

Background

Contact: Kevin Lane at (412) 848-8345 or at KLane85579@aol.com

Cybersecurity in the Pittsburgh Region

Subject matter experts available for comment on this topic include:

Kelly Kimberland
Public Relations
CERT Coordination Center

Paul Nielsen
Chief Executive Officer
Software Engineering Institute

Ronald E. Plesco Jr.
Chief Executive Officer
National Cyber-Forensics & Training
Alliance

Albert Whale
President
ABS Computer Technology

Pradeep Khosla
Dean, College of Engineering
Founding Director
CyLab

Jarrold Siket
Senior Vice President
Netronome Systems

John Foley
President, CEO and Founder
VigilantMinds

Automated tools have become so ubiquitous that attacks against Internet-connected systems are commonplace. Because of this, the number of incidents reported offers little insight into the scope and effects of these attacks. The Computer Emergency Response Team Coordination Center (CERT[®]/CC) at Carnegie Mellon University's Software Engineering Institute (SEI) no longer publishes the number of incidents reported. Instead, the CERT/CC is working with others to develop and report more meaningful metrics.

The latest E-Crime Watch survey, conducted in 2007 among 671 security and law enforcement executives by *CSO* magazine in cooperation with the U. S. Secret Service, the CERT/CC and Microsoft, showed a significant increase in reported crimes (49 percent vs. 38 percent the previous year), yet overall spending on IT security by these same respondents had been trimmed by five percent.

(more)

Twenty-five percent of respondents reported harm to their organization's reputation.

While respondents continue to be most concerned with intruders from outside their organizations, a growing number are causing damage from within. Outsiders who perpetrated some form e-crime in 2006 comprised 37 percent of the respondents' incidents, as compared to 58 percent of events the year before. Conversely, the insider threat is getting worse. Incidents experienced from within grew from 27 percent to 34 percent.

A study released in the fall of 2006 showed that 83 percent of adults who use social networking sites expose themselves to hackers and identity thieves. The study by CA (formerly known as Computer Associates) and the National Cyber Security Alliance (NCSA) was the first to study the link between specific online behaviors and the potential for becoming a victim of cyber crime. Although social networking sites, such as MySpace and FaceBook, have been examined from the standpoint of physical security issues, including sexual predators, this survey examined users' online behavior and the possibility of other threats such as fraud, identity theft, computer spyware and viruses. Highlights of the survey reveal:

- Although 57 percent of people who use social networking sites admit to worrying about becoming a victim of cyber crime, they are still divulging information that may put them at risk. For example, 74 percent have given out some sort of personal information, such as their e-mail address, name and birthday.
- 83 percent of adults engaging in social networking are downloading unknown files from other people's profiles, potentially exposing their personal computers to attacks.
- 51 percent of parents who are aware that their children use social networking sites do not restrict their children's profiles so only friends can view, leaving their child's profiles unrestricted to potential predators.
- Furthermore, 36 percent of these parents do not monitor their children on social networking sites at all.

In contrast to the popular perception that social networking is an activity enjoyed almost exclusively by tweens and teens, the CA/NCSA social networking research study revealed that 48 percent of all adults 18 years or older engage in on-line social networking. Further, it is not just young adults engaging in social networking; 53 percent of adults who use social networking sites are over the age of 35. The growing number of adults using social networking sites is an indicator of the increasing popularity and potential security risks of these sites.

(more)

On an encouraging note, the survey revealed that adults are taking safety precautions with their children. Of the parents who know their children under 17 use social networking sites, 64 percent monitor their children's profiles and 49 percent have only allowed their child's profile to be seen by his or her friends. Many adults have discussed safety precautions with their children: 94 percent have discussed how to watch for predators, 72 percent have discussed how to watch out for malicious software, and 64 percent have discussed how to watch out for individuals fraudulently trying to steal money.

A recent FBI report on cybersecurity details a wide range of known criminal cyber activities. Viruses, worms, Trojans, computer intrusions, Web site attacks and defacements, denial-of-service attacks, identity theft, privacy breaches and child pornography are included as just some of the better known examples.

Attackers fall into a range of categories, including disgruntled and dismissed employees, domestic and overseas competitors and even foreign governments and terrorists. Scores of Web sites are now readily vulnerable to international hackers and virus writers in numerous languages and cultures.

As government, global e-commerce and mass computer use continue to grow, cybersecurity initiatives become all the more pressing. Simultaneously, progressive changes in intruder techniques increase the difficulties of predicting or detecting attacks or of limiting their potential damages. In short, such sophisticated threats demand truly sophisticated responses.

Amid such a backdrop, southwestern Pennsylvania has become the premier center of excellence in cybersecurity.

CERT® Coordination Center

The Computer Emergency Response Team Coordination Center (CERT/CC), part of Carnegie Mellon University's Software Engineering Institute, is a nationally recognized cybersecurity center that has been leading the way in computer security response and research for more than 20 years.

Following the Morris worm incident, which brought 10 percent of Internet systems to a halt in November 1988, the Defense Advanced Research Projects Agency (DARPA) charged the SEI with establishing a center to coordinate communication among experts during security emergencies and to help prevent future incidents on a national basis.

Today, the CERT/CC alerts U.S. industry and computer users worldwide to potential threats to the security of their systems and provides information about how to avoid, minimize or recover from the damage. The center has played a key role in coordinating responses to major security events, such as the Code Red worm, Melissa virus and, most recently, the MS Blaster worm and the Sobig.F virus.

(more)

The CERT/CC's primary charge is to preempt or respond to any threats to the security of the Internet, and the millions of computers connected to it, and to analyze product vulnerabilities that place organizations and individuals at risk. The CERT/CC is part of the SEI's CERT program, which ensures that appropriate technology and systems management practices are used to resist attacks on networked systems, to limit damages and to ensure continuity of critical services in spite of successful attacks ("survivability"). Numerous alerts, vulnerability reports, educational guides and other statistics are published by CERT each year.

To accomplish its mission, CERT specializes in survivable enterprise management, survivable systems engineering and vulnerability analysis. The organization also is committed to increasing awareness of security issues and helping organizations improve the security of their systems by disseminating information through many channels. Although the CERT/CC no longer publishes annual totals, during the first three quarters of 2008 it catalogued 6,058 vulnerabilities, as compared to 7,236 during all of 2007.

While there is only one CERT Coordination Center, staff at the CERT/CC have helped foster more than 200 computer security incident response teams (CSIRTs) around the world, providing them with guidance and training. The CERT/CC coordinates with these teams to respond to computer security issues. Many of the teams are members of the Forum of Incident Response and Security Teams, of which the CERT/CC is a founding member.

The CERT's Virtual Training Environment (VTE) meets the needs of training Department of Defense and others in information assurance. The VTE has been well received by the DoD and its use is growing. In 2008, the VTE delivered approximately 120,000 hours in training

In September 2003, U.S. Secretary of Homeland Security Tom Ridge recognized the CERT/CC as "a key element to our national strategy to combat terrorism and protect our critical infrastructure." Accordingly, the Department of Homeland Security announced a partnership with the CERT/CC to create US-CERT, a coordination point for reducing the frequency and impact of cyber attacks.

In 2008, CERT Computer Forensics team was recognized by U.S. House of Representatives Murtha, Doyle, and Altmire for their role in the indictment of 11 individuals by the U.S. Department of Justice for the largest identity theft case in history.
(<http://www.sei.cmu.edu/about/press/releases/certforensics.html>)

The CERT's Insider Threat team also has received national recognition by trade and newspaper outlets for their research and development efforts in developing best practices to prevent insider threat attacks in organizations. CERT researchers are consistently top presenters at RSA, the largest security conference in the U.S.

(more)

US-CERT includes other partnerships with private-sector security vendors and international organizations. These groups work together to coordinate national and international efforts to prevent cyber attacks, protect systems and respond to the effect of cyber attacks across the Internet.

FBI/Pittsburgh – Computer Crimes Task Force

The Pittsburgh office of the FBI has been a leading cyber crime-fighting unit since 2000, when it became the first branch to hire an official computer science agent. During the same year, FBI/Pittsburgh and the CERT/CC joined forces in the formation of the Pittsburgh High-Tech Computer Crimes Task Force, a first of its kind in the nation.

As a unit of consolidated federal, state and local law enforcement, the task force was created with the purpose of pooling technical and investigative resources trained in computer technology and cyber crime in order to advance the mission of all enforcement agencies. The Pittsburgh High-Tech Computer Crimes Task Force provided forensic examination, intelligence and technical assistance to all agencies encountering computers during the course of their investigations.

Unlike traditional types of crimes, technology has made it more difficult to answer the who, what, where, when and how of both traditional and non-traditional criminal activity; as a result, evidence in the digital space must be handled differently. The task force meets these evolving challenges as part of its mission. A regional forensic and training center allows businesses to run test hack scenarios to measure how well security initiatives perform.

Since 2000, similar task forces have been deployed in every FBI field office. And in 2002, the FBI reorganized to create its own cyber division. This division simultaneously supports FBI priorities across program lines, assisting counterterrorism, counterintelligence and other criminal investigations when aggressive technological investigative assistance is required.

The National Cyber Forensics & Training Alliance (NCFTA) is the first partnership of its kind in the nation, and it grew out of the work performed by the Pittsburgh High-Tech Computer Crimes Task Force.

The NCFTA provides a neutral collaborative venue where critical confidential information about cyber incidents can be shared discreetly, and where resources can be shared among industry, academia and law enforcement. The Alliance facilitates advanced training, promotes security awareness to reduce cyber-vulnerability and conducts forensic and predictive analysis and lab simulations. These activities are intended to educate organizations and enhance their abilities to manage risk, develop security strategies, collaborate on best practices, detect and combat cybercrime and illicit activities.

(more)

Members of the NCFTA jointly developed and staffed facilities, where program participants benefit from cyber-forensic analysis, tactical response development, technological simulation/modeling analysis and the development of advanced training.

The NCFTA is comprised of subject matter experts from industry, academia and government, including:

Law Enforcement

- FBI
- U.S. Attorney's Offices in Pittsburgh and the Northern District of West Virginia
- U.S. Secret Service
- IRS
- U.S. Postal Inspection Service
- Pennsylvania State Police
- Allegheny County Police
- National White-Collar Crime Center
- the FBI's Internet Fraud Complaint Center and others.

Academia

- Carnegie Mellon University
- University of Pittsburgh
- Duquesne University
- The Pennsylvania State University
- Indiana University of Pennsylvania
- West Virginia University.

Private Businesses

- RAND
- Microsoft
- Ericsson
- RedSiren Technologies
- Lucent Technologies
- Federated Investors and others

(more)

Future partnerships will be established in regions where interest exists to combine resources, intelligence, and expertise more effectively. These additional partnerships will be linked together, enhancing the resources fundamental to this project. This coordinated and decentralized approach will empower regional teams with vital information and expertise in a timely and efficient manner

University Contributions

Pittsburgh is home to a number of other cybersecurity assets. In 2004, Carnegie Mellon University became one of only two institutions in the U.S. to receive National Science Foundation (NSF) funding for the study of a branch of cybersecurity, called Security Through Interaction Modeling. Carnegie Mellon received \$6.4 million, just eclipsing the University of California at San Diego, which received \$6.2 million.

Its large faculty in cybersecurity-related fields and significant levels of funding at its Software Engineering Institute are important assets in the development of a larger cybersecurity market.

Since education is a necessary component of safeguarding the computer network, Carnegie Mellon also invested \$6 million to institute CyLab, one of the largest university-based cybersecurity education and research centers in the U.S. CyLab is multi-disciplinary and university-wide, involving six colleges from Carnegie Mellon, 50 plus faculty and more than 130 graduate students. CyLab is supported by both public and private funding, predominantly government research funds and the support of its partners. Partners include, but are not limited to:

- Aruba Networks
- Bloomberg
- Boeing
- Deloitte
- Ericsson
- GM
- Honeywell
- HP
- Intel
- Lockheed Martin
- Raytheon
- SAP
- Seagate
- Sony
- Symantec

(more)

Cybersecurity in the Pittsburgh Region

Page 8

CyLab's mission is to create mutually beneficial public-private partnership between academia, government and industry-based organizations for advancing and improving the nation's capabilities in response and prediction and for developing new technologies for measurable, available, secure, trustworthy and sustainable computing and communications systems. CyLab seeks to educate individuals at all levels in addressing the threats to the country's cyber infrastructure by providing technology, resources and expertise in four areas:

- Technology transfer to and from the public sector
- Technology transfer to and from the private sector
- Development of information assurance professionals
- National awareness programs and tools

To that end, CyLab brings together more than 50 faculty and 130 graduate student researchers in six colleges throughout the university, along with the CERT/CC.

CyLab is an NSF CyberTrust Center, and it is a key partner in NSF-funded Center for Team Research in Ubiquitous Secure Technology. CyLab also is a National Security Agency (NSA) Center of Academic Excellence in Information Assurance Education, as well as a Center for Academic Excellence in Research, also designated by the Department of Homeland Security.

Carnegie Mellon previously had received three NSF Federal Cyber Service Scholarship for Service Capacity-Building Track awards (from 2002 through 2007.) This funding has been used to develop and offer six editions of an intensive, month-long, in-residence summer program to help develop information assurance (IA) education and research capacity at colleges and universities designated as minority-serving institutions (MSIs), specifically, historically black colleges and universities and Hispanic serving institutions. The program has exceeded the expectations of all participants and has made a measurable impact on the capacity of these MSIs to educate students in IA. With the last two grants, Carnegie Mellon was able to invite 36 faculty, including two department chairs in computer and information science, computer information systems and similar departments from 11 MSIs.

The Software Engineering Institute has designed and continuously is developing a curriculum to teach system and network administrators about information assurance, including a way for them to think about information security issues and a set of skills to help them integrate security policy, practices and technologies into their operational infrastructure. This Survivability and Information Assurance curriculum is to be offered at community colleges across the country, making such education affordable and accessible to professionals and employers.

(more)

Cybersecurity in the Pittsburgh Region

Page 9

At the University of Pittsburgh, the Department of Information Science and Telecommunications has established the Laboratory of Education and Research on Security Assured Information Systems (LERSAIS). This premier program focuses on the diverse problems related to security and survivable information systems, networks and infrastructures, while developing and supporting high quality education in security and information assurance.

Since the spring of 2004, LERSAIS has hosted numerous seminars on information security presented by leading experts from all over the country. As a result, The University of Pittsburgh has been designated as a National Center of Academic Excellence in Information Assurance Education since 2003 and is one of only 13 Centers in the United States with five certifications by the NSA and the Department of Homeland Security. It continues to serve as a multidisciplinary forum for the synergistic interaction among researchers within survivable information systems, as well as other experts in information assurance-related areas outside the school.

One example of this academic excellence is the NSA-approved curriculum to train security professionals in three computer security standards. These standards are: training for information systems security professionals; training for designated approving authorities; and training for system administrator professionals.

Among the university's corporate partners is Cisco, which initially awarded the LERSAIS program an equipment grant worth \$100,000. In addition, LERSAIS was given the Department of Defense Information Assurance Scholarship award for partnering with the National Defense University's Information Resource Management College (NDU/IRMC). Under this program, a student who has been studying under certificate programs at NDU/IRMC can pursue the security assured information systems (SAIS) track in the Department of Information Sciences and Telecommunication with a Department of Defense scholarship.

Private Sector

Although many large corporations and government agencies manage computer security in house by hiring their own staff of experts, the market for cybersecurity services is about \$21 billion. Part of this anticipated growth will be fueled by the financial services industry, where spending on security-related products and services is expected to reach \$2.2 billion. The federal government alone had spend \$7.4 billion on cybersecurity in fiscal 2008, and spending to protect military intelligence is expected to reach \$11 billion by 2013.

More than 40 businesses in southwestern Pennsylvania indicate some level of involvement and expertise in cybersecurity, and all are poised to take advantage of the growth trend. Included in this community are hardware and software designers, cybersecurity consulting services, developers of monitoring software and tracking devices, and manufacturers of technical surveillance and security counter-measures equipment.

(more)

Cybersecurity in the Pittsburgh Region
Page 10

ABS Computer Technology, Netronome Systems and VigilantMinds are just a few of the organizations driving the region's progressive cybersecurity efforts.

VigilantMinds offers consulting and managed security services to help assess, monitor and protect client company networks. It provides security services to several global clients in industries that include manufacturing, financial services, healthcare and federal and state government agencies. VigilantMinds was a Pittsburgh Technology 50 award winner for 2005 in the service provider category.

The Pittsburgh region continues to solidify its claim of a center of excellence in cybersecurity. The private firms that operate within this emerging cluster are only part of the picture. The presence of university-based and government agencies also attract a disproportionate share of federal funding for research, development and national cybersecurity services.

Visit: www.cert.org

www.ncfta.net

www.cylab.cmu.edu

www.sis.pitt.edu/~lersais/

www.abs-comptech.com

www.netronome.com

www.VigilantMinds.com

###

Backgrounders in this series featuring technology centers of excellence in the Pittsburgh region include:

Cybersecurity
Data Storage
Electro-Optics
Energy Technology
Entertainment Technology

Micro-electromechanical Systems
Nanotechnology
Robotics
Specialty Metals
Supercomputing

System-on-a-Chip

Tissue Engineering