Information Security Educational Initiatives to Protect E-Commerce and Critical National Infrastructures

William Yurcik
David Doss
Department of Applied Computer Science
Illinois State University
Normal, IL 61790-5150 U.S.A.

Abstract:

The number of skilled practitioners of information system security who are able to address the complexities of large, interdependent systems is very small. By moving to an educational system that cultivates an appropriate knowledge of security, we can increase the likelihood that our next generation of Information Technology workers will have the background needed to design and develop systems that are engineered to be reliable and secure. This paper describes current specific educational initiatives designed to facilitate information systems security education. We close with our own recommendations for facilitating information system security education based on similarities between the different initiatives.

Keywords: Information security, security education, critical infrastructure protection

1. INTRODUCTION

Efforts to curtail Internet attacks on E-Commerce and Critical National Infrastructure (CIP) have largely focused on information security products, outsourcing/consulting services, and law enforcement but the real solution must come from educational programs. "There is no more important part in our national agenda for protecting our information systems than education," said Jeff Hunker, senior director for infrastructure protection at the National Security Council, speaking at the National Colloquium for Information Systems Security Education (NCISSE) in Washington D.C. May 23, 2000.

"If every house in the United States were without a front-door lock, is the solution to hire more cops? I think not," says Richard Clarke, national coordinator for security, infrastructure protection and counter terrorism and senior director of transnational threats at the National Security Council (Clarke 2000). The problem will not be solved until there are people who know how to make systems more secure. Clarke adds, "The United States has not produced a group of people who can handle the new IT infrastructure. We have built a country that we cannot run because we don't have the people who know how to run it." (Clarke 2000). One stopgap measure has been the recent relaxation of H1B visas to import information systems security professionals from other countries. Without people knowledgeable about information security, the research and development needed to build security into networks will not happen.

Disruption of information services can be very expensive to businesses, life-threatening to human services, and ultimately threaten the economic security of a nation. E-commerce dot.com revenue streams are currently focused on gaining market share for future investment value at this stage of the E-Commerce evolution. One hundred per cent availability is the driving business factor over the damage cost of Internet attacks (lost revenue, replacement software/hardware, and security services). E-commerce outages have ramifications such as loss of reputation, loss of consumer confidence, and in several cases rapid stock devaluation.

Some have warned of an impending "Electronic Pearl Harbor" given the spectrum of potential threats against E-commerce and CIP including criminals, terrorists, and even foreign governments. There is a significant difference, however, in that Japan attacked Hawaii with little or no warning but in our case we have had continuous warnings given attacks by insiders and amateurs.

While the number of Internet attacks being investigated by the U.S. Federal Bureau of Investigation (FBI) doubled from 1998 to 1999 (from 547 to 1,154), there has not been a consensus that this increase represents a aggregate threat to critical infrastructures (HPCWIRE 1996). Based on a March 2000 survey of 643 major organizations, the Computer Security Institute (CSI) with the assistance of the FBI estimated that the total losses attributable to computer crime were $10 Billion for calendar year 1999 (Piller 2000). Public awareness was achieved in February 2000, when a series of coordinated denial-of-service IW attacks were launched against major US corporations.[1] Not only did the attacks prevent 5 of the 10 most popular Internet websites from serving its customers but the attacks also slowed down the entire Internet - Keynote Systems measured a 60% degradation in the performance of the 40 other websites that had not been attacked (Nelson 2000). While the consensus analysis of these IW attacks is that they were technologically unsophisticated (executing a downloadable program), it is particularly disturbing the ease at which major corporate operations can be disrupted and the lack of defenses to prevent such attacks from re-occurring in the future. These attacks made newspaper headlines and lead to a White House meeting with leading E-Commerce parties. Although these DDoS attacks did not cause critical or lasting damage, they have taken the threat out of the realm of the abstract and made them real. Given such attacks cannot currently be stopped and will likely increase in frequency a long term solution is needed.

The remainder of this paper is organized as follows: Section 2 defines the scope of information security education. Section 3 highlights recent national initiatives to facilitate more information security education. We close with a summary and future directions in Section 4.

2. THE SCOPE OF INFORMATION SECURITY EDUCATION

It has long been recognized that the control and use of information such as signal intelligence, communications intelligence, electronics intelligence, foreign instrumentation signals intelligence, and imagery intelligence is vital for military and economic security.[2] There is even the recent perception within military circles that control and use of information may be more important than air superiority in previous wars (Yurcik 1997).

The problem is that there are only a handful of dedicated computer security research centers in degree granting departments at universities in the U.S. In 1997 a leading expert stated before Congress that of the approximately 5,500 Ph.D. recipients in computer science and engineering awarded since 1992 at all U.S. universities only 16 were for security-related research contained at just four universities (only 8 of the 16 Ph.D. students were U.S. nationals) (Spafford 1997).

Information security education can be characterized into the following academic groups:

- Training – mechanics of specific systems, situational configurations (SANS Institute, USENIX, community colleges)
- Undergraduate – applying principles broadly over a breadth of applications, case studies generalize principles and provide details on how to apply principles (4-year colleges and universities)
- Masters – examines a particular area of study in depth analyzing security flaws and proposing solutions, learning analytic/experimental techniques (research I/II universities)
- Doctoral – conduct research to analyze and extend new principles to add to body of knowledge, pushing boundaries of applications, necessary credentials for research (research I universities)

[1] The companies in the order they were attacked are: Yahoo! (2/7/00), eBay (2/8/00), Buy.com (2/8/00), Amazon.com (2/8/00), CNN (2/8/00), ZDNet.com (2/9/00), E*Trade (2/9/00), Excite At Home (2/9/00), and Datek (2/9/00).

[2] Signal intelligence (SIGINT) is intelligence information comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. Communications intelligence (COMINT) is technical and intelligence information derived from foreign communications by other than the intended recipients. (ELINT) is technical and intelligence information derived from foreign non-communications electromagnetic radiation emanating from other than nuclear detonation or radioactive sources. Foreign instrumentation signals intelligence (FISINT) is technical and intelligence information derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-US aerospace, surface, and subsurface systems such as telemetry, beaconry, electronic interrogators, and video data links. Imagery intelligence (IMINT) is intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media. Definitions are from National Security Law by John Norton Moore et al., editors 1990.

Given academic education in these different forms there are also significant contrasts in consumers of information security education:

- Academic research institutes: flexibility to learn general security-relevant details emphasizing theory and underlying principles, rarely focusing on a particular system, focus on long-term contribution
- Industry: less emphasis on general principles and more emphasis on the business environment, applied security based on cost-benefit analysis, focus on short-term investor gain
- Government: mission outgrowth of government policy and/or legal requirements, focus on long-term national interest

One de facto solution that has evolved is the certification process, which is a formal process that vouches and validates the worth of something/someone – an official declaration that something/someone, exceeds established requirements or standards. Examples of such information systems certification programs include Microsoft, Cisco, Novell, Oracle, American Society of Industrial Security, Association of Certified Fraud Examiners, and Certified Information Systems Security Professional (CISSP). Shared elements of these certification programs include: (1) a standard for measuring minimum knowledge; (2) experience requirements; (3) code of ethical behavior; (4) instrument for evaluating knowledge (proficiency testing); and (4) references for validating education and experience. Motivations for students include recognition, satisfaction/self-realization, credibility to senior management, and enhanced job prospects. Employers find that certification assures an acceptable level of technical expertise.

3. SPECIFIC INITIATIVES

PCCIP

For the purposes of this paper we trace the origin of CIP to the recommendation of Critical Infrastructure Working Group (CIWG) created by the Attorney General in response to bombing of the Murrah Federal Building in Oklahoma City in 1995.[3] The CIWG conducted an intense, but short-term, examination of threats and vulnerabilities of critical national infrastructures. On 6 February 1996, the CIWG issued a report recommending the creation of two organizations to address current and future threats and vulnerabilities.

President Clinton signed Executive Order 13010 on 15 July 1996 which established the Infrastructure Protection Task Force (IPTF) as an interim coordinating measure for the short term and the "President's Commission on Critical Infrastructure Protection" (PCCIP) for the long term. Because threats to the U.S. critical infrastructure were considered authentic and impending, the IPTF was created within the Department of Justice to increase the "coordination of existing infrastructure protection efforts in order to better address, and prevent, crises that would have a debilitating regional or national impact." The PCCIP was the first long-term national effort to address the vulnerabilities created by the new information age. (Federal Register 1996)

Executive Order 13010 declared that certain "national infrastructures are so vital that their incapacity or destruction {by either physical or cyber attack} would have debilitating impact on the defense or economic security of the United States." The Executive Order detailed eight categories of critical infrastructures:

1. telecommunications
2. electrical power systems
3. gas and oil storage and distribution
4. banking and finance
5. transportation
6. water supply systems
7. emergency services (including medical, police, fire, rescue)
8. continuity of government

The President acknowledged in the text of the Executive Order that because so many of these critical infrastructures are owned and operated by the private sector, "it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation." (Federal Register 1996)

The PCCIP was chaired by retired Air Force General Robert T. Marsh and was comprised of members of the federal government and industry. A Steering Committee of senior government officials and an Advisory Committee of key industry leaders guided its work. The Commission was tasked to develop a comprehensive national strategy for protecting critical infrastructures from physical and cyber threats.

A hundred-page unclassified version of the PCCIP report entitled "Critical Foundations: Protecting America's Infrastructures" was released on 13 October 1997 (PCCIP 1997). The PCCIP report found no evidence of an "impending cyber attack that could have a debilitating effect on the Nation's critical infrastructures." The PCCIP report did, however, conclude that all critical infrastructures are increasingly vulnerable to attack and although the threat of an Internet attack (in 1997) appeared small, the prospect for

[3] Presidential Decision Directive 39 created the CIWG.

such attacks in the future was found to be significant.[4] The PCCIP identified potential threats that included insiders, recreational and institutional hackers, organized criminals, industrial competitors, terrorists, and states. Because the nation's critical infrastructures are mainly privately owned and operated, the Commission concluded that "critical infrastructure assurance is a shared responsibility of the public and private sectors," and the only sure way to protect infrastructures is through a real partnership between infrastructure owners and the government (PCCIP 1997).

Specifically on information systems security education, the PCCIP report states the following on page 71:

> "NIST, NSA, and the U.S. Department of Education work in collaboration with the private sector to develop programs for education and training of information assurance specialists and for the continuing education as technologies change. This effort should also support 'training the trainers' to provide an adequate cadre of qualified instructors to teach technicians." (PCCIP 1997)

National Plan

The 1997 PCCIP report noted an absence of national focus for infrastructure protection. Presidential Decision Directive (PDD) 63, Critical Infrastructure Protection, address this absence by outlining an administrative structure for developing a national infrastructure protection plan. The directive orders immediate federal government action, with the goal that, within 5 years that the nation's critical infrastructures will be protected.

The National Plan for Information Systems Protection is the first attempt by any nation to develop a plan to defend its infrastructure (White House 2000). Designed as a first major element of a process to develop a comprehensive national strategy for infrastructure assurance as envisioned by PDD 63, it was released on 7 January 2000 and will be periodically revised as necessary to address emerging problems.

The National Plan includes 10 programs, 3 of which are related to higher education: (1) enhancement of existing information security system programs; (2) education of students; and (3) outreach programs to improve public awareness. Three possible actions include:

1) the development of university centers of Infrastructure Assurance modeled after Materials Centers sponsored by NSF and Transportation Centers sponsored by DOT,

2) the encouragement (through incentives) of curriculum development for computer science, business schools, and distance learning,

3) the assessment of technician training via extension service, community college, and commercial programs.

While a good start, there remain challenges to this approach:

- Information security is cross-disciplinary field combining computer science, engineering, law, political science, and criminal science. However, universities are not organized for cross-disciplinary field of study – universities are commonly silo-oriented with depth in specific areas but little interaction between disciplines. It will take significant management leadership to enable cross-disciplinary study in information systems.

- For research and development to increase significantly, trained scientists are the issue with tenured faculty in information being the scarcest resource. While information security education is a national issue, most faculty are funded at the state level.

The Cyber Corp Program

One unique proposal from the current administration which acts on the National Plan is the "Federal Cyber Services Training and Education" scholarship program for information security education. Already nicknamed the "Cyber Corp" program, it is partially modeled after the Peace Corp. Core parts of the program include students being hired into the Federal Government while an undergraduate (complete with clearance requirements), serving an internship/coop with a Federal Agency, and then subsequent to graduation working for two years in the Federal Government in exchange for stipend/tuition/room/board support. The specifics of this program are currently being shaped under legislative committee for congressional budget appropriations and will be comprehensively described upon revision of this paper after this process is complete. There have been varied outlines of this program floated in the media for political purposes and there appears to be bipartisan support in Congress.

National Security Agency

The National Security Agency (NSA) has embarked on a special program for information systems security education entitled: National INFOSEC Education and

[4] The PCCIP report notes the attacker's tools are becoming more advanced and more accessible so less skill is needed to launch ever more sophisticated attacks.

Training Program (NIETP).[5] The NIETP is designed to enhance information systems security skills via community-based education and training which are national in focus, future-oriented, multi-disciplinary, and tied to both technology and business. A major accomplishment of the NIETP has been the establishment of Centers of Academic Excellence in information security education at a number of universities at both the graduate and undergraduate levels. This NSA program certifies that the following 14 universities have specific programs which meet minimum standards for information assurance education:

University of California at Davis
Carnegie Mellon University
Florida State University
University of Idaho
Idaho State University
University of Illinois at Urbana Champaign
Iowa State University
James Madison University
George Mason University
National Defense University
Naval Postgraduate School
Purdue University
Stanford University
University of Tulsa

NSA also offers online courses in the following topics as part of its outreach program: (1) Overview and Risk Management Terminology; (2) Risk Management Issues; (3) Risk Assessment and Risk Mitigation; (4) Risk Management; (5) Malicious Programs; and (6) Information Assurance. Some of this material has been adapted to the K-12 school environment with encouraging results.[6]

CERIAS

One example of a university information systems security program and arguably the lead model for public institutions is the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University.[7] In 1992 Professor Eugene Spafford established the COAST (Computer Operations Audit and Security Technology) laboratory at Purdue to provide a unified approach to research and education efforts in information security. CERIAS emerged in May 1998 as an outgrowth of the COAST laboratory. The center draws faculty and staff from a variety of schools, centers, and departments within Purdue.[8] The goals of CERIAS are to:

- Obtain data on information security issues through research and networking
- Find practical solutions to information security issues
- Provide educational programs to develop more professionals who can address information security and assurance issues.

CERIAS relies on sponsors for funding and information since these companies operate in a real-life situations demanding practical solutions. For example, sponsors of CERIAS act as partners by:

- Providing access to state-of-the-art equipment
- Giving feedback on CERIAS publications and prototypes
- Identifying research needs and trends
- Student internships
- Professional expertise

U.S. Naval Postgraduate School

For over 20 years, the Naval Postgraduate School (NPS) has been a leader in the design and implementation of information system security education. The NPS Center for Information Systems Security Studies and Research (CISR) is the world's foremost center for military research and education in information systems security.[9] NPOS CISR's mix of experienced military officers and government civilian students make it uniquely qualified to address security issues of the Department of Defense and the U.S. Government. NPS CISR classes and research examine the problem of malicious software and system subversion. Using foundational concepts and technologies as a springboard for new developments, students and faculty construct systems to provide assurance in the face of penetration attempts. Security is built into systems from the start rather than as an afterthought or as a series of continuing updates and patches.

FOSAD

Information system security educational initiatives are not limited to the United States. In September 2000 a two-week summer school has been organized under the auspices of the European Federation for Information Processing (IFIP WG 1.7), the European Educational Forum, and the European Association of Theoretical Computer Science (Italian Chapter). The International School on the Foundations of Security Analysis and Design (FOSAD) will be held at the University of Bologna covering current research in foundations of security ranging from programming languages to

[5] URL: http://www.nsa.gov/isso/programs/nietp/index.htm

[6] URL: http://www.infosec.jmu.edu/ncisse/conference98/website/nsacourses/

[7] URL: http://www/cerias.purdue.edu

[8] Founded in 1962, Purdue's Department of Computer Science was the world's first to grant degrees in computer science and offer study at all levels.

[9] URL: http://cisr.nps.navy.mil/

analysis of protocols.[10] It is intended that the series of lectures from international experts will help graduate students and young researchers who intend to approach the information system security field.

4. CONCLUSIONS

Education is the number one issue for information systems security. This paper has presented specific educational initiatives to facilitate information systems security curricula to meet the growing demand for information system security professionals.

In closing we posit our own information system security educational recommendations based on similarities between the initiatives:

- Long-term funding and infrastructure support is vital (buildings, programs, faculty).
- More partnerships between industry and universities are needed specifically in the form of student internships, funded-research, and professional exchanges.
- Making source code available to educational institutions is the single most effective information systems teaching tool.

Accepting that the present information systems technology will change drastically in the future (in ways we cannot currently conceive), it is vital to support the dreamers – people with innovative ideas that are ahead of their time and may currently appear strange. One worst case scenario is that information security education will occur only as training on specific systems leaving no one with an ability to think "outside the box."

5. ACKNOWLEDGEMENTS

This study was supported in part by a grant from the John Deere Corporation and State Farm Insurance Company.

6. REFERENCES

Clarke, Richard, 2000, Keynote Speech at The 4th National Colloquium for Information Systems Security Education (NCISSE). Washington D.C., May 23-25.

Federal Register, 1996, "Executive Order 13010 – Critical Infrastructure Protection", July 17, Vol. 61, No. 138.

HPCWIRE, 2000, "FBI Chief Says Cyber Attacks Doubled in a Year", March 31, article #17365.

Nelson, Mathew G. et al., 2000, "Attacks on E-Businesses Trigger Security Concerns," InformationWeek, February 14, pp. 28-30.

PCCIP, 1997, "Critical Foundations: Protecting Americas Infrastructures." The Report of the President's Commission on Critical Infrastructure Protection (PCCIP), October 1997. http://www.ciao.gov/CIAO_Document_Library/PCCIP_Report.pdf

Piller, Charles, 2000, "Cyber-Crime Loss at Firms Doubles to $10 Billion", Los Angeles Times, March 22.

Spafford, Eugene, 1997, "Dr. Eugene Spafford of Purdue University: Testimony to the House Science Committee", U.S. Congress, February 11.

White House, 2000, "Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to Dialogue", The White House, Washington, D.C., Jan. 7. http://www.ciao.gov/National_Plan/national_plan%20_final.pdf

Yurcik, William, 1997, "Information Warfare: Ethical Challenges of the Next Global Battleground", Proceedings of the Second Annual Ethics and Technology Conference (Ethics '97), Loyola University Chicago, Chicago, IL, June 6-7, session 6, paper 17.

[10] URL: http://cs.unibo.it/~aldini/fosad/index.html#info