InfraGard: A Neighborhood Cyber-crime Watch
Richard S. Scheuch
GSEC Practical Assignment version 1.2B
April, 25, 2001

Melissa! The I-Love-You bug! Denial-of-Service attacks against Yahoo.com and Amazon.com! Microsoft hacked! Linux Trojans Lion and Adore! Winux, an attack against dual operating systems! What's next? The December 2000 issue of SANS Security Alert projected a darkening forecast. Peter G. Neumann, Principal Scientist in the Computer Science Lab at SRI International predicts, "We are likely to see some organized, possibly collaborative, attacks that do some real damage, perhaps to our critical infrastructures, perhaps to our financial systems, perhaps to government systems – all of which have significant vulnerabilities."

News abounds with articles about cyber-crime. It's not hidden any longer. Even the Podunk Gazette prints banner headlines about the latest government agency or big company having their computers hacked. The 2000 CSI/FBI Computer Crime and Security Survey confirms that the trends in security breaches are widespread and diverse in both the public and private sectors. The range of attack covers the gamut from viruses detected, unauthorized access by insiders, systems penetrated from the outside to financial fraud. In a survey that had only 273 respondents the financial loss in 2000 amounted to over $265 million, almost doubling the previous high in 1998. According to the survey, the losses due to DDoS attacks alone during the past year could have been in the $1.2 billion range.

With cyber-crime on the rise there is still an aversion to report attacks to law enforcement. Negative publicity and competitive edge are reasons most often cited. Stephen Sandberg noted in his paper "Computer Crime: The Insecurity of Your Network" that "most serious attacks are never reported because employees perpetrate them. Companies cover them up rather than risk the loss of customer trust." Companies cringe at the thoughts of bad publicity that might be generated from reports that they had been attacked. Customer privacy presents another obstacle to the reporting of cyber-attacks. Companies want guarantees that none of their customers' information would be shared.

What would be a better deterrent to cyber-crime than a joint venture between companies and agencies with the ability to prosecute the offenders?

In 1998, former President William Clinton recognized the potential impact of cyber-crime within the United States. Presidential Decision Directive 63 (PDD63) proposed a national goal to "achieve and maintain the ability to protect our nation's critical infrastructures from intentional acts", including our cyber systems. The President directed a partnership to be established between the public and private sectors to be a cooperative effort to reduce exposures that could cripple our national resources. PDD63 alludes to the relative ease with which our critical infrastructures could be attacked while additional fortification is expensive, long term, and complex to employ.

As a result, PDD63 called for the Federal Bureau of Investigation to expand its national warning system into a National Infrastructure Protection Center (NIPC). This agency is to "serve as a national critical infrastructure entity for threat assessment, warning, vulnerability, and law enforcement investigation and response". The mission of NIPC is to respond to cyber attacks that threaten our eight infrastructures as defined by The Report of the President's Commission on Critical Infrastructure Protection, October 1997.

> Banking and Finance: a critical infrastructure characterized by entities, such as retail and commercial organizations, investment institutions, exchange boards, trading houses, and reserve systems, and associated operational organizations, government operations, and support activities, that are involved in all manner of monetary transactions, including its storage for saving purposes, its investment for income purposes, its exchange for payment purposes, and its disbursement in the form of loan and other financial instruments.
>
> Electrical Power: a critical infrastructure characterized by generation stations, transmission and distribution networks that create and supply electricity to end-users so that end-users achieve and maintain nominal functionality, including the transportation and storage of fuel essential to that system.
>
> Emergency Services: a critical infrastructure characterized by medical, police, fire, and rescue systems and personnel that are called upon when an individual or community is responding to emergencies. These services are typically provided at the local level (county or metropolitan area). In addition, state and Federal response plans define emergency support functions to assist in response and recovery.
>
> Government Services: Sufficient capabilities at the Federal, state and local levels of government required to meet the needs for essential services to the public.
>
> Oil and Gas Production and Storage: a critical infrastructure characterized by the production and holding facilities for natural gas, crude and refined petroleum, petroleum-derived fuels, and the refining and processing facilities for these fuels.
>
> Telecommunications: a critical infrastructure characterized by computing and telecommunications equipment, software, processes, and people that support:
>
> - the processing, storage, and transmission of data and information,
> - the processes and people that convert data into information and information into knowledge,
> - the data and information themselves.

> Transportation: a critical infrastructure characterized by the physical distribution system critical to supporting the national security and economic well-being of this nation, including aviation; the national airspace system; airlines and aircraft; and airports; roads and highways, trucking and personal vehicles and intelligent transportation systems; waterborne commerce; ports and waterways and the vessels operating thereon; mass transit, both rail and bus; pipelines, including natural gas, petroleum, and other hazardous material; freight and long haul passenger rail; and delivery services.
>
> Water Supply Systems: a critical infrastructure characterized by the source of water, reservoirs and holding facilities, aqueducts and other transport systems, the filtration, cleaning and treatment systems, the pipeline, the cooling systems and other delivery mechanisms that provide for domestic and industrial applications, including systems for dealing with water runoff, waste water, and firefighting.

In order to achieve its mission, NIPC engaged in four initiatives to foster the strengthening of infrastructure security.

- InfraGard: FBI agents working with local business organizations to gain enhanced protection for their information systems.

- Warnings: Distribute general awareness notices, alerts and in-progress threats on critical infrastructures.

- Analyses: Develop analytical tools to distribute information gathered from law enforcement. CyberNotes at www.nipc.gov is one such product.

- Key Asset: Development of a national database of key assets within the FBI field offices. The purpose of this initiative is to work with industry for sharing information when events occur that would threaten the infrastructure.

In the summer of 1996 the FBI began a pilot project when the Cleveland Field Office proposed "a cooperative undertaking between the Federal Bureau of Investigation, businesses, academic institutions, state and local law enforcement agencies and other participants". The pilot was framed on the principle that "InfraGard is dedicated to increasing the security of the critical infrastructures of the United States of America through the exchange of information about threats and attacks on these infrastructures. The goal of InfraGard is to enable that information flow to the owners and operators of infrastructure systems so that they can better protect themselves with the help of the United States government."

The pilot was a success and the first InfraGard chapter was born. There are currently InfraGard chapters affiliated with all 56 of the FBI field offices. An article in the January 8, 2001 issue of ComputerWorld titled "FBI Completes Rollout of Corporate Cybercrime Program" indicates the initiative is growing. "More than 500 businesses signed up and the FBI is still getting applications daily from companies that want to be part of [a chapter]", according to an FBI spokesman.

The same article notes that InfraGard is not without its detractors.

> "John Pescatore, a security analyst at Stamford, Conn.-based Gartner Group Inc., said the timing of the announcement may be a sign that the FBI is jockeying for budget influence in a future Bush administration. The InfraGard program "hasn't had much of an impact" on corporate users thus far, he added.
> "It seems like the different chapters are very personality-driven," Pescatore said. "But the FBI hasn't really institutionalized [InfraGard] or funded it to be anything very meaningful. The general feeling ... is that it is all input *to* the FBI and no output *from* them.""

One of the key objectives of InfraGard is to provide a spirit of communication among its members regarding security vulnerabilities and issues. The FBI's involvement is a coordination role to foster cooperation. The common goal is effective detection and response. Some may view their role as an invasion of corporate privacy. Reality points toward an increase in information sharing and networking between InfraGard members and the FBI field offices. There is, admittedly, a struggle in attracting members. The belief that the FBI will shut down a business while a cyber-attack is investigated is prevalent throughout the business community. Working to educate InfraGard members the FBI explains how to prepare and preserve evidence so that the bureau can find the hackers and the companies can get on with their business. That member businesses feel a trustworthy enough relationship exists to share information is instrumental to InfraGard's success.

Membership in an InfraGard chapter is voluntary. There are no implied conditions attached to the membership. Nor are there implications that information about the members will be unveiled to law enforcement agencies or other members without permission. InfraGard is not in the marketing business. Members agree not to use the organization to hawk products or services. That's not to say that contacts made through InfraGard cannot lead to business agreements as a result of membership. InfraGard is not a platform for exploitation. InfraGard members also agree not to disclose information about other members that is not part of public record. These agreements reinforce the desire for openness among the participants without which the stated goals cannot be achieved.

Always of concern is the issue of funding. Addressed in the by-laws, the article of governance states "absent from other arrangements, all participants in InfraGard will bear their own expenses." The local chapter administers any funds collected. It is also expressly stated that the FBI cannot administer any membership funds or use the fund for official FBI activities.

While local chapters operate under a set of national by-laws, each local chapter has the freedom to organize as it sees fit and to develop a program that fits its unique needs. Leadership throughout the 56 chapters has taken a variety of forms including the standard president/vice-president offices, committees and co-presiding officers. The special agents representing the FBI field offices refrain from holding leadership offices, playing the part of "just another member" while having the capacity to lend added value by way of their vast resources. One local chapter opted for the co-presidency format in order to lend more credence to the private sector presence within its InfraGard chapter. They felt recruitment, notices, press releases and conferences would be better received coming from the business aspect rather than government.

Activities that may be offered by the local chapters include:

- regular chapter meetings
- seminars and education on cyber-warfare vulnerabilities and protection
- local newsletters
- Cyber-Awareness campaigns

Of utmost importance, however, is the identification of critical infrastructure assets within the region covered by the local chapter and creation of a contingency plan in the event of an actual attack. With an attitude of individualism companies work on their own or in small, exclusive groups to keep track of cyber-crime trends and responses. Granted the more technical security people may always have more access quicker than that provided by InfraGard. This organization, however, seeks to generate a network of infrastructure owners who are aware of the impacts of a cyber-attack on each other.

Each member of InfraGard has access to a secure web site with links to related newly reported intrusions and press releases, internal links to other chapters and links to all FBI Field offices, in addition to current infrastructure information. The secure web site provides access to NIPC assessments, advisories and alerts. These warnings provide information that could have a significant impact on the infrastructure. NIPC provides encryption technology to members for voluntary reporting of attacks. Effective investigation of a cyber-attack required that raw data not be stripped down for the protection of the victims. NIPC distributes a "sanitized" description of the incident to InfraGard members so they may take appropriate action. Victims of the crime remain anonymous. If warranted, the FBI would use a full narrative for further investigation.

Firsthand experience as an InfraGard chapter member yields the following observations. First, there is a growing camaraderie developed among the members. Security issues are the common bonds for this guild of specialists. Too often there is too little contact with those of like professional interest. Chapter meetings are not cast in a light of doom and gloom. Often the lighter, funnier side of the business generates welcome belly laughs. Second, the goals of InfraGard are taken quite seriously. The membership realizes that the task of determining the critical infrastructure assets within the region and developing a contingency plan is a daunting task. It is, however, a task each member is willing to shoulder. Third, the amount and diversity of security expertise within the local chapters is astounding. Members' job titles range from Network Administrators to Cyber Counterintelligence Officers and everything in between. (This is not to imply that membership is limited to security professionals.) The interesting fact is that the tight-lipped syndrome mentioned above has not been in evidence by this observer. Everyone in the local chapter is willing to share as much as possible within the constraints of company limitations. Fourth, there is a desire to grow the membership of the local chapter. While there is a vast amount of experience represented there is also a wealth of untapped resource at hand. Finally, government agencies have shown no tendency to either control the chapter or to be "takers", contrary to the opinion of Mr. Pescatore. In our local chapter each and every member is a contributor.

Dr. Thomas A Longstaff notes in his white paper entitled "International Coordination for Cyber Crime and Terrorism in the 21st Century" that local communities are confronted by their own set of needs. Issues such as services, organizations, time zones, and legal jurisdictions all play a part in the effectiveness of response to a significant cyber-attack. InfraGard provides the platform through which resources can be pooled to meet the needs of the local security community. In the event of cyber-attacks originating from beyond our national borders InfraGard wields the full weight of the State Department, Department of Justice, Department of Defense and others. There are not many, if any, private organizations that can make such a claim.

As cyber-criminals increase their skills and security professionals strive to fortify their defenses, it is evident that, as the old cliché says, there is strength in unity. Screams go out when one vital server on a single network goes down. Imagine the impact of coordinated cyber-attacks to the local utility company on the community that it serves. InfraGard seeks to draw the security community together as a neighborhood cyber-crime watch organization for the protection of the nation's resources.

Resources:

Computer Security Institute "2000 CSI/FBI Computer Crime and Security Survey", spring 2000

Computer Security Institute "2001 CSI/FBI Computer Crime and Security Survey", press release URL: http://www.gocsi.com/prelea_000321.htm

ComputerWorld "FBI Completes Rollout of Corporate Cybercrime Program", January 8, 2001
URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO56010,00.html

InfraGard URL: http://www.infragard.net

"InfraGard Secure Access Agreement"
URL: http://www.certconf.org/presentations/1999/InfraGard/

Longstaff, Thomas A. Ph.D. "Cyber Crime and Terrorism in the 21st Century"
URL: http://www.oas.org/juridico/english/longstaff.htm

"Outreach/InfraGard"
URL: http://www.irational.org/APD/IPC/outreachinfragd.htm

Sandberg, Stephen A. "Computer Crime: The Insecurity of Your Network", December 14, 2000
URL: http://www.sans.org/infosecFAQ/threats/comp_crime.htm

SANS Security Alert "Expert Predictions for Security Trends in 2001", December 2000
URL: http://www.sans.org/SANSSecAlert2_102000.pdf

"The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63", May 22, 1998
URL: http://www.usdoj.gov/criminal/cybercrime/white_pr.htm