'Cyber resilience reshapes cybersecurity', says Seetharaman

The major objective of cyber resilience is to protect businesses against various cyberattacks and ensure business operations are delivered in the face of disruption, Doha Bank CEO Dr R Seetharaman said during a recently held webinar.

He said, "The Fourth Industrial Revolution has caused digital disruption. Digital transformation has also come with cybersecurity risks. Cyber attackers exploit organisations' digital presence. Now, cyber risk is one of the major risks and requires discussion at board rooms. More and more disruptive advanced technologies are changing the paradigm of banking in terms of customer convenience and opening doors for open banking.

"At the same time, the cyber threats are increasing rapidly. There is also an increase in web-based banking channels and interfaces to provide convenient services to customers; more cyber threats and challenges are emerging. 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 programmes 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, said Dr Seetharaman, adding that "cyber resilience reshapes cybersecurity."

Dr Seetharaman said digital disruption has contributed to cyber risks. The Internet of Things, which involves connecting various gadgets in the ecosystem is also contributing to cyber risks, he said.

"Artificial Intelligence can be used to fight back cyberattacks. Big data tools and analysis can be used to monitor cyber risk events. Traditional penetration testing is not enough. You need advanced, crowdsourced testing to find vulnerabilities in systems," he said.

Participants of Doha Bank's webinar on 'Cyber Resilience'.

"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. The State of Qatar has also brought cybercrime prevention laws, National information Assurance Policy Version 2.0, Data Privacy laws, monitoring bank websites, and alerts on probable cyberattacks in the country.

"It has conducted cybersecurity assessment and business viability of banks in Qatar. Qatar Central Bank has established the Information Security Committee and mandated all the bank's that operate in Qatar to become a member. The Ministry of Interior has provided great support in fighting cybersecurity criminals through its Cyber Crimes Investigation Centre," Dr Seetharaman said.

Ravi Baldev, Manager Systems Engineering, Data Protection and Cyber Recovery Division, Dell Technologies, spoke on 'Cyber Resilience for the New Normal'. He said cyberattacks "are the new norm," providing guidance against such attacks and post-attack scenarios.

Bharat Raigangar, head, Cybersecurity & Risk Services, APAC, MEA, Wipro Limited, discussed 'Elevated Cyber Resilience in an Organisation during Digital Transformation'. He stressed the need for cyber resilience in the digital world and provided solution themes for cyber resilience in digital transformation.

Amit Roy, head, Cybersecurity Services, ME, Turkey and Africa, Atos, spoke on 'Key Cybersecurity Threat Predictions for H2-2021 with Defense Strategies' and gave insight on the key threats in 2021, which includes conventional attacks, supply chain attacks, cloud attacks, API attacks, and external remote service attacks.

Haider Pasha, senior director & chief security officer, MEA, Palo Alto Networks, discussed 'Enterprise Cyber Resilience in the Covid Era' and gave insight on greater risks and threats to the financial and the banking sector. He highlighted the role of regulations and how to deploy a cyber-resilient framework and cybersecurity leadership principles.