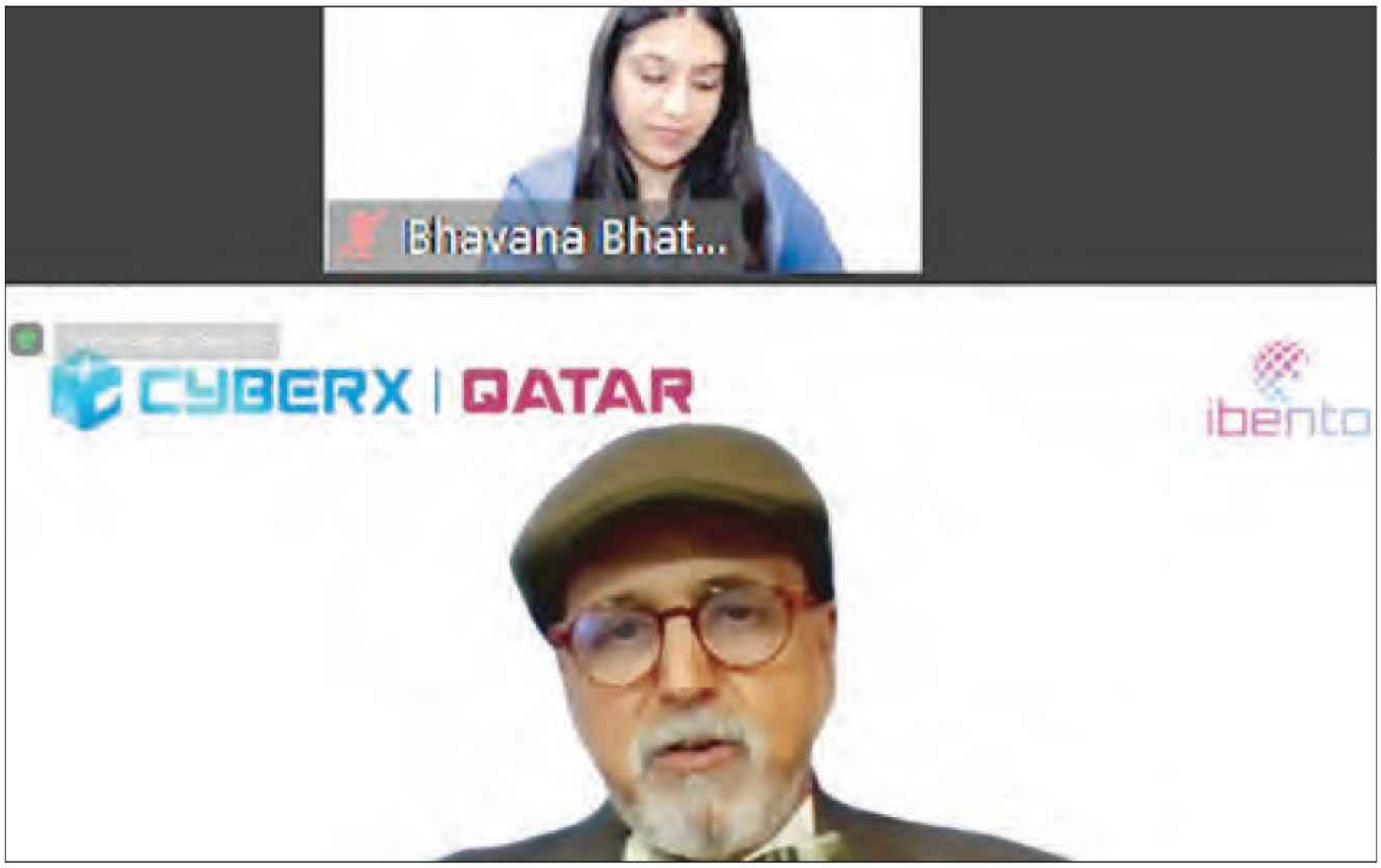
Cybersecurity culture development need of the hour: Doha Bank CEO Seetharaman

TRIBUNE NEWS NETWORK
DOHA



Doha Bank CEO R Seetharaman addresses CyberX Qatar webinar.

DEVELOPMENT of a cybersecurity culture is the need of the hour, Doha Bank CEO R Seetharaman has said while addressing the two-day CyberX Qatar webinar that began on Monday.

"Cybersecurity is not just a technology issue; it's a business risk that requires an enterprise-wide response," he said.

"Cybersecurity is also a strategic risk for financial sector as its failure could damage the reputation of a brand and erode its 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, he added.

Highlighting technology developments and their impact on cyber security, Seetharaman said, "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."

Sharing insight on digital transformation and impact on cybersecurity, he said, "Digital disruption has contributed to cyber risks, Internet of things, which involves connecting various gadgets in the eco-system also contribute to cyber risks.

"Artificial intelligence can be used to fightback 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 key to addressing cyber risks and threats is integrating cybersecurity into every phase of digital transformation process, he noted.

Seetharaman also highlighted the reforms in Qatar on cybersecurity.

"The 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. "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," he said.

"Qatar Central Bank, have established the Information Security Committee and mandated all the bank's that operates in Qatar to be a member of it. The Ministry of Interior, MOI, have provided great support in fighting Cyber Security criminals, through its Cyber Crimes Investigation Centre."

Giving insight on the making of cybersecurity culture, he said "Establish a robust governance and risk management process, Safeguard the Bank's critical information assets (CIA) and comply Data privacy requirements, Strengthen systems and increase surveillance /security monitoring to identify a cyber security event.