Testimony of Richard Bejtlich, Chief Security Strategist, FireEye
Committee on Homeland Security and Governmental Affairs
January 28, 2015

Chairman Johnson, ranking member Carper, members of the Committee, 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 2,200 customers in 60 countries, including 130 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.

Who is the threat?

We have discovered and countered nation-state actors from China, Russia, Iran, North Korea, and other countries. The Chinese and Russians tend to hack for commercial and geopolitical gain. The Iranians and North Koreans extend these activities to include disruption via denial of service and sabotage using destructive malware. We have helped companies counter organized crime syndicates in Eastern Europe and elsewhere. Our report on FIN4 described intrusions to facilitate insider trading. We have also encountered hacker teams for hire, and others who develop and sell malware.

How active is the threat?

In March 2014, the Washington Post reported that in 2013, federal agents, often the FBI, notified more than 3,000 U.S. companies that their computer systems had been hacked. This count represents clearly identified breach victims. Many were likely compromised more than once.

Who is being breached?

Serious intruders target more than government, defense, and financial victims. No sector is immune. FireEye recently published two reports, showing that 96% of organizations we could observe had suffered compromise during two six-month periods. The best performing sector was aerospace and defense, with "only" 76% of sampled organizations suffering a breach.

In 2014, the top sectors assisted by our Mandiant consultants included business and professional services, retail, finance, media and entertainment, and construction and engineering.

How do victims learn of a breach?

In 70% of cases, someone else, likely the FBI, tells a victim about a serious compromise. Only 30% of the time do victims identify intrusions on their own. The median amount of time from an intruder's initial compromise, to the time when a victim learns of a breach, is currently 205 days. This number is better than our 229 day count for 2013, and the 243 day count for 2012. Unfortunately, it means that, for nearly 7 months after gaining initial entry, intruders are free to roam within victim networks.

What is the answer?

So-called “network hygiene” only takes you so far. I recommend a “best value approach” over “low-cost, technically acceptable” technologies, but there is no purely technical solution to information security. The best strategy is to prevent as many intrusions as possible, quickly detect attackers who evade defenses, and respond appropriately, before the adversary accomplishes his mission. Strategically significant intrusions do not happen at “the speed of light.” It takes intruders time, from hours to weeks, to move from an initial foothold to the information they seek.

Defenders win when they stop intruders from achieving their objectives. To that end, organizations, including the federal government, should track the number of intrusions that occur per year, and the amount of time that elapses from the initial entry point to the time of discovery, and from the time of discovery to the removal of the threat. These metrics are “the score of the game” that mark a successful security program.

What is threat intelligence?

“Threat intelligence” refers to technical information about the tactics, tools, and procedures used by intruders to abuse software and networks. It does not depend upon sensitive information about U.S. persons. The President’s proposal is compatible with this understanding. It offers privacy protections to “reasonably limit the acquisition, interception, retention, use and disclosure of cyberthreat indicators that are reasonably likely to identify specific persons.”

Not all threat intelligence is created equal. Intelligence in the virtual world is similar to intelligence in the physical world. Acting on intelligence means placing it in proper context, assessing the trustworthiness of the source, and leveraging the capabilities of the recipient.

Will sharing threat intelligence help?

Threat intelligence can help defenders more quickly resist, identify, and respond to intrusions, but only if the organization is postured to succeed. Until one invests in sound strategy, processes, people and technology, no amount of information sharing or threat intelligence will be sufficient.

Who shares threat intelligence, and what are the challenges?

Sharing threat intelligence refers to three cases: 1) from the government to the private sector; 2) within the private sector; and 3) from the private sector to the government. All three face challenges.

In the government-to-private scenario, I encourage officials to grant clearances to private security teams not working on government contracts. The government should also augment its narrative style intelligence reports with digital appendices that list threat data in machine-readable form, similar to that offered by www.openioc.org.

In the private-to-private case, I recommend creating information sharing groups. Adversaries often target whole sectors at once, so it helps to have peer companies compare notes.

The private-to-government case is the most contentious, for two reasons. First, companies are reluctant to publicize security breaches, beyond what is necessary to comply with laws and standards. The private sector fears penalties if they disclose incidents to the government. Companies should not be held liable

for voluntarily reporting incidents. Accordingly, the White House proposal prohibits the use of so-called "cyberthreat indicators" in any regulatory enforcement action.

Second, some privacy advocates believe that liability protection will let companies submit customer personal information to the government. This position does not reflect the reality of threat intelligence as defined earlier. Proper threat intelligence contains tactics, tools, and procedures used by intruders to abuse software and networks. It does not contain personal data from or about customers, if properly formatted.

Finally, I'd like to mention an intelligence sharing pilot program organized by the Department of Energy (DoE), the North American Electric Reliability Corporation (NERC), and the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). Along with power companies, they operate the Cybersecurity Risk Information Sharing Program, or CRISP. Participants use commercial security technology at their network borders, and voluntarily share their findings with the Pacific Northwest National Laboratory (PNNL). PNNL extracts threat intelligence from the raw data, and shares it with other CRISP members, include DoE. DoE also shares what it discovers on DoE networks with CRISP participants. This program could provide a model for other sectors, and for the government as a whole.

I look forward to your questions.