Major cyberattack can devastate business

Manila Times · 10 Jun 2018 · C3 · TONY M. MAGHIRANG

ALARGE- SIZED organization in the Philippines can incur potential economic losses of $7.5 million due to a concerted cybersecurity breach, a study commissioned by Microsoft revealed recently. This is more than 200 times the average economic loss for a mid-sized company.

The Microsoft and Frost & Sullivan study titled "Understanding the Cybersecurity Threat Land- loss, damage to customer satisfaction and market reputation— as has been made all too clear AFP file photo within an hour, the same response time as those respondents (38 percent) with fewer than 10 cybersecurity solutions While more and more organizations are considering digital transformation to gain competitive advantage, the study has shown that 46 percent of respondents see cybersecurity strategy only as a means to safeguard the organization against cyberattacks rather than a strategic enabler of business transformation.

AI and other practical solutions

In a digital landscape where cyberthreats are constantly evolving and attack surface is rapidly expanding,

muscles to detect and act on threat vectors based on data insights. AI's ability to rapidly analyze and respond to unprecedented quantities of data is becoming indispensable in a world where cyberattacks' frequency, scale and sophistication continue to increase.

According to the Microsoft study, more than almost four in five (79 percent) organizations in the Philippines have either adopted or are looking to adopt an AI approach towards boosting cybersecurity.

An AI-driven cybersecurity architecture will be more intelligent and be equipped with predictive abilities to allow organizations

posture before problems emerge.

AI is but one of the many tools that organizations need to incorporate or adhere to in order to maintain a robust cybersecurity

that they can consider in improving their defense against cybersecurity threats:

Position cybersecurity as a digital transformation enabler. Connect cybersecurity practices and digital transformation effort to guide and keep the company safe through its journey.

Continue strengthening your security fundamentals. Basic best practices such as maintaining strong passwords, conditional use of multi-factor authentication against suspicious authentications, and keeping device operating systems, software and anti-malware protection genuine and up-to-date can rapidly raise the bar against cyberattacks.

Adopt integrated best-of-suite tools. Prioritizing best- of- suite tools allow your operators to hone

tools and maximize your risk coverage without the risk of introducing too many tools and complexity to the environment.

Assess review and comply continuously. The organization should be in a constant state of compliance to test for and address gaps in a rapidly organization.; and

Leverage AI and automation. Current advances in cutting-edge technologies have shown a lot of potentials not just in ensuring detection but also in enhancing capabilities and capacity to make actionable decisions.