CEOs must view cybersecurity holistically

As technology advances and businesses become more technology-driven, the rate of cybercrimes is likely to increase exponentially. According to research firm Gartner, in 2017, businesses are likely to spend over $90 billion to secure their systems against potential cyberattacks, which is expected to reach $113 billion by 2020.

The first two quarters of 2017 saw cybersecurity attacks ranging from leaks related to voter record information, leaks of spy tools from the US intelligence agencies to the outrageous ransomware threats. WannaCry ransomware spread around the world targeting thousands of public and large corporations; another malware, Petya, was modified to be more complex and caused devastating impact at even higher levels.

While the world was still recovering from the impact of these major attacks, HBO became the prime target of the cyber underworld, where hackers claimed to have stolen an estimated 1.5 terabytes of data and demanded about $6 million to stop the leaks.

Indian enterprises have also increasingly become a target for cyberattacks. According to the Indian Computer Emergency Response Team (CERT-In), India has seen a total of 171,000 cybercrimes in the past three years with 27,482 cases being reported between January and June 2017. Given the growth of cybercrime incidents in India, board members and C-level executives of many companies are forced to identify the spread of ever-changing cybersecurity risks as one of the greatest challenges for their organizations.

Last year, India witnessed one of the biggest security breaches, placing about 3.2 million debit card users at high risk. Further, according to a study, mobile apps of seven Indian banks were found to be infected with malware. There have been a lot of opinions on the kind of harm that cybercriminals are expected to cause to various sectors. While the banking and financial services market faces the greatest cybersecurity risk, India also aims to transform itself digitally on the back of the Digital India initiative undertaken by the government, which, consequently, may lead to greater risk for government bodies, as consumers are moving towards digital transactions using smartphones. India’s cybersecurity preparedness has been challenged—a case in point being the recent HBO cyberattack that focused on the vulnerability of our media and entertainment industry, as an unreleased episode of HBO’s *Game of Thrones* was leaked online.

According to KPMG India’s CEO Outlook Survey 2017, over 89% of Indian CEOs agree that mitigating cyber risk is now at the top of the boardroom agenda, and almost 84% of them plan to invest significantly in it over the next three years. About 45% of the CEOs surveyed in 2017 said that they feel prepared for a cyber event, up from 17% in 2016. While CEOs now feel they have a better understanding of cybersecurity, many still do not ‘own’ cyber to the extent where they need to properly manage risks associated with it.

Another key highlight from the survey is that humans have emerged as one of the weak links in cybersecurity attacks and it is imperative to focus on cyber hygiene and awareness. About 62% of Indian CEOs acknowledge that the biggest threat to enterprise security lies within an organization in the form of its own employees, who have access to sensitive information and company assets. This puts the staff at an inherent risk, a challenge compounded by the always-connected environment that they operate in. Knowingly or unknowingly, insiders could provide an opening for malicious external attacks.

The ‘fear factor’ apart, there is another very good reason to view security differently—it has the potential to generate revenues and achieve differentiation for businesses. Until recently, cyber was

considered part of risk and was seen as a function of the information technology (IT) environment. However, CEOs are now gradually becoming cognizant of the business opportunities in building cyber resilience across the board: 76% of CEOs view cybersecurity as an opportunity to innovate and find new revenue streams. At a time when clients and consumers are wary of security breaches, businesses are employing digital technologies to create value and increase operational agility for competitive differentiation—a well-designed cybersecurity programme can help organizations build trusted customer relationships.

With the growing sophistication of the cyberworld and the rapid pace of cyberattacks, the need of the hour is to deal with cybersecurity in a holistic manner, rather than treat it as a technology risk alone. As the nature of the threats evolves, so should an organisation’s efforts to secure its data and intellectual property. The current IT environment demands that we look beyond traditional security measures and, instead, create an agile and flexible security capability.

Akhilesh Tuteja is partner and head of risk consulting, KPMG in India.

END