# Cyber security synchronisation is key to mitigating business risk

**DR R. SEETHARAMAN**
INDUSTRY INSIGHT

***Cyber security is not just a technology issue; it's a business risk that requires an enterprise-wide response. — AFP***

THE rapid rise of cyber risks and their potential to disrupt global financial stability have elevated cyber security to a top policy priority. Cyber risks are now regarded as a leading threat to the global financial system by policymakers. Cyber security risks arise from debilitating worms and computer viruses which have demonstrated destructive capabilities as evidenced by the damage caused by such programmes as Sasser, Blaster and Code Red.

Security management has evolved over a point in time. The computers have evolved from mainframes, then shifted to personal computers and then to internet, cloud technology and mobile. IT Security has also evolved on account of developments in computer.

In information security management risks associated in the mainframe include unauthorised access, disaster recovery, back-up of data and computer dependency. The risks have further compounded today due to privacy concerns, vulnerabilities, cyber terrorism, insider sabotage, mobile computing, wireless access, worms, trojan horses and spyware. Information security is now viewed as a key risk management and compliance issue. The focus is on accountability and integrity. Cyber security is not just a technology issue; it's a business risk that requires an enterprise-wide response. The cyber security is 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. 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. 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.

Threats are increasingly targeting governments, the energy sector, financial services industry and telecommunications sectors in the GCC. The types of cyber-attacks includes hacktivism, when criminals launch attacks based on their ideology, the second is to destabilise a company and the third is the one where most people associate cybercrime for financial ends.

Under this scenario, people do either a phishing attack of use viruses that block the computer or data for a ransom. Ransomware continues to pose a threat to organisations, with the malware development lifecycle being so short that a strong defense is still a major challenge for many organizations. The sectors with financial inclusion became a victim of cyber-attacks in GCC.

> Governments must set up a centralised national cyber security body

Many UAE financial institutions 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 website 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 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.

Banks introduce new policies and standards that address the dynamic nature of Information Security. Banks conduct security assessment of ATMs to prevent the increased security risks related to the related hardware and software. Physical security controls have been enhanced in the premises bank, which also implement many cyber security controls to reduce the impacts of online phishing attacks.

IT security controls improved through a number of progressed measures that includes Data Leakage Prevention (DLP), controls over email, web, and endpoints with new ways of DLP detection and prevention techniques, along with other requirements such as removable media security, security operations centre, formalised process for code reviews to identify application level threats, and common infrastructure security reviews.

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 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. Cyber security is key to mitigate business risk.

*The writer is Group CEO at Doha Bank. Views expressed are his own and do not reflect the newspaper's policy.*