ISSN: 1545-679X

Information Systems Education Journal

Volume 5, Number 39 http://isedj.org/5/39/ December 14, 2007

In this issue:

Thinking Globally: Incorporating an International Component in Information Security Curricula

Garry L. White
Texas State University San Marcos
San Marcos, TX 78666 USA

Ju Long
Texas State University San Marcos
San Marcos, TX 78666 USA

Abstract: With the expansion of globalization, information security has become an international issue. Most of the security breach incidents and cyber crimes can be traced to sources outside the United States. Information systems educators and information system practitioners must consider a multi-cultural environment that arises from global information systems, which goes beyond national judicial boundaries. Based on three pilot surveys we conducted on the contents of information security certifications, curricula, and college text books, we show a general lack of international perspective on information security education and training. The solution to incorporate international components in the information security curriculum must be interdisciplinary. Along with technical and management skills, learners' understanding and knowledge in international laws and policies found in political science are also necessary. Based on this perspective, we propose several essential learning objectives for an international component to be included in information security curricula.

Keywords: international issues, cyber crimes, security curriculum, privacy, ethics, Internet

---

Recommended Citation: White and Long (2007). Thinking Globally: Incorporating an International Component in Information Security Curricula. *Information Systems Education Journal, 5* (39). http://isedj.org/5/39/. ISSN: 1545-679X. (Also appears in *The Proceedings of ISECON 2006:* §2324. ISSN: 1542-7382.)

This issue is on the Internet at **http://isedj.org/5/39/**

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: 8 Sep 2003. • Title: Information Systems Education Journal. Variants: IS Education 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)

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.

Thinking Globally: Incorporating an International Component in Information Security Curricula

Garry L. White
gw06@txstate.edu

Ju Long
jl38@txstate.edu
Department of CIS & QM
Texas State University – San Marcos
San Marcos, TX 78666 USA

ABSTRACT

With the expansion of globalization, information security has become an international issue. Most of the security breach incidents and cyber crimes can be traced to sources outside the United States. Information systems educators and information system practitioners must consider a multi-cultural environment that arises from global information systems, which goes beyond national judicial boundaries. Based on three pilot surveys we conducted on the contents of information security certifications, curricula, and college text books, we show a general lack of international perspective on information security education and training. The solution to incorporate international components in the information security curriculum must be interdisciplinary. Along with technical and management skills, learners' understanding and knowledge in international laws and policies found in political science are also necessary. Based on this perspective, we propose several essential learning objectives for an international component to be included in information security curricula.

Keywords: International Issues, Cyber Crimes, Security Curriculum, Privacy, Ethics, Internet

1. INTRODUCTION

The Internet has connected local information systems into a global system, which goes beyond nations' judicial boundaries. Hence, businesses that use the Internet now operate on an international level (Oz, 1994). Information security educators and practitioners must consider a multi-cultural environment that arises from global information systems. There are differences in cultures and values, laws and ethics. This leads to new international security issues and problems. For example, a major issue for global business security is privacy (Chandran et al., 1987; Zuckerman, 2001). Different countries may have different privacy definitions and laws (Milberg et al., 2000; Zuckerman, 2001). In one country, the individual owns the personal data; while in another country, it may be the collector or the government who owns the personal data. Different countries may also have different levels of security technologies. Some countries may have more advanced technologies, while other countries' information technologies may lag behind. Such is the case with Chinese companies. They are experiencing more attacks and lack sophisticated software to defend their computer systems (D'Antoni, 2005). This can be of concern for the USA businesses that outsource to China.

There are issues of different privacy laws, security risks in foreign outsourcing, and security risks in doing business with foreign companies. There maybe a lack of enforcement in many countries and the information

security professional can do nothing. However, the information security professional needs to be able to point out the risks and options to management before a decision is made to do business overseas. The international perspective does little to prevent attacks and spam. But the knowledge of the problems and risks can impact business decisions. Therefore, our proposed content focuses on external considerations and foreign security risks.

Our research is set to address these challenges that globalization has brought to the information security education. We propose that information security educators incorporate an international component into the information security curriculum. We first examine the transnational nature of information security issues and the imperative needs to think globally when teaching information security. We then examine the global components in current information security education and training. Our examination is based on an empirical content analysis of sampled current curricula, textbooks and certifications. We conclude that there is a general lack of international perspective in current curricula. We then propose our solutions by introducing new topics on global information security issues in the information security curriculum design.

2. INFORMATION SECURITY: A GLOBAL CHALLENGE

In this section, we focus on the reasons why we need to incorporate a strong and clear global perspective into computer information security curriculum. We base our arguments in the following reasons.

First, most of the security breach incidents and cyber crimes can be traced to the sources outside the U.S. We will use detailed and up-to-date data to show the severity of this phenomenon. This makes the computer information security an ever more urgent global issue.

Second, unlike the physical world, the Internet is without national boundaries. This very nature of cyber space consequently defined that the attacks and crimes committed in it are not confined to a single country or region. The nature of cyber crimes are often transnational and across multiple national territories.

Finally, in order to prosecute the attacks, we need a global collaboration platform. It should include multiple countries and regions to form strong allegiances and adapt international laws and policies to fight against cyber crime. Moreover, to prevent these attacks, same collaboration among nations should also be crucial.

Computer Security Attacks Become More International

In the months from July to December in 2005, countries other than the U.S originated nearly 70% percent of the cyber attacks, increasing from 42% in the previous six months (Symantec, 2006a). More than two thirds of these attackers were from international sources. In the U.S. government sector alone, for example, attacks from foreign countries accounted for nearly 45% of the total incidents detected by the government security sensors in 2005 (Symantec, 2006b). This data strongly indicates that attack activity is becoming more international. It also shows the urgency to broaden our curriculum and study the security issues from a global perspective.

The security threat from abroad is only going to get more serious as the globalization expands to more countries. For example, China saw the largest overall increase in originating attacks; such attacks increased by 153% over the last period, compare with the global average of 81% (Symantec, 2006a).

Examining the sources of the frequently used attack methods, we could see that most of these attacks could be traced to foreign countries. In terms of the bot-infected computers (A bot is a software agent that was installed secretly by an attacker on a computer to make it part of a computer network. The attackers could use the network of these bot-infected computers to launch vicious attacks), the countries outside the U.S. have nearly 75% of the world's bot-infected computers at the end of 2005 (Symantec, 2006a). During the last six months of 2005, Denial of Service (DoS) attacks originated from outside the U.S. accounted for nearly 70% of the total attacks (Symantec, 2006a). During the same period, about 44% of all spams detected worldwide originated in the countries outside the United States (See Table 1) (Symantec, 2006a). In terms of country of origin, most phishing

fraud originated from the United States, South Korea, China, and Taiwan (APWG, 2006).

Country	July–Dec 2005	Jan–June 2005
United States	56%	51%
China	12%	5%
South Korea	9%	14%
Canada	7%	7%
Belgium	4%	3%
United Kingdom	3%	2%
Japan	3%	2%
France	2%	2%
Remaining EU countries	2%	n/a
Spain	2%	1%

Table 1: top 10 countries of spam origin

Source: Symantec Corporation (Symantec, 2006a).

The nature of the Internet is intrinsically transnational

The Internet—and Internet-based crimes—renders national borders essentially invisible. Such an intrinsic nature of the Internet makes the cyber crimes spreading at a global level effortlessly. In the virtual world, there are no clear judicial boundaries between nations; nor border patrols or customs. Anyone with a computer and an Internet connection could roam from this country to another with one mouse-click. This borderless characteristic of the cyber space makes it very attractive for criminal activity. When authorities attempt to police this virtual world, however, borders and national jurisdictions loom large -- making extensive investigation slow and tedious, and many times, almost impossible (Ferrell, 2004).

Cyber crimes, like any other crime, often breed from those countries or regions that have weak capacity to enforce the law (Williams, 2001). After the "I Love You" virus rampaged through the planet and cost business billions of dollars, the FBI finally identified the attacker as a student in the Philippines. But because there was no law to prosecute such crimes in Philippine at that time, the FBI could not do anything with the attacker (Sofaer and Goodman, 2006). Even worse, new developing countries, such as China and South Korea, are motivated to create better investment environment and attract more business. They might intentionally take a permissive attitude toward information law enforcement. For example, China has been a hot spot of Bot-controlled network. One of the reasons is the fast development of broad-band Internet in that country while at the same time; it does not have the equivalent law enforcement to match the infrastructure development.

Cyber crimes and security threats are innately a global issue

When attackers launch their attacks, the first thing they do is to disguise their true identity. To do that, they frequently hop through numerous systems or use previously compromised systems to obscure their locations prior to launching the actual attacks. Many of the Bot network owners attack computers outside their own countries of residence simply to disguise their identity. By relaying the commands through computers in different countries, they can make it more difficult for the law enforcement to track them down. By doing that, these attackers also take advantage of the differences between national laws and enforcement, always targeting the more vulnerable countries with less prosecution power. For instance, in a recently DoS attacks, an attacker in South Korea launched a DOS attack from an infected system located in Taiwan against a Web application server in Europe (Ferrell, 2004). Evidences also show that many phishing attacks are well-coordinated network of criminals located in various countries. It was discovered that zombie computers located in another country can be used to launch phishing attacks without revealing the attacker's identity (APWG, 2006).

Fighting cyber crime needs global collaboration

In order to fight against cyber crimes, collaboration on a global platform is necessary. Countries need to have laws and policies, including extradition and mutual legal assistance treaties (MLATs), that allow governments to share information and evidences with each other (Williams, 2001). Besides appropriate laws, it is also important that governments and law enforcement agencies develop the capacity to implement these laws. Each country should establish and train specialized units that flight against cyber crimes. They can act as the liaison be-

tween the countries for international cooperation and collaboration (Williams, 2001). . The other important component of a strategy to combat cyber crime is partnership between governments and industry, especially the information technology sector (Williams, 2001). The European Union (EU) has already taken a very promising initiative towards the international cooperation on fighting cyber crimes, such as increasing the collaboration efforts, recognizing the value of fostering co-operation, and adopting appropriate legislation (Council of Europe Cybercrime Treaty).

In summary, because of the transnational nature of cyber crimes, to fundamentally understand cyber security, the challenges and the strategies; we need to adopt an international perspective in our education curriculum. The students are going to be the future IT managers, CTOs and CIOs. If they lack the insights from a global perspective when dealing with information security, they could blind themselves to the true nature of cyber crimes, let alone fight against it.

3. LACK OF AN INTERNATIONAL PERSPECTIVE IN CURRENT CURRICULA AND TRAINING IN INFORMATION SECURITY

While the need to incorporate a global perspective in the information security education is imperative, such an international component has been generally missing in current curricula and training materials. Our conclusion is drawn from our empirical sampled survey of the contents of current information security certifications, textbooks and curricula.

Appendix B shows a survey of 7 security certifications. These certifications in information security only dealt with corporate and local security issues and local security systems. Like the college textbooks and curricula, which will be discussed later, these certifications show what knowledge is expected from the current information system security practitioners. Based on our survey, we find that there is a serious lack of international component requirement in these certifications. Only the domestic issues and laws and ethics of the United States were included and required. The CISSP did include some international topics, but were mostly with the European Union.

The industry and vendor certifications were primarily technical in nature. The focus was how to protect the computer information system by using the vendor's product. Vendor and industry certifications, such as Security+, fail to address international issues, too.

Another indication of corporations lacking a global perspective on information security is from a survey of 2,540 U.S.A. information technology and security professionals. The survey focused on protecting internal computer systems (Claburn, 2005). It did not mention any international issue. To protect the enterprise data system with a single vision on the corporate itself is not enough. Corporation information system executives and practitioners need to take into consideration the threats from outside the corporate world and from the international sources. We could start to increase such awareness by incorporating international components into our curricula when educating our future corporate executives. However, this solution appears to be also lacking in our current curricula.

As indicated from two other surveys, there is a lack of international components in college textbooks and curricula that deal with information security issues. Results of these surveys can be found in Appendix A and C.

Appendix A shows the content of 8 college security textbooks. All of them tended to focus on local infrastructure technology and U.S.A. perspective on privacy laws and ethics. Protecting the corporation's information was the main point. What few international contents there were, they mostly dealt with European countries.

Appendix C shows 9 college security curricula. Among the graduate curricula, one is a graduate management and policy course (Carnegie Mellon, 2006). It had some international components, such as cyber-terrorism and international laws, within a security and terrorism course. However, that course was not computer information specific. Its content also included weapons of mass destruction and military response. Another graduate curriculum in Internet Security covered Internet laws from the School of Business Law (Armstrong & Jayaratna, 2002). All undergraduate curricula tended to focus on local management issues and the technology used on local systems. Some of

the undergraduate courses, containing legal issues and ethics, focused mostly on the domestic contents. Two curricula used the CISSP certification as a reference, which also lacks international perspective as we discussed in the previous section (Logan, 2002; Grimaila & Kim, 2002).

4. SOLUTION–THE PROPOSED NEW TOPICS AND LEARNING OBJECTIVES ON INTERNATIONAL INFORMATION SECURITY CURRICULUM

The nature of international information security is interdisciplinary (Surendran et al. 2002). Along with technical and management skills, a background in criminal justice and national/international issues found in political science are needed. The literature has shown the collaboration with Criminal Justice (Surendran et al., 2002; Logan, 2002). Political Science, Criminal Justice, and Business Law departments can provide the necessary resources to meet the needed learning objectives of an international component in an information security curriculum. Based on this multi-disciplinary perspective, we propose several new topics that could be added in the current information security curricula:

1. Introduction on International information security risks.
2. Identify international sources and techniques of cyber-crime and cyber-terrorism
3. Information & privacy laws from foreign countries and how they differ.
4. Various measures and technologies that different governments and foreign agencies are using in fighting international cyber-crime and how they differ.
5. Current international laws and policies on cyber security and how these laws are enforced in different countries.
6. How international organizations, such as U.N. and E.U. are coordinating the global efforts in fighting against cyber-crime and cyber-terrorism
7. The incentives for governments and companies of developing nations to enforce security regulations and policies.
8. The obstacles for governments and companies of developing nations to improve their information security infrastructure.
9. Different cultural values and ethics concerning information security.
10. Introduction on information warfare.

These topics and learning objectives are related to the specific concerns we have addressed in the previous sections. For instance, our second topic on international sources and techniques of cyber crime and cyber terrorism is related to the security attacks we examined before, including DoS attacks and phishing attacks. In addition, we also select several topics on how international organizations and governments could coordinate the global efforts to address the security concerns. It is also in line with our discussion that the international nature of information security calls for collaboration on the global level.

Because this component is multi-discipline and go beyond technical and local management content, a team teaching approach may be in order. To meet these learning objectives, expertise and collaborations from Political Science, Criminal Justice, and Business Law departments are required.

5. SUMMARY

In this research, we propose to add more international issues and global perspectives when teaching information system security, which have been lacking in most of the current curricula. We argue that with the expansion of globalization, information security has become an essentially global issue that is not confined within a single country. Most of the security breach incidents and cyber crimes can be traced to the sources in foreign countries. We emphasize that information systems educators and information system practitioners must consider a multicultural environment that arises from global information systems and incorporate international components in the information security curriculum. We propose a list of multidisciplinary learning objectives that include not only learner's understanding of technical and management issues, but also knowledge in international laws and policies. To our knowledge, our research is among the first to identify the needs to add the international perspective in the IS security curriculum. To IS education research, our study could con-

tribute to the better understanding of how to enhance IS security curriculum. For IS security educators and practitioners, our research provides useful suggestions on how to adapt the curriculum and prepare our learners to meet the security challenges from globalization.

6. REFERENCES

APWG (2006). January Phishing Trends Report, Anti-Phishing Working Group (APWG), March, 2006.

Armstrong, H. & Jayaratna, N. (2002). "Internet Security Management: A Joint Postgraduate Curriculum Design." Journal of Information Systems Education, 13(3), 249-258.

Berinato, S. (2005). "The Global State of Information Security," CIO, Sept. 15, 2005. (Accessed from http://www.cio.com /archive/091505/global.html?action=print on Feb. 27, 2006)

Carnegie Mellon (2006a). "Our Program: MISM = Information Technology + Management + Strategy." http://www.mism .cmu.edu/Information-Systems/Program /curriculum.asp (Accessed on March 29, 2006).

Carnegie Mellon (2006b). "Master of Science in Information Security Policy and Management (MSISPM)." http://www .heinz.cmu.edu/msispm/ (Accessed on March 29, 2006).

Chandran, R.; Phatak, A.; and Sambharya, R. (1987). "Transborder Data Flows: Implications for Multinational Corporations." *Business Horizons,* 30(6), 74-83.

CISCO (2006a). Career Certifications & paths, 642-567 ASFE. http://www.cisco .com/web/learning/le3/current_exams/642 -567.html (accessed on March 3, 2006).

CISCO (2006b). Security Solutions for Systems Engineers http://www.cisco.com/web /learning/le3/current_exams/642-564.html (accessed on March 3, 2006).

Claburn, T. (2005). The Threats Get Nastier. InformationWeek, Aug 29, 2005. (Accessed from http://www.informationweek .com/story/showArticle.jhtml?articleID =170100709 on Feb. 27, 2006)

CompTIA (2006). Security+ Examination Objectives. http://www.comptia.org /certification/Security/Security_Objectives. pdf (accessed on March 3, 2006).

Council of Europe Cybercrime Treaty, Convention on Cybercrime, Budapest, 23.XI.200, http://conventions.coe.int /Treaty/EN /Treaties/Html/185.htm

D'Antoni, H. (2005). IT Security in China shows Cracks. InformationWeek, Oct. 31, 2005. (Accessed from http://www. informationweek.com/shared/printable Article.jhtml?articleID=172901194 on Feb. 27, 2006)

Ferrell, K. (2004). Cybercrime Spins Out Of Control, TechWeb.com, Wednesday, September 22, 2004

Grimaila, M. R. & Kim, I. (2002). "An Undergraduate Business Information Security Course and Laboratory." Journal of Information Systems Education, 13(3), 189-119582.

Hazari, S. (2002). "Reengineering an Information Security course for Business Management Focus." Journal of Information Systems Education, 13(3), 197-204.

Hsu, C. & Backhouse, J. (2002). "Information Systems Security Education: Redressing the Balance of Theory and Practice." Journal of Information Systems Education, 13(3), 211-218.

ICCP (2006). Examination Subject Outlines, Systems Security. http://www.iccp.org /iccpnew/outlines.html#12 (accessed on March 3, 2006).

Internet Security Threat Report: Government Data Sheet, Symantec Corporation, published January, 2006

Kennesaw State University. Information Security Education at KSU. http://infosec .kennesaw.edu/education.html (Accessed on March 29, 2006).

King, T. (2003). Security+. Que Certification Publishing, Indianapolis, Indiana 46240.

Krutz, R. L. & Vines, R. D. (2004). The CISSP Prep Guide, 2nd Ed. Wiley Publishing, Indianapolis, IN 46256.

Lewis University. Masters of Science in Information Security. http://www.lewisu.edu

/academics/msinfosec/curriculum.htm (Accessed on March 29, 2006).

Linkletter, T. (2000). Certified Computing Professional Examination Review Outlines. Institute of Certification of Computing Professionals (ICCP), Des Plaines, Ill 60018.

Logan, P. Y. (2002). "Crafting an Undergraduate Information Security Emphasis within Information Technology." Journal of Information Systems Education, 13(3), 177-182.

Microsoft (2006). Preparation Guide for Exam 70-298. http://www.microsoft.com /learning/exams/70-298.asp (accessed on March 3, 2006).

Milberg, S., Smith, J. & Burke, S. (2000). "Information privacy: Corporate management and national regulation." Organization Science, 11(1), 35-57.

Novell (2006). Novell Training Services Test Objectives. http://www.novell.com /training/testinfo/objectives/770btobj.html (accessed on March 3, 2006).

Oz, E. (1994). "Barriers to international data transfer." Journal of Global Information Management, 2(2), 22-29.

Sofaer, A. D. and Goodman, S.E. (2006). "Cyber Crime and Security." The Transnational Dimension.Hoover Press, http:// www.hoover.org/publications/books/fulltext/ cybercrime/1.pdf (Accessed on May 8, 2006)

Stevens, K. J. & Jamieson, R. (2002). "A Popular Postgraduate Information Systems Security Course." Journal of Information Systems Education, 13(3), 219-225.

Surendran, K. & Kim, K. & Harris, A. (2002). "Accommodating Information Security in our Curricula." Journal of Information Systems Education, 13(3), 173-175.

Symantec Internet Security Threat Report, Trends for July 05–December 05, Volume IX, Published March 2006, https: //enterprise.symantec.com/enterprise /whitepaper.cfm

University of Texas. 2004-2005 Undergraduate Catalog: Bachelor of Business Administration Degree in Infrastructure Assurance. http://www.utsa.edu/ucat /chapter2/BBAIa.cfm (Accessed on March 29, 2006).

Weber State University. Course Listings. http://documents.weber.edu/catalog/ current/catcrs.htm (Accessed on March 29, 2006).

Williams, P. (2001). "Organized Crime and Cybercrime: Synergies, Trends, and Responses, Global issues, arresting transnational crimes." An Electronic Journal of the U.S. Department of State - August 2001 Volume 6, Number 2

Zuckerman, A. (2001). "Order in the courts?" World Trade, 14(9), 26-29.

APPENDIX A

Sampled Survey of 8 college security text books

Whitman, M. E. & Mattord, H. J. (2004). Management of Information Security. Thomson-Course Technology, Boston, Mass 02210.

Covers primarily U.S.A. laws and issues. There is mention of international laws and organizations on one page of the book. Content is awareness of three international organizations dealing with international law; European Council Cyber-Crime Convention, a U.S.A. based effort from the Digital Millennium Copyright Act (DMCA), and the United Nations Charter involving information warfare.

Merkow, M. & Breithaupt, J. (2006). Information Security: Principles and Practices. Pearson-Prentice Hall, Upper Saddle River, NJ 07458.

Deals with more management issues for a corporation. The Laws, Investigation, and Ethics chapter does have one page on International Privacy Issues. It covers the European Union and the U.S.A. work on Safe Harbor Privacy Principles. The chapter covers a U.S.A. perspective on privacy laws and ethics.

Ciampa, M. (2005). Security+ Guide to Network Security Fundamentals, 2nd ed. Thomson-Course Technology, Boston, Mass 02210.

Covers local system technology and network administration. There is no coverage of international issues and laws.

Whitman, M. E. & Mattord, H. J. (2005). Principles of Information Security, 2nd ed. Thomson-Course Technology, Boston, Mass 02210.

Stresses relevant U.S. laws. The Legal, Ethical, and Professional issues chapter does have three pages on international issues. European Council Cyber-Crime Convention and the United Nations Charter involving information warfare. There are two paragraphs dealing with ethical differences across cultures.

Volonino, L. & Robinson, S. R. (2004). Principles and Practice of Information Security. Pearson-Prentice Hall, Upper Saddle River, NJ 07458.

Deals with liabilities, risk management, policies, privacy, laws. Topics included USA Patriot Act, USA Health Insurance Portability and Accountability Act, and U.S.A Federal statutes. Coverage of international issues and laws was not found.

Panko, R. R. (2004). Corporate Computer and Network Security. Pearson-Prentice Hall, Upper Saddle River, NJ 07458.

Content is from a U.S.A. perspective of laws and privacy. There is a section on cyberwar and cyber terror. However, content is generic and lacks references to international issues.

Easttom, C. (2006). Computer Security Fundamentals. Pearson-Prentice Hall, Upper Saddle River, NJ 07458.

This book is technical oriented and presents a U.S.A. perspective on Internet fraud, cyber stalking, and laws. Of 5 cases presented on industrial espionage, only one involved an international incident. The rest were all U.S.A. incidents.

Solomon, M. & Chapple, M. (2005). Information Security Illuminated. Jones & Bartlett Publishers, Sudbury, Mass.

This book stresses local management and protection of network systems. There is no coverage of international issues and laws.

APPENDIX B

Sampled Survey of 7 Security Certifications

PROFESSIONAL

Certified Information Systems Security Professional (CISSP) by the International Information Systems Security Certification Consortium.

One of the Domains of the common body of knowledge for the CISSP is Law and Ethics. The content focuses on U.S.A laws, regulations, and directives. CISSP does include some international topics with the Europe Union. Ethics is covered with generic codes of conduct and guide lines from the U.S. Department of Health, Education, and Welfare Code of Fair Information Practices (Krutz & Vines, 2004, p. 421, 424-432, 441).

Certified Computing Professional (CCP), Systems Security specialty by the Institute of Certification of Computing Professionals.

The specialty exam Systems Security for the CCP covers local management issues and local systems. This is no indication of international issues or Internet issues in the subject outline (ICCP, 2006; Linkletter, 2000).

INDUSTRY

Security+ by CompTIA.

The Security+ certification is similar to the ICCP Systems Security specialty exam. It covers local management issues and local systems. This is no indication of international issues or Internet issues in the subject outline (King, 2003; CompTIA, 2006).

VENDOR

Designing Security for a Microsoft Windows Server 2003 Network (Exam 70-298) by Microsoft (Microsoft, 2006)

Internet Security Management with Border Manager (Exam 050-650) by Novell (Novell, 2006).

Advanced Security for Field Engineers (Exam 642-567) by CISCO (CISCO, 2006a)

Security Solutions for Systems Engineers (Exam 642-564) by CISCO (CISCO, 2006b).

These four vendor security exams all focus on the technology of the vendors' product. Like the CompTIA Security+ and the CCP Security specialty, they cover local management issues, technology, and local systems. This is no indication of international issues or Internet issues in the subject outlines.

APPENDIX C

Sampled Survey of 9 College Security Curricula

Carnegie Mellon, Pittsburgh, PA

This institution offers two Information Systems Masters degrees; the Masters of Information Systems Management and the Master of Science in Information Security Policy and Management. The first Masters degree has an Information Security Management specialist concentration. It lacks any international components (Carnegie Mellon, 2006a). Its' focus is local infrastructure technology. The second Masters is not an information systems degree. However it contains one elective course dealing with cyber-terrorism (Carnegie Mellon, 2006b). The course is: 90-712, National Security and International Terrorism Law and Policy.

University of Texas, San Antonio, TX

The Bachelor of Business Administration Degree in Infrastructure Assurance lacks a course with an international component. The focus is on protecting the business infrastructure. (University of Texas, 2004-2005)

Weber State University, Ogden, UT

The Information Systems & Technologies Bachelor Degree has two security courses: IST 4600 Information Security I and IST 4700 Information Security II. The course descriptions/objectives lack any international component (Logan, 2002; Weber State University, 2006).

Texas A&M University, College Station, TX

Information Assurance and Security (IAS) curriculum has one undergraduate course on information security. The lecture outlines indicate no international component. The focus of the course is to protect the internal system. (Grimaila & Kim, 2002)

University of Maryland, College Park, MD

IS curriculum has an elective course called BMGT727: Security and Control of Information Systems. Its content closely follows the Price Waterhouse Coopers (PWC) Enterprise Security Model and the Certified Information System Professional (CISSP) Common Body of Knowledge. The course and PWC model focus on the protection of the internal system. A reference in the article describing the course is made to the World Trade Center attacks for the purpose of stressing system recovery plans. There appears to be no international component other than what is covered in the CISSP. (Hazari, 2002).

University of New South Wales, Sydney, Australia

IS curriculum has an elective course called INFS5984: Information Systems Security. The course objectives and syllabus for 2001 focus on the protection of the internal system. There are topics of legal and ethical issues. However, no international component was found. (Stevens & Jamieson, 2002).

Curtin University of Technology, Western Australia

A postgraduate curriculum in Internet Security Management has an Internet Law course from the School of Business Law. This course covers critical issues in national and international law. (Armstrong & Jayaratna, 2002).

Lewis University, Romeoville, IL

The Masters of Science in Information Security lacks a course with an international component. Focus is on protecting the business infrastructure. The courses are primarily technical. (Lewis University, 2006).

Kennesaw State University, Kennesaw, GA

Course descriptions for a BS in Information Security and Assurance indicate no international component. Focus is on technical aspects of the information systems. (Kennesaw State University, 2006).