Department of Justice

STATEMENT OF

GORDON M. SNOW
ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON JUDICIARY
UNITED STATES SENATE
CRIME AND TERRORISM SUBCOMMITTEE

ENTITLED

"CYBERSECURITY: RESPONDING TO THE THREAT OF CYBER CRIME AND TERRORISM"

PRESENTED

April 12, 2011

Good afternoon Chairman Whitehouse, Ranking Member Kyl, and members of the Subcommittee. I'm pleased to appear before you today to discuss the cyber threats facing our nation and how the FBI and our partners are working together to protect United States (U.S.) government and private sector networks.

Countering efforts by foreign countries to steal our nation's secrets, evaluating the capabilities of terrorists in a digital age, and fighting cyber crime are the FBI's highest priorities. It is difficult to overstate the potential impact these threats pose to our economy, our national security, and the critical infrastructure upon which our country relies.

The Cybersecurity Threat

As the Subcommittee is aware, the number and sophistication of cyber attacks has increased dramatically over the past five years and is expected to continue to grow.

The threat has reached the point that given enough time, motivation, and funding, a determined adversary will likely be able to penetrate any system that is accessible directly from the Internet.

It is difficult to state with confidence that our critical infrastructure—the backbone of our country's economic prosperity, national security, and public health—will remain unscathed and always be available when needed.

The recent security breach by unauthorized intruders into the parent company of NASDAQ is an example of the kind of breaches directed against important financial infrastructure and illustrates the difficulty of determining clear attribution. As we would in response to any such breach, the FBI is working to identify the scope of the intrusion and assist the victim in the remediation process.

The FBI has identified the most significant cyber threats to our nation as those with high intent and high capability to inflict damage or death in the U.S., to illicitly acquire assets, or to illegally obtain sensitive or classified U.S. military, intelligence, or economic information.

As both an intelligence and law enforcement agency, the FBI can address every facet of a cyber case—from collecting intelligence on the subjects in order to learn more about their networks, to dismantling those networks and prosecuting the individual perpetrators. The ability to take action on the information we collect is critical because what may begin as a criminal investigation may become a national security threat.

In addition, the FBI’s presence in Legal Attachés in 61 cities around the world assists in the critical exchange of case related information and the situational awareness of current threats, helping to combat the global scale and scope of cyber breaches. The FBI is also changing to adapt to the ever-evolving technology and schemes used by cyber criminals. Intelligence now drives operations in the FBI. The Bureau is working in new ways with long-standing and new partners to address the cybersecurity threat.

Cyber Threats Against the Private Sector

Cyber criminal threats to the U.S. result in significant economic losses. But the threat against financial institutions is only part of the problem. Also of serious concern are threats to critical infrastructure, the theft of intellectual property, and supply chain issues.

Cyber Threats to U.S. Critical Infrastructure

U.S. critical infrastructure faces a growing cyber threat due to advancements in the availability and sophistication of malicious software tools, and the fact that new technologies raise new security issues that cannot always be addressed prior to adoption. The increasing automation of our critical infrastructures provides more cyber access points for adversaries to exploit.

New “smart grid” and “smart home” products, designed to provide remote communication and control of devices in our homes, businesses, and critical infrastructures, must be developed and implemented in ways that will also provide protection from unauthorized use. Otherwise, each new device could become a doorway into our systems for adversaries to use for their own purposes.

Industrial control systems (ICSs), which operate the physical processes of the nation’s pipelines, railroads, and other critical infrastructures, are at elevated risk of cyber exploitation.

The FBI is concerned about the proliferation of malicious techniques that could degrade, disrupt, or destroy critical infrastructure. Although likely only advanced threat actors are currently capable of employing these techniques, as we have seen with other malicious software tools, these capabilities will eventually be within reach of all threat actors.

Intellectual Property Theft and Supply Chain Risks

Intellectual property rights (IPR) violations, including theft of trade secrets, digital piracy, and trafficking counterfeit goods, also represent high cyber criminal threats, resulting in losses of billions of dollars in profits annually. These threats also pose significant risk to U.S. public health and safety via counterfeit pharmaceuticals, electrical components, aircraft parts and automobile parts.

Cyber crime that manipulates the supply chain could pose a threat to national security interests and U.S. consumers. Poorly manufactured computer chips or chips that have been salvaged and repackaged infringe on intellectual property rights and could fail at critical times, posing a serious health and safety threat to U.S. citizens. Malware could be embedded on the chips to exfiltrate information from computers and result in the theft of Personally Identifiable Information (PII) that could then be used in future cyber crimes. As the quality of counterfeit goods increases, U.S. consumers may be challenged to tell the difference between authentic and fraudulent goods.

Operation Cisco Raider is a joint initiative between the U.S. and Canada that targets the illegal distribution of counterfeit network hardware manufactured by private entities in China. The use of counterfeit network components can lead to exploitation of cyber infrastructure vulnerabilities and even network failure. Since 2006, Operation Cisco Raider has seized over 3,500 network components amounting to $3.5 million of Cisco retail products. Ten individuals have been convicted as a result of the joint initiative.

The Booming Business of Botnets

Botnets are networks of compromised computers controlled remotely by an attacker. Criminals use botnets to facilitate online schemes that steal funds or data, to anonymize online activities, and to deny access by others to online resources. The botnets run by criminals could be used by cyber terrorists or nation states to steal sensitive data, raise funds, limit attribution of cyber attacks, or disrupt access to critical national infrastructure. Today’s botnets are often modular and can add or change functionality using internal update mechanisms.

Today’s cyber criminals are business savvy. These criminals are building businesses based on the development, management, and sale of botnets. These criminal groups have programmers who write the malicious software, salespeople who sell the code or lease out botnet services, and, in some instances, dedicated support personnel. These criminals are working to make botnets easier to deploy and more difficult to detect.

Successful botnet development and operations use techniques similar to legitimate businesses including the involvement of personnel with various specialties, feature-based pricing structures, modularization, and software copy protection. The development and sale of kit-based botnets has made it easier for criminals with limited technical expertise to build and maintain effective botnets. Botnet development and management is approached in a business-like fashion. Some criminals rent or sell their botnets or operate them as a specialized portion of an ad hoc criminal organization. At least one botnet kit author implemented a copy protection scheme, similar to major commercial software releases, which attempts to limit unauthorized use of the botnet kit.

Botnets that specialize in data exfiltration are able to capture the contents of encrypted webpages and modify them in real time. When properly configured, criminals can ask additional questions at login or modify the data displayed on the screen to conceal ongoing criminal activity. Criminals purchase the base kits for a few thousand dollars and can pay for additional features to better target specific webservices.

The "Not for Profit" Cyber Criminal

Hacktivist groups such as 'Anonymous' undertake protests and commit computer crimes as a collective unit. Anonymous does not have a leader or a controlling party but instead relies on the collective power of individual participants. Its members utilize the Internet to communicate, advertise, and coordinate their actions. Anonymous has initiated multiple criminal Distributed Denial of Service (DDoS) attacks against the Recording Industry Association of America (RIAA), the Motion Picture Association of America (MPAA), the Church of Scientology, and various businesses in support of WikiLeaks.

Just last month, Anonymous hacked into the website of a U.S. security firm with U.S. government contracts and stole approximately 72,000 e-mails from the company and posted them online. This attack was in response to the claim that a researcher at the company had identified key members of Anonymous.

Financial Estimates of Damages

Cyber criminals are forming private, trusted, and organized groups to conduct cyber crime. The adoption of specialized skill sets and professionalized business practices by these criminals is steadily increasing the complexity of cyber crime by providing actors of all technical abilities with the necessary tools and resources to conduct cyber crime. Not only are criminals advancing their abilities to attack a system remotely, but they are becoming adept at tricking victims into compromising their own systems. Once a system is compromised, cyber criminals will use their accesses to obtain PII, which includes online banking/brokerage account credentials and credit card numbers of individuals and businesses that can be used for financial gain. As cyber crime groups increasingly recruit experienced actors and pool resources and knowledge, they advance their ability to be successful in crimes against more profitable targets and will learn the skills necessary to evade the security industry and law enforcement.

The potential economic consequences are severe. The sting of a cyber crime is not felt equally across the board. A small company may not be able to survive even one significant cyber attack. On the other hand, companies may not even realize that they have been victimized by cyber criminals until weeks, maybe even months later. Victim companies range in size and industry.

Often, businesses are unable to recoup their losses, and it may be impossible to estimate their damage. Many companies prefer not to disclose that their systems have been compromised, so they absorb the loss, making it impossible to accurately calculate damages.

As a result of the inability to define and calculate losses, the best that the government and private sector can offer are estimates. Over the past five years, estimates of the costs of cyber crime to the U.S. economy have ranged from millions to hundreds of billions. A 2010 study conducted by the Ponemon Institute estimated that the median annual cost of cyber crime to an individual victim organization ranges from 1 million to 52 million dollars.

According to a 2011 publication released by Javelin Strategy and Research, the annual cost of identity theft is $37 billion. This includes all forms of identity theft, not just cyber means. The Internet Crime Complaint Center (IC3), which aggregates self-reported complaints of cyber crime, reports that in 2010, identity theft schemes made up 9.8% of all cyber crime.

Addressing the Threat

Although our cyber adversaries' capabilities are at an all-time high, combating this challenge is a top priority of the FBI and the entire government. Thanks to Congress and the administration, we are devoting significant resources to this threat. Our partnerships within industry, academia, and across all of government have also led to a dramatic improvement in our ability to combat this threat.

The FBI's statutory authority, expertise, and ability to combine resources across multiple programs make it uniquely situated to investigate, collect, and disseminate intelligence about and counter cyber threats from criminals, nation-states, and terrorists.

The FBI is a substantial component of the Comprehensive National Cybersecurity Initiative (CNCI), the interagency strategy to protect our digital infrastructure as a national security priority. Through the CNCI, we and our partners collaborate to collect intelligence, gain visibility on our adversaries, and facilitate dissemination of critical information to decision makers.

The FBI has cyber squads in each of our 56 field offices, with more than 1,000 advanced cyber-trained FBI agents, analysts, and forensic examiners. We have increased the capabilities of our employees by selectively seeking candidates with technical skills and enhancing our cyber training.

In addition, as part of the FBI's overall transformation to an intelligence-driven organization, the Cyber Division has implemented Threat Focus Cells, which bring together subject matter experts from various agencies to collaborate and address specific identified cyber threats.

Partnerships

However, one agency cannot combat the threat alone. Through the FBI-led National Cyber Investigative Joint Task Force (NCIJTF), we coordinate our efforts with 20 law enforcement and Intelligence Community (IC) entities, including the Central Intelligence Agency (CIA), Department of Defense (DoD), DHS, and NSA. The FBI also has embedded cyber staff in other IC agencies through joint duty and detailee assignments.

We have also enhanced our partnership with DHS, forming joint FBI-DHS teams to conduct voluntary assessments for critical infrastructure owners and operators who are concerned about the network security of their ICSs. DHS has provided more than 30 FBI agents and intelligence analysts with specialized training in these systems.

In addition, because of the frequent foreign nexus to cyber threats, we work closely with our international law enforcement and intelligence partners.

We currently have FBI agents embedded full-time in five foreign police agencies to assist with cyber investigations: Estonia, the Netherlands, Romania, Ukraine, and Colombia. These cyber personnel have identified cyber organized crime groups targeting U.S. interests and supported other FBI investigations. We have trained foreign law enforcement officers from more than 40 nations in cyber investigative techniques over the past two years.

We have engaged our international allies, including Australia, New Zealand, Canada, and the United Kingdom, in strategic discussions that have resulted in increased operational coordination on intrusion activity and cyber threat investigations.

Government and Private Sector Information Sharing

The FBI has developed strong relationships with private industry and the public. InfraGard is a premier example of the success of public-private partnerships. Under this initiative, state, local, and tribal law enforcement, academia, other government agencies, communities, and private industry work with us through our field offices to ward off attacks against critical infrastructure. Over the past 15 years, we have seen this initiative grow from a single chapter in the Cleveland field office to more than 86 chapters in 56 field offices with 42,000 members.

The exchange of knowledge, experience, and resources is invaluable and contributes immeasurably to our homeland security. Notably, DHS has recognized the value of the program and recently partnered with the InfraGard program to provide joint training and conferences during this fiscal year.

With outside funding from DHS, the newly formed Joint Critical Infrastructure Partnership will host five regional conferences this year along with representation at a number of smaller venues. The focus of the program is to further expand the information flow to the private sector by not only reaching out to the current InfraGard membership but also reaching beyond current members to local critical infrastructure and key resource owners and operators. The goal is to raise awareness of risks to the nation's infrastructure and to better educate the public about infrastructure security initiatives. This partnership is a platform which will enhance the risk management capabilities of local communities by providing security information, education, training, and other solutions to protect, prevent, and respond to terrorist attacks, natural disasters, and other hazards, such as the crisis currently facing Japan. Ensuring that a country's infrastructure is protected and resilient is key to national security.

Experience has shown that establishing rapport with the members translates into a greater flow of information within applicable legal boundaries, and this rapport can only be developed when FBI personnel have the necessary time and resources to focus on the program. This conduit for information results in the improved protection of the infrastructure of the U.S.

In addition to InfraGard, the FBI participates in other activities with the private sector, like the Financial Services Information Sharing and Analysis Center (FS-ISAC). A good example of this cooperation is the FBI's identification of a bank fraud trend in which U.S. banks were unaware that they were being defrauded by businesses in another country. As a result of FBI intelligence analysis, a joint FBI/FS-ISAC document was drafted and sent to the FS-ISAC's membership, alerting them to these crimes and providing recommendations on how to protect themselves from falling victim to the same scheme.

In the last few years, there has been a push to partner FBI intelligence analysts with private sector experts. This is an opportunity for the intelligence analysts to learn more about the industries they are supporting. They then can better identify the needs of those industries as well as FBI information gaps. Additionally, they develop points-of-contact within those industries who can evaluate and assist in timely analysis, and the analysts mature into subject matter experts.

Other successful cyber partnerships include the Internet Crime Complaint Center (IC3) and the National Cyber-Forensics and Training Alliance (NCFTA). Established in 2000, the IC3 is a partnership between the FBI and the National White Collar Crime Center that serves as a vehicle to receive, develop, and refer criminal complaints regarding cyber crime. Since it began, the IC3 has processed more than 2 million complaints. Complaints are referred to local, state, federal and international law enforcement and are also the basis for intelligence products and public service announcements. The FBI's IC3 unit works with the private sector, individually and through working groups, professional organizations, and InfraGard, to cultivate relationships, inform industry of threats, identify intelligence, and develop investigative information to enhance or initiate investigations by law enforcement.

The NCFTA is a private nonprofit organization, composed of representatives of industry and academia, which partners with the FBI. The NCFTA, in cooperation with the FBI, develops responses to evolving threats to the nation's critical infrastructure by participating in cyber-forensic analysis, tactical response development, technology vulnerability analysis, and the development of advanced training. The NCFTA work products can be provided to industry, academia, law enforcement, and the public as appropriate.

The FBI also partners with the U.S. private sector on the Domestic Security Alliance Council (DSAC). This strategic collaboration enhances communications and promotes effective exchanges of information in order to prevent, detect, and investigate criminal acts, particularly those affecting interstate commerce, while advancing the ability of the U.S. private sector to protect its employees, assets, and proprietary information.

The DSAC is in a unique position to speak on behalf of the private sector because the DSAC members are the highest ranking security executives of the member companies, who directly report to the leaders of their organizations.

Successes

Our partnerships and joint initiatives are paying off, especially in the national security realm. In 2010, the FBI strengthened our efforts to counter state-sponsored cyber threats, increasing the number of national security computer intrusion cases by 60%.

While we increased our emphasis on national security, we continued to see successes on the criminal side. In 2010, we arrested a record 202 individuals for criminal intrusions, up from 159 in 2009. We obtained a record level of financial judgments for such cases of $115 million, compared to $85 million in 2009. Those arrests included five of the world's top cyber criminals. Among them were the perpetrators of the Royal Bank of Scotland (RBS) WorldPay intrusion. Due to our strong partnership with the Estonian government on cyber matters, the case resulted in one of the first hackers extradited from Estonia to the United States.

Conclusion

As the Subcommittee knows, we face significant challenges in our efforts to combat cyber crime. In the current technological environment, there are numerous threats to private sector networks, and the current Internet environment can make it extremely difficult to determine attribution.

We are optimistic that by strengthening relationships with our domestic and international counterparts, the FBI will continue to succeed in identifying and neutralizing cyber criminals, thereby protecting U.S. businesses and critical infrastructure from grave harm.

To bolster our efforts, we will continue to share information with government agencies and private industry consistent with applicable laws and policies. We will continue to engage in strategy discussions with other government agencies and the private sector to ensure that American ingenuity will lead to new solutions and better security. We will continue to build a skilled workforce to operate in this challenging environment.

We look forward to working with the Subcommittee and Congress as a whole to determine a successful course forward for the nation that allows us to reap the positive economic and social benefits of the Internet while minimizing the risk posed by those who would use it for nefarious purposes.