IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4464

Teaching Data Security for IT Specialists

Lech J. Janczewski
Department of Management Science and Information Systems, The University of Auckland, Private Bag 92019
Auckland, New Zealand, 64-9-373 7599, fax: 64-9-373 7430, lech@auckland.ac.nz

ABSTRACT

At present, data security is a rapidly expanding discipline resulting from the simple fact that for government, manufacturing or servicing organisations, damage to data can have disastrous results. In recent years awareness of these problems has grown significantly and there is pressure to offer more training in these fields. Numerous training arrangements already exist and a review of these arrangements is discussed. The paper concentrates on the issues of setting up introductory courses in this domain. A world review of the university offerings in the field of information security education is also presented.

1. INTRODUCTION

At present, data security is a rapidly expanding discipline. For government, manufacturing or servicing organisations, damage to data could have disastrous results. A very interesting document was published in 1998 by the Center for Strategic and International Studies, [CSIS, 1998]. The mood of this publication is clearly indicated by its title: "Cybercrime, Cyberterrorism, Cyberwarfare, Averting an Electronic Waterloo". The main hypothesis is that the American society is highly vulnerable to an attack launched by means of information technology. In the text there are a lot of statements like: ".. the statistics and our current cases demonstrate our dangerous vulnerabilities to cyberattacks." [ibid, p 26]. Mass media are also full of similar titles:

- "Timothy Lloyd, a disgruntled computer programmer detonated a digital "bomb" that cost Omega Engineering Corp over $10 million to fix",
- "Federal investigators seized memos that document an alleged plot where Reuters hired a computer consulting firm to steal information from Bloomberg",
- "A CIA audit showed Harold Nicholson had unauthorized access to several computers and top secret data on his laptop".

2000 CSI/FBI Computer Crime Security Survey revealed that among 643 responses from security professionals in corporations, government, financial institutions and universities:

- 70% reported computer security breaches in 2000,
- Total losses of $265589940 for 273 respondents who could quantify them, which constitutes 50% increase from 1998, [CSI/FBI 2000].

All those indicate the growing importance of information security issues and, as a consequence, the increased numbers of publications. Therefore, let's have a quick look at what areas were covered by perhaps the most representative conference in the field; IFIP/SEC. During the last six conferences: [Singapore, 1992], [Toronto, 1993], [Curacao ,1994], [Cape Town, 1995], [Samos, 1996], [Copenhagen, 1997], and [Vienna, 1998], over 310 papers were presented. These papers can be divided into the following categories:

- Presentation of data security cases in an organisation or groups of organisations. Publications usually contain collections of facts, analyses, and conclusions / recommendations,
- Analysis of various aspects of data security/EDP audit problems. Again, publications draw conclusions and generalisations from the collected facts,
- Theoretical aspects of data security/EDP audit. Most of these presentations deal with cryptography, risk assessment and network design
- Data security/EDP audit education. These publications mainly present curricula of training on offer.

It is worth noting, that only nine papers dealt directly with the educational aspects of data security and EDP audit. Only during the last three conferences special workshops on security education in the form of Working Group 11.8 were arranged. This Group organised the first World Conference on Information Security Education in Kista, Sweden, in June 1999 (with 21 papers presented [WISE1, 1999]). The next conference of this Group is planned during summer 2000 in Perth, Australia. All these indicate that tertiary organisations indeed became interested and involved in this area.

The aim of the paper is to report on the progress in the area of information security education with a special emphasis on the general information security education at a tertiary level. The paper starts with comments on the types of training and briefly outlines a suggested curriculum of information security specialists (at master's level). Then examples of information security training programmes from various universities are presented. Following that a suggestion of a general paper, an introduction to information security is outlined with a discussion on the delivery methods.

2. IS PROFESSIONALS DATA SECURITY TRAINING, IN GENERAL

The most important segment of the information security education is the one provided by universities. The format and content of such education is strongly related to the overall objective of a particular programme. The following delivery modes can be differentiated:

- In-subject training. It is the most popular method of presentation of information security issues. It is based on the discussion of security issues related to the particular mainstream topic. For instance significant parts of data communication or database management courses can be devoted entirely to security issues.
- Introductory course to information security. An introductory course should be offered to all Computer Science and Information Systems students during their final year of undergraduate studies. An advanced version could be offered at the graduate level, for those who wish to specialise in the field. Despite the fact that in the opinion of many, including the author of this paper, such a course should be taken by all the information technology students (especially at masters level), there is still significant resistance to such a suggestion. For instance, the ACM and AIS accepted "MSIS 2000 Model Curriculum and Guidelines for Graduate Degree Programs in Information Systems", authors: John T. Gorgone, Paul Gray, David L. Feinstein, and others, does not list such a course at all! In their opinion the afore mentioned in-subject training on

This paper appears in *Managing Information Technology in a Global Economy*, the proceedings of the Information Resources Management Association International Conference.

information security within the data communications and database courses is sufficient enough.

- Specialised training in information security. An information security specialist must have a very wide knowledge of information systems, both theoretical and practical. It seems highly unlikely that such knowledge could be gain through a regular undergraduate programme. Hence these programmes are usually placed at the masters level. There is pressure to establish qualification authorities and set up standard curricula of the disciplines, similar to the concept of the IDMA or ACM curricula.

3. MODEL INFORMATION SECURITY EDUCATION

The best known model of an information security curriculum is the one prepared by the Erasmus Group. The Erasmus report [Katsikas S., Gritzalis D., 1995] has been widely commented on various conferences such as IFIP, IRMA or WISE1 and all interested readers could find detailed descriptions there. Here we will summarise the basic tenets of the programme only.

The Erasmus Group suggest that the programme leading towards a Master of Science degree should contain four mandatory and four elective courses plus a thesis. The 4 mandatory courses are:

- Introduction to Information Security

Concept of security. Basic definitions. Principles of information systems analysis for security. Principles of risk, contingency, communication, secure system design. Principles underlying the semantics of security, integrity as a question of consistency, ethics and moral standards. Fundamental concepts in hacking and sabotage; misuse in the technical systems, malicious damage, and physical security.

- Introduction to Cryptography

  Basic definitions of ciphers, attacks and cryptanalysis. Various types of stream and block ciphers. Symmetric and asymmetric ciphers. Key management. Issue of identification and authentication, practical cryptographic products and services.

- Management of Information Security

  Management of information security models and frame works. The function of a security manager. Risk management and contingency management / planning. Auditing Information Security functions. Personnel management. Development and maintenance of information Security Policy.

- Computer Systems Security

  Formal security models. Formal specification and verification methods. Basic security mechanisms: covert channels, identification and authentication, hardware security mechanisms, unauthorised software handling.

The number of elective courses is considerable. The following list covers only those, which seem to be the most important:

- Computer Security Legislation,
- Telecommunication Security,
- Social and Ethical issues of secure computing,
- Database Security,
- Data security standards, certificates and evaluation criteria,
- Advanced Cryptography,
- Applied Cryptography and Cryptography Policies,
- Advanced Data Communications.

Close to the above curriculum is a model curriculum set up by the Information Systems Audit and Control Association. Interested readers may find that curriculum on the ISACA web pages [ISACA, 2000]. We will not discuss that curriculum here, as system audit is different from information security.

4. REVIEW OF THE INFORMATION SECURITY TRAINING

During the course of this research a number of universities from around the world were contacted and information on their information security training was collected. Below is the list of these universities with short descriptions of their offerings in this field. In no way is this list complete and it should be treated only as a partial reference. For this reason the relevant Internet contacts are provided. Also the evolution of the teaching programmes is quite rapid. Information in the survey was valid at the time of writing (December 1999) and reviewed in January 2001, but may become quickly out of date. The presentation is done in alphabetical order, based on the official name of the institution.

Notes:

1. Name of the university
2. Unit responsible for the delivery of the training
3. Name of the training/course/module
4. Basic structure of training
5. Contact Email or WEB page

The above list of information security training contains three types of programmes:

- Basic course/subject offered usually for the terminal year of undergraduate studies or at the graduate level,
- Diploma in information security, at graduate or post-graduate level,
- Masters of Science with a major in information security.

The listing brings sample programmes from universities in European, American and Pacific Rim countries. It is interesting to

• James Madison University, Harrisonburg, VA 22807, USA
• Center for Research in Information Systems Security Education
• Master of Science
• 20 months, 10 subjects
• www.infosec.jmu.edu/program

• Lund University, Lund, Sweden
• Department of Informatics
• Security in Networks and Database
• undergraduate subjects, advance level courses, one semester
• www.ehl.lu.se/spring01.htm

• Purdue University, West Lafayette, IN, USA
• Graduate School in Computer Science
• Computer Security
• Graduate course , one semester
• http://www.cs.purdue.edu/courses/descriptions.html

• Royal Holloway College, The University of London, Egham, United Kingdom
• Information Security Group
• —MSc in Information Security —MSc in Secure Electronic Commerce
• Master programmes, 2 years
• http://isg.rhbnc.ac.uk/

• University of Glamorgan, Pontypridd, United Kingdom
• School of Computing
• MSc Information Security and Computer Crime
• Graduate program, 2 years
• http://www2.comp.glam.ac.uk/soc

• University of Maryland, College Park, MD, USA
• The Robert H. Smith Business School

• University of New South Wales, Sydney, Australia
• School of Information Systems
• Information System Security
• graduate subject, one semester
• http://www.publications.unsw.edu.au/handbooks/courses/08309.htm

• The University of Auckland, Auckland, New Zealand
• Department of Management Science and Information Systems
• Data Security
• Graduate course, one semester
• www.business.auckland.ac.nz/Department/msis/index.cfm?fuseaction=rebuild

– The University of Queensland, Brisbane, Australia
– Department of Commerce
– • Information Systems Control and Auditing
– Graduate course, one semester
– http://www.commerce.uq.edu.au/postgrad/cources-pg.html#833

• Queensland University of Technology, Brisbane, Australia
• Information Security Research Centre
• Graduate Certificate in Information Technology (Information Security)
• postgraduate diploma, four units (modules)
• http://www.qut.edu.au/pubs/hbk_current/courses/IT50.html

note that during the data collection phase many sources reported that their offering is in the preliminary stage and the course in question will be run for the first time in year 2000.

As it was said earlier in the text the list is not complete. Readers are encouraged to do their own search for similar security-oriented programs. A good starting point is the web page of the American Society for Industrial Security (biased toward physical security) [ASIS, 2000] or the Gradschools search engine [Gradschools, 2000].

5. BASIC INFORMATION SECURITY TRAINING

The major thrust of this paper is to examine the content and delivery methods of a university course/subject, which is an introduction to the information security field. What could be the content of such a course? There are definite topics, which should be included like:

- Basic cryptography,
- Public Key Infrastructure,
- Risk management,

etc, but what other topics should be there?

[White et al, 1999] suggested the following basic list:

- Fundamental computer security principles (Confidentiality, Integrity, Availability),
- Risk analysis,
- Authentication,
- Access controls,
- Basic Principles of cryptography,
- Knowledge of the types of malicious software that exist,
- Basic network security (including a discussion of web security).

[White et al] aimed at the computer science majors. One may expect that information systems majors could have slightly changed curricula including topics more related to the managing of information security issues within business organizations. For instance such topics should be included as:

- Managing clearances and classification
  Who is allowed access to which documents, either hard or soft.
- Physical protection of information resources
  How to assure that only authorized personnel has physical access to the information. In this case it includes information in any form: electronic, paper, audio or graphic. This means that such issues as eavesdropping are also presented.
- Information security polices
  Setting up, implementing and controlling implementation of rules related to the maintenance of information security within business organizations.
- Security measures of the most popular operating systems (UNIX, Windows NT, etc)
  Information security specialists should know the security features of the most important software in their systems.
- Legal and ethical issues
  There are numerous laws (privacy law, security standards, ethical standards, etc) governing the implementation of security issues and professionals should be aware of them.

Hence, a comprehensive list of topics for a general course on information security may look as follows:

1. Overview of Computer Security
2. Identification and Authentication
3. Access Control
4. Security Models
5. The Security Kernel
6. Physical Security
7. Unix Security
8. Windows NT Security
9. Security Evaluation
10. Encryption techniques
11. Distributed Systems Security
12. Database Security
13. Eavesdropping
14. Legal and Ethical Issues
15. Managerial issues
16. Future Trends

A couple of courses similar to the above has been run for a number of years at The University of Auckland, New Zealand. The courses are located within the Computer Science / Information Systems studies but are open to all the students interested in the implementation of information technology. The courses were and are very well received by students. For most of them it is their first encounter with the information security issues and it shows them the importance of this discipline. These courses are offered at the graduate and postgraduate level. As the courses are a general introduction to the domain of information/data security they were not limited to issues related to computer security only but included several topics regarding managerial issues.

Setting up the list of topics of such an introductory course is only the first part of the whole problem. Equally important are the methods of the course delivery. The possible methods could be as follows:

- Direct lecturing by one lecturer,
- Seminar presentations (each session is presented by a leading specialist),
- Class discussions,
- Case studies,
- Experiments and other forms of laboratory activities,

or a mixture of the above.

The course in question is an introduction to a discipline and, in the opinion of the author, direct lecturing is the most effective way of presenting the knowledge. On the other hand it is the most difficult (and boring!) form of the academic presentation. The experience indicates that mixing all the above forms could lead to

obtaining the best results. Hence the recommended format of such a subject is a direct presentation of the material interspersed with the other activities like:

- Two or three guest speakers
  Usually guest speakers are highly regarded experts in their discipline but in many cases they lack lecturing skills. Also, to make their presentation logically coherent, they tend to repeat the material presented before or planned for presentation in the future. Hence a detailed briefing of each guest speaker before every presentation is a must.
- Demonstration
  It is almost impossible to lecture information security course without having the classroom wired for Internet access. A demonstration of the security related software and web pages during lectures dramatically enhances the perception of the presentation. For instance the best method of description of unprotected and protected mode of operation is the live observation of the padlock icon changes on the screen.
- Experiments
  The experiments could be very theoretical (breaking of a ciphertext) or very practical (demonstration of the Window NT). During fall 1999 the author observed how enthusiastically students reacted to receiving a ciphertext encrypted with the use of a substitution cipher. Some of them spent a number of sleepless nights trying to break the code. During 2000 a firewall lab was set up and students were encourage to develop a security policy and test it in a real-life environmet. It is worth noting that there was an effort to generate a database of possible experiments used for enhancing the information security education processes [Jonsson, E. and Janczewski, L., 1997]. The authors developed a taxonomy of possible experiments, from a simple dem onstration for presentation during a lecture to the real-life information security projects. The taxonomy was supported by the description of over 30 experiments.
- Class discussions. Presentation of several topics, due to their controversial nature, should be done via class discussion. It is especially relevant to the privacy protection and ethical issues. The best example is the protection of personal data (for example, the issue of an individual identification card). The opinions of the Japanese students are usually dramatically different from their USA counterparts.
- Case studies
  The progress in the field of information security makes the development of more expanded case studies quite difficult. Almost at the moment of publishing the case could be outdated. There have been very few efforts to publish such a collection. The best known, perhaps, is a book written by [Dhillon,1997]. However there is a num ber of periodical publications which could be used as a source for case studies discussions, like Datapro Reports or Auerbach Reports.
  The mass media are bringing every day information about security violation. In a significant number of cases the reality of the event is substantially different to that presented by the press or TV. Therefore it is a good policy to ask students to conduct in-depth studies of interesting recent cases discussed by the mass media and/ or specialists.
- Site visits
  Information security includes the issue of physical security. The author of the paper noticed that all the class discussions of this topic could not replace a visit to a real computer facility to observe in action the equipment and procedures introduced to protect the site.

The proposal outlined above has a strong information system bias. Many computer science specialists would reject it. A computer science lecturer commented on the proposal as being "too wide". For him the essence of information security lies in cryptography and all the rest is an unwanted addition. In the opinion of the author it is time perhaps to start to differentiate between information security and computer security. Information security would deal more or less with the issues outlined in the proposal while computer security would concentrate solely on the processes inside computers. This would make both information systems and computer science specialists happy.

6. CONCLUSIONS

In recent years we have observed an increase in the number of courses on data security offered by various professional organisations and universities. This is indirect proof that the discipline is growing and expanding. A number of initiatives took place to co-ordinate developments in teaching data security subjects. The Erasmus project was the first attempt to develop a curriculum in this discipline and it should be continued. In the opinion of the author there is a definite need to introduce some co-ordination of efforts. The survey conducted by [Gritzalis, 1995] indicated that at 11 universities surveyed almost 130 different textbooks were used and only one textbook was used in four places, one - in three places and 12 - in two places. There is no need to insist on a single text but the above variety of the basic source of information is astounding!

This does not mean that there is a need to establish an international watchdog organisation imposing their data security education standards but it does mean that a well researched and developed information security curriculum would make the life of the educators and trainees much easier.

Equally it is important to develop a standard curriculum of a introductory course in the information security field. Such a course should became a part of a universally recognised curriculum. As a matter of fact during the 2000 Information Resources Management Association conference in Anchorage a group of academics from Australia, New Zealand and United States set-up a group who are currently working on this topic.

REFERENCES

[ASIS, 2000]. http://www.asisonline.org/aps_weblinks.html[Capetown, 1995], Information Security - the Next Decade, ed Eloff, J. and von Solms, S., Chapman & Hall, London, 1995.

[Copenhagen, 1997], Information Security in Research and Business, ed Yngstrom, L. and Carlsen, J., Chapman & Hall, London, 1997.

[CSI/FBI 2000], 2000 CSI/FBI Computer Crime and Secuirty Survey, Computer Science Institute, USA, 2000.

[CSIS, 1998]), Cybercrime, Cyberterrorism, Cyberwarfare, Averting an Electronic Waterloo, Center for Strategic and International Studies, Washington, DC, USA, 1998.

[Dhillon, G., Managing Information System Security, Macmillan Press, 1997.

[Gradchools, 2000], http://www.gradschools.com

[Gritzalis, 1995], University Programmes on Information Security, Dependability and Safety, ed. Gritzalis, D., European Commission, Erasmus ICP, Project ICP- 94(&95)-G-4016/11,

Report IS-CD-3c, Athens, 1995.

[ISACA, 2000], http://www.isaca.org/modelc1.htm,

[Jonsson, E. and Janczewski, L., 1997], Taxonomy and over view of information security Experiments, in Information Security in Research and Business, ed. Yngstrom, L. and Carlsen, J. in Information Security in Research and Business, Chapman & Hall, London, 1997.

[Katsikas S., Gritzalis D., 1995], eds. A proposal for a post graduate curriculum in Infromation Security, Dependability and Safety, European Commission, Erasmus ICP, Project ICP-94(&95)-G-4016/11, Report IS-CD-4c, Athens, 1995.

[Samos, 1996], Information Systems Security, Facing the information society of the 21st century, ed. Katsikas and Gritzalis, Chapman & Hall, London, 1996.

[Singapore, 1992], IT Security: the Need for International Cooperation, ed Gable, G., Caelli, W. North-Holland, Amsterdam, 1992.

[White,G., Marti,W., Huson,L.,, 1999], Incorporating Security Issues Through the Computer Sceince Curriculum, Proceedings of the IFIP TC11.8 First World Conference on Information Security Educxation, June 1999, Kista, Sweden. p 19-26.

[Vienna, 1998], Global IT Security, ed Papp, G., Posh, R., Osterreichische Computer Gesellschaft, Vienna 1998.

[WISE1, 1999], Proceedings of the IFIP TC11 WG 11.8 First World Conference on Information Security Education, 17-19, June 1999, Kista, Sweden, Dept of Computer and Systems Sciences, Stockholm University.