CURRENT STUDIES IN COMPARATIVE EDUCATION, SCIENCE AND TECHNOLOGY, VOLUME 2, NUMBER 2, 2015, PP. 403-425

Barriers to Quality Information Security Awareness Program in Computer Science

Onwudebelu Ugochukwu
Federal University Ndufu-Alike Ikwo, Abakaliki, Nigeria

Ifeanyi-Reuben Nkechi Jacinta
Rhema University, Aba, Nigeria

Uchenna C. Ugwoke
Federal University of Technology, Minna, Nigeria

ABSTRACT Information Security has become a serious concern not just for corporations but also for academic institutions for their normal functioning. No one is immune from cyber attacks which might be coming from various sources such as email, Facebook, ecommerce sites etc. Securing our information technology infrastructure is a major challenge with no simple solutions, nevertheless, education plays a critical role in creating a safe and secure computing environment. However, looking at the academic sector we are bound to ask if the sector is actually playing its part in educating the undergraduates on the issues of information security. Consequently, the Computer Science program in each institution needs to initiate the development of a rich set of courses and experiences to provide students with a solid foundation in information security awareness. The Computer Science department curriculum must reflect the reality concerning the threats posed by hackers as hackers cannot be completely stopped from trying to breach the networks. The users on their part need to know the perpetual battle that is raging in the cyber space as the intensity of the battle increases users' awareness likewise need to be up so as to keep abreast to most current innovative cyber threats. This paper assesses the quantity and quality of information security awareness programs from eleven universities as well as it discusses the barriers to quality information security awareness program in Computer Science.

Keywords: Information Security, Information Assurance, Curriculum, Undergraduate, Computer Science Curriculum, Hackers, Security Awareness

Introduction

Prior to 1999, universities in Nigeria were all entities of federal or state governments and the mission of those universities is to improve literacy, increase scientific and technological research as well as train human resources for the developmental needs of the country (Nnadozie & Nnadozie, 2008). With a need to deregulate and liberalize higher education, the government monopoly of universities in Nigeria was broken in 1999 with the licensing of the first private universities. Most commenced academic activities almost immediately and have been contributing to the Nigerian nation since then.Information is the lifeblood of any corporation as well as any nation. It is fundamental to the success of all business functions, from the daily operations of the various business units to supplying records on any aircraft when requested by the proper authorities. If any of the information is improperly disclosed, manipulated, or deleted, the results can be costly and disastrous. The Internet has come to stay and is becoming a part of everyone's daily lives. Simple things such as shopping, sharing files, chatting, and working now happen over the Internet. Today, the online environment is much less collegial and trustworthy. Furthermore, it contains dangerous files, scammers, virus and risks (PhysOrg, 2014). Therefore, information security becomes one of the biggest issues we face today. Many organizations are trying to deal with the shortage by focusing on internal promotion and educational efforts. Security has been a technically challenging problem with computers almost from the first instance of their operational use. Besides, networking brought greater security challenges and the arrival of the Internet (network of networks) is bringing even greater challenges (Al-Hamdani, 2006). Part of the challenge is the fact that information systems are changing quickly, and at the same time security menaces also change very quickly as new threats, vulnerabilities and attack tools are introduced. Consequently, it is an attractive target for attackers to operate and carry out their mischievous activities, making Internet attacks easy to accomplish, difficult to detect and hard to trace.

Constant reports of government network and computer compromises illustrate the importance of providing opportunities for awareness program in information security (Radha, 2005; Savola, 2007). Recently new threats such as social engineering attacks, denial of service attacks, cyber attacks amongst nations along with various vulnerabilities have cemented the need for information security awareness and hence governments commitment to research in security. Awareness as defined in NIST, "is not training". The purposes of awareness presentations in this case are simply to have knowledgeable on or to be well-informed about information security issues. Moreover, awareness presentations are intended to allow individuals to recognize IT security con-

cerns and respond accordingly. Awareness also implies understanding the reality of risk, Internet threats and vulnerabilities. In simple terms, the number of vulnerabilities continues to rise, while hacker tools are becoming more powerful and easier to use. At the same time, prevention is much more difficult because the technology changes rapidly. A few examples of IT information security awareness materials/activities include promotional specialty trinkets with motivational slogans; a security reminder banner on computer screens, which comes up when a user logs on; information security awareness videotapes; and posters or fliers (Al-Hamdani, 2006).

Information security awareness must be discussed along side with information assurance. Information Assurance is critical to the protection of any data or knowledge management system (Multari, 2004; Bhagyavati, Olan, Naugler & Frank, 2005; Weiss, 2007). If implemented correctly, it can ensure the following four attributes: confidentiality, integrity, availability and non-repudiation. Though, Information Security is an emerging area there are enough solutions and products available which are being deployed at various levels (Multari, 2004). Also, information security practices and policies has been in place (Bhilare, Ramani & Tanwani, 2009). However, the problem is that, how is this reflected in our curricula, moreover, especially in Computer Science curricula across the country both in public and private universities?

The Nigeria Government and its various departments are becoming more dependent on computer networks, systems and software and therefore more vulnerable to hostile intelligence gathering as well as computer network attack just like the U. S. Government (Hamilton, Owor, Dajani & Tapia, 2009). In a November 1957 Presidential address entitled "Science in National Security," Eisenhower observed that “one of our greatest and most glaring deficiencies is the failure of us in this country to give high enough priority to scientific education and to the place of science in our national life.” He also declared that the shortage of workers in highly skilled fields was “the most critical problem of all.” President Eisenhower’s 1957 assessment is valid in 2015 even in Nigeria. A new study carried out by RAND Corporation suggested that the nationwide shortage of cyber security professionals in USA is posing risks for national and homeland security (PhysOrg, 2004; ZDNet, 2004; Halzack, 2014). Leading industry experts say this talent gap is only getting worse. This is despite the fact that their students are given proper orientation concerning security information awareness received from their undergraduate and graduate level. In Nigeria the level of such awareness and orientation is very low as would be seen in the content of the curriculum of several universities investigated.

With the popularity and availability of web-based technology and application combined with the growth of revenues in the ecommerce sector, there has been an increasing demand for education of concepts and skills in the area of Information Security (IS), especially with regard to the Internet

(Shaikh, 2004). In this paper, we survey a few of the currently available academic programmes in Computer Science departments in eleven Nigerian universities. The purpose of the survey is not only to compare the different programmes offered but also to give the readers an idea of the IS subject area in the tertiary institution in Nigeria. We hope the survey will serve as a starting point for those readers who are interested to learn more about the scope of information security education in Nigeria.

Vaughn et al. (2004) suggested that information and computer security courses should be integrated into degree programs in at least the following three areas: computer science, software engineering, management information systems. Since it has been recommended that an entire degree program should not be created for IT security, moreover as it concerns our case in Nigeria, although some schools have done that successfully in USA. Tammy et al. (2005) lamented the fact that security professionals often focus on the need for IS/IA curriculum at the undergraduate and graduate levels. However, IS/IA training is often overlooked at the primary-school education level. They suggested one way to combat this epidemic which is to support the promotion of IA education at a much younger age. Specifically targeting elementary-level school communities with IA curricula will provide computer literacy and empowerment to those who are too often the victims of these types of crimes.

Information security awareness programs could cover the followings topics: password construction/ management, authentication, Internet usage, telephone fraud, physical e-mail usage and security, virus protection and detection, PC security, backups, building access, social engineering, identity theft and home office security (Al-Hamdani & Griskell, 2005; Ghafarian, 2007). It is often not sufficient to protect systems. No system is completely secure. It becomes necessary to be able to find out how those systems were attacked and find evidence to prosecute the attackers. We would conclude this section by saying: If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle. (Sun Tzu, ART OF WAR)

The rest of this paper is organized as follows. Section 2 describes the data used in this study. It illustrates the related information security contents derived from the academic programmes in Computer sciences departments in Nigeria universities. Section 3 discusses the implications of our findings as well as the notorious barriers as presented in Sections 3.1, 3.2, 3.3, 3.4 and 3.5. Section 4 cited the recommendations from the researchers. Finally, section 5 concludes by providing the study's contributions, and limitations.

Methodology

This research was conducted to find current IS/IA contents in the CS programs developed for undergraduate and graduate students in some selected Nigerian Universities to see if computer security topics were actually well covered in the curricula. The curriculum of 11 universities were studied in detailed, course code and course titles whose contents were related to security related topics were extracted and tabulated as demonstrated in tables 1, 2, 3 & 4. The universities were a mixture of Federal, state and private universities. A major problem we have faced is on getting the curricula, we wanted to assess all the universities curricula of the federal, state and private universities in Nigeria, but that was not the case because of this hitches. Consequently, we were able to obtain 5 Federal, 1 state and 5 private universities curricula. The tables 1, 2, 3 & 4 are the summary of our analysis. These research will help to evaluate the reality of these curricula and if there is need for enhancements or modifications.

Table 1: National Universities Commission (NUC) – CS Curriculum

S/No.	**Course Code**	**Credit Unit**	**Course Title**	**Course Contents Relating to IS**
1	CSC 304	3	Data Management 1	Information Privacy and Security
2	CSC 321	3	Systems Analysis and Design	System Design – Security
3	CSC 421	3	Net-Centric Computing	Network Security
4	CSC 432	3	Distributed Computing Systems	Security: Access Control, Key Management and Cryptography

Table 2: Federal Universities – CS Curricula

F1. University of Ibadan (UI), Oyo, Oyo State				
S/ No.	**Course Code**	**Credit Unit**	**Course Title**	**Course Contents Relating to IS**
1	CSC 221	3	Introduction to O. S.	Storage organization and protection
2	CSC 421	3	Computer Operating System II	Resource protection
3	CSC 472	3	Database Systems	Security, privacy, quality and integrity protection mechanism
F2. Nnamdi Azikiwe University (NAU), Awka, Anambra State				
1	CSC 261	2	Information technology	Computer in society – security, ethics and law
2	CSC 321	2	Operating System	Security and multimedia
3	CSC 481	3	Net- Centric and distributed Computing	Fault tolerance, security, access control, key management, cryptography
4	CSC 561	3	Data creation and management	Database security
5	CSC 62I	3	Computer Network	Computer Network Security
F3. Federal University Ndufu Alike Ikwo (FUNAI), Abakaliki, Ebonyi State				
1	CSC 107	1	Practical Skills in Computer Science	System threats: protection and security
2	CSC 307	2	Database Systems I	Information privacy, integrity and security
3	CSC 421	2	Net-Centric Computing	Network security
4	CSC 432	2	Distributed Computing Systems	Security: Access control, key management, cryptography

F4. Federal University Lokoja (FUL), Lokoja, Kogi State			
2	Introduction to Computer Applications	Computer System Protection (Virus, Trojans,	
3	Data Management I	information privacy, integrity, security; scalability, efficiency	
3	System Analysis and Design	Security	
3	Information Technology Law	Intellectual Property Laws, Computer Law and Cybercrimes, Copyright, Trademark, Privacy Protection, Piracy,	
3	Data Communica-	Network Security –	
3	Operating System 1	Design Issues influences of Security	
3	Net-Centric Computing	Fundamentals of cryptography Authentication protocols, Public-key algorithms. Types of attack, e.g., denial of service, flooding, sniffing and traffic redirection. Basic network defense tools and strategies Intrusion Detection, Firewalls, Detection of malware Kerberos, IP-Sec,	

8	CSC411	2	Introduction to Cryptography	Symmetric Encryption: The Enigma Machine, Information Theoretic Security, Modern Stream, Block Ciphers, Symmetric Key Distribution, Hash Functions and Message Authentication, Public Key Encryption and Signatures: Basic Public Key Encryption Algorithm, Primality Testing, Security Issues: . Attacks on Public Key Security, Definitions of Security, Provable Security: With Random Oracles, Provable Security without Random, advanced Protocols: Secret Sharing Scheme, Commitments and Oblivious Transfer, Zero-Knowledge Proofs, Secure Multi-Party Computation

F5.	**Federal University of Technology (FUT), Minna, Niger State**			
CSS 216	3	Cryptography Theory I	Shift Cipher, Substitution Cipher, Affine Cipher, Vigenere Cipher, Permutation Cipher, Stream Cipher. Cryptanalysis: Cryptanalysis of Affine, Cryptanalysis of Substitution Cipher, Cryptanalysis of Vigerene Cipher, Cryptanalysis of Hill Cipher, Cryptanalysis of Streams Ciphers. Perfect Secrecy. Entropy: Huffman Encoding, Properties of Entropy, Spurious Keys and Unicity distance, product cryptography	
CSS311	3	Cyber Crime and Counter Measures	cyber terrorism, cyber pornography, defamation, stalking, online gambling, e-mail spoofing, electronic transaction forgery, etc	
CSS 312	3	Cryptography Theory II	Security of ELGamal: Bit Security of Discrete Logarithms, Semantic Security of ElGamal Systems, Diffie-Hallman problems.	

4	CIT315	3	Internet Security	Security policy, strategies for a secure network, the ethics of computer security, security threats and levels, security plan, Classes of attacks: stealing passwords, social engineering, bugs and backdoors, authentication failures, protocol failures, information leakage, exponential attacks, viruses and worms, denial-of-service attacks, botnets. Active attacks: Computer security; viruses, Trojan horse and worm. Firewalls, packet filters, filtering, Cryptography: introduction to basic encryption and decryption, Diffie, Hellman key exchange, concept of Public key and Private key, digital signatures.

5	CSS 323	2	Cyber Crime Law	Cybercrimes, including computer crimes, Internet fraud, e-commerce and threats to national infrastructure. Policies, legal issues, and investigative techniques and strategies, and implications or investigation and enforcement on a global scale. Introduction to cyber law; Studies in cyber law application at the international and national levels with examples from European, North American, South American and Asian Countries; the cyber law framework in Nigeria.; Challenges and opportunities for enforcement in
6	CPT 326	2	Computer and Network Security	threats, risks and vulnerabilities, data security, policies/administration, security procedural control, security models, designing secure systems, effects of hardware on security, operating systems security, network security, database security, programming language security, cryptography, distributed systems security and information systems security

7	CPT 324	2	Information Management	Social issues in information technology: Intellectual property; computer crime; privacy; security and civil liberties; Security and control issues**:** overview of problems and standard solutions; database integrity; transactions; the role of encryption.
8	CPT 418	2	Electronic Commerce Technology	Security for electronic commerce.

Table 3: Private Universities – Computer Science/ Information Technology Curricula

P1. Rhema University (RU), Aba, Abia State				
S/ No.	**Course Code**	**Credit Unit**	**Course Title**	**Course Contents Relating to IS**
1	CSC 214	3	Operating System 1	Influences of Security
2	CSC 215	2	Introduction To Information Processing and File Structure	Data Security and Control
3	CSC 314	3	System Analysis and Design	System Design – Security
4	CSC 411	2	Database Design and Management 1	Information System Security

P2. Bells University of Technology (BUT), Otta, Ogun State				
1	CSC 203	2	Introduction to Software Engineering	Security and Reusability
2	CSC 205	2	Introduction to Operating System	Privacy and Security
3	ITP 301	3	Introduction to Internet Technology	Internet Security
4	ITP 306	3	Information Science	Security in Information Exchange across Net-
5	ITP 405	3	Management Information System	Information Privacy, Integrity, Security and
6	ITP	3	Information System	Information System and
P3. Covenant University (CU), Ota, Ogun State				
1	CSC	2	Computer Application	Safety precaution
2	CSC 214	2	High Performance Computing & Database Management I	Information privacy; integrity, security, efficiency and effectiveness.
3	CSC 225	3	Operating System II	Design Issues Influences on Security
4	CSC	3	Systems Analysis and	System Design: Security
5	CSC 315	3	Internet Programming	Network Security
6	CSC 414	3	High Performance Computing & Data	Recovery and security issues.
7	CSC 427	3	Distributed Computing Systems	Security: Access Control, Key Management,

P4. Crawford University, Igbesa, Ogun State				
1	CSC 201	2	Web design and security	The content has no related topic on security
2	CSC 206	3	Operating System I	Protection and security in operating systems
3	CSC 307	4	Database design and management	Database privacy, security, failure and recov-
4	CSC 308	3	Operating System II	Network structure & security in O. S.
P5. Salem University (SU), Lokoja, Kogi State				
1	CSC 206		Computer Architecture, organization and	Influences of security
2	CSC 303		Database design and Analysis (data man-	Information privacy, integrity, security
3	CSC 308	3	Operating System II	Network structure & security in O. S.
4	CSC 406		Cryptography, Network Control & Security	Intrudes, Viruses, Worms, Disaster Recovery, developing secure computer system, network and telecommunication security, effectiveness of database security

Table 4: State University – CS Curriculum

S1.	**Benue State University (BSU), Makurdi, Benue State**			
S/ No.	**Course Code**	**Credit Unit**	**Course Title**	**Course Contents Relating to IS**
1	CMP 341	2	Information management	Information privacy, integrity, security, and presentation scalability, efficiency and effectives.
2	CMP 462	2	Social and Professional Issue	Risk and liabilities of computer based systems, computer crime
3	CMP 464	2	Computer Center Design and Management	Security management, Use of passwords and access control mechanisms, security issues and firewalls, Network Security – Fundamentals of cryptography, secret key algorithms, public key algorithms, Authentication protocols, digital signature

As can been seen from tables 1, 2, 3 & 4, many Computer Science (CS) departments does not have courses in information security or assurance. Although, the course contents of some of the course titles contained topics on IS/IA, nevertheless, no course title was entitled information security or information assurance. Such assessment gives an idea of present state of security awareness of a student graduates from these institutions and exposes areas where more attention is required. Every student in CS both undergraduate and graduate should be able to understand the underlying concepts/ technological approaches of IS and have significant knowledge of IA.

Discussion

Recently, there has been a surge in the rate at which users of computer systems are being defrauded via email, Facebook, fictitious or masquerading web sites leading to the need for the development of academic programmes focusing on information security awareness. The increasing body of theory and knowledge in this particular field and industry are the main driving force behind this trend – cyber crime. Interestingly, the IS education in Nigeria is being developed and delivered at various different levels catering to the demand of students both in undergraduate and postgraduate study. The discussion that follows provides a suggested approach that will lead to a better taught and more information security awareness undergraduate program in CS courses that is offered. In all the tables above, no computer forensics course or content was cited either as a stand-alone course or content in the entire program.

In addition to including security topics in the courses above, it is important to offer a concentrated and focused security course that helps to tie the above together. This course should include laboratory exercises, past and current security attacks and their historic basis. Information security courses should be made a compulsory course rather than a required or an elective one for all CS students. Students from other discipline who have an interest in information security area or those students who want to get an idea of what this specific field entails should take it as an elective course. This approach will help the student from an example point of view to connect the theory approach and real world application. Furthermore, it is expedient to expand information security courses across university disciplines and thus build a diverse, regional concentration of expertise that will help students from other discipline to be well prepared to survive in this Internet age.

As cyber-attacks have increased and there is increased awareness of vulnerabilities, there is more demand for the professionals who can stop such attacks and guard themselves against such attacks. Analyzing the tables it is obvious that most tertiary institutions such as F1, F2, F3, P1, P4, P5 and S1, do not have a comprehensive information security program as a stand-alone curriculum already. But educating, recruiting, training, and hiring these cyber-security professionals take time. That is why it is essential to start educating and training students in the first year of study, sadly, as can be seen from our tables, there was virtually no course content for first year students in their curricula except in F3 and F4 where we have CSC 107 (systems threats: protection and security) and CSC 102 (computer system protection: virus, Trojans and worms) respectively. Consequently, universities should be encouraged to offer information assurance (IA) and information security (IS) courses in their curricula from the first year. Analyzing the IS content of the

available curricula, we discover that there were some barriers that mitigate a proper establishment of information security awareness program in CS departments in Nigeria.

The Lack of Up-To-Date Lecture Material

In order to satisfy the needs of information professionals from industry, government and others there is a need to develop IS/IA course to enhance education. A serious challenge we have faced is that there is a rapid change in CS, IT and security techniques. A well developed information security course should be designed in such a way as to reflect these changes in a timely manner as well as keeping the lecture material up-to-date. For example, F1, F2, F3, P1, P4, P5 and S1 were not updated as current topics on information security issues were not included. This IS course should include: the basic notions of confidentiality, integrity, availability, authentication models, protection models, security kernels, audit, intrusion detection, personnel/ operational/ physical security issues, policy formation and enforcement, trust modelling, risks and vulnerabilities assessment, basic issues of law and privacy, trade secrets, employee covenants, database protection, access control, secure operating systems and others. Keeping the lecture material up-to-date is a key issue for teaching the IS course. This allows students to learn new advanced technology and most recent cyber attacks and new threats in relationship to today's technology. After students had learned basic knowledge and techniques of IS, they can be introduced into advanced Web security related research topics, such as client side security, server security, security visualization and Web applications security, modular intrusion detection etc. This is very necessary because as a Web server provides more functionality, it is however easier to be attacked and exploited by hackers (Yu, Liao, Yuan & Xu, 2006).

The Lack of Cyber Defender Laboratory (CDL)

The lack of cyber defender laboratory connecting the classroom knowledge with real world applications is another barrier that must be overcome. The absence of a dedicated lab or use of a remote and isolated lab makes it essential to furnish exercises that, on the one hand, provide meaning to theoretical concepts and, on the other, can be conducted on students' home machines or work systems (Bhagyavati, 2006). Making a connection between the classroom knowledge and real world Web applications in a laboratory will help in creating or imparting information awareness program in Nigeria. We cannot teach the IS course entirely in the classroom because IS/IA and Web security is the field where network meets the real world. Students will have the opportunity to practice learned knowledge in the CDL. All the universities (FI-

F4, P1-P5, S1) in the tables lack a dedicated lab for information security except F5, nonetheless, each can still make use of their computer lab as a makeshift arrangement.

The Lack of Access to Reputable Journals and Websites

Students should be given access to reputable journals such as IEEE, ACM etc. Furthermore, they should be guided to choose and read the published papers to keep up with the pace of new technologies and associated security threats. Each student must select and read recently published papers, present them using power point, discuss their opinions in the classroom, and write a report. Our experience from other courses exhibits that using the hybrid teaching approach can successfully integrate education, research and real world applications into the IS course. This will stir students to gain important insights into how theoretical and practical concepts apply to real world application problems, and draw their interest towards security research. Apart from reputable journals, students need to be exposed to reputable websites and useful resources that contain freeware such:

www.belarc.com/free_download.html
www.mailwasher.net/download.php
www.sourceforge.net
www.insecure.org
www.annoyances.org
www.sans.org and the CERT agency.

The Lack of Stand-alone Courses on Information Security

Information security and information assurance are important topics that compel the attention of future computer scientists. Looking from our tables F1, F2, F3, P1, P3, P4 & S1, it is obvious that undergraduate students in CS programs today are not exposed to these concepts at the end of their education in stand-alone courses on IS. Only P2 has a stand-alone course entitled, “Information System Security”. As IS educators, we perceive the need to incorporate IS topics throughout the undergraduate CS curriculum as a standalone course. Notwithstanding in institutions where additional course cannot be offered in the department as a result of making an already tight curriculum even tighter, in such circumstances, the only feasible option is to insert information security and assurance across the computer science curriculum, incorporating appropriate topics in existing courses. To do this, the topics must fit well with existing topics, augmenting rather than replacing. For instance, data integrity can be taught in a database course, the vulnerabilities of memory leaks and buffer overflows can be illustrated in a course on

operating systems, and so on. Accordingly, there are a number of topics besides security that compelling arguments can be made for inclusion in an already crowded curriculum as mentioned in (North, Roy, Shujaee & Alonza, 2005).

The Lack of Resources to Incorporate Hands-On Exercises

Some challenges that might erupt are the excess of other important topics, the lack of time, the lack of commitment among lecturers, and the lack of resources to incorporate hands-on exercises, especially in online environments. Students need to learn to design and to program from their teachers. Most of the software security problems are in code written by students whom we, as a professional, taught to program however, lack of commitment among staff will truncate such benefits. Consequently, only a few students would be exposed to ideas and material that all CS students should see and obtain.

We were disappointed by the fact that most students will not be exposed to IS/IA courses in their first year even simple topic as vulnerability, was not mentioned form the tables. Vulnerability is a weak point that can be exploited from both inside and outside of an organization's network system. The World Wide Web as the fastest growing part of the Internet is also the most vulnerable part to be attacked. External vulnerabilities include viruses, worms, script kiddies, spyware, and denial of services attacks (Bhagyavati, 2006; Ghafarian, 2007). These topics should be targeted toward the undergraduates as introductory classes in their first year. Students at such level sometimes do not have the background to harden their systems against threats that are common knowledge to security professionals.

It is a hands-on exercise for students to download and execute a freely available Internet security scanner found at www.securityfocus.com/ tools/676. The direct benefits of a hands-on exercise include satisfying course objectives, covering the syllabus as well as satisfying students' curiosities about information security with long-term benefits. These make students to be involved in the learning process, suggest new activities, become motivated, engage in further research in computer security issues, and grow professionally. Finally, we are subject to use some non-traditional awareness programs (that is, non-class method), such as: TV programs on nationwide level, Video and CD classes, simple guidelines publication, etc. All these should be carefully prepared and focused the level of awareness on the general public as they cannot be left behind in the issue of information security awareness program in Nigeria.

Recommendations

- Each CS department should maintain an up-to-date record of major IS risks.
- IS awareness should be revised because in each month there are many new threats.
- The lecture notes should be updated every semester based on published research results to keep the lecture material up-to-date.
- The CS program should have plans for general studies and interdisciplinary courses incorporating IS/IA related topics to be offered with Criminal Justice Program.
- Government, universities and companies entities should all focused on finding ways to close the gap created by these barriers through proper IS awareness programs.

Conclusion

Information security/information assurance is becoming more and more important in practice and needs to be integrated into the CS curriculum. The barriers and hurdles towards the rapid awareness of IS in CS in Nigeria are: the lack of up-to-date lecture material, the lack of cyber defender laboratory, the lack of access to reputable journals and websites, the lack of stand-alone courses on information security and the lack of resources to incorporate hands-on exercises. It is the opinion of authors that where CS program exists, IS courses should be included in the curriculum. There are two ways to do that: a specialized course and components that can be integrated with existing courses at different levels (in the case of a tighter curriculum). Security is, after all, a user requirement that must be satisfied. Given that the so-called social engineering, corporate policy, disgruntled employees, insufficient background checks, etc. are a major security concern, it is imperative that undergraduate and graduate students consider the holistic nature of information security. We also emphasize the importance of practical sessions. Security and reliability can only be assured if our students develop good programming habits (training and retraining) so that even under pressure they check all input, document their code and test appropriately. Students with such a background will be ready and prepared for more specialized IS/IA courses.

The purpose of the survey is not only to compare the different programmes offered but also give the readers an idea of the IS subject area in the tertiary institution in Nigeria. We hope the survey will serve as a starting point for those readers who are interested to learn more about the scope of IS education in Nigeria. A major problem we have faced is on getting the curricula and we hope various institutions will have an online version of their curricula. Our findings and experience shows that integrating education, research and practical applications into the information security course are es-

sential for a sound IS education. Using this approach instructors and students are able to connect knowledge in the classroom to real world applications. This will attract students to the security area and train students to become IS professionals that will help the government, industry and higher research institutions.

Correspondence

Onwudebelu Ugochukwu
Computer Science Department
Federal University Ndufu-Alike Ikwo, FUNAI
P.M.B. 1010, Abakaliki
Ebonyi State, Nigeria
Email: anelectugocy@yahoo.com

Ifeanyi-Reuben Nkechi Jacinta
Computer Science Department
Rhema University, Aba
Abia State, Nigeria

Uchenna C. Ugwoke
Department of Mathematics & Computer Science
Federal University of Technology (FUT)
P.M.B. 65, Minna
Niger State, Nigeria

References

Al-Hamdani, W. A. 2006. Assessment of Need and Method of Delivery for Information Security Awareness Program, Information Security Curriculum Development (InfoSecCD'06) Conference, ACM, pp. 102 -108

Al-Hamdani, W. A. & Griskell, I. J. 2005. A Proposed Curriculum of Cryptography Courses Information Security Curriculum Development (InfoSecCD'05) Conference, pp. 4 – 11

Bhagyavati (2006) Laboratory Exercises in Online Information Assurance Courses, ACM Journal on Educational Resources in Computing, 6(4), pp. 1-5

Bhagyavati, Olan, M., Naugler, D. & Frank, C. E. 2005. Information Assurance in the Undergraduate Curriculum, 43rd ACM Southeast Conference, pp. 25-26

Bhilare, D. S., Ramani, A. K. & Tanwani, S. 2009. Information Security Assurance for Academic Institutions Using Role Based Security Metric: an Incremental Approach, International Conference on Advances in Computing, Communication and Control (ICAC3'09), ACM, pp. 535-540.

Ghafarian, A. 2007. Ideas for Projects in Undergraduate Information Assurance and Security Courses by ITiCSE'07, ACM, p. 322

Hamilton, J.A., Owor, R. S., Dajani, K. F. & Tapia, R. 2009. Building Information Assurance Education Partnerships with Minority Institutions, Celebration of Diversity in Computing Conference, ACM, pp. 58 - 63

http://www.PhysOrg.com Shortage of Cybersecurity Professionals Poses Risk to National Security (06/18/14)

http://www.ZDNet.com Cybersecurity's Hiring Crisis, August 25, 2014

http://www.iwar.org.uk/comsec/resources/canadaia/ infosecawareness.htm

Multari, N. J. 2004. Information Assurance Technical Challenges**,** SIGMOD 2004, ACM

Nnadozie, C. O & Nnadozie, C. D. 2008. The Information Needs of Faculty Members in a Nigerian Private University: A Self-Study Library Philosophy and Practice

NIST Special Publication 800-50 Building an Information Technology Security Awareness and Training Program

North, S. M., Roy G., Shujaee, K., & Alonza M. 2005. Collaborative Information Assurance Capacity Building at a Consortium of Colleges and Universities, 43rd ACM Southeast Conference, ACM, pp. 361-362

NSTISSI No. 4014 August 1997 National Training Standard Information Security Officers (ISSO)

Radha P. 2005. Information Assurance in Manets and Wireless Sensor Networks, SASN'05, ACM, p. 32

Savola, R. M. 2007. Towards a Taxonomy for Information Security Metrics, Quality of Protection (QoP'07), ACM, pp. 28 – 30

Shaikh, S. A. 2004. Information Security Education in the UK: a proposed course in Secure E-Commerce Systems, Information Security Curriculum Development (InfoSecCD'04) Conference, ACM pp. 53- 58

Tammy A. & Rackley, C. C. 2005. Integrating Information Assurance (IA) Into K-5 Curriculum Information Security Curriculum Development (InfoSecCD'05) Conference, ACM, pp. 1-3

Vaughn Jr., R. B., Dampier, D. A. & Warkentin, M. B. 2004. Building an Information Security Education Program, Information Security Curriculum Development (InfoSecCD'04), ACM, pp. 41 - 45

Halzack, S. 2014. Washington Post: Shortage of Cybersecurity: Workers Is a Problem That Will Solve Itself.

Weiss, R. 2007. Adding Information Assurance to the Curriculum: Tutorial presentation, Consortium for Computer Science in College **(**CCSC): North western Conference, pp. 46-48

Yu, H., Liao, W., Yuan, X. & Xu, J. 2006. Teaching a Web Security Course to Practice Information Assurance, SIGCSE'06, ACM, pp. 12 – 16**.**