BANKING ON KNOWLEDGE

Banker's Take

GCC economies should gear up to address cyber security challenges

By Dr R Seetharaman

Economies have become more dependent on information and communications technology (ICT) and hence they are becoming more vulnerable to network attacks. The most serious cyber security risks are those that threaten the functioning of critical information infrastructures, such as those dedicated to financial services, control systems for power, gas, drinking water, and other utilities; airport and air traffic control systems; logistics systems; and government services.

Although the prevailing rationale for cyber security is to ensure a favourable climate for ICT investment, national and international security concerns are becoming equally important rationales. In the developing economies, foreign direct investment as a whole may eventually be affected by the safety and integrity of data networks available to investors in host countries. In advanced economies, basic public trust in modern economies and the electronic networks on which they depend is eroded when electronic data is stolen, becomes corrupted, or can no longer be authenticated.

Cyber security is thus a collective concern that is comprehensive in scope—the Internet has no national boundaries. Whereas security is typically regulated at the government level, cyber security is at once national, international, public and private in character. No single strategy, set of governance arrangements, or operational practices will be right for every country. However, it is imperative that countries develop improved lines of communication based on trust to discuss cyber security both within and among themselves.

Some of the recent cyber attacks impacting organsiations are as follows.

GCC organisations have been the target of "Whaling". The attack is mostly

relying on "Social Engineering" using spoofed or bogus email addresses impersonating the CEO of the target organisation. Attackers conduct information gathering using social media to identify the time of attack and organisation staff to be targeted, i.e. CEO, CFO. US tech company Ubiquiti Networks lost $47mn to this scam. The 'Carbanak, gang used carefully crafted e-mails to trick employees into opening malicious software files. The hackers were then able to get into the internal network and track down administrators' computers for video surveillance.

Once the hackers become familiar with the banks' operations, they use that knowledge to steal money without raising suspicions, programming ATMs to dispense money at specific times or setting up fake accounts and transferring money into them.

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.

GCC economies should gear up to handle cyber security challenges. The measures to develop a comprehensive cyber security framework across GCC economies are as follows.

Governments must set up a centralised national cyber security body. The cyber security body needs a precise mandate so that it can promote a national cyber security agenda and exercise oversight so that are no inconsistent or conflicting cyber security agendas in the country.

The cyber security body also needs a separate, independent body that can be impartially convene stakeholders and encourage cooperation.

The cyber security body must define and promote a national cyber security strategy which will be consistent with country's national development goals and involve all key national stakeholders. The cyber security body must initiate a national discussion on cyber security to inform companies and citizens about strategy and integrate them into cyber security behaviour.

The cyber security body needs to develop preventive cyber security capabilities, such as national cyber security standards and policies, and a national cyber security compliance body. The cyber security body must create reactive cyber security capabilities, including a national computer emergency readiness team. Such teams must work harmoniously with national cyber security strategy.

The cyber security body must create and implement a national talent strategy. This is a challenging activity given the limited capabilities of the digital ecosystem in many countries of GCC region.

Dr R Seetharaman is Group CEO of Doha Bank. The views expressed are his own.