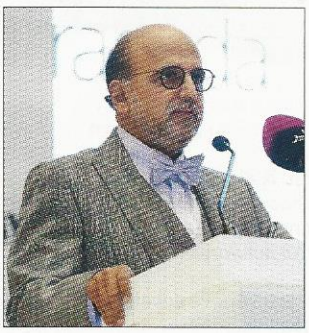
PPP model needed in cybersecurity governance, says Doha Bank CEO

By Peter Alagos
Business Reporter

Building a public-private partnership (PPP) model will benefit cybersecurity governance in the financial sector, according to a senior banking executive, who noted that cybercrime incidents in the GCC have doubled in 2015.

Doha Bank Group CEO Dr R Seetharaman said over 12,200 cybercrimes like spoofing, phishing, spam, and DDoS attacks were launched in the GCC last year, 45% of which occurred on mobile phones and 35% over social media.



Dr Seetharaman delivering his speech during the conference. **PICTURE**: Jayan Orma

Addressing dignitaries and participants of the '3rd Annual Information Security Conference for the Financial Sector', organised by the Qatar Central Bank yesterday, Seetharaman suggested the option of building PPPs and the integration of banking systems and regulations, as well as unifying external processes.

"We need to recognise the magnitude of the problem and start coming together to build a private-public partnership model, and that is going to make the difference for us. We need to articulate a collective response with a public-private partnership model, further integrate ourselves and build a model society to make sure we protect every single citizen. The opportunities are endless for us to come together," Seetharaman said in his speech.

Speaking to reporters on the sidelines of the event, Seetharaman said the financial industry can manage cyber threats better than individual institutions under a PPP model.

"Instead of investing on their own capital maintenance, like we do the NAPs (Network Access Protection), we should have associated systems measured, managed, and controlled as one infrastructure," he explained.

He also stressed that building a knowledge society is "the only way to minimise risk," and for institutions to reinvent themselves by utilising global case studies in the financial, telecom, banking, and energy sectors, which, he said, are most vulnerable to cyberattacks.

According to Seetharaman, cyber risks are now regarded as the leading threat to the global financial system by policymakers. He noted that the key cybersecurity vulnerability from a systemic risk perspective is related to the heavy reliance of financial institutions on information technology and communications, and in particular the highly-interconnected nature of these systems.

"Collaborate, contribute, consume and create knowledge about today's top security trends, help to identify security issues that are relevant and emerging as well as issues that need more guidance," he emphasised.

Seetharaman also lauded the measures taken by the Qatar government, particularly the development of a cybersecurity framework as mandated by the Qatar Central Bank circular 105/2012, the National Information Assurance Policy, and requirements from the International Information protection standards such as the ISO 27001:2013 version and National Institute of Standards and Technology (NIST) Cyber Security Framework.

"The initiative was well-received by all the banks since it provided the opportunity to proactively prepare us for any future cyberattacks. The assessment has helped to understand the current cybersecurity posture of our bank and our readiness to mitigate the risks emerging from cyber-attacks," Seetharaman added.