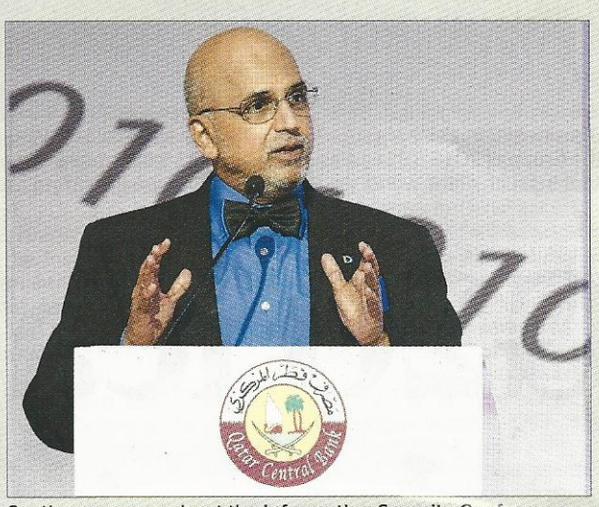


Seetharaman speaks at the Information Security Conference for the Financial Sector in Doha yesterday.

# Cyber security not just a technology issue; but a business risk, says Seetharaman

Cyber security is not just a technology issue; it is a business risk that requires an enterprise-wide response, said Doha Bank CEO, Dr R Seetharaman.

Addressing the Information Security Conference for the Financial Sector organised by the Qatar Central Bank yesterday, he said cyber security was also a strategic risk for financial sector as it could create damage to organisation brand and reputation resulting in loss of share value and market confidence.

Seetharaman said it could also impact the financial and intellectual property resulting in loss of competitive edge and could cause system inoperability caused by a breach resulting in inability to execute trades and access to information.

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

"In some cases, a risk committee, executive/ operating committee or the audit committee will be given the oversight charge. These committees should be well informed about the company's processes, and they should leverage that information to understand whether management has the right people and processes in place. The governance should give thrust on cyber security risks in financial services sector."

On cyber-attacks globally, he said, "There was a massive cyber-attack against an American bank associated with over 83mn accounts, which was disclosed in September 2014.The bank declared that log-in information associated with the accounts was not compromised but names, email and postal addresses, and phone numbers of account holders were obtained by hackers, raising concerns of potential phishing attacks. About 56mn customer debit and credit cards were put at risk after hackers broke into the American retailers' payment systems in April 2015.

"Hackers used a vendor's stolen log-on credentials to penetrate retailer's computer network and install custom-built malware that stole customer payment-card data and e-mail addresses. The malware that stole the credit card data resided on its computer systems from April until September 2014. The retailer is expected to pay $62mn to cover the costs of the attack, including legal fees and overtime for staff, and causing an estimated $90mn in costs for banks to replace 7.4mn debit and credit cards."

Seetharaman gave insight on cyber-attacks in the GCC region.

"An oil and gas company in Saudi foiled the fraud attempt of $30mn involving scammers pretending to work for an oil and gas Company in India. The fraud was committed on the assumption that Saudi's company would not notice a minor change in the email address of the India's oil and gas company representative, with whom they had been communicating.

"Many UAE banks were hit by targeted Distributed-Denial-of-Service (DDoS) attack, which cripples the banking operations and web applications. The attackers made successful 'denial of service' attack on the applications and web site of the banks. The attack leads to unavailability of internet banking and other banking services to the users for several hours.

"A DDoS attack uses tens, sometimes hundreds, of thousands of computers to synchronise a bombardment of packet-traffic on a server. In the absence of sophisticated mitigation solutions, servers can be brought down and services brought to a halt. The attackers choose the last day of the month to make the maximum disruption."