

Banking industry needs to step up governance on cyber security

SATISH KANADY
THE PENINSULA

DOHA: 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, Dr R Seetharaman, CEO of Doha Bank, said yesterday.

Delivering the keynote address on the opening day of the two-day conference on Information Security for the Financial Sector, organised by the Qatar Central Bank here yesterday, Dr Seetharaman said various industries are getting redefined in the changing environment.

"The health sector can be reimagined, 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," he said.

"Banks need to manage the change by redefining their business models and to manage



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

various stake holders such as customers, regulator and shareholders."

Citing some of the specific cyber attacks case studies, Dr Seetharaman said hackers implemented credit card skimming malware on Rail Europe website between November 2017 and February 2018. About 23000 accounts are compromised by a data breach at Health equity in April 2018 when employee fell for a phishing scam.

Hackers hacked Amazon DNS servers of Myetherwallet.



Dr R Seetharaman, CEO of Doha Bank, delivering the keynote speech at the opening session of Conference on Information Security for the Financial Sector, yesterday. PIC: SALIM MATRAMKOT / THE PENINSULA

com. Users who accessed such site were directed to a fake site in April 2018. There were threatening mails for Distributed Denial of Service (DDOS) for some of the organizations and SQL Injection based attacks across the Qatar Banking and

Financial Institutions in the first half of 2018.

However, these attacks were successfully handled by the industry with the help of Internal monitoring systems and Telecom service providers. Cyber-attacks are capable of deteriorating insti-

tutions performance and economies' growth, he said.

Dr Seetharaman highlighted on technology developments and its impact on cybersecurity. He said more and more disruptive advanced technologies are changing the paradigm of Banking.

At the same time, the cyber threats are increasing rapidly. Increased web-based Banking channels and interfaces to provide convenient services to customers, the more Cyber threats and challenges.

Data is central to contemporary data-driven businesses and mandates a business-relevant strategy for the governance and growth of such vital assets.

Data governance programs and initiatives are undertaken by enterprises with the goal of increasing revenue and profitability, enhancing the value of services, products, and decision-making, managing cost and complexity, and/or increasing awareness of risk and/or vulnerability."

On General Data protection Regulation (GDPR) and Qatar Data Privacy Law, Dr Seetharaman said: "The GDPR becomes important in the light of all major Banks and FI 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 Data processor / controller.

Various other countries are also coming up with similar laws hence, considering the global operations of Qatar Companies, it is better to implement optimum controls to protect Personal information of Customers and employees there by try to meet the requirements of local and international Privacy laws. Cyber security Governance is an important area to be focused and Pragmatic cyber security governance is key for Qatar's sustainable growth."