Cybersecurity culture development need of the hour: Doha Bank CEO

THE PENINSULA — DOHA

It is important to foster a culture of cybersecurity that promotes safe and appropriate use of cyberspace across stakeholders and contribute towards strengthening financial sector resilience at various levels, Doha Bank CEO Dr. R. Seetharaman **(pictured)** has said yesterday.

In his keynote speech at a two-day virtual CyberX Qatar seminar which opened yesterday, Seetharaman spoke on "The Making of Cybersecurity Culture" and highlighted the importance of cybersecurity as well as the various cybersecurity reforms implemented in Qatar.

He said: "The Qatar Central Bank (QCB) 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 brought cyber-crime prevention laws, National information Assurance Policy V 2.0, data privacy laws, monitoring bank websites and alert on probable cyber-attacks in the country. It has conducted cyber security assessment and business viability of banks in Qatar. The QCB has also established the Information Security Committee and mandated all the banks that operate in Qatar to be a member of it. The Ministry of Interior (MOI) has provided great support in fighting cybersecurity criminals, through its Cyber Crimes Investigation Center".

Seetharaman added: "Cybersecurity is not just a technology issue; it's a business risk that requires an enterprise-wide response. The cybersecurity is also a strategic risk for financial sector as it could create damage to organisational brand and reputation resulting in loss of share value and market confidence. It can also impact the financial and intellectual property resulting in loss of competitive edge and can cause system inoperability caused by a breach resulting in

inability to execute trades and access to information. G7 countries simulated cross-border cyber-attack on banks in May 2019 and are also concerned with cyber-attack during COVID-19."

During the event, Seetharaman highlighted on technology developments and their 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. There are increased web-based Banking channels and interfaces to provide convenient services to customers, amid growing 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."

Seetharaman also gave insight on digital transformation and its impact on cybersecurity. He said digital disruption has contributed to cyber risks, Internet of things, which involves connecting various gadgets in the eco-system which also contribute to cyber risks.

He added: "Artificial intelligence can be used to fight back cyber-attacks. Big data tools can be used to monitor cyber risk events. Traditional penetration testing is not enough, you need advanced, crowdsourced testing to find vulnerabilities in systems. The major cyber-attacks in 2021 includes Canadian plane manufacturer, Bombardier, which suffered a data breach; Australian broadcaster Channel Nine was hit by a cyber-attack; the London-based Harris Federation suffered a ransomware attack; CNA Financial suffered a ransomware attack, as well as the Cyber-attack in US gas pipelines and the Air India cyber-attack. The key to addressing cyber risks and threats is integrating cybersecurity into every phase of digital transformation process".

Speaking about the making of a cybersecurity culture, Seetharaman said: "Establish a robust governance and risk management process, safeguard the Bank's critical information assets (CIA) and comply data privacy requirements. Also, strengthen systems and increase surveillance and security monitoring to identify a cyber security event, enhance measures to limit its impact and quickly recover from cyber security incident, foster a culture of cyber security that promotes safe and appropriate use of cyberspace across the stakeholders and contribute towards strengthening financial sector resilience at various levels," he added.