Awareness of cybersecurity still lacking

BY **Edwin Yap**

As the year wound down and the enterprise IT world forged ahead, one topic that seemed to have stayed in the background, despite its importance, is cybersecurity. With more enterprises depending on IT these days, companies can no longer afford to back-burner cybersecurity when it comes to IT priorities.

According to the 6th Global Economic Crime Survey conducted by PricewaterhouseCoopers (PwC) recently, cybercrime now ranks as one of the top four economic crimes globally with 23% of respondents reporting that they were victims of cybercrime. In Malaysia, 5% of respondents report being victims of cybercrime while 28% say they are likely to experience cybercrime perpetrated against their business and organisation in the next 12 months.

The global survey, conducted between June and November 2011, polled 3,877 respondents from 78 countries, 93 of whom were from Malaysia.

"In a world where most enterprises rely on technology, businesses are increasingly opening themselves up to the risk of criminal activity," says Lim San Peen, senior executive director at PwC Advisory Services, Malaysia.

PwC notes that the perception of cybercrime as a predominantly external threat is changing and organisations are now recognising the risk coming from within organisations as well. Malaysian respondents say the information technology (IT) department is the most likely source of cybercrime internally, the survey notes. IT was cited by 61% of respondents, followed by operations (57%), sales and marketing (50%) and finance (34%).

PwC also notes that many respondents in Malaysia lack best practices in cybercrime crisis response and are not aware of having one. Examples of such responses include the investigation, controlled emergency network shutdown procedures and media communications. Interestingly, 29% of respondents in Malaysia say their organisation does not monitor social media sites.

"Rising incidents of data loss and theft, computer viruses and hacking and other forms of electronic crime demonstrate the need for a more cyber-savvy approach to fraud prevention," says Lim. "There are many ways to protect your organisation against economic crime, including conducting regular fraud risk assessments and instilling a cyber risk-aware culture."

CIP programmes ignored

One area of urgent concern is the protection of the critical infrastructure sector, which comprises industries such as finance, telecommunications, public services, energy, healthcare, manufacturing, government, transport and public works.

Lim: In a world where most enterprises rely on technology, businesses are increasingly opening themselves up to the risk of criminal activity

Susanna: The focus must move from short-term fixes to a more holistic approach integrated with long-range strategic corporate goals

In a global survey polling companies on how engaged they are with their respective critical infrastructure protection (CIP) programmes, security firm Symantec notes that respondents were less aware and not as engaged with their respective national CIP programmes in 2011 compared with 2010.

The survey reveals that 36% were "somewhat" aware of such plans being discussed in their respective country compared with 55% in 2010. In addition, 26% say they were "neutral" or had "no opinion" of their government's CIP programmes compared with 42% last year.

CIP programmes are policy-based, educational awareness programmes undertaken by governments to ensure providers of critical infrastructure in their respective countries are prepared to respond in the event of an emergency. In Malaysia, for instance, CIP programmes come under the purview of CyberSecurity Malaysia.

The survey, conducted for the first time in Malaysia, notes that 34% of respondents in Malaysia felt unengaged in the government's CIP programmes while 36% were neutral or had no opinion on such initiatives.

Ilias Chantzos, senior director of government affairs for Symantec Asia-Pacific, Japan and Europe, the Middle East and Africa, says the decline in awareness globally was likely due to the rise of information security attacks in 2011 compared with 2010, when these companies struggled to battle such attacks and prioritised them over other issues, such as finding out more about CIP programmes.

"It's understandable that every critical infrastructure provider has finite resources, limited manpower and money, especially in today's economic environment," Chantzos explains. "These providers are limited to what they can throw at the problem."

Asked how Malaysia is faring in this area, Chantzos says it is hard to say, noting that this was the first time Malaysia was included in the survey.

Smartphone, tablets a new threat?

The rush to adopt new technologies and media by global companies could also be forcing enterprises to treat security threats as an after-thought, notes a study by Ernst & Young (E&Y).

In its 14th annual Global Information Security Survey released recently, E&Y found that moving into the increasingly borderless world of cloud computing and social media, a growing gap is developing in global organisations between business needs and the ability to tackle new and complex security threats.

With 80% of organisations currently using or considering using mobile tablets and 61% using or considering the use of cloud computing services within the next year, the threat of security breaches has become an after-thought in the rush to adapt to the rapidly changing landscape.

Susanna Lim, E&Y Advisory Malaysia IT risk leader, notes that more major businesses and industries are being run on software and delivered as online services.

"The focus must move from short-term fixes to a more holistic approach integrated with long-range strategic corporate goals," she says.

Another area surveyed that is of great interest is the impact of social media on security. According to E&Y, most respondents (72%) claim that external malicious attacks are their top risk. These attacks, it says, may be fuelled by information obtained through the use of social media that was used to send targeted phishing messages to targeted individuals.

To help address potential risks posed by social media, organisations seem to be adapting a hard-line response, with more than half (53%) saying they would block access to sites rather than embrace the change and adopt enterprise-wide measures.

Interestingly, the survey shows that only 12% of respondents are presenting information security topics at each board meeting and less than half (49%) of survey respondents state that their information security function is meeting the needs of the organisation.

Susanna says there is a need to have a pragmatic and proactive response rather than a reactive one, noting that information security needs to be more visible in the boardroom with a clearly defined strategy that will support the business in the cloud and elsewhere.

"In order to effectively manage IT risks in general, organisations need to get a broad and comprehensive view of the entire IT risk landscape. This holistic perspective will provide companies with a starting point to help identify and manage current IT risks and challenges as well as those that may evolve over time." E