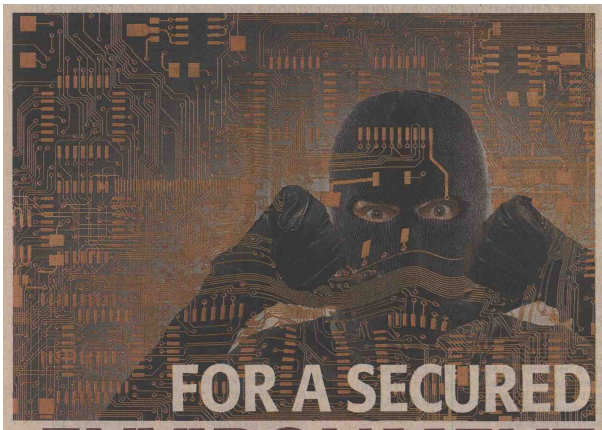

FOR A SECURED ENVIRONMENT

WITH THE PM'S DIGITAL INDIA INITIATIVE FOCUSSED ON EMPOWERMENT, DEVELOPMENT, GROWTH AND GOVERNANCE, THE CORPORATE WORLD REALISES THE DIRE NEED FOR A STRATEGIC APPROACH TO SECURITY CHALLENGES

Neha.Bhatia@timesgroup.com

India is a major hub of the IT services and software sector. While she has gained global recognition in these fields, the standardisation in the field of IT security is essential to reap its benefits to the fullest.

Talking about cyber security, R Chandrashekhar, President, NASSCOM, says, "Cybersecurity is a multi-dimensional concept, which includes many disciplines and fields. Nations have to take appropriate steps in their respective jurisdictions to create necessary laws, promote the implementation of requisite security practices, incident management, and information sharing mechanisms, and continuously educate corporate and home users about cybersecurity. It's a global problem that has to be addressed by all stakeholders jointly."

Agrees Rajendra Pawar, Chair, NASSCOM Cyber Security Task Force and Chairman, NIIT, "Securing the cyberspace has become an important priority for governments, businesses and citizens across the world. In line with the Prime Minister's vision of making India a cyber-security expert nation and his recent exhortation to the industry, we have created the cyber security taskforce, which aims to make India a global hub for providing cyber security solutions, including cyber security products and services. The taskforce will focus on the four key pillars: industry development, policy enablement, technology development and skill development."

Even the results of an international survey of 102 security professionals conducted at this year's e-Crime Congress press on the need for strong security guidelines. Nearly all respondents (98 per cent) believe that the law should address serious data breaches that expose consumers' data loss through punishments such as fines (65 per cent), mandatory disclosure (68 per cent), and compensation for consumers' affected (55 per cent).

Respondents feel that companies that are not taking action against data loss and theft have it as an agenda item, but it's not yet a high enough priority (45 per cent). Furthermore, 70 per cent say the CEO should hold ultimate responsibility should a breach arise. And the pressure is mounting, as 93 per cent of all respondents believe the advent of the Internet of Things will make companies even more vulnerable to data theft.

Neil Thacker, Information Security & Strategy Officer at Websense, explains, "The more we talk about the issues and share the common techniques used to breach organisations and abuse, steal or damage data, the better. With the increasing data deluge that will only increase with the Internet of Things, and the dilemma of an increasing information security skills shortage, organisations have a tough challenge ahead. Implementing a data theft prevention control that provides a data-centric approach to security, alongside building a culture of security accountability across the business through collaboration, is essential to keep data protected."

BYOD and IoT devices has opened up huge security risk to not only home users but also in enterprises where business continuity remains key to their success. Today's digitally connected enterprises need security solutions that not only protects the end points but also the mobile devices.

Govind Rammurthy
CEO and MD, ESCan

In the face of an ever-evolving cyber threat landscape, organisations need continuous innovation to help them protect their critical data and applications wherever they choose to host them; on their premises, in the cloud or a hybrid of both.

Raj Samani, EMEA chief technology officer, Intel Security, feels that it is imperative to close the gaps. "Our goal is to enable businesses around the globe to more aggressively and effectively defend against data security incidents and targeted attacks. We plan to close the gaps between detection and remediation by creating and managing a security ecosystem designed to enable real-time communication, intelligence exchange and response across security tools," he states.

Mar. McLaughlin, president and chief executive officer at Palo Alto Networks, agrees as he points out, "Security is now a top concern for every business, and with continued growth in both the volume and sophistication of attacks, a breach prevention-focused strategy is essential to ensure a safe digital future for organisations and individuals alike."

According to industry experts, a tougher lining around their cloud services is what is needed by enterprises in all sectors at the moment. India is a major hub of the IT services and software sector and has gained global recognition in these fields. The standardisation in the field of IT security is the need of the hour. Dr. Gulshan Rai, National Cyber Security Co-coordinator, Government of India, says that standards have been bringing much business impact in various industries, including telecom and ICT. "But as the threats are expanding each day, standards or making of standards in the cyber security is a much daunting and complex task; hence harmonised and collaborative efforts from various sectors and bodies are required to address the emerging technologies in this area. I am glad an assertive step in this area has already been started which will help programmes of Digital India and Make in India," he concludes.