Time to talk about business-driven security

India is as vulnerable to cybercriminals and cyberattacks as other parts of the world. According to the Indian Computer Emergency Response Team, at least one cybercrime was reported every 10 minutes in just the first six months of 2017. These attacks ranged from ransomware, phishing, scanning or probing and site intrusions to defacements, virus or malicious code and denial of service attacks.

There are no official figures available on the loss of business due to cyberattacks. But unofficial analysis done by some of the cybersecurity firms show this figure is around $4 billion every year. The bigger problem in India is the secrecy around cyberattacks where the firms or promoters would rather put a lid on cybercrime than come out in the open. The problem with this is that other companies which are potential targets don’t get a chance to even be prepared, while hackers tend to share their secrets on the dark Web—a platform where hackers interact, buy and sell information anonymously.

According to cyber experts, India was among the countries worst hit by the recent WannaCry ransomware. Several isolated incidents were reported in states such as Gujarat, Kerala, Andhra Pradesh, Tamil Nadu and West Bengal.

Companies can no longer look at cybersecurity as an afterthought. Rather, there is an urgent need to bring cybersecurity policy to take centre stage in all business decisions.

The greatest risk comes from the fact that firms are not considering cybersecurity as a business driver. Sometime back, McKinsey and the World Economic Forum undertook joint research to develop a fact-based view of cyber risks, assess their economic and strategic implications, and lay a path forward. They found that despite years of effort, and tens of billions of dollars spent annually, the global economy is still not sufficiently protected against cyberattacks. The risk of cyberattacks could materially slow the pace of technology and business innovation with as much as $3 trillion in aggregate impact.

While everyone generally agrees that security breaches are bad, balancing the cost of prevention against other business priorities can be trickier. Unified in preventing breaches, these same stakeholders diverge when forced to choose between security and business values such as profitability, operational uptime, or ease of use. We should start to think beyond just the technology and connect the security incidents to business context for a business-driven approach to security. The following are the first few steps organizations can take:

Raise executive awareness: Risks should be made part of boardroom discussions to receive the visibility they need to be properly addressed. Technology risks are still not translated well enough into business value terms that executives can understand to make educated decisions on courses of action.

Strengthen the human factor: Not changing passwords or opening unknown emails or links increases exposure to a host of cyberthreats including ransomware. This makes people one of the weak points in the defence against cyberthreats. Test and measure vulnerability, then provide essential education to raise user awareness of security issues.

Focus on what is critical: Business impact analysis (BIA) should be performed regularly to identity which business processes are most critical to the organization’s objectives. Highly critical business processes, systems, devices and information assets should receive prioritization for resiliency and recovery efforts.

Maintain your systems: Firms must employ an upgrade and maintenance cycle to reduce their attack surface. Failure to patch, update and upgrade (especially away from unsupported operating systems) can permanently ruin a firm's reputation or even put public safety at risk.

Back up your data: Not being able to retrieve lost data can heavily impact an organization. During BIA, should you determine that critical information assets were lost, find out how far back in time you can reasonably recreate the data. Organizations must have mechanisms to ensure data is backed up accordingly.

Perform continuity planning: What happens if the system you use to do your job is not available? Some functions can stop until the system is available. Others, such as medical services or airline flights, cannot. A critical step to building resiliency is to plan for the inevitable disruption to business processes, systems or facilities. Continuity or recovery plans should be documented and tested for potential threat scenarios to ensure functional continuity.

The current state of cybersecurity at most enterprises is not uniformly mature to detect, prevent and respond to these threats in a timely manner. Cyber risk is but one dimension of risk an organization faces. The best way to thwart and respond to a cyberattack is to take a business risk management approach.

Rajnish Gupta is regional director for India and South Asian Association for Regional Cooperation at RSA Security Llc, a Dell Technologies Inc. business.

END