newswit.com

17 January 2014
Source: Website newswit.com
http://www.newswit.com/.it/2014-01-16/10fbec75a4baec26bfa86e14be5a7f8a/

PwC Urges Firms to Bolster Information Security as Risks Mount

Information technology security breaches rose 25% across the globe in the past year even as companies spent a record amount of money to stop them, according to The Global State of Information Security® 2014 by PwC in conjunction with CIO and CSO magazines.

Businesses must seek to ensure that they have robust information security safeguards in place to protect their operations as IT-related risks continue to rise despite a rise in overall security spending in the past year and increased confidence among executives in thwarting attacks.

Business leaders are overly optimistic about the strength of their security frameworks, the survey warned, adding adversaries are expected to outpace them unless companies actively update their security practices to keep pace with growing threats.

PwC's 16th annual survey on The Global State of Information Security® 2014, which featured interviews with more than 9,600 top-ranking executives from 115 countries, found that the number of security incidents detected in the past 12 months rose 25% to 3,741. Average financial losses associated with security incidents also climbed 18% over the same period.

Average information security budgets totalled $4.3 million in 2013, a 51% jump from a year earlier. Despite this increase, however, security measures account for only 3.8% of the total IT spending.

Vilaiporn Taweelappontong, Partner at PwC Consulting (Thailand) Ltd, said the rise in global security incidents combined with outdated strategies that leave information technology systems vulnerable to attack are key challenges for companies.

"As security incidents in the world rise, so do the financial costs," Vilaiporn said. "Many executives are still too optimistic about the strength of their information security systems. That leaves their businesses open to fraud and makes them less attractive to potential clients."

"It's also troubling to see that the number of companies that are unaware of security breaches has doubled over two years. This may be because they're investing in outdated security solutions."

According to the study, 74% of respondents believe their organisation's security precautions are effective, with top executives even more optimistic. Thirty percent (30%) of respondents are from large organisations with more than $1 billion in revenue.

Optimism also runs high when half of respondents (50%) considered their organisation as 'front-runners' ahead of the pack in strategy and security practices, a 17% increase over last year. This means that they believe they have an effective strategy in place and are proactive in executing the information security plan.

However, the survey found that only 17% actually qualify as true information security leaders. PwC defines 'leaders' as companies that have an overall information security strategy; employ a chief information security officer (CISO) or equivalent in place; have measured and reviewed the effectiveness of their security in the last year; and understand exactly what types of security events have occurred.

While insiders, particularly current or former employees, are most likely to perpetrate security incidents, hackers (32%) lead the pack as a source of outsider security incidents, followed by competitors (14%), organised crime (12%), activist groups (10%), and terrorists (8%) among others.

Technologies move faster than security

As mobile devices, social media, and the cloud become commonplace both inside the enterprise and out, the survey found that the adoption of technology is moving faster than security.

Sira Intarakumthornchai, CEO for PwC Thailand, said that another key risk to data security is the surge in the use of smart phones, tablets, the "bring your own device" (BYOD) trend, and the proliferation of cloud computing.

Survey respondents indicate that efforts to implement mobile security programmes don't show substantial gains over last year and continue to trail the increasing use of mobile devices.

"While the use of mobile devices has generated a massive flood of business data, but deployment of mobile security hasn't actually kept pace with use," Sira said.

According to the report, almost half (47%) of respondents use cloud computing, yet only 18% say they have policies governing cloud services. While most companies have implemented traditional security safeguards including VPNs, firewalls, encryption of desktop PCs, they're less likely to have deployed tools that monitor data and networks to provide real-time intelligence about today's risks.

Respondents say the top three obstacles to improving security in the long term include insufficient capital funding, inadequate understanding of how future business needs will impact security and a lack of leadership from the CEO, senior management and board members.

Looking at security spending outlook, the survey showed that nearly half of respondents expect security spending over the next 12 months will increase, up from 45% a year earlier.

Regionally, South America and Asia Pacific lead the world in security practices and performance. Sixty-six percent of South American and 60% of Asia-Pacific businesses expect to boost security spending over the next 12 months, while Europe and North America lag in many aspects.

"Asia-Pacific companies remain among the global leaders in security spending. Average budgets have increased 85% over last year, and our region spends the most on information security as a percentage of overall IT spending," he said, citing the report.

Given today's elevated threat landscape, it's vital that Thai companies rethink security strategies so they are integrated with business needs and prioritised by top executives.

"Security models of the past will only take you so far," Sira said. "We can't defend future threats with yesterday's strategies."

Businesses should create a security culture that starts with top executives and cascades throughout the company and supply chain, Sira said. This involves engaging in public-private collaboration for enhanced threat intelligence.

"Today's elevated risk landscape demands a new approach to security," Sira said. "Otherwise Thai businesses will find themselves vulnerable to attack and risk entering the Asean Economic Community unprepared."