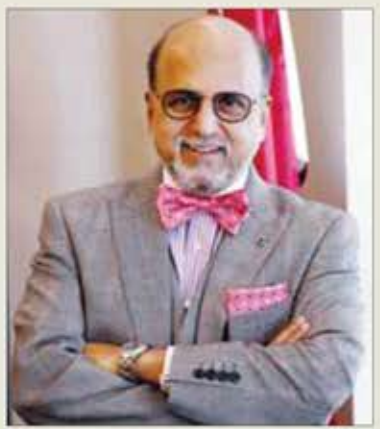
BANKING ON KNOWLEDGE

Risk integration is key to better cybersecurity management

By Dr R Seetharaman



Digital connectivity plays an anchor role in unlocking innovation and prosperity around the world, but increasing cyber threat is a roadblock to collective path of progress.

The fourth industrial revolution, which combines advanced technologies in innovative ways, is set to dramatically reshape the way people live, work and relate to one another. As per Cybersecurity Ventures, the cybercrime will cost the world $6tn annually by 2021, this is up from $3tn in 2015.

Cybercrime costs include damage and destruction of data, stolen money, lost productivity, and theft of intellectual property, theft of personal and financial data, embezzlement, fraud, and post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

The work space is undergoing changes, robotics and artificial intelligence are going to play important roles and the customer will be more empowered in the digital environment. Data breaches in 2018 compromised the personal information of millions of people around the world.

The latest victims were Marriott hotels, which recently revealed that hackers had accessed the information of an estimated 500mn customers. Payment card information and personal data such as billing addresses, phone numbers and e-mails of British Airways were hacked. For Cathay Pacific, passenger data was accessed without authorisation. Centre for Internet and Society (CIS) also pointed out that about 130mn Aadhar numbers along with other sensitive data were available on the Internet.

The reason for the data leak was narrowed down to four government-run schemes ranging from National Social Assistance Programme by the Ministry of Rural Development, the National Rural Employment Guarantee Act (NREGA), also by the Ministry of Rural Development, Daily Online Payment Reports under NREGA by the government of Andhra Pradesh and the Chandranna Bima Scheme, also by the government of Andhra Pradesh.

The public and private partnership model should be adopted to face the challenges.

This can be done by establishing areas of common interest, supporting capacity building and resource pooling and developing benchmarks for resilience.

There are various reasons for cyber-attacks/data breach incidents – few of them are as follows. In effective vulnerability management, lack of security monitoring, human errors – accidental publishing, hacking, targeted attack, business e-mail compromise, phishing and social engineering attacks, inadequate encryption, on-adherence to strong password policy, state sponsored terrorism/attacks and corporate espionage.

The various cyber-attacks, which have left significant impact on global organisations. Institutions need to be more collaborative on security issues.

Banks need to manage the change by redefining their business models to manage various stake holders such as customers, regulator and shareholders.

The involvement of the company's board is required which should set the tone for enhancing security and determine whether the full board or a committee should have oversight responsibility.

Board of directors are starting to take note, particularly members of the audit committee, who list cyber security among their top concerns.

Test effectiveness of existing security devices/ solutions and fine tune. Adopt new technologies such as artificial intelligence and machine learning to identify abnormal behaviour in networks.

Maintain IT system hygiene i.e., effective patching, hardening and baseline. Develop blue/red and purple teams to have balanced check on the vulnerability exploitation, effective threat monitoring and countermeasures. Develop cyber crisis management plan and establish breach response plan.

Qatar Central Bank has brought IT security strategy and technology risk circulars, which will provide directions for the banks to build their strategy while adopting advanced technologies. It also took the initiative for formation of Banking CIRT (Critical incident response team), which will act as platform for sharing of security incidents and enable quick response for its members. The State of Qatar has brought cyber-crime prevention laws, data privacy law, monitoring bank websites and alert on probable cyber-attacks in the country.

"The GDPR becomes important in the light of all major banks and FIs in Qatar having their branches/offices where they are collecting personal information of EU resident customers and processing/storing such information in Qatar and EU.

The Qatar Data Privacy Law speaks about controls over the data in rest/ processing/transmission and role & responsibilities of data processor/ controller. "Risk integration is key towards cybersecurity management".

■ *Dr R Seetharaman is Group CEO of Doha Bank.*