Submission to the

5th National Colloquium for Information Systems Security Education

May 22-24, 2001-03-28

TITLE: **Information Security Education Resources for Professional Development**

AUTHOR: **M. E. Kabay, PhD, CISSP**

Security Leader, INFOSEC Group, AtomicTangerine, Inc.

255 Flood Road

Barre, VT 05641-4060

V: 802-479-7937

F: 802:479-1879

E: mkabay@atomictangerine.com

SPEAKER: Patricia Gilmore, CISSP

Cyberdean, Information Security University, AtomicTangerine Inc.

149 New Montgomery Street, 2nd Floor

San Francisco, CA 94105

V: 415-901-4903

F: 415-901-4885

E: pgilmore@atomictangerine.com

ABSTRACT

Many information technologists and others are interested in learning about information security. Some people want to teach themselves about the field; others are willing to take courses from academic centers.

This paper reviews a range of options for anyone seeking knowledge of INFOSEC. The format uses questions similar to those that practitioners may receive from correspondents. Topics include helpful books for beginners, courses (live, computer-based and Web-based), videos, associations, conferences, certificate programs and academic programs. The author hopes that the questions, answers and appendices containing specific recommendations and sources will be helpful to all INFOSEC educators.

Information Security Education Resources for Professional Development

1 Introduction

With the growing visibility of information security in today's hacker-beset e-commerce world, many people are becoming interested in careers as information security specialists. All indications are that there aren't enough people with security knowledge and skills to fill all the open positions; as a result, salaries have been rising steadily in the industry. This article looks at some frequently-asked questions and provides pointers for knowledge-hungry readers. Readers should note that (1) these questions are not necessarily quoted from specific people – some are amalgamss of queries from different people; (2) opinions in this article do not represent endorsement by the author's employer or associated institutions; (3) exclusion does not imply criticism – I had to stop somewhere.

2 Q: "I've been using computers since I was a two and have been hacking into systems ever since I was eight. I'm thirteen now. How can I earn a living hacking?"

A: Sorry, but you're asking the wrong question, son. Information security is *not* primarily about hacking. Penetration testing and technical vulnerability analysis are tools, not goals, of information security professionals. Contrary to the myths perpetuated by criminal hackers, learning to hack into other people's systems without permission is *not* a sound approach to becoming such a professional. Information security is about protecting confidentiality, possession or control, integrity, authenticity, availability and utility of information and information systems. If you'd like to find out more about the foundations of security, read "Why Kids Shouldn't Be Criminal Hackers" http://www.securityportal.com/kfiles/files/kidcriminals.html which is aimed at young people (and their parents and teachers) or anyone interested in finding out what information security is really about.

Some young people are trying to make a living through theft, fraud and extortion; they are stealing credit-card numbers, engaging in pump-and-dump stock fraud, and threatening to reveal stolen information unless they are paid by their victims. Increasingly, victims are turning to law enforcement to find the perpetrators of such crimes, and the victimizers are being caught, tried and sentenced. Nobody with any sense will advise a kid to become a criminal, so be suspicious of the people you meet at hacker meetings and conventions when they pretend that criminal hacking will give you a bright future.

Security today involves a wide range of challenges including a grasp of business and management issues, good interpersonal skills, and a thorough grounding in the technology of computing and networking. Although the media celebrate notorious criminal hackers such as Kevin Mitnick, and although some companies even hire hackers (convicted or not) with a limited

grasp of professional ethics, by far the majority of people involved in securing computers and networks are honest folk who have never used other people's computing resources without permission.

You will be able to earn a living using your computing skills, including perhaps working in penetration analysis, by reading widely, getting a solid education with plenty of technology courses but also lots of humanities courses too, and by focusing on how you can help people protect their privacy and prevent damage from intruders or malicious software. If you decide to join the military, you can aim for the technically-demanding positions and maybe get involved in information warfare studies and practice.

You want to be a successful human being who works in security? Get involved in all kinds of good activities; make friends with a wide variety of people; keep up with (or get ahead of) your schoolwork; learn to read and write quickly and well; read about computers and security; and most of all, learn to think both critically and with imagination. Then you can be whatever you want to be – including a security expert, if that's what you decide on.

3 Q: "I've seen some neat videos like *War Games, Sneakers, The Net* and *The Matrix* and I really like computers. I'm fifteen now and I think I'd like to learn more about information security and see if I'd be interested in pursuing this as a career."

Movies don't have very much to do with reality. Contrary to the images you see, computers don't normally have banks of tape drives moving back and forth continuously, nor do programs written for PCs run equally well on mainframes (or, for that matter, on computers running alien spaceships). Criminal hackers don't necessarily live in palatial apartments, have state-of-the-art computers, or consort with nifty friends wearing scanty clothing. But you can certainly learn a lot about computers and security at your age. Appendix 1 is a list of some entertaining URLs and books that will give you a sense of what's involved in security and get you into reading more serious books if you remain interested.

4 Q: "I'm just beginning my university education and I think I would like to work in the information security field some day. What courses should I take?"

In general, a computer science or management information systems degree with as many security courses as were offered plus extensive reading will help you get a job in information security when you graduate. There are so few people interested in the field that we are much in demand.

Ideally, you would develop a strong background in computer science, engineering and other "hard" disciplines. The obvious choices for training include (but are not limited to) logic, programming, operating systems, data structures, quality assurance, cryptography, data communications, information systems management and other information security courses that are offered by your school or by nearby schools (find out about away terms). You will

also find courses in probability and statistics, psychology, English, at least one foreign language, philosophy, ethics, and history valuable in general in life and in particular in security.

Many contributors to information security have law degrees; because of widespread public concern about privacy, many attorneys are deeply involved in privacy issues.

A wide range of experience can stimulate you to come up with novel solutions to problems you will encounter in your security career; the "soft" courses (history, etc.) will give you perspectives that will help you understand people's motivations and the social factors that influence behavior – and understanding and modifying human behavior is one of the core concerns of security today.

You can usually discuss assignments with your teachers and see if you can work in some element of information systems or information security into your projects. For example, you might put together interesting term papers on, say, the history of cryptography, social psychology and corporate culture change, or ethical reasoning among members of the local criminal-hackers' club. In your programming courses, perhaps your projects can involve cryptography and cryptanalysis; in your networking classes, perhaps you can write a paper on, say, public-key infrastructure. Your operating-systems theory course can give you a chance to study the security kernel of various OSs in more detail than the lectures provide.

5 Q: "After five years in the US Air Force, I took advanced courses in computing when I went to university and then took a masters degree in computer science (I worked on artificial-intelligence systems). Later I worked in a manufacturing company doing real-time process control and then moved to a hospital where I helped design a medical-records system. In my current job, I'm doing project management for a group developing a wireless network application for the construction industry. I enjoy your magazine and find that whenever security is mentioned I seem to get interested and excited about it; is it too late for me to move into information security as a career?"

A: Not at all. An individual's wide experience, such as yours, is a good start for a productive shift into informational security. One of the dynamic aspects of INFOSEC that makes practitioners so interesting is our diversity. This is also true of how an individual can approach their pathway to learning; creativity in how one approaches learning can help tremendously and offer great rewards.

Many security experts begin their careers in the military by volunteering or applying for training and positions in SIGINT, INTEL, COINTEL, PSYOPS and military police. Other individuals pursue internships locally, as was the case with one of the authors (PSH). In this particular instance, Holt spent eight months as a member of the security group at large Internet service provider. This experience was rewarding and served as a solid stepping stone into INFOSEC. Some take on security responsibilities as part of system and network operations or management;

others come from the administrative side rather than the technical side. Kabay, for example, began working with security issues when he was involved in systems engineering for Hewlett-Packard in 1980 and then had to apply his knowledge when he ran technical support at a large computer-services bureau. Many security personnel have extensive backgrounds in Unix, Windows or mainframe-based systems administration; some also have years of experience in information-systems consulting. Such experiences lay a solid foundation on which the INFOSEC specialist can build a comprehensive set of tools and real-life working experience.

6 Q: "I've been working with computers as an operator, a programmer and a network administrator for the last ten years. Lately I've been helping more and more with the security functions and I'm getting interested in concentrating in this area. Can I read up about the subject to improve my technical knowledge and skills?"

Definitely. You can always search the online booksellers (e.g., http://www.amazon.com or http://www.bn.com) for keywords of interest. Appendix 2 is a list of some more advanced books that I recommend; some of the older ones are out of date but may be available in your local public or academic libraries or from booksellers specializing in remainders.

7 Q: "I need to know more about securing our LAN, our Web site and our e-commerce business. Are there any on-line or CD-ROM courses I could take to increase my knowledge of information security in general?"

There certainly are. Appendix 3 lists a number of courses and videos of value for trainers and training.

8 Q: "What about courses on securing our operating and network systems in particular? Or about specific firewalls, intrusion-detection systems and access-control products?"

Your best bet is to go to the Web site run by each vendor. Many vendors have decreased their technical support costs by providing computer- or Web-based training modules for their specific products. In addition, major training vendors often include platform- or product-specific live training in their offerings. Finally, some conferences include platform-specific training among the workshops and seminars. See also the *Step-by-Step Guides* from SANS http://www.sans.org/newlook/publications/index.htm for information on Windows NT, Solaris and Linux security.

9 Q: "Could you recommend some good live classes we could send our staff to so they can improve their information security skills?"

There are lots of possibilities. Some involve local colleges and universities; others are presented by various companies and institutes. In addition to regularly-scheduled classes from training groups, there are often excellent one- or two-day workshops associated with conferences. Several of the organizations listed in Appendix 4 can bring their courses to your site to save

travel expenses; you'll have to look at the costs of in-house training to determine the break-even number of participants.

10 Q: Are there any associations I could join to help me progress towards my goal of becoming an information security specialist?

Indeed, and participating in professional organizations is an excellent and inexpensive way of furthering your information security interests. Many of these organizations have regular (often monthly) meetings at modest cost (often in the $25 range) and usually have several dozen to a hundred participants. This intimacy offers a great opportunity to get to know your colleagues (or future colleagues) and to ask questions, learn from their experience, and get friendly guidance and pointers from more experienced security professionals. Another way of learning is to write newsletter articles or to present lectures on specific topics – organizing knowledge so you can help colleagues learn is an excellent way of acquiring and consolidating your own knowledge.

Some of the key associations are listed in Appendix 5.

11 Q: "Ever since I signed up to receive your magazine, I keep getting all sorts of fliers about conferences. Some of my co-workers tell me conferences are a waste of time and that all you hear is a bunch of salespeople talking about how great their products are. Do you think there's any point in going to security conferences?"

Oh definitely. Conferences provide an incredible value for the money, since you can pick lectures, workshops and even entire courses to meet your specific needs. But most important is the mental stimulation you can derive from listening to world-famous experts telling you about the latest issues they, their colleagues, their clients and *you* are facing in various facets of security.

Take advantage of the introduction sessions offered at many conferences; you will learn to make the best possible use of your time by knowing how to interpret the conference catalog, take advantage of special events, and make your way around the facilities – which are sometimes so huge as to be intimidating to novices.

As for salespeople, you will meet many excellent product representatives in the associated floor shows at many conferences; don't sneer at these people: they can be very useful to you by answering specific product-related questions. Many of them are at least as knowledgeable as their clients. Take advantage of the product displays; you can often save a great deal of time when you are shopping for possible solutions, and even if you're not, you may get some ideas that can help you solve some of the practical problems you and your colleagues are facing in your work.

12 Q: "Which security conferences do you think are worth going to?"

A: Which type of hand-tool do you think is worth having? Can't answer that, eh? You need to specify *for what* whenever you try to decide among tools – and conferences. Some

conferences cater to technical specialists interested in securing particular platforms; others to security experts wishing to exchange the most recent research results. Some are of general interest to all security experts. Appendix 6 is a short list of some of the top events.

13 Q: "I left college half-way through twenty years ago because I got married and had a baby. I always wanted to finish my degree – I always got really good grades -- but felt I also wanted to stay home for my daughter. Now, though, my husband and I have decided that it's the right time for me to go back to university and finish my degree. My husband telecommutes and is really supportive, so we can move anywhere we like in the USA. I know I want to work in the information security field, so can you tell me where I could get a degree in the subject?"

In alphabetical order, Appendix 7 provides some brief descriptions of major colleges and university centers offering degrees with specialization in information security. The asterisks (*) indicate *Centers Of Academic Excellence In Information Assurance Educatio*n designated by the US National Security Agency (NSA); see http://www.nsa.gov/isso/programs/coeiae/index.htm for details of the National INFOSEC Education and Training Program (NIETP).

14 Q: "Are there information security programs outside the USA? I live in England / Europe / Asia / Australia and would like to pursue a degree in INFOSEC."

Yes, there are several recognized centers of information security education you should consider. However, before deciding to take advanced training abroad, it is wise for US students to check with the institutions where they intend to study or work after their foreign study to see if foreign academic credentials will be accepted. Appendix 8 is a short list of some non-US options.

15 Q: "I used to be what you keep referring to as a criminal hacker, although I have never thought of myself as a criminal. I've already been turned down by several firms who found out that I was convicted of hacking under the Computer Fraud and Abuse Act (18 U.S.C. §1030). How can I convince these idiots that it's over now and that I'd make a great employee?"

Well first you might lose the nasty attitude. If you penetrated other people's systems without permission then you *were* engaging in criminal activity, and your conviction simply confirmed that you *were* a criminal. Calling people idiots is hardly the way to convince anyone that you have changed your mind about the wisdom of violating the law – and normal rules of civility. Yes, some criminals can truly change; others can't. It's going to be a challenge for you to demonstrate that you don't intend to betray your employers and your clients in the same ways that you betrayed others in your youth. Being honest about your past is a first step. Abandoning your pride in hacker handles is another; I recall a candidate for a job in a security firm who refused to agree to stop writing under his hacker name and insisted that he had the right to

continue participating in criminal-hacker conferences and news groups. He certainly had the right, but the firm also had the right to refuse to hire him.

16 Q: "How do you suggest that I keep up with developments in the field of information security?"

Paper publications not only have useful technical articles, they also often include news summaries, industry news, and useful advertisements. In addition, there are hundreds of security-related USENET groups; however, unmoderated lists have such low signal-to-noise ratios (the average signal-to-noise in specific news groups sometimes falls as low as 5%) that interested readers should find out about them and evaluate them for themselves.

Appendix 9 lists some useful INFOSEC publications, both paper and electronic.

17 Q: "I've seen people like you put letters after their names like CISSP and CISA. What do they mean and what good are they?"

Certification is a useful milestone in professional development. It tells colleagues and potential employers that you take your profession seriously and are willing to abide by the code of professional ethics associated with each designation. There is a list of articles about security certification at http://www.isc2.org/newscissparticles.html . Some of the more important certifications for information security specialists are described briefly in Appendix 10.

Appendix 1. Books and Other Resources for Beginners in INFOSEC.

Campen, A. D., D. H. Dearth, & R. T. Goodden, eds. (1996). *Cyberwar: Security, Strategy, and Conflict in the Information Age.* AFCEA International Press (Fairfax, VA). ISBN 0-916159-26-4. vii + 296.

Fialka, J. J. (1997). *War by Other Means: Economic Espionage in America.* W. W. Norton (New York). ISBN 0-393-04014-3. xiv + 242. Index.

Forester, T. & P. Morrison (1990). *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*. MIT Press (Cambridge, MA). ISBN 0-262-06131-7. vi + 193. Index.

Freedman, D. H. & C. C. Mann (1997). *@Large: The strange case of the world's biggest Internet invasion.* Simon & Schuster (New York). ISBN 0-684-82464-7. 315 pp. Index.

Garfinkel, S. (2000). *Database Nation: The Death of Privacy in the 21st Century.* O'Reilly (Sebastopol, CA). ISBN 1-56592-653-6. vii + 312. Index.

Goodell, J. (1996). *The Cyberthief and the Samurai: The True Story of Kevin Mitnick--and the Man Who Hunted Him Down.* Dell (New York). ISBN 0-440-22205-2. xix + 328.

Gordon, S. (1993). Inside the mind of Dark Avenger (abridged). Originally published in *Virus News International* (January 1993). http://www.research.ibm.com/antivirus/SciPapers/Gordon/Avenger.html

Gordon, S. (1994). Technologically enabled crime: Shifting paradigms for the year 2000. Originally published in *Computers and Security.* http://www.research.ibm.com/antivirus/SciPapers/Gordon/Crime.html

Gordon, S. (2000). Virus writers: The end of innocence? Presented at the 10th International Virus Bulletin Conference. http://www.research.ibm.com/antivirus/SciPapers/VB2000SG.htm and http://www.research.ibm.com/antivirus/SciPapers/VB2000SG.pdf

Hafner, K. & J. Markoff (1991). *Cyberpunk: Outlaws and Hackers on the Computer Frontier.* Touchstone Books, Simon & Schuster (New York). ISBN 0-671-77879-X. 368. Index.

Kabay, M. E. (2000). Making ethical decisions: A guide for kids (and parents and teachers too). http://www.securityportal.com/kfiles/files/ethicaldecisions.html

Littman, J. (1996). *The Fugitive Game: Online with Kevin Mitnick--The Inside Story of the Great Cyberchase*. Little, Brown and Company (Boston). ISBN 0-316-5258-7. x + 383.

Power, R. (2000). *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace.* Que. ISBN: 0-78972-443-X. 450 pp.

Schwartau, W. (1991). *Terminal Compromise* (novel). Inter.Pact Press (Seminole, FL). ISBN 0-962-87000-5. 562 pp.

Shimomura, T. & J. Markoff (1996). *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw--by the Man Who Did It.* Hyperion (New York). ISBN 0-7868-6210-6. xii + 324. Index.

Slatalla, M. & J. Quittner (1995). *Masters of Deception: The Gang that Ruled Cyberspace.* HarperCollins (New York). ISBN 0-06-017030-1. 225 pp.

Smith, G. (1994). *The Virus Creation Labs: A Journey into the Underground*. American Eagle Publications (Tucson, AZ). ISBN 0-929408-09-8. 172 pp.

Sterling, B. (1992). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. Bantam Doubleday Dell (New York). ISBN 0-553-08058-X. xiv + 328. Index.

Stoll, C. (1989). *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.* Pocket Books (Simon & Schuster, New York). ISBN 0-671-72688-9. viii + 356.

Winkler, I. (1997). *Corporate Espionage: What it is, why it is happening in your company, what you must do about it.* Prima Publishing (Rocklin, CA). ISBN 0-7615-0840-6.

Appendix 2. More Advanced Reading in INFOSEC.

Allen, J., A. Christie, W. Fithen, J. McHugh, J. Pickel, E. Stoner (2000). *State of the Practice of Intrusion Detection Technologies.* CERT-CC http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028abstract.html and PDF file at http://www.sei.cmu.edu/pub/documents/99.reports/pdf/99tr028.pdf

Amoroso, E. & R. Sharp (1996). *PCWEEK Intranet and Internet Firewall Strategies: Identify Your Security Requirements and Develop a Plan to Protect Your Information.* Ziff-Davis Press (Emeryville, CA). ISBN 1-56276-422-5. xxi + 218.

Anonymous (2000). *Cyberliability: An Enterprise White Paper.* Elron (Burlington, MA). http://www.elronsoftware.com/enterprise/iupguide.pdf

Anonymous (2000). *Internet Usage Policy Guide.* Elron (Burlington, MA). http://www.elronsoftware.com/enterprise/iupguide.pdf

Bace, R. B. (1999). *An Introduction to Intrusion Detection And Assessment.* http://www.icsa.net/html/communities/ids/White%20paper/index.shtml

Bace, R. B. (2000). *Intrusion Detection.* Macmillan Technical Publishing (Indianapolis, IN). ISBN 1-57870-185-6. xix + 339. Index.

Brownlee, N. & E. Guttman (1998). *Expectations for Computer Security Incident Response.* RFC 2350. http://www.cis.ohio-state.edu/htbin/rfc/rfc2350.html

BSI (1997). *IT Baseline Protection Manual: Recommended Measures to meet Medium-Level Protection Requirements.* Prepared by the Bundesamt für Sicherheit in der Informationstechnik of the German Federal Government. English version at http://www.bsi.bund.de/gshb/english/menue.htm

Diffie, W. & S. Landau (1998). *Privacy on the Line - The Politics of Wiretapping and Encryption. MIT Press (Cambridge, MA).* ISBN 0-262-04167-7. 342 pp.

Felten, E. & G. McGraw (1999). *Securing Java: Getting down to business with mobile code.* John Wiley & Sons (New York). Also free and unlimited Web access from http://www.securingjava.com

Ford, W. & M. S. Baum (1997). *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption.* Prentice Hall (Upper Saddle River, NJ). ISBN 0-13-476342-4. xxv + 470. Index.

Fraser, B. (1997), ed. *Site Security Handbook.* RFC2196 (Network Working Group). http://www.cis.ohio-state.edu/htbin/rfc/rfc2196.html

Garfinkel, S. & G. Spafford (1996). *Practical UNIX and Internet Security, 2nd edition.* O'Reilly & Assoc (Sebastopol, CA). ISBN 1-56592-148-8. xxix + 971. Index.

Garfinkel, S. & G. Spafford (1997). *Web Security and Commerce.* O'Reilly & Assoc (Sebastopol, CA). ISBN 1-56592-269-7. 483 pp. Index.

Hinsley, F. H. & A. Stripp (1993), eds. *Code Breakers: The Inside Story of Bletchley Park.* Oxford University Press (Oxford, UK). ISBN 0-10-820327-6. xxi + 321. Index.

Kabay, M. E. (1995-1999). The INFOSEC Year in Review. http://www.securityportal.com/kfiles/iyir/

Kallman, E. A. & J. P. Grillo (1996). *Ethical Decision Making and Information Technology: An Introduction with Cases, Second Edition.* ISBN 0-07-034090-0. xiv + 138. Index.

Kaner, C., J. Falk, & H. Q. Nguyen (1993). *Testing Computer Software, Second Edition.* International Thomson Computer Press (New York). ISBN 1-85032-847-1. xv + 480. Index.

Khare, R. (1998), ed. *Web Security: A Matter of Trust* [World Wide Web Journal 2(3)]. O'Reilly (Sebastopol,CA). ISSN 1085-2301, ISBN 1-156592-329-4. ix + 272 pp.

Kovacich, G. L. (1998). *The Information Systems Security Officer's Guide: Establishing and Managing an Information Protection Program.* Butterworth Heinemann (Woburn, MA). ISBN 0-7506-9896-9. xv + 172. Index.

Lessig, L., D. Post & E. Volokh (1997). *Cyberspace Law for Non-Lawyers.* Published via e-mail. http://www.ssrn.com/update/lsn/cyberspace/csl_lessons.html

Lessig, L. (1999). *Code and Other Laws of Cyberspace.* Basic Books (New York). ISBN 0-465-03912-X. xii + 297. Index.

Marsh, R. T. (1997), chair. *Critical Foundations: Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection*. See http://www.pccip.gov/info.html for details and ordering information.

McGraw, G. & E. W. Felten (1997). *Java Security: Hostile Applets, Holes and Antidotes -- What Every Netscape and Internet Explorer User Needs to Know.* Wiley (New York). ISBN 0-471-17842-X. xii + 192. Index.

National Computer Security Center (1983-). Rainbow Series (so-called). Monographs on many aspects of information systems security. For an excellent summary of the series and its topics, see Appendix E of Russell & Gangemi (below), p. 359 ff. The series items are available from Director, National Security Agency / INFOSEC Awareness / Attention: X71 / 9800 Savage Road / Fort George G. Meade, MD 20755-6000 / phone 301-766-8729.

National Research Council (1991). *Computers at Risk: Safe Computing in the Information Age.* National Academy Press (Washington, DC). ISBN 0-309-04388-3. xv + 302.

Nichols, R. (1998). *The ICSA Guide to Cryptography.* McGraw-Hill (New York). ISBN 0-07-913759-8. xxxix + 837. Index. CD-ROM.

Parker, D. B. (1998) *Fighting Computer Crime: A New Framework for Protecting Information.* Wiley (NY) ISBN 0-471-16378-3. xv + 500 pp; index

Peltier, T. R. (1998). *Information Security Policies and Procedures: A Practitioner's Reference.* Auerbach Publications (Boca Raton, FL). ISBN 0-8493-9996-3. 250 pp, CD-ROM. $245

Pfleeger, C. P. (1996). *Security in Computing, 2nd ed*. Prentice-Hall (Englewood Cliffs, NJ). ISBN 0-1333-7486-6. 574 pp. Index.

Ranum, M. J. (1996). *Firewalls FAQ*. http://non.com/news.answers/firewalls-faq.html

Rose, L. J. (1994). *NetLaw: Your Rights in the Online World.* Osborne/McGraw-Hill (New York). ISBN 0-07-882077-4. xx + 372. Index.

RSA (1999). *RSA Laboratories' Frequently Asked Questions About Today's Cryptography.* http://www.rsasecurity.com/rsalabs/faq/questions.html

Schneier, B. (1995). *Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition.* John Wiley & Sons (New York). Hardcover, ISBN 0-471-12845-7, $69.95; Softcover, ISBN 0-471-11709-9. xviii + 618. Index.

Schneier, B. (2000). *Secrets & Lies: Digital Security in a Networked World.* Wiley (New York). ISBN 0-471-25311-1. xvii + ~400. Index.

Schwartau, W. (1996). *Information Warfare, Second Edition*. Thunder's Mouth Press (New York). ISBN 1-56025-132-8. 768 pp. Index.

Stallings, W. (1995). *Network and Internetwork Security: Principles and Practice*. Prentice Hall (Englewood Cliffs, NJ). ISBN 0-02-415483-0. xiii + 462. Index.

Stein, L. D. (1998). *Web Security: A Step-by-Step Reference Guide.* Addison-Wesley (Don Mills, ON). ISBN 0-201-62489-9. 448 pp.

Stephenson, P. (1999). *Investigating Computer-Related Crime: A Handbook for Corporate Investigators.* Auerbach Publications (Boca Raton, FL). ISBN 0-849-32218-9. 328 pp. Index.

Tannenbaum, A. S. (1987). *Operating Systems: Design and Implementation.* Prentice-Hall (Englewood Cliffs, NJ). ISBN 0-13-637406-9. xvi + 719. Index.

Tipton, H. F. & M. Krause (2000), eds. *Information Security Management Handbook, 4th edition.* Auerbach (Boca Raton, FL). ISBN 0-8493-9829-0. xiii + 711. Index.

Appendix 3. INFOSEC Learning Aids on CDs, Videos and on the Web

- The CISSP Open Study Guide (OSG) http://www.cccure.org/ is a new collaborative project offering online documentation to help people study for certification as CISSPs (Certified Information Systems Security Professionals).

- Commonwealth Films http://www.commonwealthfilms.com/home.htm makes superb training videos about information and computer security, communication, records, software, workplace laws, sexual harassment, antitrust compliance, depositions, discovery, defense, and compliance with regulatory laws; see MK's review of four information security titles at http://www.securityportal.com/kfiles/files/securityreview.html

- "Dataware™ is an online mini-course that contains the most current and essential elements necessary in order to practice prudent data security, to help avoid security errors and proactively protect a company's information." The Web-based course costs $1 a seat and up and full information is at http://www.itsecurity.com/products/prod311.htm

- George Mason University's Hyperlearning Center http://cne.gmu.edu/ includes many valuable free Web-based courses; the course called "The Core of Information Technology" http://cne.gmu.edu/modules/itcore/ has modules on security at http://cne.gmu.edu/itcore/security/ that cover fundamentals, authentication, encryption, exchange transactions in e-commerce, and digital signatures.

- Organisational [sic] Communications: Security Procedures. This UK course is described as follows: "Your first few days or even weeks in a company can be a confusing time. You have to learn a lot about the company itself: how it operates, your role and what's expected of you. This course will help you to understand the importance of confidentiality and security in your workplace. It examines what can be stolen from an organisation and what you can do to prevent it. It also outlines ways of protecting the confidential information held electronically by organisations." The full description is available at http://www.xebec-online.com/uk/online/ipages/orgcomms/securityprocedures_enuk.html and information about Xebec Online is at http://www.xebec-online.com/uk/online/online2.htm

- The US National Institutes of Health (NIH) has a Computer Security Awareness Training Web page free for anyone at http://wwwoirm.nih.gov/sectrain/

- Information Security University's online security courses (created by AtomicTangerine Inc. and delivered by SecurityPortal Inc.) are described at http://www.infosecu.com and there are some two free courses available as demonstrations (one on information security fundamentals and the other on privacy). MK is deeply involved in this project as a subject-matter expert and is helping to build a roster of several dozen courses covering information security with four different orientations: beginner, intermediate, advanced and management.

- Purdue University's CERIAS (Center for Education and Research in Information Assurance and Security) http://www.cerias.purdue.edu/ offers free security seminars that are Web-cast in real-time from Lafayette, Indiana from 16:30 - 18:00 (4:30 PM – 6:00 PM)

Eastern Time Wednesdays; see http://www.cerias.purdue.edu/secsem/streaming.php for instructions and links to the schedule of upcoming presentations.

- The System Administration and Network Security (SANS) Institute has a wide range of courses offered at its conferences; see http://www.sans.org/giactc.htm for the home page of the Global Incident Analysis Center (GIAC), where there are pointers to three levels of courses of increasing depth. The first two levels include courses that are available for Web-based training. See also the home page, http://www.sans.org/newlook/home.htm for more pointers to SANS online training courses.

WISE (Web-based Internet Security Education) http://www.infosec.spectria.com/products/wise.htm from Rainbow Technologies includes courses on information security basics, PC & LAN security, Internet security, system server security, database security and preparation for the CISSP exam. The same organization offers a systematic approach to security awareness employees called SAFE (Security Awareness for All Employees) http://www.infosec.spectria.com/products/safe.htm

Appendix 4. Some Live INFOSEC Courses.

- Avi Rubin has an extensive list of college security courses in the USA and the rest of the world; it is at http://avirubin.com/courses.html and if you live near one of the academic institutions listed you can look into having your staff participate. Typically such courses are not expensive by industry standards.

- Computer Emergency Response Team Coordination Center (CERT-CC) offers courses; see the home page http://www.cert.org for links to upcoming sessions.

- The Computer Security Institute (CSI) has a catalog of its excellent live courses at http://www.gocsi.com/csi2001.pdf and also offers generous discounts for multiple courses or multiple people in the same course.

- DCI http://www.dci.com/ offer a wide range of IT courses and symposia including a dozen dealing with security topics.

- The (ISC)^2 (International Information Systems Security Certification Consortium) offers preparatory courses that can help bring staff up to speed on security issues; see

- The MIS Training Institute http://www.misti.com offers its courses not only at its conferences but also on-site for groups of employees.

- SANS, described in the section just above, has individual courses you can use for your staff. See http://www.sans.org/newlook/home.htm

Appendix 5. Key INFOSEC Associations and Other Organizations

- Association for Computing Machinery (ACM) Special Interest Group – Security, Audit and Control (SIGSAC) http://www.acm.org/sigsac/ has a newsletter and an annual conference (described below).

- American Society for Industrial Society (ASIS) http://www.asisonline.org/ has an active information security program including Cybercrime conferences.

- European Institute for Computer Antivirus Research (EICAR) has an active Web site http://www.eicar.org/ and annual meetings and is open for volunteers in Europe and around the world.

- Federal Information Systems Security Educators Association http://csrc.nist.gov/organizations/fissea.html caters primarily to "information systems security professionals, trainers, educators, and managers who are responsible for information systems security training programs in [US] federal agencies" but the association is also open to "contractors of these agencies and faculty members of accredited educational institutions."

- Forum on Privacy and Security In Healthcare (FPSH) http://www.healthcaresecurity.org/ is useful for anyone interested in their core subject.

- High Technology Crime Investigation Association (HTCIA) http://htcia.org/ is an international organization with many regional chapters. HTCIA "is designed to encourage, promote, aid and effect the voluntary interchange of data, information, experience, ideas and knowledge about methods, processes, and techniques relating to investigations and security in advanced technologies among its membership." HTCIA chapters often collaborate with ISSA chapters to host joint meetings of interest to all members.

- Information Systems Audit and Control Association (ISACA) http://www.isaca.org/ "sponsors international conferences, administers the globally respected CISA® (Certified Information Systems Auditor™) designation earned by more than 24,000 professionals worldwide, and develops globally-applicable Information Systems (IS) Auditing and Control Standards." Membership is limited to law-enforcement officials and security professionals.

- Information Systems Security Association (ISSA) http://www.issa.org/ has chapters all over the world and "provides education forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members." MK is an active member of the ISSA Northeast Chapter centered in the Boston area and very much appreciates *The Password – The Only Password You Should Share* publication and the excellent lectures presented monthly. ISSA also hosts an annual conference.

- Institute of Internal Auditors (IIA) http://www.theiia.org/ is active in all aspects of internal auditing including information security audit practices. The IIA sponsors conferences,

works with academia to encourage and support the development and implementation of internal auditing courses and curricula, and manages the CIA (Certified Internal Auditor) professional designation.

- International Systems Security Engineering Association (ISSEA) http://www.issea.org/ is a specialized group "focused on the adoption of systems security engineering as a defined and measurable discipline. The ISSEA's initial focus is the achievement of an ISO standard to guide and improve the practice of systems security engineering. The ISSEA will accomplish this through its oversight of the Systems Security Engineering Capability Maturity Model (SSE-CMM) Support Organization (SSO)."

- European readers may be interested in following the work of Sicherheit in Rechner Netzen (SIRENE) http://www.semper.org/sirene/ which is "a loosely collaborating group of researchers from different organizations" in Finland, Germany and Switzerland who "share an interest in security and privacy." They publish technical papers in electronic commerce, medicine, mobile communication, theoretical cryptology and distributed systems.

- SECEDU http://groups.yahoo.com/group/secedu is an informal moderated list run by Fred Cohen that caters to information security educators.

Appendix 6. Short List of Useful INFOSEC Conferences

- The Annual Computer Security Applications Conference (ACSAC) http://www.acsac.org/ is organized by The Applied Computer Security Associates (ACSA) and the Association for Computing Machinery (ACM) Special Interest Group – Security, Audit and Control (SIGSAC). This small conference appeals to security experts at a high level; the next one is in New Orleans in December 2001.

- The Computer Security Institute (CSI) is famous for the quality of its conferences. See http://www.gocsi.com/ for general information and http://www.gocsi.com/#netsec_01 for details of its upcoming NetSec Conference in June in New Orleans, LA.

- In Europe, the European Institute for Computer Antivirus Research (EICAR) has good conferences; see http://conference.eicar.org/ for news on the next conference, which will be in Berlin in the summer of 2002.

- The MIS Training Institute http://www.misti.com has many security conferences; see http://www.misti.com/conference.asp for a list of over a dozen conferences all over the world (e.g., Boston, Brussels, Chicago, Dallas, Dublin, Hong Kong, Jeddah, London, Orlando, Washington DC).

- RSA Data Security Inc. has a highly respected conference every year; see http://www.rsaconference.com/rsa2001/ for details of the April 2001 conference in San Francisco and check the extensive list of other interesting possibilities on RSA's event listing at http://www.rsasecurity.com/events/

- SANS has many conferences, international, national and regional: see http://www.sans.org/newlook/home.htm for a list of around a dozen upcoming conferences. These conferences have a wealth of courses and lectures for people interested in security – from beginners to experts.

An extensive list of upcoming security events is at http://www.cs.utah.edu/flux/cipher/cipher-hypercalendar.html and there's another list that includes many *Call for Participation* pages at http://www.cerias.purdue.edu/hotlist/detail.php?arg1=410&arg2=Events+%26+Call+For+Papers+/+Present

Appendix 7. Some Major INFOSEC Academic Programs in the USA.

- Carnegie Mellon University* in Pittsburgh, PA is home to the Software Engineering Institute (SEI) http://www.sei.cmu.edu/ and the Computer Emergency Response Team Coordination Center (CERT-CC) http://www.cert.org

- Dartmouth College in Hanover, NH has a new Institute for Security Technology Studies http://www.ists.dartmouth.edu/ that focuses on "cyber-security and information infrastructure protection research [and] counter-terrorism technology research, development and assessment."

- Eastern Michigan University (EMU) http:/www.emich.edu/ in Fayette (Upper peninsula), MI offers an undergraduate track that lends itself towards specialization in INFOSec; for details of the Graduate *INFOSec* Certificate Program see http://www.emich.edu/public/bted/infosec.html

- Florida State University* http://www.fsu.edu/ in Tallahasee, FL has a new Information Technology Assurance and Security initiative http://www.cs.fsu.edu/infosec.html focusing on software reliability, information assurance, and computer and communications security.

- George Mason* University (GMU) in Fairfax, VA offers an academic / commercial certification program related to the CISSP (Certified Information Systems Security Professional) certification managed by the International Information Systems Security Certification Consortium (ISC)^2 . This certification track is available within the Masters & PhD programs. GMU offers a virtual tour of their Center For Secure Information Systems (CSIS) http://www.isse.gmu.edu/~csis/ .

- George Washington University (GWU) in Washington, DC has graduate INFOSEC programs in its School of Engineering and Applied Sciences (SEAS). The list of programs at http://www.seas.gwu.edu/~seaswww/v5.0/admission/handbook/graddegrees.html shows D.Sc. Programs specialize in such areas as information assurance, cris/emergency/risk management, reliability, quality control, and risk analysis.

- Idaho State University* http://www.isu.edu in Pocatello, ID has a Center of Excellence http://security.isu.edu/ in operation.

- Information Resources Management College* http://www.ndu.edu/irmc/ at the National Defense University http://www.ndu.edu/ in Washington DC is a Center of Excellence.

- Iowa State University* http://www.iastate.edu/ in Ames, IA has an Information Assurance program that was authorized in November 2000; for a brief article about the project, see http://www.ait.iastate.edu/newsletter/200012200112/article15.html

- James Madison University* http://www.infosec.jmu.edu/ in Harrisonburg VA has a Master's program in INFOSEC that uses on-line distance learning.

- Purdue University* http://www.cs.purdue.edu/ West Lafayette, IN has excellent undergraduate and graduate programs and research opportunities. Many students from the programs have been awarded high salaries and positions after graduation.

- Stanford University* http://www.stanford.edu/group/tdr-security/ in Palo Alto, CA has a detailed calendar listing about its B.Sc., M.Sc. and Ph.D. programs in computer sciences, with courses in security and security-related topics. Download the PDF file from http://www.stanford.edu/dept/registrar/bulletin/pdf/CompSci.pdf

- University of California at Davis* http://seclab.cs.ucdavis.edu/ has programs emphasizing identification and authentication research, and research and development in cryptology, cryptanalysis and public-key infrastructure.

- University of Idaho* http://www.uidaho.edu/ in Moscow, ID has a Certificate of Completion in Secure & Dependable Computing Systems; see http://www.uidaho.edu/evo/newhtml/sccrdis.htm for details.

- University of Illinois at Urbana-Champaign* http://www.uiuc.edu/ has a Center of Excellence which is described at http://ciae.cs.uiuc.edu

- University of Tulsa* (OK) http://www.utulsa.edu/ has graduate programs in computer science with concentration in security; see http://euler.mcs.utulsa.edu/grad.cs.courses.html for details.

Appendix 8. Some INFOSEC Academic Programs Outside the USA.

- Algonquin College (a community college, not a university) in Ottawa, Canada has a one-year full-time program for a certificate in information security
  http://www.algonquinc.on.ca/acad_menus/current/0445X1FWO.html#Program Description

- At Cambridge University in England, the main research facility for security is the Center For Communications Systems Research (CCSR) http://www.ccsr.cam.ac.uk/ is famous for its longstanding, world-caliber quality of research. In 1997, Bill Gates gave Cambridge $70M to build a research center in computer science; however, only citizens of the European Union can receive financial support from the University. They have no scholarships, financial aid, or grants for non-European students.

- University of Hamburg http://www.informatik.uni-hamburg.de/ (in German) or http://www.informatik.uni-hamburg.de/welcome_eng.html (in English) is home to the Virus Test Center http://agn-www.informatik.uni-hamburg.de/vtc/naveng.htm under the direction of Prof. Klaus Brunnstein.

- Georgian College (also a community college) in Barrie, Ontario has a 48-week residency program leading to a post-graduate diploma in cyberspace security
  http://georgianc.on.ca/calendar/programs/cyberspace_security.htm

- Queensland University Of Technology (QUT) in Brisbane, Australia has an Information Security Research Centre http://www.isrc.qut.edu.au/ with strong ties to the AUSCERT (Australian Computer Emergency Response Team).

Appendix 9. Some Useful INFOSEC Publications.

Some paper publications are listed below:

- *Computer Security Alert* (monthly) and *Computer Security Journal* (quarterly). Both are benefits of membership in the Computer Security Institute) http://www.gocsi.com and http://www.gocsi.com/excerpt.htm (editorial archives)
- *INFOSECURITY News Magazine* (free) http://www.scmagazine.com
- *Information Security Magazine* (free) http://www.infosecuritymag.com/
- *SC Information Systems Security* ($175/year for six issues) Auerbach Publications http://www.auerbach-publications.com/contents/issad.htm

Some useful electronic publications that cover information security news which you can receive by e-mail (free unless otherwise noted) include the following (pointers to subscription information are given wherever possible):

- ACM TechNews includes security news as well as general information industry news (thrice weekly; free to ACM members) http://www.acm.org/technews/
- Benton Project Communications-related Headlines (daily) http://www.benton.org/News/
- Bugtraq (see subscription form in frame on) http://www.securityfocus.com/
- CERT-CC *Advisories* and *Summaries* http://www.cert.org/contact_cert/certmaillist.html
- *EDUPAGE* http://listserv.educause.edu/cgi-bin/wa.exe?SUBED1=edupage&A=1
- FindLaw's *DOWNLOAD THIS! A Weekly Newsletter Covering Law and the Internet* http://my.findlaw.com
- *Help Net Security* (weekly) http://www.net-security.org/text/newsletter/
- Network World Fusion's Security Newsletter (twice weekly tutorials and articles by MK) http://www.nwfusion.com/newsletters/sec/
- Pete Moss Publications -- newsletters about Spam, Security, MP3, E-Commerce, Privacy, Viruses and Censorship http://petemoss.com/
- *POLITECH* (daily) moderated by Declan McCullagh http://www.politechbot.com/info/subscribe.html
- *RISK Forum Digest* (irregular) moderated by Peter G. Neumann http://www.CSL.sri.com/risksinfo.html
- *SANS NewsBites* mailto:sans@sans.org with the subject: Subscribe NewsBites

- SearchSecurity Newsletter (daily)
  http://searchsecurity.techtarget.com/searchSecurity_Member_Benefits_Page/0,282323,1,00.html

- *Security Intelligence News Service* (weekly) http://dso.com/cgi-bin/dsoindex.cgi/?cartid=983070559&next=newsletter.html

- SecurityPortal (weekly) newsletters on BSD, CheckPoint, Linux, Microsoft, General Security News, PGP, Raptor, Solaris, Tools, and Viruses http://listserv.securityportal.com/SCRIPTS/WA-SECURITYPORTAL.EXE?SUBED1=securityportal-l&A=1

- *Security Wire Digest* (twice weekly)from Information Security Magazine
  http://infosecuritymag.industryemail.com

As for finding further information about information security, I suggest the following Web sites as good starting points (in addition to several of the sites mentioned above, which have daily news updates online):

- CERIAS Hotlist http://www.cerias.purdue.edu//hotlist/

- ICAT Metabase (search engine for CVE -- Common Vulnerabilities and Exposures – Database) http://icat.nist.gov/icat.taf

- ICSA Labs / Trusecure Corporation's *Hype or Hot* index
  http://www.trusecure.com/html/tspub/hypeorhot/index.shtml

- Information Security Resources http://security.isu.edu/

- InfoSec and InfoWar Portal http://www.infowar.com/

- INFOSYSSEC, a truly awesome collection of links, news and search engines
  http://www.infosyssec.com/infosyssec/index.html

- International Computer Security Laws http://www.mossbyrett.of.no/info/legal.html

- Network/Computer Security Technology http://jotruitt.home.mindspring.com/sectech/

- Security and Cryptography links http://www.semper.org/sirene/outsideworld/security.html

- SecurityFocus http://www.securityfocus.com/

- SecurityPortal http://www.securityportal.com

- TechRepublic configurable Web pages (browse by topic or sign up using link on)
  http://www.techrepublic.com

Appendix 10. Certifications in INFOSEC.

- Certified Information Systems Auditor (CISA) is described at http://www.isaca.org/cert1.htm

- Certified Information Systems Security Professional designation (CISSP) from the (ISC)^2 involves a minimum of three years of experience working as an information security professional plus a passing grade in a 250-question examination with a six-hour time limit. For full details see https://www.isc2.org/cissp_appreq.html

- Graduate Certificate Program In Information Systems Security (ISS) http://www.isse.gmu.edu/~csis/isscert.html from George Mason University in Fairfax, Virginia. The ISS is offered though GMU's School of Information Technology & Engineering (SITE) and its research center CSIS. This certificate may be pursued concurrently with any of the graduate programs available at SITE.

- Systems Security Certified Practitioner (SSCP) from (ISC)^2 is described at https://www.isc2.org/sscp_appreq.html and requires only one year of direct work experience in security.

About the author:

M. E. Kabay mkabay@atomictangerine.com began learning assembler at age 15 in 1965. In 1976, he received his PhD from Dartmouth College in applied statistics and invertebrate zoology. In 1979, he joined a compiler team for a new 4GL and RDBMS in the U.S. and then joined Hewlett-Packard Canada in 1980, winning the Systems Engineer of the Year Award in 1982. He has published over 250 technical papers in operations management and security, has published a textbook on security, and is currently Editor of the 4th Edition of the *Computer Security Handbook* (Wiley, 2001). After nine years as Director of Education for the National Computer Security Association (later ICSA, Inc.), he became Security Leader for the INFOSEC Group of AtomicTangerine, Inc. in January 2000. He currently writes two columns a week for Network World Fusion; archives are at http://www.nwfusion.com/newsletters/sec/ . For archived articles, see the K-Files on SecurityPortal at http://www.securityportal.com/kfiles/index.html .

