THE SURGE IN THE CYBER SECURITY MARKET

By Neha Gangwani and Apurva Chaudhari, Aerospace and Defense Analysts, Markets and Markets.

The increasing use of the cyberspace for communication and data exchange has brought in new business opportunities. This technology incites open markets and societies but is exceptionally vulnerable to threats and attacks. The complex and dynamic environment of cyberspace has made it arduous for organisations to develop counter measures. In the few years the frequency of cyber-attacks has increased and the direct and indirect ramifications have been hassled almost every industry. Developing contingency plans to tackle these attacks is a key focus for every organisation, which is using a secured network.

The declining defense budgets in North American and European countries have not impacted the spending towards cyber security. Cyberspace has become a fundamental component for the aerospace and the defense industry too. To tackle the cyber-attacks, the government organisations along with the private organisations are taking steps beyond the traditional purchases of cyber security software systems. Their key focus is on developing analytical protectionist and prognostic measures. Among the developed countries, U.S., U.K., and China were registered to have the highest cyber security breaches in the past few years.

UNITED STATES (U.S.)

In United States, President Obama has identified cyber security as one of the most important social as well economic challenge. In February 2015, U.S. President Barack Obama has announced to invest $14 billion in cyber security solutions for better protection of federal and private networks from hacking threats. The funding is more inclined towards deployment of intrusion detection and preventive capabilities and increase in sharing the data with the private companies. The concern for cyber security has increase in the nation after the Sony hacking incident in month of December. The president has also announced several law enforcement tools to encounter cybercrime which usually includes prosecution of the sale of botnets, computer networks established for the purpose of cybercrime and other related activities.

The U.S Government has also declared that, no funding would be allocated to business projects unless the issue of cyber security is properly addressed which is actually arising a sense of awareness among the businesses across all regions. The selection of 15 prime contractors, CSC being one of them, by the US Homeland Security for continuous diagnosis and mitigation of cyber threats, is also pushing the cyber security solutions to be readily deployed by the public and private units of the region.

UNITED KINGDOM (U.K.)

In the National Security Strategy, cyber-attacks are recognised as one of the tops risks. In 2014, malicious software topped the list of the means of cyber-attacks faced by the organisations in U.K. The U.K. government set the budget of £650 million in 2010 for developing the counter measures for the cyber-attacks, with a prime focus on the security in line with the privacy and fundamental rights. In 2014, though the number of security breaches faced by the organisations reduced as compared to 2013, but the overall cost of these breaches to the organisations was significantly high.

The U.K. government issued “the Ten Steps” guidance as a reliable measure to counter the cyber threats. Organisations across U.K. are adopting these guidelines and are among the most popular measures. Defence Science and Technology Laboratory (DSTL) is a key contributor to help U.K. to develop the critical cyber infrastructure for military operations. In 2014, Cyber Defence Capability Assessment Tool (CDCAT) was launched by DSTL’s technology transfer company - Ploughshare Innovations Ltd. Lockheed Martin in consociation with Restoration Partners, technology merchant bank in London, contrived Virtual Technology Cluster (VTC), developed a single platform for cyber security industry stakeholders, academia and the investment community. VTC is an opportunity for the private cyber entrepreneurs to trade with established companies and share intelligence & ideas. The U.K. government supports such initiatives, enabling the private sector to support the U.K. cyber innovation.

CHINA

China is one of the most dominating nations in cyber security due to the growing information and communication technology in the country. It accounts for online transactions for worth $2.1 trillion which implies its dependency on the internet for its financial transactions. The banks and financial institutions are the main targets of the cyber-attacks. One of the other issues gaining greater attention in the country is the need to protect intellectual property rights.

This has triggered the need for imposition of political control in the field of network security. Recently it has suggested a cybersecurity legislation to secure its information technology structure. The government of Beijing is one of the most effective in cyber space and similar to countries like United States, which has developed various cyber units to monitor the digital world. In 2015, it is suggested that they would be investing 20 to 30 percent more comparatively to the previous years. The new regulations are being laid, which requires the companies to sell computers to the Chinese banks to provide secret source code and also establish back doors into hardware and software. It is also encouraging the use of localised technology by its own people. Services such as Google and Microsoft are banned in this country. It is driven this way to protect the longevity of the Chinese Communist Party.

The high vulnerability of the developing countries for the cyber-attacks, have increased the need for potential cyber security solutions. These countries face a high threat to the public security, governance, state infrastructure, business organisations, and individuals, among others. The high dependency on the internet connected systems has led to a need for a reliable and a secure cyberspace. India, Brazil, Argentina, Chile, Israel, United Arab Emirates, and Egypt are among the developing countries with high cyber security breaches. These countries are also the opportunistic markets in the private and the defense sector for the private cyber entrepreneurs. ■

Neha Gangwani

Apurva Chaudhari