Developing a framework for an information security paper

Shaneel S. Narayan **Sheetal Narayan**

School of Computing and
Information Technology
UNITEC
Auckland, NZ
snarayan@unitec.ac.nz

In this paper we explore the extent to which New Zealand's tertiary education providers are offering course options that equip future Information Technology professionals to assess threats to information systems, recognise vulnerabilities and find technology solutions to counteract a number of security issues. An audit of computing degrees and equivalent qualifications in New Zealand is undertaken to assess what level of information security is taught in different programmes. A comparison is then made with courses offered in other information systems and related qualifications available globally. Finally, the security requirements of the industry are analysed to identify any gaps between what is being taught and what is required of Information Technology professionals.
By comparing what New Zealand institutes currently offer with what the industry demands of its Information Technology professionals in relation to security, strategies for developing a framework for an Information Security paper will be proposed.

Keywords

Security, undergraduate computing degree.

1. INTRODUCTION

Just as we witnessed an industrial revolution of the 18th and the 19th centuries, a technology boom in recent times brings with it a significant revolution. With such a major advancement, as with any other major development, come negative and positive effects on society. One of the major positives of this revolution has been the creation of a global community and a system that has the ability to share information instantly and cost effectively. Currently there are some 160,000,000 computers in the world with the ability to connect to one another (Internet ready) and of that approximately 8,000,000 are online at any given instance (Hinchcliffe, 2003).

The major negative impact of this development is the continual increase in "information" threat. Not only are the perpetrators able to exploit the old existing vulnerabilities in new and creative ways, the number and the nature of these are on a continuous rise with ever increasing sophistication. The Computer Emergency Response Team (CERT) in the United States reports that the total number of annual reported systems vulnerabilities has skyrocketed from 171 in 1995 to over 3784 in 2003. The total number of reported vulnerabilities since 1995 through to the end of 2003 was more than 12,946 (Tarte, 2003). The total increase in reported vulnerabilities since 1995 was more than 7571%. Information systems vulnerabilities have grown exponentially over the years.

Many of the vulnerabilities that exist in today's information systems are directly related to the advancement in technology. Thus, these vulnerabilities are not confined to any one area of the technology; they range from vulnerabilities in servers, databases, applications, scripting, protocols and socially engineered situations, outlined in the SANS Institute's top 20 vulnerabilities.

With approximately 8,000,000 Internet ready computers, the possibility of exploiting these vulnerabilities and turning threats into reality is a major concern. According to the KPMG 2002 Global Information Security Survey of world's largest organisations "average direct loss of all breaches suffered by each organisation is USD$108,000."

2. NEW ZEALAND TERTIARY AUDIT

After analysing the contents of all Bachelors level qualifications offered by tertiary institutes in New Zealand, the following can be concluded:

- Only one programme has a few dedicated papers in Information Security or equivalent topic.

- All programmes have some aspects of security taught in certain papers.
- No programme has enough courses to qualify security as a dedicated thread (major).
- None of the courses have contents exceeding more than half in Information Security (except one).
- There are many courses that do not investigate any aspect of security, although security is fundamental to the contents of such paper.
- There are a few papers on network and web security at level 2 and 3 of the NZQA framework (certificate level).

Thus is can be deduced that small amounts of this subject are definitely taught in little pockets in different programmes, making Information Technology graduates "generalists" in the area of Information Security. When compared with the "IT-Security Instructional Model" of the National Institute of Standards and Technology in United States (Gilbert, 2003), Information Technology graduates in New Zealand are receiving training at "beginning" to an "intermediate" level of coverage of the domain only. According to this model, training at beginning level provides foundation knowledge only whist intermediate level enhances breadth and/or depth of security knowledge and skill.

None of the programmes provide platform for "advanced" or "expert" level training. An individual trained at this level will be able to apply knowledge and skill attained through training to mission critical Information Technology security problem solving and technology assessment.

3. INDUSTRY SECURITY CERTIFICATIONS

There are a number of industry based certifications that contain some aspects of Information Security, depending on the certifier. Most are continually updated in content and structure, reflecting the ever changing nature of the Information Security arena.

Microsoft offers a number of courses related to security. Certifications at the lower end of the spectrum does not necessarily contain specific modules about security however higher end certifications like MCSA, MCSE and MCSD have dedicated modules to the topic. Not only that, MCSA and MCSE are now offered with security as a specialisation. This highlights the importance of Information Security.

Cisco offers a number of modules in its different certifications that contain some aspect of security to a reasonable technical level and its highest certification CCIE is offered with security as a specialisation. All modules of all certifications from Cisco have a reasonable amount of coverage about Information Security.

Novell's Master CNE certification contains a module specifically dedicated to security while all other certifications have various levels of coverage. Its entry level certification CNA has minimal coverage.

While the above is a sample of what the industry offers in terms of vendor specific certifications related to security, there is another group of these known as vendor neutral certifications. CompTIA's Security+ certification is one such example. It covers a range of industry-wide topics, including communication security, infrastructure security, cryptography, access control, authentication, external attack and operational and organization security and allows one to attain a good foundation of the basic essential concepts of security. Not only is this a security certification per say, it can also be cross-credited into other advanced qualification like MCSE.

Certified Information System and Security Professional (CISSP) certification is the ultimate for any Information Security practitioner. For one to be become a CISSP, the candidate needs to pass the appropriate examination, have a college degree and at least three years of work experience in a relevant domain. "An inch thick and mile wide" is a statement that is commonly used to describe the nature of this certification.

The above industry based certifications have a few common elements. Most need the holder to sit refresher examinations after certain time constraints, others expire and some require ongoing maintenance by attending security conferences, delivering guest speeches or participating in other similar Information Security related activities. Secondly, all certifications cover topics across multiple domains in Information Technology (application, databases, networking and programming). And finally all have curriculum that changes frequently.

4. WHAT THE INDUSTRY WANTS

One of the key findings of "Australian computer crime and security survey 2003" is that 30% of respondents (organisations in Australia) were dissatisfied with the level of IT security qualifications, training or experience within their organisation. This report also found that 42% had experienced attack against security. "Deloitte's 2003 Global security survey" reiterates this by finding that 39% of their respondents acknowledged that their systems had been compromised in one way or another within the last year.

These and other similar reports all enforce that the nature and sophistication of Information Security attacks is on an ever increasing tangent. Not only do organisations need Information Technology professionals with maximum dedication to the Information Security arena, they also want professionals who have "expert" level security knowledge about all domains of Information Technology spectrum to combat daily Information Security situations.

5. FRAMEWORK FOR INFORMATION SECURITY PAPER IN BACHELORS DEGREE

Undoubtedly, the contents of the Bachelors programmes in New Zealand do not provide ample coverage of Information Security in its different courses. Currently, Information Security is taught in little nuggets in different courses. Such syllables only prepare graduates to attain beginner to an intermediate level of exposure to this complex and important domain. By equipping them with advanced level knowledge about Information Security, a path will be carved for them to become "experts" in the domain of Information Security if they choose to do so.

Preferably a number of courses at different levels, exploring diversity of the domain should be offered to students. By doing so, Information Security will receive a comprehensive coverage providing all the necessary knowledge to the students. This in the long term will give rise to Information Security as a legitimate thread in Bachelors degrees.

In the short term, framework for at least one course should be developed and offered to students in all Bachelors of Information Systems and equivalent programmes. The following specific strategies are proposed for developing a framework for such a paper:

- The course should be pitched at the highest level in the degree programme. By the time the students are qualified to undertake this course, they would have had a good exposure to all disciplines of Information Technology and will appreciate the importance of the topic.
- There needs to be a multi discipline approach to Information Security, that is, the contents of the course should address security issues related to applications development, multimedia, databases, web development, networking and programming. This will allow students to explore security concerns that arise from an inter-discipline environment, like in the real world.
- The course should have technical rather than management focus delving into intricacies of Information Security. This will develop students' skills at troubleshooting, implementing and managing security solutions.
- Incorporate practical workshop sessions with simulations where students will attain hands-on exposure to real world security vulnerabilities, threats and exploits.
- A commitment to revise contents frequently to incorporate new developments in Information Security. This can be achieved by analysing what the industry wants of its security specialists, seeing what industry certifications deliver and researching about Information Security regularly.
- Align the course with some industry certification e.g. CISSP. Not only will this allow the institute to gauge what they are teaching, it will provide exposure to the students about what they have to do on continual basis to stay abreast with cutting edge knowledge about the security domain.

6. CONCLUSION

The importance of Information Security training, awareness and education is now more than ever a priority for all education providers. As technology advances and connectivity increases, the need to protect information from threats, vulnerabilities and

exploits becomes more important. This can only be achieved if professionals attain an expert level of education about the complex domain of Information Security. To provide this high level of knowledge, dedicated courses need be incorporated in all Bachelors of Information Systems and equivalent programmes. While developing a framework for such a course, a holistic approach needs to be adopted that incorporates the views of the industry, other security certification providers and professionals from all disciplines of Information Technology domain.

REFERENCES

Australian Computer Crime and Security Survey (2003). Accessed May 4, 2004 <http://www.auscert.org.au/render.html?it=2001>

Deloitte (2003) 2003 Global Security Survey. Accessed May 2, 2004. <http://www.deloitte.com/dtt/cda/doc/content/Global%20Security%20Survey%202003.pdf>

Gilbert, C (2003) "Developing an Integrated Security Training, Awareness, and Education Program". Accessed May 6, 2004. <http://www.sans.org/rr/papers/47/1160.pdf>

Hinchcliffe, F. (2003) "Creating the Effective Security Awareness Program and Demonstration". Accessed May 5, 2003. <http://www.giac.org/practical/GSEC/Fred_Hinchcliffe_GSEC.pdf>

KPMG (2002) "Global Information Security Survey". Accessed May 6, 2004. <http://www.kpmg.com/microsite/informationsecurity/isssurvey.html>

SANS (2004) "The SANS Top 20 Internet Security Vulnerabilities". Accessed May 6, 2004. <http://www.sans.org/top20>

Tarte, J. (2003) "The Need for Information Security in Today's Economy". Accessed May 2, 2003 <http://www.giac.org/practical/GSEC/Jeff_Tarte_GSEC.pdf>