



Department of Justice

STATEMENT OF

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

BEFORE THE

HOUSE FINANCIAL SERVICES COMMITTEE
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS
AND CONSUMER CREDIT

ENTITLED

“CYBER SECURITY: THREATS TO THE FINANCIAL SECTOR”

PRESENTED

September 14, 2011

Good afternoon Chairman Capito, Ranking Member Maloney, 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 the financial sector and American consumers.

Cyber criminals can significantly threaten the finances and reputations of United States (U.S.) businesses and financial institutions. Given the abundance of potential victims and profits, cyber criminals will likely continue to target these entities. The FBI is committed to addressing these threats through innovative and proactive means and making the Internet more secure for financial institutions and U.S. consumers alike.

The Cyber Threat to the Financial Sector

As the Subcommittee is aware, the number and sophistication of malicious incidents has increased dramatically over the past five years and is expected to continue to grow. As business and financial institutions continue to adopt Internet-based commerce systems, the opportunities for cyber crime increase at retail and consumer levels.

Account Takeovers

Cyber criminals have demonstrated their abilities to exploit our online financial and market systems that interface with the Internet, such as the Automated Clearing House (ACH) systems, card payments, and market trades. In these instances, cyber crime is easily committed by exploiting the system users, rather than the systems themselves. This is typically done through the compromise of a legitimate user's account credentials.

Fraudulent monetary transfers and counterfeiting of stored value cards are the most common result of exploits against financial institutions, payment processors, and merchants. While the losses that result from these exploits generally fall upon the financial institution, consumers experience the inconvenience of changing accounts and replacing cards associated with their compromised information, as well as the emotional impact associated with being a victim of a cyber crime.

The FBI is currently investigating over 400 reported cases of corporate account takeovers in which cyber criminals have initiated unauthorized ACH and wire transfers from the bank accounts of U.S. businesses. These cases involve the attempted theft of over \$255 million and have resulted in the actual loss of approximately \$85 million.

Often, the attack vector is a targeted phishing e-mail that contains either an infected file or a link to an infected website. The e-mail recipient is generally a person within a targeted company who can initiate fund transfers on behalf of the business or another valid online banking credential account holder. Once the recipient opens the attachment or navigates to the website, malware is installed on the user's computer, which often includes a keylogging program that harvests the user's online banking credentials.

The criminal then either creates another account or directly initiates a funds transfer

masquerading as the legitimate user. The stolen funds are often then transferred overseas. Victims of this type of scheme have included small and medium-sized business, local governments, school districts, and health care service providers.

In 2008, a Pennsylvania school district discovered that over \$450,000 was missing from their bank account. The following year, a New York school district reported that approximately \$3 million had been transferred out of their bank account. The New York's school district's bank was able to recover some of the transfers, but \$500,000 had already been withdrawn from the account before the transaction could be reversed.

Recently, two trucking companies were victimized by fraudulent electronic account transfers, and lost approximately \$115,000. Compared to some loss figures, this might not seem significant. One of the companies currently has annual revenues worth roughly \$79 million, so their loss was nearly .1% of their gross revenue. That amount is approximately enough to purchase an additional tractor-trailer and provide another driver with a job.

In March 2010, an Illinois town was the victim of a cyber intrusion resulting in unauthorized ACH transfers totaling \$100,000. When an authorized individual logged into the town's bank account, the individual was redirected to a site alerting her that the bank's website was experiencing technical difficulties. During this redirection, the criminal used the victim's authorized credentials to initiate transactions. The town was able to recover only \$30,000.

Third Party Payment Processor Breaches

Sophisticated cyber criminals are also targeting the computer networks of large payment processors, resulting in the loss of millions of dollars and the compromise of personally identifiable information (PII) of millions of individuals.

In November 2008, a U.S. payment processor discovered that hackers had breached the company's computer systems and compromised the personal data of over 1.5 million customers; roughly 1.1 million social security numbers were also exposed. The criminals used the stolen data to create fake debit cards and withdrew more than \$9 million from Automated Teller Machines (ATMs) worldwide.

In January 2009, it was discovered that cyber criminals compromised the computer network of a U.S. payment processor that completes approximately 100 million transactions monthly for more than 250,000 U.S. businesses. The criminals were able to obtain over 130 million customer records, which included credit card numbers, expiration dates, and internal bank codes.

Securities and Market Trading Exploitation

Securities and brokerage firms and their customers are common targets of cyber

criminals. The typical crimes against these firms include market manipulation schemes and unauthorized stock trading.

In 2010, law enforcement agencies and financial regulators observed a trend in which cyber criminals initiated unauthorized financial transactions from compromised victim bank or brokerage accounts. These transactions were paired with a Telephone Denial of Service (TDoS) attack, in which the victim's legitimate phone line was flooded with spam-like telephone calls to prevent the banks or brokerage firms from contacting the victim to verify that the transactions were legitimate.

In December 2009, a victim in Florida filed a police report stating that \$399,000 had disappeared from his online brokerage account while he was simultaneously targeted in a TDoS attack. The online withdrawals occurred in four increments, with progressively larger amounts being withdrawn each time.

Cyber criminals target not only those who trade in securities but also the exchanges in which the securities are sold. These TDoS and Distributed Denial of Service (DDoS) attacks show a desire by cyber criminals to focus their efforts on high-profile financial sector targets.

Beginning in July 2009, two U.S. stock exchanges were victims of a sustained DDoS attack. The remote attack temporarily disrupted public websites but had no impact on financial market operations. A parent company of one of the exchanges stated that it had not experienced any degradation in service on its public website or core trading and data systems, which operate on a private network.

In February 2011, criminal actors placed an online advertisement infected with malicious software onto the public website for a foreign stock exchange. The malicious advertisement appeared on the victims' computers as a pop-up, alerting the user to non-existent computer infections in an attempt to trick the users into paying for and downloading rogue "antivirus" software.

Also in February, the parent company of NASDAQ confirmed that they had been the victim of a security breach by unauthorized intruders into their Director's Desk web application, a system that was not directly linked to their trading platforms, but was instead used as an online portal for senior executives and directors to share confidential information.

These types of malicious incidents highlight not only the targeting of important financial infrastructure by cyber criminals, but also the difficulty of determining consequences and intent. For example, although it seems no real-time trading environments have been compromised in these incidents, cyber criminals could be more interested in obtaining valuable insider information than in disrupting the markets.

ATM Skimming and Point of Sale Schemes

ATM skimming is also a prevalent global cyber crime. A criminal affixes a skimmer to the outside or inside of an ATM to collect card numbers and Personal Identification Number (PIN) codes. The criminal then either sells the stolen data over the Internet or makes fake cards to withdraw money from the compromised accounts.

The technology of the skimmer devices continues to improve. This technique is also being used to steal credit and debit card information from customers at gas station pumps. Bluetooth-enabled wireless skimmers were found at a string of gas stations in the Denver area attached to the inside of the gas pump. The wireless capabilities of the skimmers allowed the criminal to download the information from the skimmers instantly, as long as they were in range of the wireless network.

Even as technology improves to protect against skimming, cyber criminals are creating devices to mimic the security features of legitimate ATM hardware. For example, ATM vendors have created new anti-skimming tools that include a backlit green or blue plastic casing around the card slot to prevent skimmers from being attached. In Ireland in early 2011, cyber criminals attached several skimmers that appeared identical to the new security devices.

Point of sale (POS) terminals, which are primarily used to conduct the daily sale operations in restaurants, retail stores, and places of business, have been a primary target for cyber criminals engaging in credit card fraud and have resulted in the compromise of millions of credit and debit cards the U.S. For example, in March 2008, three men were charged with hacking into several “smart” cash registers belonging to a U.S. restaurant chain. The criminals installed “sniffer” programs that were used to steal payment data as the information was being sent from the POS terminals in the restaurant to the chain’s corporate office. The stolen data resulted in more than \$600,000 in losses.

Mobile Banking Exploitation

As more mobile devices have been introduced into personal, business, or government networks, they have been increasingly targeted for stealing PII. The spread of mobile banking provide additional opportunities for cyber crime. Cyber criminals have successfully demonstrated man-in-the-middle attacks against mobile phones using a variation of Zeus malware. The malware is installed on the phone through a link imbedded in a malicious text message, and then the user is instructed to enter their complete mobile information. Because financial institutions sometimes use text messaging to verify that online transactions are initiated by a legitimate user, the infected mobile phones forward messages to the criminal, thwarting the bank’s two-factor authentication.

Cyber criminals are also taking advantage of the Twitter iPhone application by sending malicious “tweets” with links to a website containing a new banking Trojan. Once installed, the Trojan disables Windows Task Manager and notifications from Windows Security Center to avoid detection. When the victim opens their online banking account or makes a credit card purchase, PII is sent to the criminal in an encrypted file.

Insider Access

The high level of trust and confidence in U.S. financial markets is based on their long-standing reliability in protecting and ensuring the integrity of their systems. Unfortunately, individuals with direct access to core processing centers may be in a position to steal intellectual property, insider information, or data that can damage the reputation of the company. An individual could leverage this information to affect stock prices or to provide other companies with a competitive advantage.

In 2010, the FBI investigated two high profile cases involving the theft or attempted theft of source code for high-frequency trading programs. The theft of these programs could cost the victim company millions of dollars in losses, allow a competitor to predict a company's actions, or give a competitor the opportunity to profit using the victim companies' strategies.

Supply Chain Infiltration

The production, packaging, and distribution of counterfeit software or hardware used by financial institutions or critical financial networks by cyber criminals could result in the compromise of proprietary data, system disruption, or complete system failure. Gaining physical and technical access to financial institutions could be accomplished by compromising trusted suppliers of technical, computer, and security equipment, software, and hardware.

Financial firms have become regular targets of supply chain attacks. For example, ATMs have been delivered with malware installed on the systems, fake endpoints on the ATM networks have been created, and individuals have posed as ATM maintenance workers. Additionally, vendors who supply services to the banking and finance sector are constant targets of cyber criminals, including those who provide services like security, authentication, and online banking platforms.

Telecommunication Network Disruption

Financial networks are highly dependent on the availability of telecommunication infrastructure. Although cyber criminals may not be able to directly target the core processing centers that support the critical financial markets, they may target the telecommunication networks to directly impact the functionality of key financial players.

In market trading, infrastructure is crucial to the success of firms that specialize in high-frequency trading as milliseconds of saved time during data processing and transmission can impact profits. As a result, many firms co-locate and buy space near the main processing center of the major exchanges. The close proximity of these networks adds a shared reliance on telecommunication infrastructures, which could be significant if there is a disruption to the infrastructure.

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.

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. Additionally, the Administration's National Strategy for Trusted Identities in Cyberspace (NSTIC) seeks to address this threat by increasing the security of online transactions through the development of more trustworthy digital credentials which will help to reduce account takeovers and raise overall consumer safety levels.

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 plays a substantial role in 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, 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.

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), Department of Homeland Security (DHS), and National Security Agency (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 industrial control systems (ICSs). DHS has provided more than 30 FBI agents and intelligence analysts with specialized training in these systems.

To support small businesses, we have also partnered with the National Institute of Standards and Technology (NIST) and the Small Business Administration (SBA) since 2002 to sponsor computer security workshops and provide online support for small businesses through the InfraGard program. These workshops, which are held across the country, feature security experts who explain information security threats and vulnerabilities and describe protective tools and techniques which can be used to address potential security problems.

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.

The FBI has worked with a number of regulatory agencies to determine the scope of the financial cyber crime threat, develop mitigation strategies, and provide Public Service Announcements where appropriate, to include the U.S. Department of Treasury – Financial Crimes Enforcement Network (FinCEN), Financial Services Information Sharing and Analysis Center (FS-ISAC), the Securities and Exchange Commission (SEC), the Office of Comptroller of Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), the Federal Reserve Board, and the Federal Reserve Bank.

In addition, the FBI partners with criminal investigators from the Internal Revenue Service (IRS), the U.S. Secret Service (USSS), U.S. Immigration and Customs Enforcement (ICE), the Department of State’s Bureau of Diplomatic Security Service (DSS), and the U.S. Postal Inspection Service to further investigations.

Additionally, the FBI works with a number of industry governing entities such as NACHA – the Electronic Payments Association and the Financial Industry Regulatory Authority (FINRA) to understand and investigate cyber crime problems affecting a particular industry segment.

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 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 can then 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 and DHS 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.

Threat Mitigation

The FBI has been able to mitigate a number of fraud matters by sharing identified threat data amongst financial sector partners. The FBI participates in other activities with the private sector, like the 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.

Another recent success was the combined efforts of the FBI, DOJ, and industry subject matter experts to takedown the "Coreflood" botnet. This botnet infected user computers and transferred banking credentials and other sensitive information to the botnet's command-and control services. This botnet infected millions of computers and the criminals used the stolen information to steal millions of dollars from unsuspecting consumers. In this instance, government and private industry worked together to provide an innovative response to a cyber threat. Not only was the Coreflood botnet shut down through a temporary restraining order, the government was authorized to respond to signals sent from infected computers in the U.S. in order to stop the Coreflood software from running. This prevented further harm to hundreds of thousands of unsuspecting users of infected computers in the U.S.

Conclusion

As the Subcommittee knows, we face significant challenges in our efforts to combat cyber crime. In the current technological environment, there are growing avenues for cyber crimes against the U.S. financial infrastructure and consumers. Modifications to business and financial institution security and risk management practices will directly affect the future of these types of crimes, and the adoption of best practices may be negated by the lack of security-conscious behavior by customers.

Malicious cyber incidents are costly and inconvenient to financial institutions and their

customers, and although most businesses take action to recover quickly, limit impact to customers, and ensure long-term operational viability, the increasing sophistication of cyber criminals will no doubt lead to an escalation in cyber crime.

To bolster the efforts of the FBI against these cyber criminals, 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 cyber threats are countered swiftly and efficiently. We will also continue to explore innovation methods of mitigating the threats posed by cyber crime. We look forward to working with the Subcommittee and Congress as a whole to determine a successful course forward.