Statement for the Record

Richard Bejtlich

Chief Security Strategist

FireEye, Inc.

Before the

U.S. House of Representatives

Committee on Financial Services

Subcommittee on Oversight and Investigations

A Global Perspective on Cyber Threats

June 16, 2015

Chairman Duffy, Ranking Member Green, members of the Subcommittee, thank you for the opportunity to testify. I am Richard Bejtlich, Chief Security Strategist at FireEye. I am also a nonresident senior fellow at the Brookings Institution, and I am pursuing a PhD in war studies from King's College London. I began my security career as a military intelligence officer in 1997 at the Air Force Information Warfare Center. My employer, FireEye, provides software to stop digital intruders, with 3,400 customers in 67 countries, including 250 of the Fortune 500. Our Mandiant consulting service, known for its 2013 report on Chinese PLA Unit 61398, helps companies identify and recover from intrusions. In 2014, we conducted hundreds of investigations in 13 countries.

The title of this hearing includes the phrase "cyber threat." Understanding the threat is necessary, but not sufficient. We should expand our focus and discuss "risk" associated with specific damaging scenarios, and incorporate threats, vulnerabilities, and consequences. Risk is a function of these three factors, and influencing any one or more changes our overall level of security. Furthermore, while risk is a forward-looking concept -- we worry about what could happen -- some scenarios have already occurred, making a theoretical risk an actualized event.

I separate damaging scenarios into two categories: chronic and acute. Chronic scenarios occur over an extended period, with impact spread across time in ways that can be difficult to measure. Acute scenarios involve immediate and distinct impact, usually with obvious physical or virtual damage. Thankfully, we have not yet seen a combination of these two categories, i.e., long-term, highly-visible, costly damage. Hopefully that will remain the case.

The United States is currently suffering three important chronic damage scenarios. First, foreign nation state actors are stealing sensitive data and commercial secrets from private organizations, for use by their domestic industries. Second, these actors are stealing sensitive and classified data on American military and intelligence plans and technologies, to benefit their strategic interests. Third, foreign actors are stealing personally identifiable information and financial instruments from citizens and organizations, to benefit national capabilities and fuel underground crime. The theft of commercial, government, and personal data is an actualized risk, and it remains a current and future risk.

The United States is also susceptible to two acute damage scenarios. First, many security professionals worry about attacks against critical infrastructure. The electrical grid, finance sector, water supply, and

telecommunications systems are the “big four” targets. To date, according to public testimony and reporting, some foreign actors have infiltrated elements of critical infrastructure, while others have attempted to at least disrupt critical infrastructure. The second acute damage scenario involves disruption or destruction of virtual infrastructure. In two public examples, foreign actors have infiltrated American companies and destroyed data on thousands of computers.

With this understanding of risk due to specific scenarios, let’s briefly discuss threat actors. Security professionals classify threats into four broad categories: nation-states, organized criminals, terrorists, and activists. There is some overlap and mixing among the teams or individuals in these categories, along with their motivations for action. Traditional cyber security tools, tactics, and processes are generally sufficient when countering current terrorist and activist capabilities. Organized criminals are adopting more of the capabilities of nation-state groups. Nation-states are the top of the pack, and more of them are entering the digital arena. Therefore, I focus on my testimony on the top four nation-state threat actors: Russia, China, North Korea, and Iran.

Russia poses chronic and acute challenges. Russian government and affiliated forces can conduct full-spectrum information operations, and they possess top tier cyber capabilities, including the ability to preserve operational security and partially frustrate forensic analysis. According to open sources, Russian forces have infiltrated some elements of American critical infrastructure, but these forces have not used that access to inflict damage. Russian and Russian-speaking criminal actors are a major source of financial hardship for American companies and individuals. Geopolitically, Russia is a cause for worry due to the ongoing war in Ukraine.

China also poses chronic and acute challenges. Chinese government and affiliated forces can conduct full-spectrum information operations, although not at the Russian level. What they lack in top-tier sophistication they make up for in volume and persistence. Chinese theft of commercial and sensitive data from American companies is unequalled, and ongoing. According to open sources, Chinese forces have also infiltrated some elements of American critical infrastructure, but have not used that access to inflict damage. Chinese criminal actors are active but not to the degree seen by their eastern European counterparts. Geopolitically, China is a cause for worry due to the escalating tensions in the East China Sea and South China Sea.

North Korea primarily poses acute challenges. North Korean government and affiliated forces have invested heavily in developing their cyber capabilities. In contrast with their Russian and Chinese counterparts, North Korean forces have stepped beyond the espionage line in order to inflict virtual damage, first against South Korean targets, and then against an American victim, Sony Pictures Entertainment, in November 2014. Geopolitically, North Korea is a cause for worry due to their aggressive posture towards the West.

Iran primarily poses acute challenges. Iranian government and affiliated forces are enhancing their cyber capabilities. Similar to North Korea, Iranian forces have stepped beyond the espionage line in order to inflict virtual damage, first against targets in the Middle East, and then against an American victim, Sands Casino, in February 2014. Iran has also demonstrated specific interest in degrading the American financial sector, via distributed denial of service attacks in 2012. Geopolitically, Iran may be less of a cause for worry, depending on the outcome of the P5+1 nuclear talks.

Although I just outlined four nation-state threats, note that other countries are developing capabilities to harm American national interests. Furthermore, these four nation-states, and others, may collaborate with criminal groups, terrorists, and activists, sometimes obscuring the identity of the responsible party. However, advances in attribution during the last five years have enabled the American intelligence community to act with confidence when investigating strategically significant intrusions.

I will conclude by mentioning the last two elements of risk, which are vulnerabilities and consequences. American interests and infrastructure remain largely vulnerable to the chronic and acute scenarios I outlined earlier. In the private sector, financial and defense companies are best resourced and postured to counter threat actors. However, I remind the Subcommittee that even these industries are worried. Last year, Bloomberg reported a private proposal by the Securities Industry and Financial Markets Association (SIFMA) for a "cyber war council" with the US government.[1] Beyond finance and defense, the remainder of the American economy and population remains in danger. Government at federal, state, local, and tribal levels is similarly at risk, although the primary threats to the military and intelligence communities appear to those of untrustworthy insiders. It is increasingly difficult for

[1] Carter Dougherty, "Banks Dreading Computer Hacks Call for Cyber War Council," Bloomberg, July 8, 2014. http://www.bloomberg.com/news/articles/2014-07-08/banks-dreading-computer-hacks-call-for-cyber-war-council

organizations to detect and respond to intrusions on their own. In 2014, only 31 percent of organizations discovered, via their own resources, that they were breached – down from 33 percent in 2013 and 37 percent in 2012.

In terms of consequences, costs continue to increase. On the financial crime front, the 2015 Cost of Data Breach Study by IBM and the Ponemon Institute reported that "the average cost for each lost or stolen record containing sensitive and confidential information increased from $201 to $217," while "the total average cost paid by organizations increased from $5.9 million to $6.5 million."[2] Worse, the types of personally identifiable data being stolen increasingly include "permanent data," such as Social Security numbers and health care records. Although credit cards are easily replaced at minimal cost to the victim, there is no business process to recover from the theft of Social Security numbers or health records. On the national security front, we are all aware of the series of devastating breaches in the news.

I look forward to your questions, where I hope we can discuss strategies for mitigating these risks.

[2] IBM and the Ponemon Institute, "2015 Cost of Data Breach Study," http://www-03.ibm.com/security/data-breach/