Corporations falling behind on cyber security

BY AHMAD NAQIB IDRIS

KUALA LUMPUR: After the recent spate of high-profile cyberattacks on global and local corporations, such as the hacking of Apple Inc's iCloud servers and the "hijacking" of Malaysia Airline Systems Bhd's webpage, businesses are becoming more aware of the importance of cyber security as part and parcel of their operations.

In the latest Annual Global CEO survey by PricewaterhouseCoopers (PwC), CEOs had highlighted cyber security as one of the key concerns, as vast quantities of corporate information are made accessible via the Internet.

In Malaysia, while corporations are more aware of the risks involved, Neil Meikle, associate director at PwC Consulting Services (M) Sdn Bhd, said that there has been a lack of action in addressing the matter.

"We seem to be in a state of 'business as usual' now when it comes to cybercrime. Cyber security investments aren't going up, but the number of high-profile attacks continues to go up," he said.

Meikle, who specialises in cyber security, said the frequency of cyberattacks is increasing in Malaysia, as indicated by PwC's 2014 Global Economic Crime Survey.

According to the survey, 31% of Malaysian respondents said they had experienced a cybercrime over the previous two years — a sharp increase compared with 5% in 2011. Out of the 31%, 9% of respondents believed that they have suffered financial losses of more than US$1 million (RM3.71 million).

"There's a risk that it's becoming normal. It's serious, but leaders maybe are not seeing how serious it is because it is still business as usual for these companies," said Meikle.

PricewaterhouseCoopers Consulting Hong Kong Ltd manager Dan Kelly, who specialises in cyber threat detection and response, said that cybercrimes such as targeted attacks are usually aimed at stealing information, or even finances.

Kelly said this is possible through the transmission of malicious software (malware), which collects and transmits information to the attacker, while remaining undetected in the system.

Meikle: Cyber security investments aren't going up, but the number of high-profile attacks continues to go up. **Photo by Sam Fong**

He noted one case where a breach of a multinational company, orchestrated by an extremely active hacking group in Southeast Asia, had spanned over 12 different countries. The malware remained in the company's system for about 14 months undetected.

"This is very common for big companies with a big international presence. We would come to a breach assessment exercise, find a compromise, initiate the instant response process, and find that it spans every continent," he said.

Over the years, Meikle noticed that the attack methods employed are getting more and more sophisticated compared to a decade ago, where businesses resisted attacks through the use of traditional perimeter defences such as firewalls and antivirus software.

"Obviously, these are still required, but the game has changed. Now you've got these super agents which can parachute in over the defences very easily with these advanced persistent threats (APTs)," he said.

Meikle added that a deep technical knowledge is not required in orchestrating an attack, noting that the requirement of technical abilities for an attack has significantly decreased over the past 10 years.

This is attributed to the wide availability of exploit packs and malware creation kits on the web, which are user friendly and very effective.

Looking ahead, Meikle expects the sophistication and incidences of attacks to increase, and hopes businesses show more initiative in addressing the issue.

"Companies need to invest in line with their threat level, depending on the industry they're in, the nature of their company, who's going to attack them and why," he said.

He added that there has been a shift from the traditional usage of perimeter defences, as companies should place their investments around its critical information rather than spending a huge sum to protect all of its data.

Similarly, Kelly hopes businesses start reacting, as the cost associated with the risk of cyber threats can be exponential.

"It's not just something you should be saying 'okay we're now aware of it,' it's something you should be planning for. At the end of the day, if you don't have a plan, it's just conversation," said Kelly.