Abstract

This paper investigates the New Zealand tertiary education system: is it geared to provide information technology professionals with appropriate tools to countermeasure information security threats, vulnerabilities and exploits. Arriving new technologies will render existing information security measures obsolete and will increase security risks in both new and legacy environments. In an endeavour to address the issue of whether or not the New Zealand tertiary education system is equipping our future information technology specialists with skills to combat these security risks, an audit of a range of Bachelor's qualifications offered at New Zealand tertiary institutes was undertaken. The level of information security taught in different programmes was assessed and industry security requirements were analysed to identify possible gaps. Based on the results, a framework for the development of an undergraduate information security paper is proposed.

Keywords

Information security, undergraduate degree, information technology

1. Introduction

Like the industrial revolution of the 18th and the 19th centuries, we have witnessed a technology boom in recent times that falls no short of a significant revolution. As with any major advancement, it affects the society both negatively and positively.

One of the major positive effects 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 of information threats. As organisations continue to move more of their business online and as they upgrade to newer, better, faster, feature-laden software, their vulnerability to cyber attacks grows, and so does the pressure on security professionals entrusted to keep the infrastructure safe (Kuhr, 2004). Not only are the perpetrators able to exploit the old existing vulnerabilities in new and creative ways, but their number continues to rise and the nature of the threats becomes more and more sophisticated.

The CERT coordination centre in the United States reports that the total number of the annually 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 12946 (Tarte, 2003). The total increase in reported vulnerabilities since 1995 was more than 7571%. Information systems vulnerabilities have grown exponentially over the years. According to Captain Robert Renko, operations chief for the Defence Computer
Forensics Lab (a division of the Defence Cyber Crime Centre), it is not really the latest and most technological exploits that are the cause of an attack but rather the poor security practices that "facilitate" the greatest intrusions (Armstrong, 2004).

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 (SANS, 2004).

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 the world's largest organisations, "...average direct loss of all breaches suffered by each organisation is USD$108,000."

2. New Zealand Tertiary Audit

The information security programmes that were offered in semester 1 and 2 in 2003 and semester 1 in 2004 were first analysed and the results presented at the NACCQ conference in July 2004. After this initial analysis, further research was conducted on the information security programmes offered in semester 2, 2004 and summer school 2004/2005 (for those institutes that offered these programmes in summer school). After analysing both sets of results, it was concluded that there had been no major change in the types of courses offered in these programmes and that the findings of the previous study and the findings of the current study remain the same i.e.: only one undergraduate programme has a few dedicated papers in information security or the equivalent:

- All programmes have some aspects of security taught in certain papers.
- No programme has enough courses to qualify "security" as a dedicated stream (major).
- None of the courses have content which is more than half "information security" (except one).
- There are many courses that do not investigate any aspect of security, even though security is pertinent to the contents of the paper.
- There are a few papers on network and web security at level 2 and 3 of the NZQA framework (certificate level).

Both the previous and the current study reiterate the fact that although small amounts of this subject are definitely taught in little pockets in different programmes, no specialisation in information security is being offered. This basically means that New Zealand information technology graduates are currently only being taught how to be "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 (IT) graduates in New Zealand are receiving training only at "beginning" to an "intermediate" level of coverage of the domain. According to this model, training at beginning level provides foundation knowledge whilst intermediate level enhances breadth and/or depth of security knowledge and skills.

None of the programmes provide platform for "advanced/expert" level training. An individual trained at this level will be able to apply knowledge and skills attained through training to mission critical information technology security problem solving and technology assessment. However, the New Zealand tertiary sector is not producing such graduates.

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. Certification at the lower end of the spectrum does not necessarily contain specific modules about security however higher end certification programmes such as 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 certification programmes some of which
focus on certain aspects of security to a reasonable technical level; its highest certification CCIE is offered with security as a specialisation. All modules of all certifications from Cisco has a reasonable amount of coverage about information security.

Novell's Master CNE certification contains a module specifically dedicated to security while all other certification programmes have various levels of security 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. This security certification can also be cross-credited to other advanced qualification like MCSE.

Certified Information System and Security Professional (CISSP) certification is the ultimate goal for an information security practitioner. To become a CISSP, the candidate needs to pass the appropriate examination, to have a college degree and to have 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 several common elements. Most needs the holder to resist refresher examination after a certain time period; others simply, while some require ongoing maintenance by attending security conferences, delivering guest speeches, or participating in other similar information security related activities. Secondly, all certification programes cover topics across multiple domains in information technology (application, databases, networking and programming). And finally all curricula change frequently.

**4. What the Industry Wants**

One of the key finding of the 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% 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.

Looking overseas, the financial services industry in the United States of America has spent untold billions on security infrastructure policies and plans. However, despite spending billions, more than half of IT and security professionals working for financial companies say they are unprepared for a cyber attack (Information Security survey - cited in Barlas et al, 2004). The information security survey further illustrates that about two-thirds of telecom IT sector respondents, more than half of the energy sector respondents, and more than three quarters of government security professions surveyed believe that their industry isn’t prepared for a cyber attack (Barlas et al, 2004). According to Symantec's latest report on Internet security, attacks on the e-commerce industry (defined as industries that conduct their businesses online-- e.g. Amazon.com) have increased by 400 percent, while attacks on small businesses have risen threefold (Perry, 2004). As the Deloitte & Touche USA LLP study states, there has been a fundamental shift in the marketplace; from the traditional to the volatile dotcom economy - the emerging marketplace is moving fast, with even more threats of disruption.

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 areaa, they also want professionals who have "expert" level security knowledge about all domains of the information technology spectrum, to be able to handle combat the daily occurring information security situations. As attacks and exploits continue to evolve and evade each new security technology achievement (Kuhr, 2004), IT security will remain a major executive's concern for the "foreseeable future" (Gartner, as cited in Jaques, 2004). The industry need experts who have built their reputations around getting security right for the business - whether it is someone from within the industry, or a dedicated third party
managing security. Such experts will know how to respond to the new paradigm of "maximum uncertainty".

5. A Framework for an Undergraduate Information Security Paper

Undoubtedly, the contents of the Bachelor's programmes in New Zealand do not provide ample coverage of information security in different courses as the audit of the 2003/2004 Bachelor in Information Systems or equivalent qualifications survey has illustrated. Currently information security is taught in little nuggets in different courses. Such syllabi prepare graduates only 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 could be carved for them to become "experts" in the domain of information security should 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 stream in Bachelor's degrees.

In the short term, a framework for at least one course should be developed and the paper offered to students in all Bachelor of Information Systems and equivalent programmes. The following specific strategies are proposed 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 should have had a good exposure to all disciplines of information technology, in order to be able to appreciate the importance of the topic.
- The paper should be offered as a core paper for all IT graduates rather than as an elective so that all graduates could obtain a fair understanding of security issues before graduating.
- There needs to be a multi-discipline approach to information security: 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 be technical rather than management oriented, delving into intricacies of information security. This will develop students’ skills at troubleshooting, implementing and managing security solutions.
- Incorporating practical workshop sessions with simulations will expose students to to real world security vulnerabilities, threats and exploits.

There needs to be a commitment to revise contents frequently to incorporate new developments in information security. This can be achieved by analysing what the industry wants from its security specialists, by checking what industry certification programmes deliver, and by general and regular research about information security. The course could be aligned with an industry certification programme, e.g. CISSP. This will allow students to understand better their their future task and to stay abreast with the cutting edge knowledge in the security domain.

6. Conclusion

The importance of informations 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, a dedicated course needs be incorporated in all Bachelor of Information Systems and equivalent programmes. While developing a framework for such a course, a holistic approach needs to be adopted that incorporates the view of the industry, of other security certification providers and of professionals from all disciplines of the information technology domain.

References
