Overview

This past year has witnessed some of the most sophisticated and highly targeted cyber attacks on high-profile institutions like Google, Iran's Nuclear power plant and most recently on NASDAQ, American Stock Exchange. In 2011 cyber attacks are on the rise and will only get 'better' with increase in targeted attacks on individuals and critical IT infrastructures.

The cost of the downtime caused by cyber attacks is high and for corporations, the average cost can be up to $6.3 million a day, according to McAfee Research Lab, causing an outage of "at least 24 hours, loss of life or failure of a company". Not only are IT security personnel challenged by the proliferation of social networking but also with the rise of cloud and mobile computing. Many of the professionals, however, admitted they needed more training to manage these technologies, yet, reported that such tools were already deployed without security in mind.

New Technology, New User Generation
All technological trends today, by nature, are open targets for privacy attacks. More so as internet anonymity disappears, with the popularity of web applications like Facebook and Twitter, the rise of the 'internet generation' coupled by high levels of personal technology adoption have complicated privacy controls further by causing an irreversible change in end user attitudes towards personal information protection and privacy.

Many senior executives also put themselves at risk by revealing far too much information about themselves on corporate websites and social networks that can easily be used to create 'email traps' and 'piggyback' attacks on correspondents of target. The vast majority of cyber espionage in the US which are linked to hacking into computer networks have been traced to emails with plausible-looking attachments that use part of Microsoft word and other commonplace programs to extract info and channel it to unauthorized people over the internet.

Data Loss, Threats and Human negligence
As industrial espionage catapulted to a position of great relevance, many of the world's top companies as technology changes becomes of growing importance in business. Illicit means by rival companies and their agents to disrupt operations and gain access to their competitors secrets. Industrial espionage is particularly prevalent critical IT infrastructure such as the defense, banking, energy and pharmaceutical sectors. Commercial espionage has become a big business among hackers as tactics used to gain access to highly prized data take a variety of forms.

Companies and Information security leaders today are facing a changing business environment, where traditional enterprise boundaries are quickly evaporating. It is also an environment driven by an increase in workforce mobility, greater decentralization of IT processes with the adoption of cloud computing services and a growing use of social media and collaborations tools within the company. The reality of trends such as cloud computing is that the trade-off for cost and management efficiency is the loss in direct control over data and applications.

Unfortunately, the implementation of information security policies or ISO 27001 compliance is often over-complicated or is avoided as it is viewed as a waste of time. This leaves organisations vulnerable to both accidental or malicious incidents that can damage reputation, customer confidence and result in large fines.

Only less than a third of global businesses have an IT risk management program in place capable of addressing the risks related to the use of new technologies. In spite of the rapid emergence of new technology, just one in ten companies consider examining new and emerging IT trends a priority activity for the information security function to perform.

Information is the life blood of an Organization
With 60 million cyber attacks a day worldwide, there is no time for complacency. However, despite the risk and dailythreats, that often go unnoticed, many companies are still under investing in updating their systems and staff security protection measures to secure their data.
Information is at the core of most businesses and recent cases of high profile data loss has highlighted how critical it is to protect information within organisations. CDW Security Straw Poll 2010, highlighted data loss emerges as the number one cybersecurity challenge/threat for IT security professionals. According to the IT managers:
•Data loss from internal threats, negligence and/or accidents was rated the "next big
threat" by 37 percent of respondents, revealing that human factors are the greatest challenge

•One-fourth of respondents identified “evolved forms of current threats” as their top future challenge, suggesting they are still struggling with threats for which there are proven solutions
•Despite high-profile news coverage of botnet attacks, botnets showed as the top concern of only 14 percent of respondents

Now, with the Data Protection Act coming into place in Asia this year, will this provide a legal framework that will help bring cyber criminals to court or will it become a burden for regulatory compliance especially to companies that deal with large exchange of customer information daily?

This 2-day Conference brings together experts, practitioners and researchers in a collaborative environment to present and discuss issues relating to cyber security. It provides a platform for the next generation to be able to share their knowledge and experiences and to develop new ideas and promote a more proactive and holistic approach to improve the level of security in information technology.

The conference will ensure you leave with greater knowledge and tools that will help you and your company:
•Integrate security into an effective IT risk management framework
•Build a security strategy to manage network security, data protection and leakage
•Understand the implication and guidelines to comply with the Privacy Data Protection (PDP) Act 2009
•To adopt a practical approach to ISO 27001
•Improve security in a mobile environment
•Understand and manage the risk associated with social media and new technologies like Cloud Computing.
•Develop Data Recovery, Mitigation and Contingency planning
•Utilise appropriate techniques to keep your organization secure

Target Audience
•Chief Information Security Officer (CISO)
•CIOs and CTOs
•CEOs and HODs
•IT Security Managers/Officers/Analysts/Specialists
•Information Security Managers/Officers/Analysts/Specialists
•Network and Infrastructure Managers
•Risk Managers
•Compliance Managers
•Heads of IT /ICT

Target Industries
•Public-Listed Companies
•Government-Linked Industries
•Ministries and Agencies
•Small Medium Enterprises
•Small Medium Industries
•Universities
•Across the board industries

Sponsored by

KEMENTERIAN PENERANGAN KOMUNIKASI &KEBUDAYAAN

Supported by

MSC MALAYSIA National ICT Initiative

IMPACT

MOSTI

OWASP The Open Web Application Security Project

CyberSecurity MALAYSIA