Testimony of

Steven R. Chabinsky

Jointly before the
United States House of Representatives
Committee on Science, Space, and Technology

Subcommittee on Oversight
and
Subcommittee on Research and Technology

"*Can Technology Protect Americans from International Cybercriminals*?"

March 4, 2014

Introduction

Good morning Chairmen Broun and Bucshon, Ranking Members Maffei and Lipinski, and distinguished Members of the Subcommittees. I am pleased to appear before you today to discuss the role of technology in protecting Americans from international cybercrime. Within this context, I have been asked to provide an overview of the evolution of cyber intrusions against U.S. industry -- from rogue hackers, to sophisticated international crime syndicates, and to foreign governments. I also have been asked to describe the complex cyber security issues facing industry and how the risk of cyber threats and intrusions can best be managed.

Background

I have spent over fifteen years committed to reducing the security risks associated with emerging technologies. Most of my efforts have been with the Federal Bureau of Investigation, where I last served as Deputy Assistant Director of the Cyber Division, after having organized and led the FBI's cyber intelligence program and served as the FBI's top cyber lawyer. Today, I am the General Counsel and Chief Risk Officer of the cybersecurity technology firm CrowdStrike, as well as an adjunct faculty member of George Washington University and the cyber columnist for *Security* magazine. The observations and conclusions I am sharing today in my individual capacity are the culmination of a career spent in government, industry, and academia.

The Evolution of Computer Intrusions

As is the case with more traditional threats, we see a wide range of actors who are capable of, and engaged in, computer network intrusions and attack. Although rogue hackers have the ability to cause substantial harm against specific targets (especially when they are insiders), the far greater problem is that most hackers no longer work alone. Rather, over the past ten years, industry has faced a well-orchestrated hacking epidemic. Foreign intelligence services are siphoning off our intellectual property and weakening American competitiveness, while organized criminal groups steadily gain access to corporate and consumer credentials that have been used to defraud Americans out of billions of dollars.

On the nation-state side, China and Russia continue to conduct massive economic espionage hacking campaigns that impact thousands of corporate victims daily, not just in the United States but worldwide. As expressed in May 2013 by the Commission on the Theft of American Intellectual Property, the impact on victim economies are twofold. The first harm takes the form of lost revenues and lost jobs. The second harm is the erosion of "both the means and the incentive for entrepreneurs to innovate, which will slow the development of new inventions and industries."

Switching our focus to financially motivated cybercrime, we can break down the most common activities into two broad categories. First, there are traditional forms of fraud that now occur using email rather than regular mail, like the infamous Nigerian Letter scam. These schemes rely on social engineering, but they do not involve unauthorized computer access. Second, there are the more pernicious cybercrimes that seek to install malware on victim computers in order to control their processes and/or steal their data from afar. Hackers have a variety of techniques for installing malware on computers. They may rely upon phishing emails with links or attachments, supply chain infections, or compromised websites. Others may engage in remote computer intrusions that exploit software weakness, or take advantage of an ability to obtain, guess, create, or bypass legitimate user credentials. Regardless, cybercriminals in this second category typically gain access to a large number of victim networks, and obtain the ability to see and do most anything on them.

A few years ago, the FBI identified ten specializations within a typical cyber conspiracy. It is worth repeating them here to demonstrate the extent of capabilities available in the world of organized cybercrime. First, there are “coders” who write the malware, exploits, and other tools necessary to commit the crime. Second, there are “distributors” who trade and sell stolen data. Third, are the “techies” who maintain the criminal infrastructure. Fourth are the actual “hackers” who search for and exploit application, system, and network vulnerabilities. Fifth, there are “fraudsters” who create and deploy social engineering schemes, including phishing, spamming, and domain squatting in order to gain unlawful access. Sixth are ‘hosters” who provide “safe” hosting of illicit content servers and sites, often through elaborate botnets and proxy networks. These individuals specialize in the area of anonymization, setting up elaborate network infrastructures with encrypted servers running on networks that, by design to cater to criminals, do not log user activity and do not shut down websites regardless of complaints of unlawful conduct. Seventh are “cashers” who control drop accounts for money. Eighth are “money mules,” some of whom are sent to the U.S. on student visas with the purpose of moving money for criminals. Ninth, are “tellers” who help transfer and launder illicit proceeds through digital currency services and between different world currencies. And finally, tenth are the “leaders,” many of whom don’t have any technical skills at all. They choose the targets, choose the people they want to work each role, decide who does what, when, and where, and take care of personnel and payment issues. With respect to planning and logistics, when a new opportunity presents itself, these criminal organizations often start executing within hours.

The Location of Cybercrime

Over the years, it appears that a disproportionate amount of financially motivated cybercrime is tied to Eastern Europe. Of the FBI’s current Top Ten Cyber Most Wanted, seven have connections either to Russia, Ukraine, or Latvia. In some cases, international cybercriminals are suspected of receiving the protection of local authorities. Regardless, even to the extent cybercrime ringleaders may aggregate in certain areas of Europe, they typically are part of criminal conspiracies that span the globe.

For these reasons, it is imperative that law enforcement agencies throughout the world build strong relationships with one another and resource the capabilities that are necessary to quickly work together in common cause, whether to collect evidence, to recover stolen property, or to bring criminals to justice. One cannot overstate the importance of programs like the overseas FBI Legal Attaché assignments. The FBI testified last June that it had embedded cyber agents with law enforcement in several key countries, including Estonia, Ukraine, the Netherlands, Romania, and Latvia, and that it was expanding its Cyber Assistant Legal Attaché program to the United Kingdom, Singapore, Bulgaria, Australia, Canada, the Republic of Korea, and Germany. These efforts, together with complementary actions taken by the United States Secret Service, are designed to decrease the number of hackers worldwide (whether through arrests or based on their threat deterrent effect), and are likely to demonstrate consistent benefits over time that far outweigh their costs. These efforts also help fulfill a primary role of government to protect its citizens and their property.

The Victims of Cybercrime and Cyber Economic Espionage

Next, it is important to consider the victims associated with cybercrime, and to recognize that many of them do not have the resources to mount a significantly stronger defense than they currently are against computer attacks. It certainly is the case that the cyber intrusion headlines tend to focus on the Fortune 100 being hacked; but they're not the only victims. Naturally, since 99.9% of all U.S. businesses have less than 500 employees, and few of those retain dedicated information security staff, cyber criminals find small and medium enterprises (SMEs) to be attractive targets as well. Making matters worse, targeted attacks against SMEs appear to be increasing.

Core Tenets of Security

In order to get security risks under control, whether in the "physical" or cyber worlds, security experts rely upon the levers of vulnerability mitigation, threat reduction and, should the first two fail, consequence management. In the area of cybersecurity, vulnerability mitigation has been our nation's predominant approach. Unfortunately, the majority of our government and private sector resources focus on having potential victims fear for the loss of their data, rather than having actual hackers fear for the loss of their freedom.

We have retained this focus on vulnerability mitigation despite it being well understood that securing networks is a daunting task even for the most experienced. As stated in Verizon's 2013 Data Breach Investigations Report, "breaches are a multi-faceted problem, and any one-dimensional attempt to describe them fails to adequately capture their complexity." On the technical side—the web servers, e-mail servers, databases, firewalls, routers, embedded network devices, internal networks, global remote access, custom applications, off-the-shelf applications, backup and storage areas, and all telephone, PBX, and VoIP systems require attention. On the human side, the physical infrastructure must be protected, employee accesses and permissions must be restricted, and connections to business and corporate partners (often operating under different legal regimes) have to be managed. Of course, these are just the basics, and each aspect of cybersecurity must be monitored and updated regularly, as the technologies, users, and adversaries change constantly.

In order to reduce the likelihood of harm, information security professionals deploy a wide range of defensive controls. In answer to the question posed by this Hearing, one of those controls most certainly involves the use of technology. In the risk management community these are commonly referred to as *technical* controls. Examples of technical controls include the use of smart cards with encryption, passwords and biometrics, endpoint activity monitoring, firewalls, and intrusion detection and prevention systems. In my professional opinion, technical controls (not "people," as often is said) are best positioned to be a company's first line of cyber defense. Technical controls are particularly well suited to reduce the time necessary to detect unlawful activity and to substantially limit the consequences of a successful breach. Still, although technical controls often are necessary for security, they are seldom sufficient. Security professionals also commonly deploy *physical* controls (such as locks on doors) and *administrative* controls (such as acceptable computer use policies and pre-employment background checks). Each of these controls, deployed together as a "defense in depth," serves to protect industry from cybercrime.

To get a better feel for the difficulties of being a cybersecurity professional, it is worthwhile to consider, at the 30,000 foot level, the following seventeen different categories that NIST recommends network defenders review (keeping in mind that each of these is then broken down further into more discrete, tactical methods):

1. access control;
2. awareness and training;
3. audit and accountability;
4. certification, accreditation, and security assessments;
5. configuration management;
6. contingency planning;
7. identification and authentication;
8. incident response;
9. maintenance;
10. media protection;
11. physical and environmental protection;
12. planning;
13. personnel security;
14. risk assessment;
15. systems and services acquisition;
16. system and communications protection; and

17. system and information integrity.

Continuously reviewing and implementing the technical, physical, and administrative controls within each of these seventeen categories can help prevent some aspects of international cybercrime altogether and, in the event of a successful breach, can quickly detect the intrusion and mitigate the consequences. However, relying upon the owners and operators of networks to be primarily responsible for stopping well-resourced, determined actors – without a similar or greater alignment of government resources to bring international offenders routinely to justice -- has turned out to be exorbitantly expensive and ineffective over time.

In this regard, it is also worth noting that hackers usually take advantage of the easiest path to exploit a system. For this reason, it often is difficult to anticipate the long-term impact of industry best practices and costly mitigation efforts: will the hackers be foiled, seek a different victim, pull something else out from their existing criminal toolkit, or devise a new exploit? I am reminded of costly efforts that the banking and finance sector adopted a few years back, providing business customers with key fobs in which the pin numbers changed every sixty seconds. The bad guys simply redirected the pin numbers to themselves the moment the customers entered them into their infected web browsers. To similar effect, I also recall Intellectual Property Rights investigations that uncovered thieves who invested tens of thousands of dollars to buy machines that added hologram stamps to their counterfeit software CDs and DVDs. I have also observed that bad guys tend not to get discouraged by minor setbacks, and they will continue their unlawful activities unless they get caught or believe they will get caught. After all, cybercrime is big business, and the bad guys have time to seek out new vulnerabilities and explore new techniques. In the context of today’s discussion about crimes against the retail industry, we cannot forget recent experiences in the United Kingdom where, after spending in excess of one billion dollars on new technologies, one media headline read, “Card fraud hits record high despite fortune spent on chip-and-pin security.” A professor at Cambridge University then lamented, “It has simply led to a change in [criminal] tactics.”

Conclusion

There is no doubt that cyber threats present considerable risk to our economic and national security interests, and that these threats continue to grow at an alarming rate. Despite billions of dollars of investment in cybersecurity defensive efforts, and the prospect of spending billions of dollars more, many experts see no hope on the horizon that the overall cyber threat against our country will level off, no less begin to decline. It is my professional opinion that this downward spiral is not inevitable and that we can improve our security considerably. However, it also is my professional opinion that improving our security posture requires that to a certain extent we reconsider, rather than simply redouble, the nature of our efforts.

Fundamentally, we need to ensure that our cybersecurity strategies, technologies, market incentives, and international dialogue focus greater attention on the challenges of more quickly detecting and mitigating harm, while in parallel locating and penalizing bad actors. Doing so would align our cybersecurity efforts with the security strategies we use in the physical world. In the physical world, vulnerability mitigation efforts certainly have their place. We take reasonable precautions to lock our doors and windows, but we do not spend an endless amount of resources in hopes of becoming impervious to crime. Instead, to counter determined thieves, we ultimately concede that an adversary can gain unlawful entry but, through the use of burglar alarms and video cameras, we shift our focus towards instant detection, attribution, threat response, and recovery. When the alarm monitoring company calls a business owner at 3 a.m., it does not say, "We just received an alarm that your front door was broken into. But, don't worry, we've called the locksmith." Rather, it is only obvious, immediately necessary, and the reason people purchase alarm systems, that they call the police to stop the felon. It is surprising then and suggests a larger problem that, in the world of cyber, when the intrusion detection system goes off the response has been to call the Chief Information Security Officer, and perhaps even the CEO, to explain what went wrong and to prevent it from happening again. It is my hope for the future that the blame for, and the costs of, cybercrime will fall more squarely on the offenders than on the victims, that in doing so we will achieve greater threat deterrence, and that businesses and consumers will benefit from improved, sustained cybersecurity at lower costs.

Thank you for the opportunity to testify today. I would be happy to answer any questions you may have.