Criminal Division

Remarks of
Deputy Assistant Attorney General Laura H. Parsky

Joint Meeting of the
Financial and Banking Information Infrastructure Committee and the
Financial Services Sector Coordinating Council

(September 14, 2004 – Chicago, Ill.)

Thank you very much for your invitation to speak this morning on a topic of wide-ranging significance for American business, government, and society at large: the security of computer networks and the Department of Justice's response to increasing incidents of cyber crime in the financial sector.

The nature of the problem and the DOJ's response

The worldwide damage to computers and data and the productive time lost as a result of worms, viruses, and hacking incidents are valued in the billions of dollars. In addition to the damage they cause, viruses and worms are also used to steal confidential data from computer systems.

Such confidential data, of course, has a monetary value, and we have seen a consequent shift in the stereotypical hacker paradigm from mischief motivated by claimed "intellectual curiosity" to computer intrusions and virus releases motivated by financial gain.

Moreover, the potential for monetary gain has captured the attention of organized criminal groups, particularly in Eastern Europe, who increasingly are using computer attacks as part of highly organized and lucrative fraudulent schemes.

Unfortunately, given the public's increased reliance on computers and computer networks for communication and to transact business, and the rich target these systems present to criminals, we expect increasing virus and worm attacks which are not designed to damage computers but to steal information. Fraudulent schemes perpetrated over the Internet, such as "phishing" email and identity theft, damage consumers' confidence and their wallets.

The rise in computer crimes is complicated by special challenges those crimes pose for law enforcement. Unlike traditional crime, criminal conduct on the Internet may result in thousands of victims in far-flung jurisdictions. Furthermore, since the Internet has no national boundaries, many of the perpetrators of these fraudulent schemes and attacks are located outside of the United States even though they target our institutions and consumers.

Fraudsters also take advantage of the potential anonymity of the Internet to launch their attacks and hide their digital footprints – often by routing their activities through several countries. Emboldened by the seeming anonymity and reach of the Internet, criminals are constantly inventing and refining clever schemes to prey on our citizens and our businesses.

For instance, as I know you all are keenly aware, phishing is an especially dangerous marriage of spam and fraud that has grown exponentially this year.

In a phishing scheme, a customer receives an email purportedly from a legitimate company, often one with which the customer does business regularly. The email requests that the recipient update personal information – such as a username and password – and directs the recipient to a spoofed website that is used to steal that personal information. These spoofed websites can be remarkably sophisticated and give few clues to the user that the website is not legitimate.

Undoubtedly, phishing attacks are growing in part because they are an effective means of fraud. FBIIC and FSSCC's May 2004 report notes that 3% of adult internet users responded to this sort of fraudulent email, often sent to thousands of customers.[1]

This conduct has an undeniably adverse effect on important sectors of our economy and potentially undercuts the security of some of our nation's critical infrastructure, including the financial sector. There is bipartisan recognition of the fact that phishing facilitates identity theft on a large scale and diminishes confidence in the Internet's system of addressing and linking.[2]

---

[1] "Lessons Learned by Consumers, Financial Sector Firms, and Government Agencies during the Recent Rise of Phishing Attacks," prepared by the Financial and Banking Information Infrastructure Committee and the Financial Services Sector Coordinating Council, May 2004.

[2] Statement of Senator Patrick Leahy, Congressional Record, July 9, 2004,

Department Resources Focused on Computer Crime

In response to the problem of cyber crime, the Department of Justice has devoted significant resources to investigating and prosecuting persons who commit crimes on the Internet.

In addition, the Department has worked with the international law enforcement community to ensure that foreign laws and investigative techniques are up-to-date, so that criminals cannot hide simply by routing their information through third countries.

Although tracking cyber criminals is difficult, the Department of Justice is fully committed to investigating such attacks and to bringing the perpetrators of these crimes to justice.

A cornerstone of this effort is the Criminal Division's Computer Crime and Intellectual Property Section – or "CCIPS," which I supervise. CCIPS is comprised of experienced, tech-savvy prosecutors who coordinate investigations into computer intrusions, viruses, and worms both in the United States and internationally.

CCIPS prosecutors work closely with the more than 220 Computer and Telecommunications Coordinators located in each of the 94 federal law enforcement districts to ensure that high-tech expertise is brought to bear on computer crime investigations.

In addition, to address the high incidence of computer crimes, the Attorney General established a cadre of specialized Computer Hacking and Intellectual Property – "CHIP" -- units in strategic districts across the country. Since his arrival at the Justice Department, the Attorney General has expanded the number of CHIP units from one to thirteen.

This expansive network of federal prosecutors, working with the specialized computer crime task forces of law enforcement agencies such as the U.S. Secret Service and the FBI, provides an integrated and aggressive approach to prosecuting cyber crime in the United States.

---

http://leahy.senate.gov/press/200407/070904c.html (last visited September 1, 2004).

Increased Penalties

The Department has also taken the lead, working with Congress and the United States Sentencing Commission, to strengthen the penalties for computer crime and ensure that the punishment accurately reflects the economic harm that these crimes cause. Penalties for serious violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030) now range from 10 years in prison for first-time offenders to 20 years for subsequent offenders.

In addition, President Bush recently signed the Identity Theft Penalty Enhancement Act which provides an additional penalty of 2 years in prison for identity theft in connection with the commission of a felony. Identity theft in connection with major felonies associated with terrorism adds an additional 5 years to a defendant's sentence.

Of course, accessing computers to facilitate fraudulent schemes such as "phishing" violates not only section 1030 but also various anti-fraud statutes, particularly 18 U.S.C. Section 1343 -- the Wire Fraud Statute. The penalty for wire fraud affecting a financial institution is up to 30 years imprisonment and a fine of up to one million dollars.

International Cooperation

Just as the financial networks that connect us are global, however, the crimes committed on these networks are similarly international in scope. Accordingly, these investigations frequently have an international component that draws upon the Department's contacts with law enforcement counterparts abroad. International cooperation is a critical foundation of the Department of Justice's strategy for combating cyber crime.

Among other things, CCIPS and the investigative agencies have built operational networks of law enforcement contacts around the world to respond to fast moving cyber cases. A prime example of this work is the G-8's 24/7 Network, set up by the G-8 Subgroup on High-Tech Crime, a group chaired by CCIPS. The G-8's 24/7 Network now has expanded to forty member countries, with prosecutors or investigators available 24 hours-a-day, 7 days-a-week, to respond to emergency requests for assistance on computer crime.

This international cooperation, normally out of reach for private companies working alone, is essential for an effective response to the fraud and computer crime that weaken global financial networks.

Successful prosecutions

The Department's commitment to pursuing cyber criminals is paying off. We are meeting the challenges inherent in investigating computer crime by identifying and prosecuting high-profile perpetrators.

For example, in 2001, David Smith of New Jersey pleaded guilty to unleashing the "Melissa" computer virus that infected untold numbers of computer networks and caused millions of dollars in damage.

Jeffrey Lee Parson recently pleaded guilty in Seattle to charges stemming from his release of a variant of the Blaster worm. This is not the end of the Blaster worm investigation, however, because we are continuing to work to find the original author of the worm and those responsible for the other variants of the worm that have emerged.

The Department of Justice has also prosecuted dozens of hacking cases specifically aimed at the financial sector.

For instance, Alexy Ivanov was convicted in Connecticut for his role in a conspiracy originating in Russia, in which he and his confederates hacked into dozens of computers throughout the United States, stealing usernames, passwords, credit card information, and other financial data, and then extorted those victims with the threat of deleting their data and destroying their computer systems.

Another defendant, Oleg Zezev, was convicted for conducting a scheme to extort money from Bloomberg LLP and its founder, Mayor Michael Bloomberg. Zezev illegally entered Bloomberg LLP's computer system and accessed a number of accounts, including Michael Bloomberg's account. Zezev sent an e-mail to Michael Bloomberg threatening that if Michael Bloomberg did not send him $200,000 he would disclose to the media and Bloomberg's customers that he was able to gain unauthorized access to Bloomberg's computer system. In sentencing Zezev, United States District Court Judge Kimba Wood recognized that the defendant's "crime was a very serious one because of its threat to international commerce and

the integrity of data that the financial community relies upon to do its business."

Although several years ago those who attacked computer networks often received only probation, in each of the cases I have just highlighted, and many more, the perpetrators received substantial jail sentences – a strong deterrent message that we are dedicated to reinforcing.

Operation Web Snare

Another sign of the Justice Department's aggressive efforts to prosecute economic crimes committed on the Internet is "Operation Web Snare," announced just last month by Attorney General John Ashcroft.

Operation Web Snare was the largest and most successful collaborative law-enforcement operation ever conducted to prosecute online fraud, stop identity theft, and prevent other computer-related crimes.

Between June 1st and August 26th, 2004, Operation Web Snare yielded more than 160 investigations in which more than 150,000 victims lost more than $215 million.

As a result of this operation, there were:

- more than 350 subjects of investigation;
- 103 arrests;
- 53 convictions to date;
- a total of 117 criminal complaints, indictments, and informations; and
- the execution of more than 140 search and seizure warrants.

The success of Operation Web Snare was due largely to the concerted efforts of numerous law-enforcement partners. We received aid and cooperation from:

- 36 United States Attorneys' Offices;
- the Criminal Division of the Justice Department
- 37 of the 56 FBI field divisions
- 13 of the 18 Postal Inspection Service field divisions
- the Federal Trade Commission
- the United States Secret Service, and

- the Bureau of Immigration and Customs Enforcement of the Department of Homeland Security.

In one of the cases brought during Operation Web Snare, a federal grand jury in Kansas City returned an indictment charging five individuals with conspiracy to commit identity theft, access-device fraud, and unlawful access of a protected computer. According to the indictment, Ganiyat Ishola stole several pages from an employee roster with the Social Security numbers of her coworkers. Ishola allegedly gave the information to her boyfriend Soji Olowokandi. The indictment alleges that information was then taken here to Chicago, where it was used by several members of the alleged conspiracy to apply for credit cards.

In another case, in June 2004, a Ukrainian national was extradited from Cyprus to face a 40-count indictment, returned in the Northern District of California, charging him with credit-card trafficking and wire fraud. According to the indictment, the Ukrainian allegedly used Internet chat rooms to traffic in credit card information belonging to thousands of individuals, that credit card information having been illegally obtained from sources around the world, including credit card processors and merchants.

Of course these are charges, and they have yet to be proven, but they are examples of work that the Department is doing right now to protect against fraud on financial institutions.

Furthermore, the Department of Justice is implementing an aggressive strategy to investigate and prosecute the persons responsible for spam email. Spam is frequently the vehicle for financial fraud committed on the Internet and is the principal avenue for phishing schemes.

In a recent case, Zachary Keith Hill of Houston, Texas, was convicted for devising a scheme to defraud consumers of personal financial information via spam email. Hill sent spam email to consumers leading them to believe that the email was actually from America Online or Paypal. The email asked for passwords and usernames to financial accounts. Earlier this year, Hill was sentenced to 46 months in prison.

We have also begun to bring prosecutions under the new CAN-SPAM Act, which criminalizes specific fraudulent conduct in connection with sending unsolicited commercial email. Prosecutions under this new

legislation have been brought in New York, Detroit, and Los Angeles, with additional investigations underway.

Although we have accomplished much, we recognize that there is always more work to be done.

Corporate Network Security is a Partnership

While we are doing everything we can to catch cyber criminals, we cannot do it alone. The majority of computer networks in this country are privately-owned and operated, and often good corporate network security practices are the first, and usually the best, line of defense against cyber risks.

Furthermore, the only way to effectively prosecute cyber attacks is with immediate and full cooperation from the victims.

Though criminal prosecution and increased penalties can send a strong deterrent message, that is not enough without robust corporate network security to help prevent these crimes in the first place. Network security programs should include risk assessment and management, with accountability for security breaches.

Corporate best practices that can reduce risks of Internet crime include the following:

1. Establish corporate policies and communicate them to customers. For example, a number of companies advise their customers that personal information such as a password will never be requested by email.

2. Provide a way for the customer to confirm that the email is legitimate.

3. Employ stronger authentication at websites using information other than social security numbers. If companies don't ask for sensitive information like social security numbers on websites, this information won't be at risk.

4. Monitor the Internet for phishing websites that spoof your company's legitimate sites[3].

5. Establish risk management programs and accountability at the corporate-officer level for security practices. Good, corporate information security programs recognize that security is not an after-thought but is a foundation for business success in today's world.

6. Improve communication with law enforcement and understand the criminal investigative process.

7. You and your member institutions are entitled to all of the special protections provided to any victim of a serious crime, including: notification of significant events in the case (whenever possible); maximum efforts to safeguard confidentiality, proprietary information, and victim identification; minimal disruption of ongoing business operations; and, where appropriate, recognition of the victim's valuable cooperation and responsiveness.

8. Have internal procedures in place to handle computer crime incidents. Make sure your personnel know the procedures and the points of contact inside your organization for reporting incidents. In addition, make sure there are procedures in place for properly preserving vital evidence, such as computer logs and other relevant data.

9. If an incident occurs, immediately report the crime to authorities. The FBI has established cyber crime squads around the country, and the U.S. Secret Service has set up Electronic Crimes Task Forces in a number of major cities. Each U.S. Attorney's Office also has specially trained prosecutors to deal with these types of crimes.

10. An immediate response in these cases is important, because the electronic trail is fleeting. Even if you are filing an SAR or other crime report try to make personal contact with law enforcement as soon as possible.

Good security programs should include consumer awareness and user

---

[3] Anti-Phishing Remedies for Institutions and Consumers, McAfee Research – Network Associates, Inc, http://www.networkassociates.com/us/_tier2/products/_media/mcafee/wp_antiphishing.pdf

training, because people are frequently identified as the weakest link in the security chain.

Effective customer education messages include precautions about:

- $ any email request for personal financial information;
- $ about using hyperlinks in an email to get to any web page;
- $ about email forms that ask for personal financial information; and
- $ about giving credit card or account information by means of anything other than a secure website or the telephone.

Customers should also be advised to regularly check bank and credit card statements to confirm that all transactions are legitimate.

Good computer security and careful consumer use of the Internet amount to cyber crime prevention. When incidents do occur, prompt reporting to federal law enforcement authorities is an essential part of good corporate security.

Why reporting computer crime is important

Law enforcement stands ready to work with you to help protect your computer networks, but we need your assistance and cooperation. Good security and prevention alone are not enough – there must be consequences for those who inevitably try to overcome that security.

The best locks on doors will not reduce burglary attempts unless there is a penalty to be paid for the crime. There can be no penalty and no justice, however, if victims don't report the crimes to us.

Unfortunately, it has been estimated that approximately 80% of network hacks in the financial sector go unreported to law enforcement. A recent PricewaterhouseCoopers survey notes that 46% of the fastest growing small companies in the United States have suffered a recent breach of information security.[4] 83% of these companies suffered monetary loss, and nearly 25% of them suffered some network downtime.

---

[4] Sacramento Business Journal, November 24, 2003.

While a systems administrator may be content to fix a hack or purge a worm or virus on his system and not report it to management or to law enforcement, this provides little true security. Not only is that hacker free to continue exploiting other company networks, but the hacker community, which maintains an active underground, will certainly learn of the exploit and, emboldened by the lack of any law enforcement response, try other attacks against that system.

Immediate reporting helps law enforcement preserve critical evidence right away, before it is destroyed or deleted by intermediary internet providers.

Furthermore, reporting helps us see patterns in attacks over time. Without a pattern, we don't know whether an incident is an isolated event or a widespread scheme until it is too late.

The benefits of prompt reporting and close cooperation between law enforcement and the private sector can be seen in the Bloomberg case that I previously mentioned. In that case, the victim immediately reported the crime and fully cooperated with authorities. Law enforcement was then able to lure the perpetrator from his native Kazakhstan to London, where evidence could be obtained, an arrest made, and extradition to the United States initiated. Had the victim not brought in law enforcement, such results would not have been possible.

Furthermore, the victim's prompt and exemplary cooperation in apprehending the perpetrator was publicly recognized and praised. This sent a strong message to the victim's customers and to other would-be attackers: there will be severe consequences for attacking this company.

Consumer confidence in the security of private data increases when the public sees that there are serious penalties for violating that security.

In general, there is a lot of talk about public-private partnerships. However, in this area, such partnership can produce tremendous results: targets can be made less vulnerable; perpetrators can swiftly be brought to justice; and future attacks can be deterred.

I greatly appreciate this opportunity to speak with you, and I look forward to developing ways in which we at the Department of Justice can

better serve your needs and partner effectively with you to combat this serious threat to the Nation’s security and prosperity.

Thank you.