BANKING ON KNOWLEDGE

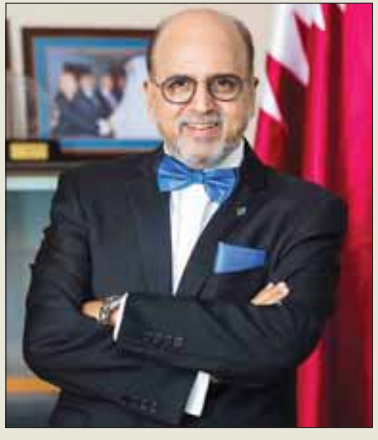
Qatar's cyber security framework enhanced through regulatory reforms

By Dr R Seetharaman

The malicious use of Information and Communication Technologies (ICT) in cyberspace could disrupt financial services, undermine security and confidence and endanger financial stability.

The WannaCry ransomware attack this year is one of the recent cyber-attacks which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. The impact of the attack was felt over 10,000 organisations and 200,000 individuals in over 150 countries, according to European authorities.

At the Global Level, G20 aims to promote the resilience of financial services and institutions in G20 jurisdictions against the malicious use of ICT, including from countries outside the G20. With the aim of enhancing cross-border cooperation, G20 has asked the Financial Stability Board to perform a stock-taking of existing relevant released regulations and supervisory practices in its jurisdictions, as well as of existing international guidance, including that to identify effective practices.



Qatar has envisioned to establish and maintain a secure cyberspace to safeguard national interests and preserve the fundamental rights and values of the country's society. To achieve this vision, Qatar seeks to fulfill the objectives, namely safeguard national critical information infrastructure (CII), respond to resolve and recover from cyber incidents and attacks through timely information sharing, collaboration and action, establish a legal and regulatory framework to enable a safe and vibrant cyberspace, foster a culture of cybersecurity that promotes safe and appropriate use of cyberspace and develop and cultivate national cybersecurity capabilities.

To make progress against the objectives, Qatar will develop and implement laws, regulations, and national policies to address cyber security and cybercrime; increase capabilities to combat cybercrime; build and maintain strong international relationships to establish cyber security norms and standards; invest in research to develop and commercialise innovative cyber security technologies and solutions; continuously monitor the security posture of CII; establish and continuously enhance incident response capabilities.

The Qatari government developed a robust plan for 2014-2018. The action plan is organised by objectives. Various stakeholders from government entities and institutions, including the Ministry of Defence, the Ministry of Information and Communications Technology, the Ministry of Interior, Public Prosecution and other organizations must work collaboratively with many others to implement these actions for the benefit of Qatar.

The Qatari government promulgated a Cybercrime Prevention Law (No 14 of 2014) in an effort to increase the tools for combating online and cybercrimes. Qatar's new approach to cyber security balances the need to protect interconnected Informational and Communication Technology (ICT) products and services with the need to provide opportunities that maximise the benefits and efficiencies found in ICT advances.

The Qatar Central Bank (QCB) has published a detailed framework for combating cyber risks and crimes. The key highlights of this framework are Management of Technology Risks; Defined Technology Risk Organisational Structure; Defined Roadmap for Business Continuity; Framework for Incident and Fraud Management; and Detailed Process Risk controls.

The QCB issued multiple strong controls which needs to be implemented by the Banks. Banks hold sensitive information such as customer records, account information as well as personal information such as names, birth dates, addresses, Qatar Identity number and many others.

Banks must take all necessary measures to ensure proper protection of these records. The QCB issues several circulars on regular basis to combat with cybercrimes for financial sector.

The State of Qatar has issued a new law concerning the Privacy and Protection of Personal Data being Law No 13 of 2016 (the 'Data Protection Law'). This law aims to establish a certain degree of protection for, and prescribes the guidelines for the processing of, personal data within Qatar. The law includes provisions related to the rights of individuals to protect the privacy of their personal data. Banks operating in Qatar should consider taking some precautionary steps as per privacy law such as (i) Raise awareness internally and amongst its service providers; (ii) Review internal documents, agreements, policies, disclaimers, consents etc. from the perspective of complying with the Data Protection Law and also identify matters which need to be addressed; (iii) Conduct internal training for the relevant departments such as IT, legal, marketing, technical support etc. to address any questions or concerns that the customers may have in relation to the Data Protection Law and their rights thereunder; (iv) Broadly identify potential issues, consult internally and take steps to rectify those issues or where the risk is still unclear, put in place appropriate holding measures; (v) Revisit all security measures implemented by the bank and the service providers and assess whether any further steps can be taken or investments be made to protect customer data.

On the whole we are seeing Qatar Cyber security framework enhanced through regulatory reforms, which will be beneficial to Qatar Banking Sector.

■ *Dr R Seetharaman is Group CEO of Doha Bank.*