

Statement of
The Honorable Mike Doyle
Duquesne University-Pittsburgh InfraGard Chapter
Small and Medium-Sized Business Information Security
Seminar

October 7, 2003

Good morning. It is a pleasure to be here with you today.

Information security is an increasingly important concern for small and medium sized businesses, and it's understandably difficult for any such business to keep up with the rapidly evolving technology of cybercrime. Outreach and education efforts such as this seminar can play an important role in helping small and medium sized businesses meet the challenge of protecting themselves from cyber-crime and cyber-terrorism.

I want to thank Duquesne University for sponsoring this seminar, and I want to commend Dean Stalder and Professor Saban for organizing it. I also want to thank today's speakers and panelists - especially Dr. Dougherty, Ms. Jones, and Special Agent Shore - for taking the time to join us here today to discuss this important subject.

As we all know, computers and other automated equipment play an important role in the American economy today. The adoption of such advanced information technology is in no small part responsible for the tremendous increases in productivity that our industries have experienced in recent decades, and it is that increased productivity that is responsible for the higher quality of life that we all enjoy today. But, as is often the case, our strengths are also our weaknesses. We have only benefited from these amazing technologies by becoming dependent upon them. And as we have become more dependent upon them, we have become more vulnerable to potential disruptions to our information technology systems - and the consequences of such disruptions have grown markedly. With networked computers controlling trains, pipelines, factories, and our air traffic control system - and with major industries like telecommunications and finance completely dependent upon such systems - the potential for serious damage and economic devastation is great.

As the sophistication of our computers increased in the 1980s and 1990s, business and law enforcement agencies became more aware of the threat posed to our economy by computer hackers, disgruntled employees, foreign governments, and rival corporations.

Moreover, in the wake of 9/11, our society has been made frighteningly aware that there are people and organizations around the world who want to hurt our country and bring our economy to its knees. Unfortunately, those people and organizations are all too well aware of the vulnerability of both our physical and cyber infrastructures. And they have every incentive to attempt to turn one of our strengths - freedom and openness - into a vulnerability. Consequently, cyber terrorism has taken its place beside cyber crime as an important concern for American business.

Cyber-crime is typically understood to consist of accessing a computer without the owner's authorization, exceeding the scope of one's authorization to access a computer system, modifying or destroying computer data without the proper authorization, or using computer time and resources without authorization. Cyber-terrorism consists essentially of undertaking these same activities to advance one's political or ideological ends. The specific nature of the threat can range from denial of service to eavesdropping, fraud, sabotage, and theft of intellectual property and proprietary information. Sending computer viruses and worms constitutes a cybercrime. So does walking out a business with a disk full of proprietary information, or willfully destroying business information.

How significant is the threat? According to the nationally known online security firm Symantec, the average company in the United States is the subject of 30 hacking attacks each week. Most of these attacks are attempts to detect vulnerability, but about one in seven are actual attempts to access a company's computers. This makes sense. Presumably, hackers scan thousands of computers and then, once they detect vulnerable computer systems, they undertake actual intrusions.

The most recent annual survey of computer crime and security conducted jointly by the Computer Security Institute and the FBI concluded that "the risk of cyber attacks continues to be high." 82 percent of the survey respondents reported virus attacks against their computers. 80 percent reported employee abuse of their network access. 42 percent reported denial of service attacks. 21 percent of respondents reported sabotage attempts, 21 percent also reported the theft of proprietary information - which, incidentally, has historically been the costliest type of computer crime. 15 percent reported financial fraud, and 10 percent reported telecom fraud.

Why should small businesses be concerned? Primarily because the effects of a cyberattack on a small or medium-sized business can be devastating. The time required to get a computer system back up and running can be quite costly to a company. It can be even more costly if computer data is lost, or if confidential business information is stolen. The theft of a business's credit card information from a single computer can unleash a wave of fraudulent purchases around the globe and create a nearly endless series of headaches for that company. And, lastly, companies can find themselves liable to expensive lawsuits if they fail to take proper precautions against cyberattacks.

As the National Strategy to Secure Cyberspace states, "Although the likelihood of suffering a severe cyber-attack is difficult to estimate, the costs associated with a

successful one are likely to be greater than the investment in a cybersecurity program to prevent it."

Moreover, to the extent that small businesses are essential parts of the supply chain for critical sectors of our economy, and to the extent that they represent the most vulnerable targets of cyberattacks, they present tempting targets for terrorists.

So, what can be done to deal with this problem? Clearly, action from both the government and the private sector is needed to successfully fight cyber crime and cyber terrorism.

There is clearly a role for the federal government to play in combating cyber-crime, and we are working very hard to meet this obligation. Federal government efforts to deal with cyber-crime predate the September 11 attacks by a number of years.

In 1987, for example, Congress enacted the Computer Security Act, which directed the National Bureau of Standards to create a computer security program for all federal agencies and give government employees the necessary computer security training.

Perhaps more importantly, in 1984 Congress enacted the U.S. Computer Fraud and Abuse Act, which made it a crime to undermine the confidentiality, integrity, or availability of data on government computers. This law was expanded in 1996 to cover the private sector as well. Given the fact that most cyber-crimes are committed across state and local jurisdictional boundaries, it makes tremendous sense to assign the primary responsibility for dealing with this problem to our national government.

In the 1980s and 1990s, the federal government was concerned primarily with protecting government secrets and the privacy of its citizens' tax, social security, and other information. Cyber-terrorism wasn't an issue at the time. Now, of course, it is - and the federal government has begun dedicating more resources and attention to the issue of cybersecurity.

Last year, in the wake of the September 11 attacks, Congress enacted the Cyber Security Research and Development Act. This law authorized \$880 million over five years for new research programs to ensure that the U.S. is better prepared to prevent and combat terrorist attacks on private and government computers.

Moreover, the U.S. Government has begun making a concerted effort to address cybersecurity issues. The Department of Homeland Security's National Cyber Security Division has taken the lead in developing and coordinating the Nation's response to cyber-security issues. The Office of Management and Budget is overseeing the implementation of government-wide policies and standards for computer security. The Pentagon tracks hacker attacks on military networks back to their origin while covertly monitoring the sources of suspicious attacks. The Department of Justice and the FBI are responsible for preventing, investigating, and prosecuting cyber-crime within the United States. The National Information Assurance Partnership, a joint initiative undertaken by

the National Security Agency and the National Institute of Standards and Technology in 1997, is working to help increase the level of trust consumers have in their information systems and networks through the use of cost-effective security testing, evaluation, and assessment programs. The CIA is responsible for assessing foreign threats to U.S. networks and information systems. And the State Department is responsible for getting other countries' governments to cooperate in efforts to prevent and prosecute cyber-crimes and cyber-terrorism. Because cyber-crime knows no boundaries, we have promoted international efforts to share information about cyber-crime and preserve information about past cyber-attacks. We have also lobbied foreign governments to make hacking illegal, and trained foreign officials how to combat cyber-crime.

There's an important role for the private sector as well in fighting cyber-crime and cyber-terrorism. This role was thoughtfully laid out in the National Strategy to Secure Cyberspace, a major federal infrastructure protection initiative stemming from the September 11 terrorist attacks. The National Strategy to Secure Cyberspace and its counterpart for our nation's physical infrastructure, the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, were the key components of the National Strategy for Homeland Security developed in response to those attacks.

The National Strategy to Secure Cyberspace recognizes the fact that the bulk of our cyberspace infrastructure is privately owned and operated. That means that, while the federal government must provide strong leadership in protecting our critical cyber-assets, most of the efforts in this struggle must come from the private sector. Consequently, the federal government has undertaken a number of important partnerships with the private sector in this area to help private sector organizations do what they need to do to protect themselves.

InfraGard is one of these partnerships, with more than 70 chapters across the country. The Partnership for Critical Infrastructure Security is another. In addition, the federal government is encouraging specific industries to establish ISACs - Information Sharing and Analysis Centers - to gather and analyze sector-specific security information in order to promote best practices and coordinate voluntary contingency planning efforts.

And, of course, in Pittsburgh, we are fortunate to have a partnership that is one of America's greatest authorities on cyber-security - the CERT Coordination Center of the Software Engineering Institute at Carnegie Mellon University. The Software Engineering Institute is a federally funded research and development center established in 1988. CERT's primary goal is to ensure that appropriate technology and systems management practices are used to resist attacks on networked systems, to limit damage from such attacks, and to ensure the continuity of critical services in spite of successful attacks. The Center was the first to respond to computer attacks like the Code Red worm, the Melissa virus, the MS Blaster worm, and the Sobig virus.

On September 15, 2003, the U.S. Department of Homeland Security announced a partnership with the CERT Coordination Center to create US-CERT, a partnership to

coordinate national and international efforts to prevent cyber attacks, protect computer systems, and respond to the effects of cyber-attacks.

CERT's other activities have expanded recently as well. CERT is part of CMU's Integrated Cyber Security Research and Response Program, which, under the direction of Dr. Pradeep Khosla, is developing technologies to guarantee the confidentiality, integrity, availability, and security of government communications and intelligence. I was able to secure \$2.5 million last year and \$6 million this year for this important national initiative.

According to CERT statistics, over 82,000 incidents of security violations occurred last year, with over 76,000 reported already this year. Clearly, incidents of cyber attacks are on the rise in both the public and private sectors.

So, what does all this mean for you, the small and medium-sized businesses of America? It means that no business can ever be completely safe from cyber attacks. But it also means that there are certain concrete, affordable steps that you can and should take. I think it's clear that businesses need to be proactive in preventing and defeating such attacks - rather than waiting until it's too late.

The National Strategy to Secure Cyberspace recommends that, at the least, small and medium-sized businesses should install firewall software and update it regularly, maintain up-to-date anti-virus software, and regularly update operating systems and software applications with the security improvements that their software vendors make available. In addition, the National Strategy to Secure Cyberspace urges all businesses to take measures to protect themselves and the Nation from potentially devastating attacks by employees by implementing adequate access controls, dividing up employee duties as much as possible, and effectively enforcing their security policies.

The CSI/FBI survey I mentioned earlier determined that nearly all businesses use anti-virus software and firewalls. The survey reported that over 90 percent of respondents, and presumably of all businesses, use some kind of physical security - like locked server rooms - to protect their computer and information assets and employ some measure of access control - such as passwords.

But the survey concluded that "many respondents simply do not know what's going on within their networks." That's not surprising, and it's not surprising that this is, in fact, the case for many small and medium-sized businesses.

Many small and medium-sized businesses want to address this problem, but they don't know where to start. Many are not large enough to have a full-time IT professional - let alone a full-time computer security expert. Moreover, the technology of both the threats and the responses changes so rapidly that it's difficult for any business to keep its cyber-defenses current.

Many businesses like yours want to know what they should be buying and doing to protect themselves. They want to know what they should be asking their vendors for.

Cyber risk insurance policies have become useful tools in managing and defending against the risk of cybercrime and cyber terrorism, and business owners want to know what they should look for when considering such policies. In short, they're looking for an unbiased source to provide them with some answers. That's where InfraGard and seminars like this can be incredibly helpful.

InfraGard is a partnership between the private sector and the FBI with the mission of encouraging the exchange of information between the government and the private sector on how to better protect our country's critical infrastructure. InfraGard focuses on eight sectors critical to the U.S. economy: government operations, emergency services, banking and finance, transportation, electric power, gas and oil storage and delivery, telecommunications, and water supply systems. Today, there is an InfraGard chapter in the jurisdiction of every FBI field office across the country.

The Pittsburgh InfraGard Chapter is here today to provide you with information to help make your business more secure. I want to thank Helen Jones, Special Agent Shore, and their associates for their participation in this seminar today - and for all of their efforts to thwart cyber-crime and cyber-terrorism. I also want to mention the private sector speakers who are here today and thank them for their contributions to helping local businesses meet the threat to their information systems.

Without further ado, at this point I'll turn the podium over to the experts who can help you make your businesses more secure from cyber crime and cyber terrorism. Thank you.