CHAPTER 8 SECURING INFORMATION SYSTEMS

CASE 2

Cyberespionage: The Chinese Threat

VIDEO CASE

SUMMARY This video examines the economic and national security costs of cyberespionage. Cyberespionage involves the theft of intellectual property, as well as valuable situational and personal information, using surreptitious means on the Internet. While many advanced nations engage in cyberespionage, China has been implicated in many major cyberespionage programs aimed at the United States. L= 21:14.

URL http://www.youtube.com/watch?v=Js52FjOsgPA

CASE Cyberespionage is very different from cyberwarfare. The objective in cyberespionage is to, without detection, gain access to computer systems that contain valuable commercial and/or military information; to remain in place for continuous data gathering; and to remove data from the target system. The point is not to destroy enemy systems, but instead to colocate inside them and continuously drain information. This is similar to the goals of the British intelligence agency MI6 during World War II, when they broke the military codes of the Germans quite early in the war. MI6 spent a great deal of effort to insure the Germans never discovered their communications were being closely monitored and intercepted for over four years. In contrast, the objective of cyberwarfare is to destroy and disrupt enemy capabilities. When cyberwarfare succeeds, the very fact of succeeding permits the enemy to become aware of the intrusion and take steps to defend itself.

continued

In October 2011, in a report to Congress by the Office of the National Counterintelligence Executive, national security officials concluded that foreign collectors of sensitive economic information are able to operate in cyberspace with relatively little risk of detection by their private sector targets. The proliferation of malicious software, prevalence of cybertool sharing, use of hackers as proxies, and routing of operations through third countries make it difficult to attribute responsibility for computer network intrusions. Cybertools have enhanced the economic espionage threat, and the Intelligence Community (IC) judges the use of such tools is already a larger threat than more traditional espionage methods.

The threat comes from adversaries as well as partners. Allegedly, according to American and European media and governments, Chinese actors are the world's most active and persistent perpetrators of economic espionage. U.S. private sector firms and cybersecurity specialists have reported an onslaught of computer network intrusions that have originated in China, but the intelligence community cannot definitively confirm who is responsible because of the possibility that the attacks originate elsewhere but use compromised Chinese computers to implement the attacks. Russia's intelligence services come in second place. They are also conducting a range of activities to collect economic information and technology from U.S. targets. In addition, some U.S. allies and partners use their broad access to U.S. institutions to acquire sensitive U.S. economic and technology information, primarily through aggressive elicitation and other human intelligence (HUMINT) tactics.

In Europe, both France and the U.S. military are accused of leading the largest cyberespionage operations against European countries, even larger than China or Russia. According to leaked U.S. diplomatic cables (WikiLeaks) from the U.S. embassy in Berlin, "French espionage is so widespread that the damages it causes the German economy are larger as a whole than those caused by China or Russia." Berry Smutny, the head of German satellite company OHB Technology, is quoted in the diplomatic note as saying: "France is the Empire of Evil in terms of technology theft, and Germany knows it." The United States is also the object of commercial and military espionage originating from its major Middle Eastern ally, Israel. U.S. national security officials consider Israel to be, at times, a frustrating ally and a genuine counterintelligence threat.

Reviewing all the various reports and allegations, from the United States, to Europe, and China, it appears that all nation states, and their commercial affiliates, engage in a variety of activities that be could called espionage, or intelligence gathering. In some cases these activities are illegal, or skirt the laws of both the target and the initiating states. The size of these cyberespionage activities reflects both the economic strength of the nations involved (advanced countries like the United States and European countries arguably have the largest and most sophisticated programs), and the demand in developing countries for stolen intellectual property.

continued

It is also difficult to estimate the economic cost of these thefts to the U.S. economy. In a 2011 report to Congress from the Office of National Counterintelligence, intelligence experts concluded that the economic cost was in the billions of dollars, and millions of jobs.

The potential impact of cyberespionage is illustrated in the following examples.

Google Attack: Commercial Espionage and Punishment

Google announced in January 2010 that it had been the target of a highly sophisticated Chinese cyberattack. At least 34 other companies, including Yahoo, Symantec, Adobe, Northrop Grumman, and Dow Chemical, were attacked at the same time. According to the experts, the attacks at defense contractors were aimed at obtaining information on weapons systems, while those on technology companies sought out valuable source code that powers these companies' software applications. At Google, the attackers also gained access to the Gmail accounts of Chinese human rights advocates in the United States, Europe, and China.

Experts say that the attacks followed the familiar "phishing" technique. A recipient opens a message that purports to be from someone he knows and, not suspecting malicious intent, opens an attachment containing a malicious program that embeds in his computer. That program then paves the way for downloading and concealing additional programs that allow the attacker to gain total control over the recipient's computer.

Subsequent investigation determined that the Google break-in started with an instant message sent to a Google employee in China who was using Microsoft's Messenger program. By clicking on a link within this instant message, the employee inadvertently downloaded malware that allowed the attackers to gain access to the employee's computer and then, through that computer, access to the computers of a critical group of software developers at Google headquarters.

Joint Strike Fighter

The Joint Strike Fighter, also known as the F-35 Lightning II, is reportedly the costliest and most technically challenging weapons program the DoD has ever attempted. Intruders apparently entered this program repeatedly during the 2007–2009 period through vulnerabilities in the networks of contractors working on the program. These include Lockheed Martin, Northrop Grumman, and BAE Systems. One example of the sophistication of these attacks is that the intruders inserted technology that encrypts the data as it is being stolen. As a result, investigators cannot determine exactly what data has been taken. The source of the attacks was traced back to China.

continued

GhostNet

Information Warfare Monitor, a Canadian research organization, conducted a detailed investigation of Chinese cyberespionage against the Tibetan community and Tibetan Government-in-Exile during the period June 2008 to August 2009. It identified an extensive network of cyberpenetration of Tibetan targets that it called GhostNet. This is relevant here not just because of the successful penetration of Tibetan targets, but for what was learned about successful penetration of other targets during a second phase of this investigation.

This investigation led to the discovery of four commercial Internet access accounts located in Hainan, China, that received data from, and sent instructions to at least 1,295 infected computers in 103 different countries. Almost 30 percent of the infected computers were what might be considered high-value intelligence targets. This included the ministries of foreign affairs of Bangladesh, Latvia, Indonesia, Philippines, Brunei, Barbados, and Bhutan; embassies of India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany, and Pakistan; the ASEAN (Association of Southeast Asian Nations) Secretariat, SAARC (South Asian Association for Regional Cooperation), and the Asian Development Bank; news organizations; and an unclassified computer located at NATO headquarters.

The GhostNet system allowed the attackers to gain complete, real-time control over the infected computers. This includes searching and downloading specific files and covertly operating any attached devices, including microphones and web cameras. It is not known whether all of the infected computers were actually being exploited by the attackers. It is possible that some of the infected computers were infected coincidentally through emails received from an infected computer.

References

"US sees Israel, tight Mideast ally, as spy threat," by Adam Goldman, New York Times*, July 28, 2012.*

"U.S. Report Accuses China and Russia of Internet Spying" By Thom Shanker, New York Times*, November 3, 2012.*

"Foreign Spies Stealing US Economics Secrets in Cyberspace," Office of the National Counterintelligence Executive, Washington D.C., November 3, 2011.

continued

VIDEO CASE QUESTIONS

1. What are cyberespionage groups stealing from the United States?
2. What does the video claim is the evidence these attacks are coming from China? Is this believable?
3. What does Adam Siegel in the video claim is the motivation of the Chinese government for conducting cyberespionage against the United States?
4. Why didn't Nortel management take the Chinese threat seriously? Why do various contributors in the video claim that American management does not take the problem seriously?
5. The video claims the attacks on American corporate and military computer systems are increasingly sophisticated. Do you believe this is true?
6. Industrial espionage is a kind of technology transfer. The video claims the very DNA of Google is being drained by China, and that the United States will lose its competitive advantages with respect to China. Do you agree or disagree? Why? How else is technology transferred? Is it possible to stop technology transfer of any kind?