ThaiPR.NET
Thailand Press Release ข่าวประชาสัมพันธ์

Date: 29 October 2014
Source: Website ThaiPR
http://www.thaipr.net/it/579197

Cybercrime continues to rise but spending falls, PwC says

Information technology security breaches rose by 48% to 42.8 million attacks across the globe in the past year as businesses spent less to stop them, according to The Global State of Information Security® 2015 by PwC in conjunction with CIO and CSO magazines.

The reported figure is equivalent to 117,339 attacks a day and represents a 66% surge of year-on-year detected incidents since 2009, a worldwide survey of more than 9,700 executives and IT directors in 154 countries reveals.

Cybercrime is rising dramatically, led by a 41% jump in the number of security incidents in Europe, 11% in North America, and 5% in the Asia Pacific.

This led to a substantial increase in the financial costs of investigating and mitigating attacks. Globally, the estimated average financial loss from cybersecurity was $2.7 million, a 34% rise from the previous year. The number of respondents reporting losses of $20 million or more almost doubled over 2013.

"Information security spending isn't keeping pace with increases in the frequency and costs of security incidents, despite elevated concerns about cyber risks," Vilaiporn Taweelappontong, Partner at PwC Consulting (Thailand) Ltd., said.

In fact, investments in information security budgets declined 4% to just $4.1 million over 2013, she said.

Security spending as a percentage of the IT budget has remained fixed at 4% or less for the past five years, the findings showed.

Worryingly, small organisations or those with revenue of less than $100 million have been particularly lax in security spending. They slashed security investments by 20% over 2013 while large and medium companies spent modestly with a 5% rise in security budget.

Even though cyber risks will never be completely abolished, "today's businesses across the world, including Thailand, must do more to ensure they implement a risk-based approach to security that prioritises their most valuable assets, while at the same time, proactively addresses the most relevant threats," Vilaiporn said.

PwC's 17th annual survey found that organisations of all sizes and in all industries are aware of the serious risks involving cybersecurity. However, larger companies do detect more breaches.
Large businesses with gross revenue of $1 billion or more detected 44% more incidents in 2014.Medium-sized companies with revenues of $100 million to $1 billion witnessed a 64% rise in the number of detected incidents, it said.

As large, well-capitalised companies implement more stringent information security safeguards, threat actors are simultaneously increasing their assaults on middle-tier companies whose security practices aren't readily in place compared to that of the larger businesses, Vilaiporn explained.

"Today, most organisations realise that cybersecurity has become a persistent, all-encompassing business risk," Vilaiporn said. "But as the frequency and cost of incidents continue to rise, many businesses have failed to update critical information security processes, technologies, employee security awareness and training programmes."

Employees are the most-cited culprits of cybercrime

Insiders—which includes current and former employees—have become the most-cited perpetrators of cybercrime.

According to the study, respondents said incidents caused by current employees rose by 10%. However, employees aren't the only source of rising insider threats. Third parties with trusted access to networks and data, including current and former service providers, consultants and contractors also ranked as top insider threats.

"When organisations overlook the threats residing inside their ecosystems, the effects can be devastating. Yet many companies haven't implemented processes and technologies to address internal incidents," she warned.

Vilaiporn said those executives who compromise or handle their organisational crimes internally instead of involving law enforcement and initiating legal charges would also leave other firms vulnerable to repeated attacks if they were to recruit these wrongdoers in the future.

Business leaders still lag when it comes to raising effective security awareness that requires top-down communication and commitment.

Another worrisome finding is a diminished commitment to employee training and awareness programmes. Fewer than half (49%) of respondents surveyed say their company has a proper cross-organisational team to manage information security issues regularly.

Forty-two percent of respondents say their Board actively participates in an overall security strategy and just 36% say the Board is involved in security policies.

The Asia Pacific sets the pace in security practices

The Asia Pacific remains a leader in implementing strategic processes and safeguards for information security, setting the pace in various practices.

The Asia Pacific remains a leader in implementing strategic processes and safeguards for information security, setting the pace in various practices.

The region is most likely to have an information security strategy that is aligned to the needs of the business (66%) and to have a senior executive who communicates the significance of security across the organisation (73%).

The Asia Pacific ties with South America and North America in one key practice with 58% of respondents from the three regions say they have security standards for external partners, customers, suppliers, and vendors.

While the Asia Pacific has led the way in security spending in recent years, the region reports a 13% decline in information security budgets in 2014. Respondents also report that financial losses due to security incidents increased by 22% over 2013.