# EDUCATING FOR SECURITY: AN ACADEMIC'S CONTRIBUTION

**Author**

Ljudmila Simeonov,

Author's affiliation

Department of Information Systems

Massey University @Wellington, New Zealand

Author's contact details

l.simeonov@massey.ac.nz

+644 801 5799 x 6418

Private Box 756

Wellington, New Zealand

ABSTRACT

Business is embracing best practices in IS security in many ways. It is developing policies and procedures and implementing various technologies to harden its security. At the same time training programmes are put in place to increase user awareness as to the danger of unsafe IT practices. Academia may be lagging behind.

While some universities have extended their programs to include information systems security, others may have to include some security components to existing papers. These components can then be used to broaden the awareness, education, and training in security, so that future industry needs can be satisfied.

The paper presents a case study, outlining an educator's individual efforts to promote and enhance IT security awareness and education. Four courses required for the completion of a three year undergraduate degree in CS / IS at a New Zealand university come under scrutiny. The security components incorporated into them are presented. Where appropriate the emphasis is to impart both current knowledge and create long lasting practical "real life" experiences.

Abbreviations used:

CS = computer science

IS = information systems

IT = information technology

KEY WORDS

security education, security awareness, training for security

# 1 INTRODUCTION

IT security in the business arena, or rather the lack of it, is in the spotlight . Many papers outline the reasons as being the acceptance of the Web and the extension of it to business and financial institutions. While market players are investing a lot of effort and money to rectify the current problems, it is up to academia to produce the people who will manage it in the future.

"Improving software security and safeguarding the IT infrastructure is a research and education issue for universities; a skill, process, and incentives issue for producers; a requirements issue for customers; a quality and testing issue for providers; a maintenance and patching issue for IT administrators; an ease-of use issue for users; a configuration issue for installers; and an enforcement issue for governments" (ITAA, 2004). The same source points that the "persistent, combined efforts of industry, academia, government and others to make long-term progress" are needed. Mendham (Mendham, 2004) broadens this further to include "A more urgent response from the education sector to both address the need for IT risk management programs and to include security as a mandatory subject in IT qualifications".

Most of the problems with security are indeed software quality issues, either design or development (SANS, 2004), and have to be addressed by the producers. Another group of problems lies with the administrators and is to be blamed on improper configuration. Yet another group of problems is mainly people related, whether intentional or not, by ignorance or by design.

It can be seen that a well-orchestrated endeavour is required by industry, academia, and business and often that takes time and effort to achieve. The paper instead investigates educational efforts in security used in other tertiary institutions, by education providers of certifications, as well as security best practices in industry, and applies some of the ideas that work to own individual context. The opportunity exists to either extend, redevelop, or include extra security components in existing papers. Those components can then be used to broaden the awareness, education, and training in security for our students, so that future needs of industry can be satisfied. Not having a security curriculum in place should not be seen as a disadvantage. With the amount of effort invested in security currently, the situation can only get better.

# 2 THE LOCAL ENVIRONMENT

A previous paper by Narayan (Narayan, 2004) surveys some IT Bachelors qualifications offered at New Zealand tertiary institutions and finds them lacking in terms of a well rounded security curriculum. Massey is not included in the publication.

The local campus of Massey Wellington reveals only one paper out of 50, namely "IS security", when searching for "security" among the IT undergraduate papers. It covers cryptography in great detail, but no practical experience is included. Surveying further the available fact sheets, which list the topics to be covered, 9 out of 21 papers include some parts of the 10 security practices as reflected in the CISSP (Certified Information Systems Security Professional) certification (informIT, 2004). The papers list privacy, ethical issues, quality assurance, risk management, and network security. The distribution is: 2 papers available both in first and third year of study, and the rest - in the second year. The graduate papers are well catered for with 4 papers available in the area. Most of our students head for the job market after they obtain their degree, rather than research. Additional knowledge and experience in IT security can only better their chances of getting employment.

# 3 LEARNING FROM OTHERS

Bacon and Tikekar (Bacon & Tikekar, 2003) describe the process of creating a computer security and information assurance (CSIA) curriculum Bachelors degree. They build on existing papers that are already in place and introduce new papers as required. The students get sufficient exposure to hands-on experiences in many of the papers. A LAN isolated from the main university network is a requirement so that real-world experiences are simulated.

Carlson (Carlson, 2004 )advises on various aspects of teaching computer and network security as part of creating a single paper (course), describing most of the exercises used. Tips on what works, and what takes too long to set up, are very helpful.

Morneau (Morneau, 2004 ) exposes an information security program for three distinct levels of information security professionals, giving professionals enough mastery and sufficient (but not too much) material. A modified information security BOK is presented and is considered useful.

## 4 ACTUAL WORK

Four papers are presented: two first year and two-second year. One of the papers does not have an explicit security component. The steps taken to raise student's security awareness, knowledge, and experiences are elaborated on. Two of the papers make use of a dedicated lab. The papers that are discussed further have to be taught within the expected learning outcomes.

Security is a system property; therefore it has to be developed through the SDLC (Systems Development Life Cycle). People, processes, and technology (P-P-T) will contribute to security during the various phases . Once the system has been developed, it has to be configured, put into operation, tuned, eventually handed over. During the maintenance phase security has to be monitored, preserved and enhanced. Every phase in the SDLC – from analysis to maintenance is important. We as educators can make contribution to any of the phases. Although the process may be fragmented – if each educator attempts it, the students will gain knowledge, skills, and experience. No matter what paper we teach – it will touch on security. As we impart knowledge – we change attitudes.

The papers that are considered are familiar to the author. They are chosen seemingly randomly. This is done to emphasise the idea that no matter whether there is a relationship between them or what contents these IT papers cover, there exists the potential to use them for security awareness.

### 4.1 157.100 Computer fundamentals – contains a security component

This is a year 1, semester one, 13 weeks paper (full semester) consisting of 4 hours lectures, 2 hours tutorials and 2 hours labs.

The paper takes the students through examples from real businesses, describing and analyzing a wide variety of IS problems. Latest emerging technical and organizational trends are presented. Leading-edge technologies: Wi-Fi networks and security; P2P (person-to-person), grid, and utility computing; the next-generation Internet and Semantic Web; Web services and enterprise application integration; business process management; and object oriented modelling are included. Limited encryption is there too. The tutorials reinforce the lectures. The labs further extend students knowledge into the (mainly Microsoft) applications.

The labs are used to convey to the students the reality that security in IT must focus on policies and behaviour. These policies have to be conveyed to our students in the first 2 to 3 sessions. End user education about the importance of security goes a long way and must start at the students' orientation.

There are induction/orientation programmes at all campuses. For IT students there is a very informal introduction to the computer labs. Security policy documents exist and the students are advised to read them. The students can get to their home page and follow the computer lab policies, which amount to a total of 36 pages. It would be interesting to know if anyone has read them. Similarly to industry – we have to train our users. Even a few minutes during the first few sessions will be beneficial.

We have to raise security awareness with new students in terms of the following:

### 4.1.1 Access controls and Resource use

User codes and Passwords have to be entered as prescribed. These are intentionally weak and are set at some default values initially. (The students bring the little piece of paper with, and everyone can see it.) The students are advised to change their passwords right into the first login so that their mates are not able to get to their accounts. Even these elementary steps are not properly followed and academic staff may find students using their initial password till the end of the academic year as well as using their friend's accounts.

What to do is easy – remind students (especially first year ones) many times what you want them to do.

Students are charged for connection time. If they stay logged on though not using any resources – they pay. It is equally important to let them know that and encourage them to log off at least at the end of ones class. Initially going around and checking that all are logged off is another step in the "security awareness" process. Provided the PC's are left logged on – other students may abuse the account in any way they know: assessing the student disk and wiping it clean, getting on the Web and assess unauthorised sites.

Students pay for using resources – notably the printers. A charge applies per printed page. If not careful – students may spend their printing budget on useless pages. That particular step is highlighted in the regulations in connection with charges only. How to get out of sticky situation – printing the whole 9999 pages of document the students came by mistake is not. "Tell them and show them" does apply.

### 4.1.2 Physical security – caring for the respective equipment

Computer equipment is sensitive and care has to be exercised when using it. While indications are that more than 80 % of students own PC's and therefore they are aware of damage that can be inflicted upon them – damaging the labs equipment is a constant problem. Students have to be told and shown how to handle floppies, CD ROM's, mice and keyboards, flash (boring, but necessary). It is not uncommon to find 3 PC's or more out of 20 in every lab to be out of circulation due to mishandled floppies, damaged mice, etc. More tips for the students:

Wait for light to go off on the floppy /CDROM/flash before pulling it out

Do not pull keyboard / mouse out

Do not switch computer off

Switch monitor off (debatable)

### 4.1.3 Backup and restore

We expect students to be aware of equipment failures. The network, the floppy, the disk, may all take a dive, never to return. When the work at hand is important – backups are mandatory. Staff has to reinforce that. Most students learn (as all humans do) by their own mistakes, and by year 2 they are good at this step.

### 4.1.4 Caring for home equipment

As students do take their work home – viruses and other malicious code may accost them. They are advised to protect their home PC's by installing security patches, antivirus on their desktops, and network firewalls. Simple guides in that respect are available at many sites and the students are advised to consult regularly the New Zealand security site. (CCIP, 2005)

### 4.1.5 Using E-mail and browsing WWW sites

Most of the IT students have full Web access. Certain guidelines apply here. We have to remind them and check on them now and again about the "objectionable material" they should not be reading, as the penalties are high. The policies information can be consulted on http://its-intra.massey.ac.nz/policies/index.htm.

### 4.2 157.126 Hardware and Data Communications – does not contain a security component

This is a year 1, semester two, 13 weeks paper (full semester) consisting of 3 hours lectures, and 2 hours labs.

The paper is mainly chock and talk and raises awareness only. It corresponds in part to the "Telecommunications and Network Security" domain of the CISSP CBK (Common Body of Knowledge). Some fundamentals, such as the OSI (Open System Interconnect) model TCP/IP are well covered. Security issues deal mainly with media and the possibility of tapping into it or intercepting traffic, as well as error detection and correction. Four special lab exercises (the special lab is described in 4.3.1) are substituted for the computer lab exercises, so that limited hardware and network troubleshooting and TCP/IP protocol analysis can be observed. The hands-on experiences are greatly appreciated by the students.

### 4.3 157.263 Operating Systems and Data Communications - does contain a security component

This is a year 2, semester one, 13 weeks paper (full semester) consisting of 2 hours lectures, and 2 hours of special labs. The prerequisite to this one is a 157.1xx paper. Any one of the preceding papers does qualify.

#### 4.3.1 The special lab

The special lab consists of 15 Pentium IV and 15 Celeron workstations equipped with 256 MB RAM, 40 GB hard disk drives, and a 100 Mbps NIC (network interface card). The hard drives are removable and are available to the students for the whole year of study or until the students return their swipe cards that entitle them to almost unlimited access to the lab. By way of the removable hard drives other groups of students can easily make use of the lab and the equipment by substituting their own drives.  Currently only two groups share the lab in both semester one and two.

There are 5 CISCO switches and 3 CISCO routers housed in a cabinet. A patch panel interconnect all devices. Structured cabling is used throughout, which makes is very flexible in terms of disconnecting and reconnecting the equipment. Extra hubs (repeaters) are available, as is a dial-up line for Web access. The network is not connected to the university network and is an ideal opportunity for investigating various technologies, security threats, and tools.

This year we acquired the following WLAN (Wireless LAN) equipment: 15 54 Mbps 802.11g PCI NIC's, 4 USB 2.0 802.11g adapters, and 2 AP's (Access Points).

#### 4.3.2 The lab exercises

The students generally install and configure peer-to-peer LAN based on MS Windows followed by Linux (Slakware 10.1) for a fictitious client in a SOHO environment. Using best practices they have to decide on desktop security, group policies, access control, shares, privileges, patch management, disaster recovery given a simple scenario. They are encouraged to relate their personal experiences to some of the configuration issues the university system has, to criticise those issues and even offer advise on how to mitigate those issues .

The lab is used to include as much experimenting as possible, so that students have "real world" experience, which is often a barrier to them for entering the job market. It is important that the students discover the application of the principles they have been taught about, as well as see the application. Students learn best by experimenting.  McClure (McClure & Scambray, 2000) expresses that by saying "Showing people how to bypass systems is the only way to get them understand how to fix those problems". Their experiences will benefit them, as well as the industry they later may join. (Often the complaint is that students do not have sufficient experience. The labs provide them with it.)

WLAN are introduced. The students build a simple WLAN, similar to a SOHO (Small Office Home Office) environment. Security is addressed by exposure to the WEP/WPA protocols that are part of the adapters' software. Similarly to effective passwords best practices, pass phrases can be effective with PSA PSK. Time permitting pass phrase crackers can be used too, as well as other analysers, such as NetStumbler. NetStumbler is a tool for Windows that allows detection of Wireless Local Area Networks (WLANs) using 802.11b, 802.11a and 802.11g. It has many uses such as:

Verify that the network is set up the way intended.

Find locations with poor coverage in your WLAN.

Detect other networks that might be causing interference with your network.

Detect unauthorized "rogue" access points in your workplace.

Help aim directional antennas for long-haul WLAN links.

Use it recreationally for WarDriving.

Open source scanners are available and are part of the exercises. As time is limited students are encouraged to experiment with the technologies, and the tools on their own too. Software is available to take home and investigate further as some of the students have small LAN at home. Mostly free SW is used.

### 4.3.3 The assignments

There are four compulsory labs (worth 2.5 % each). These are 30 min each and the students have to demonstrate 5 to 10 specific skills. This is some of the "performance level" part, as outlined in the NSTISS subject areas. (Bacon & Tikekar, 2003)

Write-ups 1 to 4 (worth 5 % each) are mini research assignments aimed at investigating current security threats, other security or operational issues. Once marked these are discussed and made available to all through the Intranet.

A case study (worth 20 %) based on a LAN design and an IP addressing scheme for a larger client includes limited access level security.

## 4.4 157.246 Project Management (PM) and Systems Implementation (SI) – does contain a security component

This is a year 2, semester one, 13 weeks paper (full semester) consisting of 2 hours lectures, and 2 hours of tutorials. It is a core paper for the many students from the PM stream of study. Assignment 1 in PM includes a substantial case study. Usually some of the latest SW, HW and/or networking technologies are included. As an example ISA Server 2003, VPN and Exchange Server 2003 were part of this year's case study. This gives the students a chance to get acquainted with current technologies to some degree.

The SI part of the course maps to many of the CISSP domains:

Documentation and implementation of security policies, standards, procedures, and guidelines, user involvement

Confidentiality, Integrity, Availability (CIA) principles as applied to data

Security methods

Operations Security: restricting privileges, identifying roles

Backups

Recovery, performance and pen tests

Disaster Recovery Planning (DRP)

Physical security, firewalls, IDS and malware protection

Training

The topics are enforced in tutorial by group work, open discussion and exchange of ideas. Extra materials such as current NIST documents (NIST, 2005) are available on the Intranet. Assignment 2 (20 %) involves a data conversion plan and report that considers all the steps above and does contribute to both the awareness and performance levels of security.

## 5 CONCLUSIONS AND FUTURE WORK

Four IT papers have been used to extend security awareness, education and training. Informal feedback is available for the second year papers. The students do appreciate current and relevant material and are keen to learn it. The "hands-on" exercises in the special lab are indispensable to keep the students interested. Other institutions often cite resources as an obstacle to proper "real-life" teaching; we are fortunate to have it. Although the lab exercises have been streamlined in terms of time, the students have to put in a lot of extra time, which presently they are eager to do.

Comparable work can be undertaken in the other five papers that have "security" or related term in their topics of study; or to papers in programming. Their exercises can be extended to "real-life" situations by using the special lab. It will be easy if we help each other and properly coordinate our efforts, as currently there is no extra assistance available and setting "hands-on" exercises is very time consuming. There is sufficient security knowledge in the faculty for that.

As advances in technologies are occurring all the time, keeping the courses current can be a challenge. The market and industry requirements have to be monitored and the contents adjusted accordingly. At the same time the producers and other market players are coming with new tools and technologies, that may one day present to us the perfect "secure" system, when we will have to look at something else to teach or do.

## 6 REFERENCES

Bacon, T., & Tikekar, R. (2003). EXPERIENCES WITH DEVELOPING A COMPUTER SECURITY INFORMATION ASSURANCE CURRICULUM. *Journal of Computing Sciences in Colleges, 18*(4).

Carlson, D. (2004 ). Teaching computer security *SIGCSE Bull. , 36* (2 ), 64-67

CCIP. (2005). *A simple guide to help keep your Personal Computer secure*. Retrieved 2/03/2005, from http://www.ccip.govt.nz/security-tips/security-tips.htm

informIT. (2004, Apr 21, 2004.). *informIT Security Common Body of Knowledge (CBK) Definitions*. Retrieved 15/02/2005, from http://www.informit.com/guides/printerfriendly.asp?g=security&seqNum=5&rl=1

ITAA. (2004). *Improving Security Across the Software Development LifeCycle*. Retrieved 10/03/2005, from http://www.itaa.org/software/docs/SDLCPaper.pdf

McClure, S., & Scambray, J. (2000). Survey points out that lack of training is first barrier to improved network security. *InfoWorld, 22*(42), 107.

Mendham, T. (2004). *Securing your future*. Retrieved 01/31/2005, from http://www.computerworld.com.au/pp.php?id=1591582976&taxid=14

Morneau, K. A. (2004 ). Designing an information security program as a core competency of network technologists In *Proceedings of the 5th conference on Information technology education* (pp. 29-32 ). Salt Lake City, UT, USA ACM Press.

Narayan, S., Narayan, S. (2004). *Information Security Qualifications in New Zealand*. Retrieved 10/02/2005, from http://www.naccq.ac.nz/bacit/0203/2004Narayan_InfoSecNZ.htm

NIST. (2005). *Information Security in the SDLC*. Retrieved 04/20/2005, 2005, from http://csrc.nist.gov/SDLCinfosec/SDLC_brochure_Aug04.pdf

SANS. (2004). *The SANS Top 20 Internet Security Vulnerabilities*. Retrieved 5/03/2005, from http://www.sans.org/top20/