S. RAJARATNAM SCHOOL
OF INTERNATIONAL STUDIES
A Graduate School of Nanyang Technological University

RSIS COMMENTARIES

No. 083/2013 dated 2 May 2013

A National Security Imperative: Protecting Singapore Businesses from Cyber-Espionage

By Senol Yilmaz

Synopsis

Cyber-espionage is a real and growing threat to businesses and economies. Some counter-measures can be taken by the private sector. But the government plays an important role in protecting its businesses from cyber-exploitation.

Commentary

OVER THE PAST few decades, Singapore's economy has moved up from a mere producer of material goods to a creative inventor of ideas. This success stands on two main pillars: Firstly, heavy investment has been made in education as well as research and development. Secondly, the rigorous protection of intellectual property rights has reassured investors that their patents, trademarks, and trade secrets are safe and that their investments will pay out. Singapore's innovation-friendliness is ranked in the list of the 20 most innovative countries in the world by the Economist Intelligence Unit; the World Economic Forum's latest Global Competitiveness Report lists Singapore's intellectual property protection regime second only to Finland's.

However, with the widespread and growing use of cyber-espionage, this success could be undone quickly and quietly. The vast majority of companies store their secret business information digitally, whether it is formulas, production processes, or customer lists. The advantages over paper-based storing are obvious: digital storage is more cost effective and data can be accessed more comfortably by employees. But it also means that cyber-spies who gain access to a company's IT network can steal enormous amounts of business secrets cheaply, easily and with little risk of detection.

A popular method of gaining illegal access is "spear-phishing", as happened in the case of a medium-sized Swiss manufacturing company recently. The sales manager received a legitimate sounding e-mail supposedly from a potential client. He double-clicked on the attached file, assuming it contained an order. In reality, the attachment installed malware, or malicious software, on the sales manager's computer. Subsequently, the malware opened a virtual door that allowed the perpetrator to access and search for information on the company's computer network and allowed transferring data to the perpetrator. In this or in similar ways, companies' innovations that may cost millions to develop can be stolen with malware that costs hundreds.

The perpetrators in these cases are difficult to identify as they can conceal their real identity and physical location. While many states engage in political and military espionage, experts argue that Chinese

organisations are especially active in economic espionage with their government at best turning a blind eye to such activities.

The magnitude of the financial damage is extremely difficult to estimate since most firms are either not aware of breaches and theft of their secrets, or not willing to report them. One estimate puts the annual damage at USD 400 billion for the U.S.A. alone. Given Singapore's emphasis and reliance on innovation combined with her inter-connectedness, it would be surprising if cyber-espionage did not cause substantial financial damage here.

A Matter of National Security

Since this City-State's economic well-being stands partly on innovation and on being a place investors can trust, cyber-espionage is a real threat to economic success, for the innovative idea stolen today is tomorrow's dollar lost. But this is not only an economic issue to be left to private companies to deal with: Joel Brenner, former inspector general of the U.S. National Security Agency, rightly argues that the boundary between economic security and national security has become indistinctive. Creativity and inventiveness are sources of national income which again finance strategic power. Therefore, Brenner points out that the theft of intellectual property is not merely an economic issue but a matter of national security. Consequently, governments must be active in helping businesses to counter cyber-espionage.

What needs to be done?

A first step to counter cyber-espionage would be information sharing about attacks suffered: Once security gaps in software applications are identified they can be closed so that cyber-spies cannot exploit the same gap to intrude other companies' systems. However, neither private companies nor government bodies like making instances of cyber-espionage public for fear of reputational damage with citizens, customers, investors, or shareholders.

To overcome this problem, governments have used the stick approach: The European Commission has made a proposal recently that would make it mandatory for companies operating in key business areas to report "significant" cases of cyber-espionage. However, companies will probably not be overly forthcoming with information, especially as they can rationalise that they did not assess a given case as "significant" enough.

An example for an innovative, non-government driven approach can be found in Sweden. Swedish banks are said to have formed a closed circle of trusted partners whose IT security representatives meet and exchange information about attacks regularly. They work on a first name basis and do not know each others' company affiliation. That way, attacks are not leaked to the media and reputational damage is averted while information is shared, software vulnerabilities closed and attacks using the same method prevented. In Singapore's business friendly environment, a similar approach where private business takes leadership could be more readily accepted than top-down government regulation.

This does not mean that there is no role for governments at all. Five initiatives could help alleviate the problem. Firstly, and most easily, a proverbial carrot could be offered to companies operating in key business areas through taxation: Those companies that make investments and upgrade their IT security could be given special tax breaks. Secondly, government contracts, funding and loans could be tied to predefined and continuously updated minimum IT security standards. This would be an incentive for all organisations in key business areas that vie for government money. Thirdly, best practices should be defined, constantly updated in cooperation with the private sector and actively promoted through outreach programmes. Fourthly, supply chain security is crucial: Hard and software must be purchased from trusted manufacturers that deliver products free of malware. Governments can help identify such manufacturers. Lastly, it is governments' task to represent the interests of its private sector internationally. Since cyber-espionage is an international problem, international cooperation among partners is essential.

Most experts agree that the threats from cyber-spies will increase in the coming years both in terms of quantity and quality. Since cyber-spies constantly search for and find new software vulnerabilities, fighting cyber-espionage resembles aiming at a moving target and will therefore be a constant struggle. The only way to keep the threat in check is to remain vigilant.

Senol Yilmaz is an Associate Research Fellow at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University.