RACONTEUR

Distributed in THE TIMES

Partnerships needed to combat future cyber threats

Urgent action is needed to counter cyber threats to UK business and national security, says **Northrop Grumman Corporation**

The UK National Cyber Security Strategy emphasises the importance of partnerships among government, industry and academia, both domestic and international, to meet the primary objective of the strategy, "making the UK one of the most secure places in the world to do business in cyberspace".

The cyber threat is broad and complex, and focuses on networks and data in both the public and private domain largely to steal money and intellectual property. Threats will grow in frequency and sophistication because adversaries can afford new technology and techniques, including cloud and mobile computing, big-data analytics and artificial intelligence. But no single organisation has the necessary capabilities to mitigate all the risks. Partnerships are therefore critical and must include information-sharing, governance, research and education.

While today's threats are significant, threats to critical infrastructure will be even greater by 2020. With industries accelerating digitisation to improve services and reduce costs, there are many new cyber threats to sectors, such as electric power, oil and gas, national security, and transportation. These threats are not only to financial and information security, but also to operations and safety. Examples such as Stuxnet and Shamoon have damaged operations in significant ways. These cases are modest compared to what could happen this decade.

Information-sharing partnerships are essential to mitigate cyber risks

In 2020, the internet will have vastly more devices and we will have far more sophisticated cyber adversaries. The "Internet of Things" brings many benefits, but also creates unknown vulnerabilities. In the wrong hands, analytical techniques can generate sophisticated cyber exploits automatically. Massive cloud malware could analyse infrastructure for vulnerabilities and develop attack strategies in seconds.

Failing to mitigate infrastructure threats could cause losses of many economic, environmental and health benefits possible through digitisation. However, there are strategies and tactics that partnerships can execute for mitigation.

First, organisations can take immediate steps. There is actionable information published on Gov.uk including, for example, 10 Steps to Cyber Security by CESG, GCHQ's information security arm. Government and industry partnerships must implement legal and regulatory measures to reduce cyber crime. Multi-national partnerships must enforce agreements addressing state-sponsored activities. Current measures are insufficient. Costs of inaction increase rapidly. We need collaborative action now.

Second, information sharing partnerships must operate faster. Most sharing centres exchange threat information manually with limited automation. Some threat analysis services provide information for automatic processing, generally lists of IP addresses and "indicators of compromise". This is reactive. Sharing partnerships must become more proactive in analysing and disseminating forward-looking cyber intelligence.

Third, government, industry and academic partnerships must be more open to innovation. For example, more approaches are needed to incubating security companies with various incentives. New ways are needed to attract people to professions that improve infrastructure security, and new frameworks for security as a science with the rigour of physics and mathematics. Newton's Laws for cyberspace have not yet been developed.

Finally, cyberspace education needs to be reassessed. Today's discussions about cyber workforce shortages focus on specialists. While clearly important, more is needed. There are basic practices that the billions of internet users should employ to improve security. Product designers and engineers learn about quality and reliability, but not enough about security. Business schools should teach entrepreneurs about opportunities in security. To some extent, education can change to reach broader populations with internet course delivery. Using the internet to protect cyberspace is a long-term, but necessary, strategy.

Making the UK one of the most secure places in the world to do business in cyberspace is our primary objective

Massive cloud malware could analyse infrastructure for vulnerabilities and develop attack strategies in seconds

Most sharing centres exchange threat information manually with limited automation

Proactive education at all levels can eventually do much to make infrastructure safer.

The global importance of cyber security and the dynamism of cyberspace are growing in recognition. Not one person or company can effect change alone. Society needs diverse government, industry and academia partnerships to create a much broader and deeper security awareness and competency in the population.