ISSN: 1545-679X

Information Systems Education Journal

Volume 1, Number 9 http://isedj.org/1/9/ September 11, 2003

In this issue:

The Implications of Information Assurance and Security Crisis on Computing Model Curricula

Denise R. McGinnis
Mesa State College
Grand Junction, CO 81501

Ken Comstock
Mesa State College
Grand Junction, CO 81501

Abstract: IT security is a complex problem that has become monumental in recent years. Identity theft is rapidly increasing. Cyberterrorism has caused new fears. With the explosive growth of the Internet and new technologies, hackers have found new ways to exploit systems. This has created a shortage of IT people trained in security. While salaries in other IT sectors are decreasing, security salaries are increasing. Government funding for security is growing, both within government agencies and for colleges. These factors imply that higher education and model curricula should include information assurance and security as a component in their programs. An examination of three computing model curricula shows inclusion of information assurance and security. Computing educators need to promote the inclusion of information assurance and security in higher education.

Keywords: information assurance programs, Homeland Security, National Colloquium for Information Systems Security Education, NCISSE, model curriculum

---

Recommended Citation: McGinnis and Comstock (2003). The Implications of Information Assurance and Security Crisis on Computing Model Curricula. *Information Systems Education Journal, 1* (9). http://isedj.org/1/9/. ISSN: 1545-679X. (Also appears in *The Proceedings of ISECON 2003:* §2431. ISSN: 1542-7382.)

This issue is on the Internet at **http://isedj.org/1/9/**

The **Information Systems Education Journal** (ISEDJ) is a peer-reviewed academic journal published by the Education Special Interest Group (EDSIG) of the Association of Information Technology Professionals (AITP, Chicago, Illinois). • ISSN: 1545-679X. • First issue: 2003. • Title: Information Systems Education Journal. Variant titles: IS Education Journal; IS Ed Journal; ISEDJ. • Physical format: online. • Publishing frequency: irregular; as each article is approved, it is published immediately and constitutes a complete separate issue of the current volume. • Single issue price: free. • Subscription address: subscribe@isedj.org. • Subscription price: free. • Electronic access: http://isedj.org/ • Contact person: Don Colton (editor@isedj.org)

The Information Systems Education Conference (ISECON) solicits and presents each year papers on topics of interest to IS Educators. Peer-reviewed papers are submitted to this journal.

EDSIG activities include the publication of ISEDJ, the organization and execution of the annual ISECON conference held each fall, the publication of the Journal of Information Systems Education (JISE), and the designation and honoring of an IS Educator of the Year. • The Foundation for Information Technology Education has been the key sponsor of ISECON over the years. • The Association for Information Technology Professionals (AITP) provides the corporate umbrella under which EDSIG operates. AITP celebrates its 50th year as a professional society in 2003.

The Implications of Information Assurance and Security Crisis on Computing Model Curricula

Denise R. McGinnis
mcginnis@mesastate.edu

and

Ken Comstock
kcomstoc@mesastate.edu

Mesa State College
1100 North Avenue
Grand Junction, CO 81501, USA

Abstract

IT security is a complex problem that has become monumental in recent years. Identity theft is rapidly increasing. Cyberterrorism has caused new fears. With the explosive growth of the Internet and new technologies, hackers have found new ways to exploit systems. This has created a shortage of IT people trained in security. While salaries in other IT sectors are decreasing, security salaries are increasing. Government funding for security is growing, both within government agencies and for colleges. These factors imply that higher education and model curricula should include information assurance and security as a component in their programs. An examination of three computing model curricula shows inclusion of information assurance and security. Computing educators need to promote the inclusion of information assurance and security in higher education.

Keywords: information assurance programs, Homeland Security, National Colloquium for Information Systems Security Education, NCISSE, model curricula

1. INTRODUCTION

Focus on Information Technology (IT) security has intensified with the Internet and post-September 11. Corporations are losing money. Security breaches are from both external and internal sources. Some suggest that an information system will never be one hundred percent secure. Billions of dollars could be spent on the problem of information assurance and security. A recent survey of 29,500 IT professionals suggested that 95% of their companies would match or increase spending on security in 2002 (George, 2002). This evidence implies a crisis in IT security.

The Alliance for Telecommunications Industry Standards (ATIS) defines **information assurance** as: "Information operations (IO) that protect and defend information and information systems (IS) by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and

reaction capabilities." (ATIS) An alternate definition of information assurance is the "trust that information presented by a system is accurate and is properly represented; its measure of the level of acceptable risk depends on the critical nature of the system's mission." (Longstaff, 2000) The term, which has spread from government use into common usage over the past two years, is sometimes synonymous with information security.

IT security and information assurance may not have identical definitions but are similar. The availability, confidentiality and integrity of information systems are an integral part of their definitions. Some would argue that the two terms are quite different. No matter how these terms are defined, there is an overwhelming interest in information assurance and security by governments and corporations.

As our nation faces the issues of information assurance and security, this paper will address the key issues related to the crisis in IT security. We present information on current government regulations, funding and educational programs that are being used to combat the crisis. We show how current computing curricula models include information assurance and security. Lastly, we make some recommendations related to the future impact of information assurance and security on undergraduate computing curricula and the IT security crisis.

2. IT SECURITY CRISIS

IT Security is a complex, serious topic with many issues and problems. Hacking, cracking, spoofing, smurfing, and sniffing are cute names that have been created for crimes against individuals and corporations. A lot of print is dedicated to discussing the crimes and problems. The government and higher education are doing research and searching for solutions. What are the key factors in IT security that caused this current crisis in IT security?

According to Colin Crook, of Wharton's SEI Center for Advanced Studies in Management, most of the IT security problems we face today boil down to three main factors: concentration of computing power, interconnectedness, and standardization (Wharton School, 2002). Concentrated computing power, a main frame or central server, has definite advantages, however, intrusions can be more disastrous and make recovery more difficult. Distributed systems, while creating site redundancy also increase interconnectedness. Although good for backup purposes, this also offers multiple access points for someone with criminal intent. "Large computerized databases containing personal information, being increasingly interconnected by means of the Internet, have become irresistible targets for criminals" (Mann, 2002). Standardization of operating systems and integrated software suites increase business portability and efficiency but are a drawback when it comes to security. Once a hacker has discovered a particular software vulnerability or hole he is able to break into other networks running the same software. The result is a constant race to keep up with the latest software vulnerabilities, patches, updates, and Service Packs. Concentration of computing power, interconnectedness, and standardization are three main causes of the current IT security crisis.

One of the goals of IT workers and network administrators is to have a "secure system." But what is a secure system? In order to answer this question one must ask, "Secure from what?" What if a hand grenade dropped on the CPU? Suppose a surveillance camera has a view of the monitor and keyboard. "Secure from whom?" A dishonest employee with network access can cause major problems. A bank must not only secure itself from consumer fraud, but also merchant fraud, teller fraud, and bank manager fraud. Crook's three key factors contribute to the security crisis but the issues and problems are much more complex.

Bruce Schneier, founder and CTO of Counterpane Internet Security, a company that specializes in managed-security monitoring, and author of *Applied Cryptography*, the first-ever guide to the practice of cryptology, is one of the leading experts on IT security. Schneier states that it is impossible to totally secure a computer system. He compares network security to an arms race where the attackers have all the advantages. After all, the defender has to

defend against any and every possible attack, whereas the attacker has only to find a single weakness (Schneier, 2001).

Corporations lose millions of dollars every year because of theft of valuable information. Yet according to experts, it is not hackers but people working inside the company that are the main culprits, and most companies are reluctant to report intrusions. A recent survey by the FBI shows some startling statistics:

> There was a time when vindictive former employees sought revenge by pilfering some office supplies or spreading a juicy rumor about the boss. But in today's computerized offices, angry workers and disgruntled employees can access computer systems and destroy data, potentially causing millions of dollars in damage….A recent FBI survey of anonymous companies showed 85 percent had a computer intrusion in the last year. Of these intrusions, 30 percent were from outside hackers, while 70 percent came from people associated with the company (Huffman & Hamilton, 2002).

A year earlier, a similar survey by the FBI reported that 80% of the money corporations spend on security was directed toward outside attackers, when in fact 80% of all attacks came from within the company (Verton, 2001).

The recent bust, of the largest identity theft ring in history, shocked authorities. In November of 2002, a help desk worker at a small company on Long Island was charged with the theft of more than 30,000 people's identities. U.S. Attorney Kevin Barrows called it "every American's worst financial nightmare multiplied tens of thousands of times." (Sullivan, 2002) This sample and the surveys imply the IT security crisis is directly related to hiring, awareness and education. In addition to Crook's main factors in the IT security crisis, there appear to be more, including this fourth key factor: a general business problem related to personnel issues.

The increase of Internet traffic has affected how rapidly viruses can be transmitted through the World Wide Web. In the mid 1980s viruses were not a big problem as they were fairly simple and detection was easier. Until a few years ago, a firewall was all you needed to be secure on the Internet. No one had heard of denial-of-service attacks. But with the explosive growth of the Internet, hackers have found new ways to exploit systems. New technologies have emerged for security such as intrusion-detection, public-key infrastructure, smart cards and biometrics. New types of networking services, wireless technology, etc. have made it difficult for CIOs to keep up with the latest trends. Consequently, there has been a shortage of Network administrators trained in information assurance and security:

> The explosion in use of the Internet is straining our scarce technical talent. The average level of system administrator technical competence has decreased dramatically in the last 5 years as non-technical people are pressed into service as system administrators. Additionally, there has been little organized support of higher education programs that can train and produce new scientists and educators with meaningful experience and expertise in this emerging discipline (Pethia et al., 2000).

In spite of the slump in the IT industry, the future looks good for security professionals. While the average salary of a system administrator has dropped by more than $2,200 over the past three years, security salaries have risen anywhere from $8,000 to $20,000 during the same period. Post September 11 fears have caused much concern over the threat of cyberterrorism. This along with the recent creation of the 170,000-person federal Department of Homeland Security, and new regulations affecting health care and other industries, has geared up the demand for information security professionals (Stevens, 2002). Thus a fifth key factor in the IT security crisis is the lack of IT administrators with IT security training.

All five of these key factors need to be studied. There needs to be more awareness and education about possible information assurance and security problems and

solutions. Companies need be careful in their hiring and training of personnel. IT security education and training should be increased. Current IT administrators should receive additional training. The government and higher education are responding to the IT security crisis.

3. GOVERNMENT AND HIGHER EDUCATION'S RESPONSE

The response to the IT security crisis is demonstrated in a number ways. Legislation related to Homeland Security includes topics related to IT security. Our government is budgeting money for IT security. Scholarships are awarded to persons willing to be trained in security. Universities have been named Centers of Excellence in Information Assurance. Numerous colleges and universities offer IT security courses, certifications and graduate programs.

The United States federal government budgeted $722 million for IT homeland security in fiscal year 2003, which amounts to roughly two percent of the $37.7 billion budgeted for homeland security (Jackson, 2002). As of November 14, 2002, a new Cybersec Funding Bill was also approved. Known as the CSRDA (Cyber Security Research and Development Act), this bill allocates $903 million for cybersecurity research, $25 million of which is earmarked for increasing the number of qualified college-level cyber-security instructors and $144 million for establishing Computer and Network Security Research Centers. The money, which will be spent over the next five years, is more than triple the previous budget (Mark, 2002). Finally, for 2004, President Bush is asking Congress for $59 billion in new information technology as a response to Homeland Security and the war on terrorism. If passed, approximately $4.7 billion of this would be used to fund computer security (Harris, 2003).

The IT security problems and the shortage of IT professionals trained in security contributed to the formation of a presidential commission in 1997. This led to a 1998 presidential directive that cited information and communications infrastructure protection and security as a national priority. By July of 2000, the National Science Foundation (NSF) had been authorized to award $8.6 million in student scholarships, which went to six universities through the Cyber Corps "Scholarship for Service" program for the school year beginning in 2001 (Jackson, 2002). In exchange for up to two years of scholarship funding, graduates must work one year for Uncle Sam for every year of scholarship support received. The Department of Defense has its own version of the Cyber Corps program, which is managed by the National Security Agency (NSA). In 2002, there were a total of 36 schools designated by the NSA as Centers of Excellence (CAE) offering similar scholarships (O'Hara, 2002).

The federal Cyber Service Scholarship for Service (SFS) program was initiated in 2000. Under this program, students can receive up to $20,000 scholarship funding with stipends for up to two years of graduate or undergraduate education, in exchange for service to US government civilian agencies such as the Department of Commerce or Department of Transportation. Congress initially authorized a budget of $11 million a year, which was to be appropriated through the NSF. At present the NSF program has at least fifteen colleges and universities participating with about 300 students receiving SFS scholarships, and the budget has grown to over $19 million. (NSF, 2002). The NSF has become the key player in the cyber security effort with responsibility for information security professionals' education and influencing the curricula for the SFS program.

About the same time that the NSF program was in the works, legislation was introduced for a similar program through the National Security Agency (NSA). Known as the National INFOSEC Education and Training program, this program has grown to include about fifty Centers of Academic Excellence (CAE) colleges and universities as of this year. Graduates of the NSA program work for the Department of Defense upon graduation rather than civilian government agencies. A key entity in the NSA program is the National Colloquium for Information Systems Security Education (NCISSE). Founded in 1997, their mission supports protecting information and infrastructure and "… to influence and encourage the development and expansion of information security curricula especially at the graduate

and undergraduate levels." (http://www.ncisse.org) NCISSE is a leading proponent "for implementing courses of instruction in INFOSEC into American higher education." The organization suggests that it is not enough to include these concepts in the information curricula but also in the general curricula.

The NSA is responsible for the CAE designation, which is common to both programs. Schools not designated as CAEs must be approved by the NSA and also must satisfy the federal National Security Telecommunications and Information Security Systems Instruction (NSTISSI) 4011 Standard for Information Systems Security Professionals.[1]

One of the recently named information security programs recognized by the NSA is the computer science program at John Hopkins University. The NSA recognized the program for the years 2003 to 2006 for its research and excellence in teaching of information and security assurance. Similar to many of the other CAEs, John Hopkins programs include a masters of science degree related to information assurance, security informatics. With the NSA and NSF guidelines encouraging a strong research component, it is not surprising to find most CAEs have programs similar to John Hopkins.

In February, 2003, the White House released a 76-page report that outlined a National Strategy to Secure Cyberspace. Although this report focuses more on cyberspace security, it evidences a continuing effort by our government to promote awareness, education and training. "Many cyber vulnerabilities exist because of a lack of cybersecurity awareness on the part of computer users, system administrators, technology developers, procurement officials, auditors, chief information officers (CIOs), chief executive officers and corporate boards." (White House, 2003, xi) One conclusion that could be drawn is that all information training should include security. It should not be limited to computer science programs or graduate degrees.

4. MODEL CURRICULA

Model curriculums are developed as guidelines or recommendations for degree programs. Institutions of Higher Education often use these guidelines to develop degree programs at schools that closely mirror or approximate the model. Although not all disciplines are related to IT security or information assurance, the topic would be relevant to degree programs in Computer Science (CS), Information Systems (IS/CIS/MIS), and Information Resource Management (IRM).

In 2002, the AITP, ACM, and AIS published a model curriculum for programs in Information Systems. In 2000, IRMA/DAMA introduced their new model curriculum for IRM. The Executive Summary of this document indicates that the document details an information resources management curriculum for a four-year undergraduate degree program. The IEEE/ACM 2001 Model Curriculum provides a "set of recommendations for an undergraduate computer science program." (IEEE Computer Society) Each of the model curricula is available at the organization's web site.

The model curricula for these three disciplines would likely be related to IT security. Using this assumption, an analysis of the current computing model curriculum was completed. A cursory search for the words "information assurance" was performed. The counts in Table 1 show that this was not a popular word in any of the model curricula. A second search for the word "security" was performed. These results are shown in Table 1. It appears that the word "security" is more popular in the model curricula but much more prevalent in the computer science curriculum than the other two.

A more thorough reading of the documents suggests that not all the references are unique. In the ACM 2001 model, there are eleven times that the word security is used for the same reference. An example of this would be the inclusion of a course title like

[1] http://www.ncisse.org/certification.htm

Table 1. Times the words "security" or "information assurance" appeared in curriculum model.

	AITP/ACM/AIS 2002	IRMA/DAMA 2000	IEEE/ACM 2001
"security"	8	17	71
"information assurance"	0	0	0

Network Security in several places throughout the document. The references in the IRMA/DAMA 2000 and the AITP 2002 models appear to be unique. A closer look was warranted since only the computer science model appeared to emphasize security and none mentioned information assurance.

AITP, ACM, AIS Model Curriculum for Information Systems

The model curriculum for information systems is "…designed to produce graduates equipped to function in entry level information systems positions with a basis for continued career growth." (Davis, et al., Executive Summary, www.IS2002.org). The 2002 model curriculum includes four goals with a reference to the word security. Table 2 includes these references.

IRMA/DAMA Model Curriculum for Information Resource Management

The IRM model states: "Modern organizations recognize the need to maintain and manage information as an organizational asset. They also recognize the need for today's managers to be well versed in information resources management." (Cohen, 2000, p. 4) A further analysis of the documents indicates that the IRMA model includes the word security ten times in their list of topics for their recommended courses. The list of topics is shown in Table 3.

IEEE/ACM Model Curriculum for Computer Science

The computer science model curriculum suggests that "Information Management (IM) plays a critical role in almost all areas where computers are used. This area includes the capture, digitization, representation, organization, access and updating of stored information, data modeling and abstraction, and physical file storage techniques." (IEEE computer society, 134) Information security, privacy, integrity, and protection in a shared environment are also emphasized in this model. The model curriculum for computer science included a reference to security in seventy-one places. Table 4 includes a sample of the inclusions for comparison to the other model curricula. The inclusions are for core courses and not for electives.

Table 2. AITP, ACM, and AIS 2002 "security" inclusions

Learning Unit Number	Course Name	Goal
13.06	Personal Productivity and IS Technology	To explain organizational database concepts, components, structures, access, security and management considerations.
39	Networks and Telecommunication	To provide awareness of the responsibilities inherent in providing telecommunication services, including security, privacy, reliability and performance.
208	Electronic Business Strategy, Architecture and Design	To explain the consideration and obligations for the protection of individual privacy as well as organizational security in interorganizational systems
67	Information Technology Hardware and Software	To introduce major concepts in operating systems including process definition, concurrent processing, memory management, scheduling, interrupt processing, security and file systems.

Table 3. IRMA/DAMA Model Curriculum "security" inclusions

Course Number	Course Description	Topic name	Subtopic
IRM1	Information Resource Management Principles	• Information Management • Value of Information	• Data Security and Control • Information Security and Control
IRM2	IS Technology	• Organizational Ethics and Security in IS Management	• Access Control • Theft of Information • Government regulations
IRM4	Data Warehousing, Mining and DSS	• Evaluation of DSS	• System security and control of DSS
IRM5	Data Resource Structures and Administration	• Data Resources and Information • Database concepts and applications	• Data security practice • Database administration and security
IRM6	IRM Design and Implementation	• Systems Maintenance and Management of IS	• Developing system security programs
IRM7	Communication Technology and Information Management	• Communication Controls	• Network Security and control • Internet Data security
IRM8	Global Information Management	• Information Technology and Global Operations	• Security in global management of operations
IRM9	Executive Information Systems Management	• Executive Direction of IS	• Control and Security of Information

Table 4. ACM 2001 Model Curriculum "security" inclusions

Course Number	Course Description	Topic name	Learning Objective
OS1	Overview of Operating Systems	• Design Issues	• Identify potential threats to operating systems and the security features design[ed] to guard against them
NC3	Network Security	• Fundamentals of cryptography • Authentication protocol	• Discuss the fundamentals of public-key cryptography • Summarize common authentication protocol
PL2	Virtual Machines	• Security issues from running code on alien machines	• Explain how executable programs can breach computer system security by accessing disk files and memory
IM1	Information Management and Systems	• Information privacy, integrity, security and preservation	• Describe several technical solutions to the problems related to privacy, integrity, security and preservation

Increasing IT Security Emphasis

Given the crisis in information assurance and security, the amount of funding to address this crisis, and the White House stance that even general education should address the crisis, the authors believe that computing model curricula should all include goals that relate to information assurance and security. None of the three computing models examined even contained the words "information assurance." Each had some goals or objectives or topics related to security. As with the government programs and CAEs, the computer science discipline contains the most emphasis on IT security. This does not appear to be sufficient since the NSA criteria include the directive that non-technical students should be introduced to information assurance. (NSA, 2002)

Faculty, administrators and the business sector need to reevaluate what higher education can provide in this arena. Computer science graduate programs assist with the crisis but more needs to be done. IS and IRM model curricula should include more goals, objectives and topics related to IT security and information assurance. Business curricula must include education on IT security. Higher education must do its part to contribute to easing the IT security crisis. Changing the model curricula is only one step but an important one.

5. CONCLUSIONS

IT security is a complex issue. With the explosive growth of the Internet and new information technologies, new methods of thwarting security have arisen. The dramatic increase of identity theft and insider cyber crime has experts worried, and legislators and IT professionals are trying to find solutions. Concentration of computing power, interconnectedness, and standardization are factors that have contributed to the IT security crisis. Additional factors, including a lack of awareness, training and education of all personnel plus the need for more IT professionals trained in IT security play a crucial role to this crisis. The NSF and NSA programs are initial steps to addressing these factors.

The critical nature of the IT security crisis is evidenced by the government's investment and the new programs in Information Assurance. With the importance of information assurance, the three curriculum models examined had no references to this exact term and a varying level of emphasis on security. Using the definition for information assurance presented in the Introduction, an IS professional, educator or student might infer that an Information Systems curriculum model would include multiple references to the terms "information assurance" and "security". An investigation of three model curricula did not prove this inference.

This cursory investigation of three computing curricula model did not include an in-depth analysis of the models and is not complete. A closer look may provide a different result than that found by this research. Other computing curricula models or related models could be investigated. SFS program's curricula and other university IT security curricula should be investigated. With the IT security crisis, additional study of the impact of information assurance and security on computing model curricula should be completed.

6. References

ATIS. Telecom Glossary 2K (2001, Feb. 28). Retrieved May 28, 2003 from http://www.atis.org/tg2k/_information_assurance.html.

Cohen, E. Curriculum 2000 Model of the Information Resource Management Association and Data Administrators Management Association, Retrieved May 29, 2003 from http://gise.org/IRMA-DAMA-2000.pdf.

George, T. "Businesses Need To Pay More To Hire Hard-To-Find Skills." InformationWeek, September 2, 2002.

Gorgone, J. G. Davis, J. Valacich, H. Topi, D. Feinstein, H. Longnecker, Jr. (2002) Model Curriculum and Guidelines for Undergraduate Degree Programs in Information Systems, ACM/AIS/AITP, Retrieved May 29, 2003 from http://192.245.222.212:8009/IS2002Doc/Main_Frame.htm.

Harris, S. (2003, Jan. 21) "Bush Seeks nearly $60 Billion in New IT Spending." GovExec.com. Retrieved June 1, 2003, from

http://www.govexec.com/dailyfed/0103/012103h1.htm.

Huffman, L. and Hamilton, J. (2002, Nov. 5) "Employee Revenge. Cybercrime." Retrieved June 1, 2003, from http://www.techtv.com/cybercrime/viceonline/story/0,23008,3386967,00.html.

IEEE Computer Society, and the Association for Computing Machinery. Computing Curricula 2001: Computer Science (2001, Dec. 15). Retrieved May 29, 2003 from http://www.acm.org/sigcse/cc2001/cc2001.pdf.

Jackson, W. (2002, Feb. 18) "Homeland IT Funds Go to INS Cybersecurity." Government Computer News, Volume 21, Number 4. Retrieved June 1, 2003 from http://www.gcn.com/21_4/news/17998-1.html.

Longstaff, T., Yacov Y. H. (2000, Aug 30) "Knowledge Management: A Requisite for Information Assurance." Retrieved May 29, 2003 from http://www.cert.org/research/isw/isw2000/papers/52.pdf.

Mann, C. (2002, Sept. 13) "Homeland Insecurity." The Atlantic Monthly, Volume 290, No. 2; pp 81–102.

Mark, R. (2002, Nov. 12) "House OKs $903M for Cyber Security Research." InternetNews.com. Retrieved February 27, 2003, from http://www.atnewyork.com/news/article.php/1499391.

NSA. National INFOSEC Education and Training Program, (2002, Sep. 3), http://www.nsa.gov/isso/programs/coeiae/measure.htm, Retrieved on May 31, 2003.

NSF. Press Release (2002, Aug 7), Retrieved from http://www.nsf.gov/od/lpa/news/02/pr0266.htm on June 1, 2003.

O'Hara, C. (2002, Aug. 5) "A Call to Service." Federal Computer Week." Retrieved June 1, 2003, from http://www.fcw.com/fcw/articles/2002/0805/mgt-cyber1-08-05-02.asp.

Pethia, R., Paller, A., Spafford, G. (2000, Feb. 23) "Consensus Roadmap for Defeating Distributed Denial of Service Attacks." SANS InstituteResources. Retrieved June 1, 2003, from http://www.sans.org/dosstep/roadmap.php.

SANS Institute. SANS / FBI Top 20 List (2002, Oct. 17).. Retrieved June 1, 2003, from http://www.sans.org/top20/.

Schneier, B. (2001, Sept. 1) "Network Security: It's Not About the Technology." CIO Magazine. Retrieved June 1, 2003, from http://www.cio.com/archive/050101/et_pundits_content.html.

Schneier, B. (2000) Secrets & Lies, Digital Security in a Networked World, John Wiley & Sons: New York, 105.

Stevens, M. (2002, Dec. 16) "Job: Security." eWeek. Retrieved June 1, 2003, from http://www.eweek.com/article2/0,3959,795963,00.asp.

Sullivan, B. (2002, Nov. 25) "Huge Identity Theft Ring Busted." MSNBC News. Retrieved June 1, 2003, from http://www.msnbc.com/news/839678.asp?0cv=CB10.

Verton, D. (2001, Nov. 15) "Users Are the Weakest Link, Security Experts Warn." ComputerWorld. Retrieved June 1, 2003, from http://www.computerworld.com/securitytopics/security/story/0,10801,65745,00.html.

Wharton School. "Could a Cyberterrorist Take Down Your Company?" (2002, Sept. 8) CNET News.com. Retrieved June 1, 2003, from http://news.com.com/2009-12-956901.html.

White House, The. The National Strategy to Secure CyberSpace, (2003, Feb) Retrieved May 31, 2003 from http://csrc.nist.gov/policies/cyberspace_strategy.pdf.

Denise R. McGinnis is a Professor of Accounting and Information Technology at Mesa State College. She joined the faculty in 1993. She has over twenty years of college teaching experience in Computer Information Systems, Mathematics and Quantitative Analysis and ten years experience in database consulting.

Ken Comstock is a senior at Mesa State College in Grand Junction, Colorado, where he is pursuing a Bachelor of Science degree in Computer Information Systems and minoring in Business Administration.