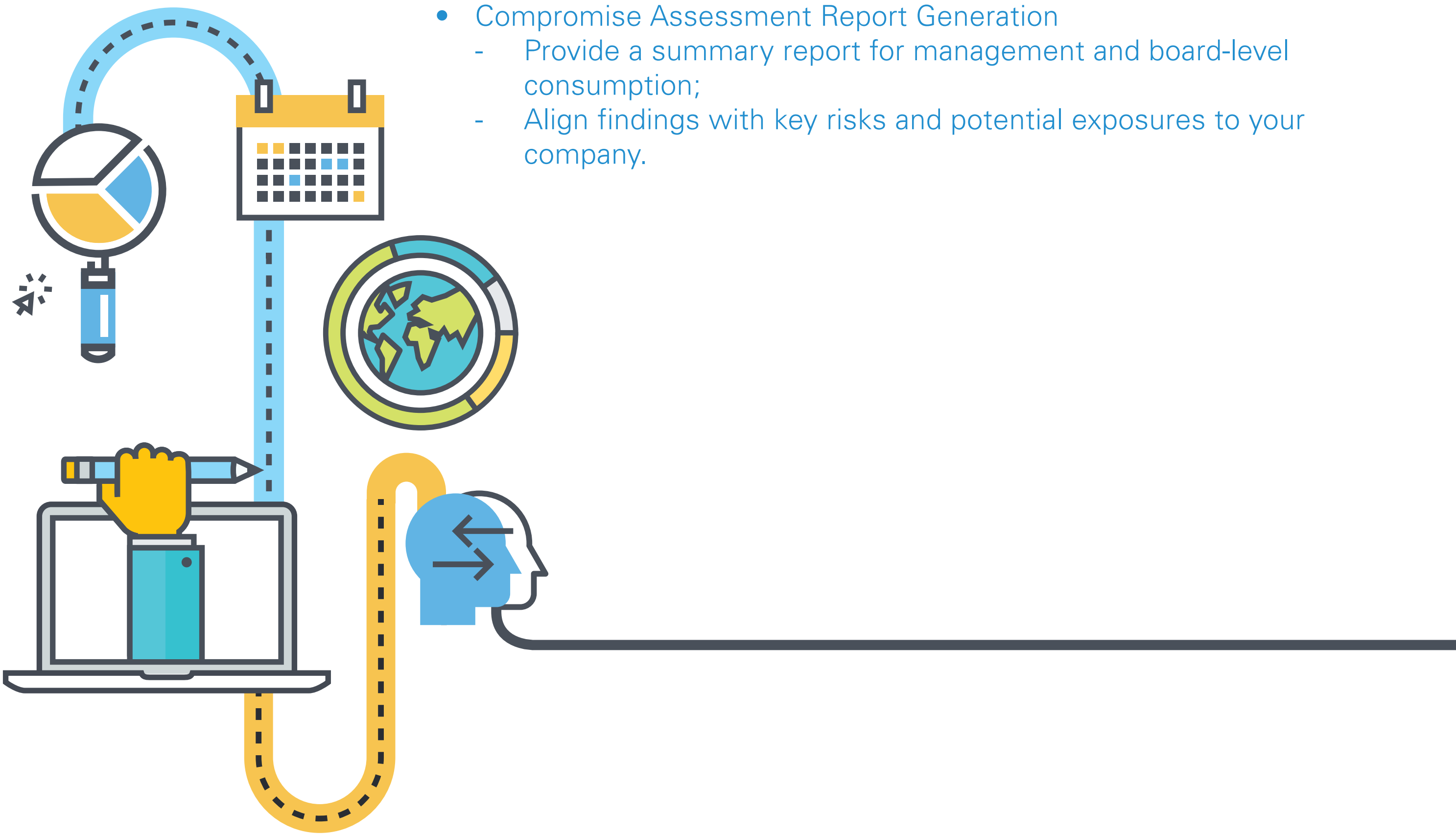
KPMG's Compromise Assessment is an independent review of the organisation's infrastructure, systems and applications to identify indicators of compromise, backdoors, unauthorised access and opportunities to further improve incident detection and response capabilities.

A Compromise Assessment results in observations about identified malware and intruder activities, and the potential associated impacts. In many cases, user activity is identified that presents a risk to the organisation, such as access to a web site known to harbour malware or file sharing services left on.

KPMG's Compromise Assessment deploys a composite team of subject matter experts (cyber defense and digital forensics) to analyse your network, systems and endpoints so as to detect and isolate any sophisticated threat that may already be residing in your organisation.

The activities include the following:

- Compromise Assessment tool deployment on network and endpoints;
- Perform an Enterprise Sweep & Network Analysis; and
  - Perform log analysis using data analytics to determine compromise or potential intrusion;
  - Review and verify alerts or notification from Compromise Assessment tool and assist your company in determining high level remediation actions and escalations.
- Compromise Assessment Report Generation
  - Provide a summary report for management and board-level consumption;
  - Align findings with key risks and potential exposures to your company.



Cyber Incidence Response

MANAGEMENT OF CYBER RISK

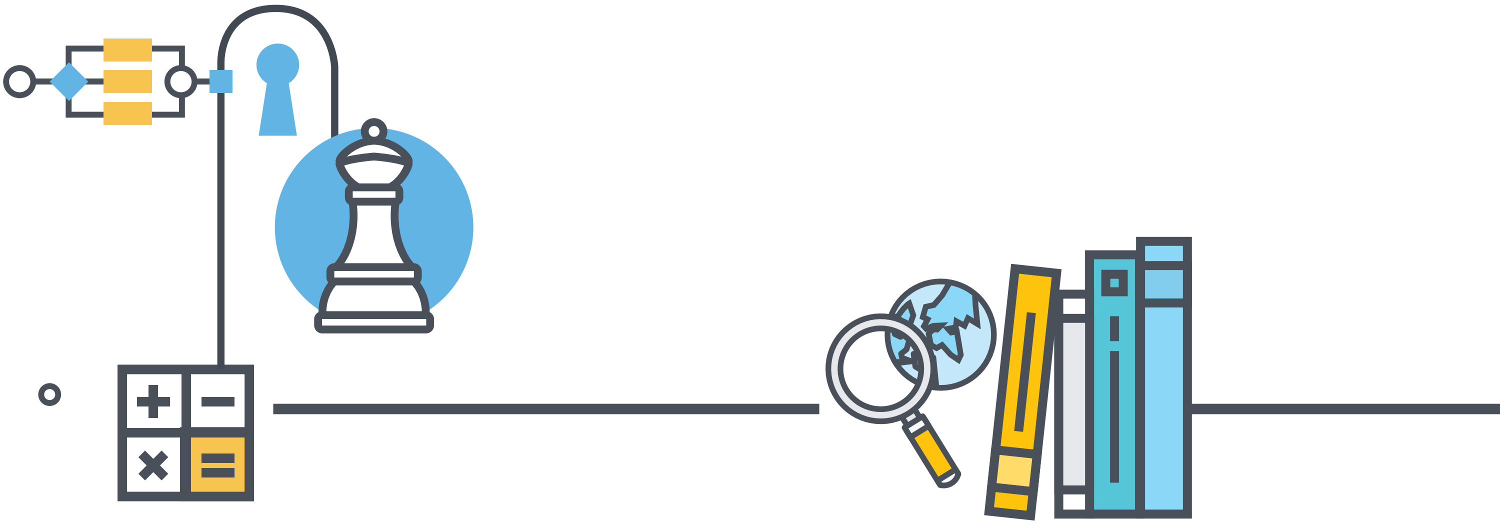
- Cyber risk measures
- Detection
- Recovery

What can you do to be prepared?

KPMG's Cyber Incidence Response aims to provide overall cyber incident management and digital forensic investigations to assist your company in handling and responding to cyber security incidents. This assistance may include, but not limited to:

- Incident response coordination;
- Detection and assessment of the nature and impact of the incident;
- Establishment of incident response communication protocols;
- Digital evidence collections;
- Entrance of data and documents into the chain of custody and analysis;
- Establishing temporary system event data and computer network data flow collection systems;
- Analysis and reverse-engineering of malicious digital artefacts;
- Assistance with communicating the incident to top management and board, or law enforcement agencies;
- Providing ad-hoc advice and recommendations on implementation of additional computer security controls to contain the incident;
- Providing ad-hoc advice and recommendations on implementation of additional computer security controls to eradicate the incident;
- Providing ad-hoc advice and recommendations on implementation of recovery steps from the incident;
- Performing forensic analysis and investigations; and
- Other tasks related to the above-referenced matter as may be identified and mutually agreed in writing during the course of this engagement.

Additionally, KPMG will provide a one (1) day training in relation to incident management and handling up to 20 participants.



Cyber Risk Awareness & Training

MANAGEMENT OF CYBER RISK

- Cyber risk measures
- Prevention

Cybersecurity - A continuous journey...

KPMG's Cyber Risk Awareness & Training for board members and directors is a customised half a day training, providing essential knowledge and insights to board members and directors in relation to cyber risks as follows:

- Cyber risk fundamentals;
- The role of the board member in cyber risk management;
- Understanding cyber risk frameworks and alignment to enterprise risk management;
- Understanding potential cyber risk exposure in business landscape – third parties, M&A, JVs, etc;
- The questions each board member should ask in relation to cyber risk;
- Understanding of cyber insurance; and
- How to test readiness.

The training aims to provide a common understanding of the cyber risks an organization faces, across all board members. The provided training will include a combination of dynamic workshops, role plays and hands-on exercises.

KPMG in Malaysia's Cyber Hub

KPMG in Malaysia recently launched our state-of-the-art Cyber & Digital Hub, which also functions as our Cyber Security Centre of Excellence.

The Cyber & Digital Hub is an interactive environment that showcases cyber security threats and trends, how they affect critical information technology infrastructure, and how organisations can protect their assets and manage cyber security risks.

With interactive touchscreens, video walls, breakout screens and tables, and simulations of actual environments such as industrial control systems, we are able to showcase how cyber security incidents could happen through simulation of cyber attacks, and what steps an organisation can take to protect their assets and minimise the threats.

It is also a platform for testing security solutions and how they can be implemented in various environments and industries.

Want to know more about Cybersecurity?

Contact Us:

- **Sia, Chin Hoe**
  PRINCIPAL | AUDIT and INFORMATION RISK MANAGEMENT
  email : chsia@kpmg.com.my
  Tel : +603 7721 3388 (ext: 3006)

- **Chua, Kenny SC**
  DIRECTOR | INFORMATION RISK MANAGEMENT
  email : kennychua@kpmg.com.my
  Tel : +603 7721 3388 (ext: 7807)

- **Michaux, Dani**
  HEAD of IT ADVISORY, ASEAN and ASPAC CYBER SECURITY LEAD
  email : danimichaux@kpmg.com.my
  Tel : +603 7721 3388 (ext: 7742)

- **Meling, Mudin**
  EXECUTIVE DIRECTOR | INFORMATION PROTECTION & BUSINESS RESILIENCE
  email : melingmudin@kpmg.com.my
  Tel : +603 7721 3388 (ext: 7753)

kpmg.com/my