SOFTWARE SECURITY AWARENESS FRAMEWORK: MANAGEMENT PERSPECTIVE

Arpita Banerjee[1]
Asst Prof , Department of Computer Science, St Xavier's College, Jaipur

C Banerjee[2]
Associate Prof, Suresh Gyan Vihar University, Jaipur

Nitesh Kaushik[3]
Associate Prof, Suresh Gyan Vihar University, Jaipur

Abstract

World's economy depends on the secure use of software and adds value to it in terms of people trust. Statistics world-wide have shown that unsecured software makes the system vulnerable, prone to attack and endangers intellectual property, business operations and services resulting in severe financial damage. A wide range of technology is readily available to safeguard the system from outside attack but when it comes to inside attacks, apart from technology, a more strategic and tactical practice needs to be adopted by organizations which influences the psychological aspect of people involved thereby creating awareness among them with focus on inter-functional and intra-functional dimension. Awareness in terms of software security can be created among two key classes of people, those who develop software in an organization and those who use software in an organization. This research paper highlights the importance and utility of various manual and automated software security awareness tools, techniques, methods, methodologies, standards, etc developed by various academic and non academic bodies with their limitations. The paper further investigates and identifies the various teams and stakeholders involved in software development and practices with special mention of the Management Team in terms of development and use. The paper further proposes a software security awareness framework from management point of view which is a step further towards addressing of the software security awareness issue in its entirety.

Introduction

People, information, operations, and systems are significant assets of any organization. The confidentiality, integrity, and availability of these assets along with its safety and protection are indispensable to maintaining productivity, compliance, and a competitive edge. Almost all organizations face frequent threats which could endanger their employees, systems, operations, and information in a very substantial way. Apart from natural disasters, threats may include computer viruses, network attacks, hacking and cracking, denial of services, fraud, etc. Various tools and procedures are adopted by organizations to protect against these threats. But it is very unfortunate that even the best tools and procedures implemented by the organization can be ineffective

1 smart_apt@yahoo.co.in
2 chitreshh@yahoo.com
3 niteshkaushik29@rediffmail.com

because of the lack of awareness about how to use them and how the security is an important factor for the survival of an organization (Security Awareness).

Since 1977, there have been reports of security breach. In recent past, some of the security incidents of significant importance are worth mentioning. A security breach leads to numerous phishing scams and countless identity theft claims in which names and e-mails of millions of customers, which were stored in more than 108 retail stores plus several huge financial firms like CitiGroup Inc. and the non-profit educational organization like College Board, were exposed in March 2011. The personal information of 35 million South Koreans was exposed after hackers breached the security of a popular software provider in July-Aug 2011 (Armerding 112-115; Kizza 112-15; "Hacking and System"). Estimated revenue losses due to piracy worldwide reached 51.4 billion dollars in 2009, with 16.5 billion dollars loss along in Asia-Pacific region as compared to 11.6 billion during 2006 (Tsipenyuk 81-84; "Training and Awareness"). In 2012, a US woman was sentenced to five years in prison for her role in phishing ring that netted members more than US$1 million and a 31 year old US man, pleaded guilty to his part in a phishing ring responsible for defrauding people of over US$1.3 million ("InfoSec in the News")

The software is attacked and the system is threatened both by the outsider and the insider. The sole intention of the outsider is breaking into the system by manipulating access rights and permission resulting in unauthenticated and unauthorized access. The organizations in this regard may use available technological controls which are extensively being used to tighten access controls and minimize persistent threats, and thereby provide shield to the system from outside attack. Further, when there is an attack from inside the system, the authenticated and authorized user goes beyond their designated access rights and permissions to corrupt the system (Banerjee 1-5). In 2010 a joint survey in the name of Cyber Security Watch Survey was conducted by CSO Mazagine, the US Secret Service DELOITTE center for Security and Privacy Solution and Software Engineering Institute at Carnegie Mellon Institute, US and it was found that almost 51% of the participants experience an inside attack. Although 15 well known security policies and procedures aimed at preventing insider's attack were implemented in the system but they lacked management angle. Another survey shows that approximately, on an average, 72% of the insiders incident are internally dealt with, and no legal action or low enforcement is involved. This shows a lack of management perspective, and due to such incidents an estimated $691 million loss was reported ("Cyber Security Watch Survey"; Cappelli).

To safeguard the entire system management perspective should be given due respect and a sound mechanism should be devised along with its technological counterpart for proper implementation of security in its entirety. One such mechanism may be adopted by providing psychological treatment in the form of awareness for the people involved supported with interfunctional and intrafunctional dimensions (Banerjee 1-5). Security awareness can be created among two key classes of people, one who develops software in an organization and one who uses software in an organization taking into account a holistic and balanced approach to technology as well as management aspects (Olzak). Many such mechanisms developed by various academic and nonacademic bodies are available in the market but none of them properly address the software security awareness issue in its entirety. Further, these awareness programs lack adequate coverage of management and its processes related to security for incorporating software development and practices (Paul).

Keeping this in mind, we present the research advances in this area. The rest of the paper is organized as follows: section II encompasses the meaning and importance of software security awareness, section III highlights the importance and utility of various manual and automated software security awareness tools and techniques, methods, standards, etc. developed by various academic and nonacademic bodies with their

limitations. In section IV, further investigations and identification of various teams and stakeholders involved in software development and practices are being presented with special mention of the management team in terms of development and use. Section V proposes a software security awareness framework from the management point of view which is a step further towards addressing of the software security awareness issue in its entirety. The conclusion and future works are reported in section VI.

Security Awareness

Security awareness can be defined as the knowledge and protection of the physical and information assets of an organization which its people should possess. The understanding and addressing of various security issues is also reflected in the attitude and motivation of an organization's people. Security awareness promotes a cultural and behavioral change among the people of an organization regarding security. If the people of an organization have awareness about security, it means that there is a clear and evident understanding that the data and other resources of an organization may intentionally and deliberately or unintentionally and accidentally be stolen, damaged or misused by some people (Security Awareness).

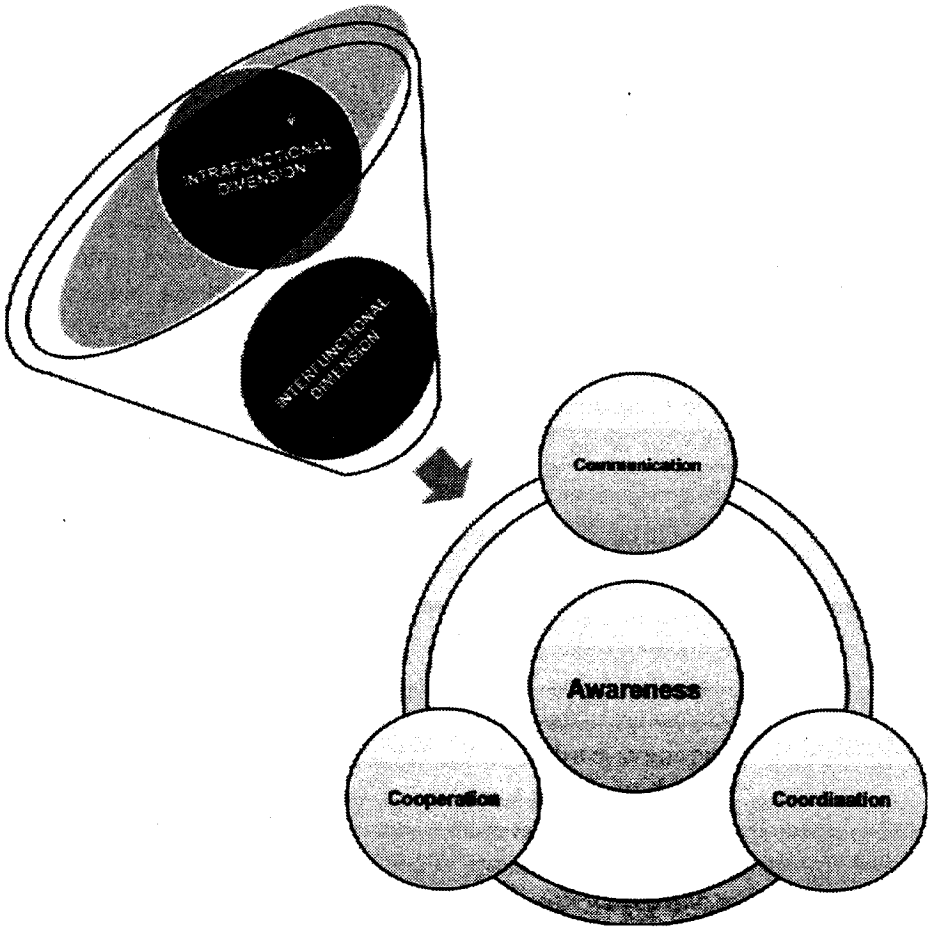


Figure 3: Cs for Creating Effective Security Awareness

Security awareness can also be defined as an organization's willingness to maintain the confidentiality, integrity and availability of information assets with a concentrated and focused attention of its employee. An individual or a group can be encouraged to recognize the various security concerns and decide how to deal with them appropriately when they arise (IT Blogs). The European Network and Information Security Agency states that awareness of the risks and available safeguards is the first line of defense for the security of information systems and networks (Sans). To promote awareness among the people with respect to technology and management perspective, the three Cs aspects needs to be dealt with as shown in the figure drawn above.

Standards, Models, Tools and Techniques of Security Awareness

Standards and models like Capability Maturity Model Integration (CMMI) (Becker 213-22), Team Software Process (TSP) (Humphrey), Trusted CMM/Trusted Software Methodology (T-CMM/TSM), Systems Security Engineering Capability Maturity Model (SSE-CMM) (Manar 83-99), Building Security in Maturity Model (BISMM) (McGraw), SysAdmin, Audit, Networking, and Security (SANS) (Information Security Research), National Institute of Standards and Technology (NIST) SP 800-50 (Computer Security) are available which, to some extent, focus on the issues of creating security awareness. Some methods like Comprehensive Light Weight Security Process (CLASP), Open Web Application Security Project (OWASP), Microsoft's Security Development Lifecycle (SDL), McGraw's TouchPoint, etc. (Pandey) are available which give due weightage to the issues of security awareness.

A number of workspace, real time and distributed architecture-awareness tools like Palantir, AUGUR, JAZZ, SeeSoft, FASTDash, etc. are available in the market for spreading security awareness (Sarma). Many researchers have proposed various security awareness techniques like awareness education and training programs, meeting the objectives like security dimensions, security strategies and policies (Olzak). Software security awareness campaign (Smith), security rules with special emphasis on the rule of awareness with focus on development of security awareness training program for acquiring new information and updation of existing knowledge related to various security aspects (Banerjee), primary level security awareness program using techniques like quiz, project and comics (Beyer), security group awareness training with emphasis on three levels of training, i.e., executive level awareness, management level awareness (Steven), and CYBERCEIGE simulation game for creating awareness regarding the need of information security and assurance (Fung).

Although many established and well-known standards are available in the market but none of them aids in spreading awareness among the stakeholders of the software development process in its entirety. Further, the models which are presently accessible are too broad to focus on the security awareness aspect of secure software development. The commercial tools available only cater to the needs of the programmer among the software engineering team. Many techniques like games, simulations, training and education, checklists, etc. are available through which any organization can spread awareness, but they are not comprehensive in nature and need massive improvisation. Further, all the present standards, models, tools and techniques are more technology oriented with less focus on the management front. Hence a more cooperative, collaborative and coordinated approach needs to be adopted in order to deal with the issue of creating optimal awareness among the people involved by exploring the unknown potentials of management perspective and blending it with technological perspective, thereby striking a balance between both of them.

Evolving Stakeholders of Software Development Process

To date, the various stakeholders of software development process – engineers, analysts, design engineers, programmers, test engineers, implementation engineers, and maintenance engineers – were seen as requirements. The individual roles were so far considered in the software development process. But with the increase in degree and complexity of software development process and the introduction of advanced software models like agile model, object oriented model, client/server model, component-based model, web-engineering model, individual teams took the place of individual roles. Specific teams like endeavor team, management team, strategy team, engineering team, post-development team and evaluation team were created to look into the specific aspect of software development process.

The endeavor team organizes and contains all other teams within an enterprise and fulfills the mission and objectives of the enterprise, program and contract.

The management team performs the following tasks:

- Oversees the development endeavor
- Performs the overall management and risk management tasks for an entire enterprise comprising of one or more related contact centers, data centers, reuse centers
- Determines when and if changes are to be implemented to baseline work products
- Manages the configuration of one or more related systems or applications and its associated work products
- Performs the disaster recovery tasks and disaster response task

The strategy team produces the digital brand identity of the customer organization's enterprise, the customer organization's new business strategy, and the technology strategy for the customer organization's reengineered business enterprise.

The engineering team performs the following tasks:

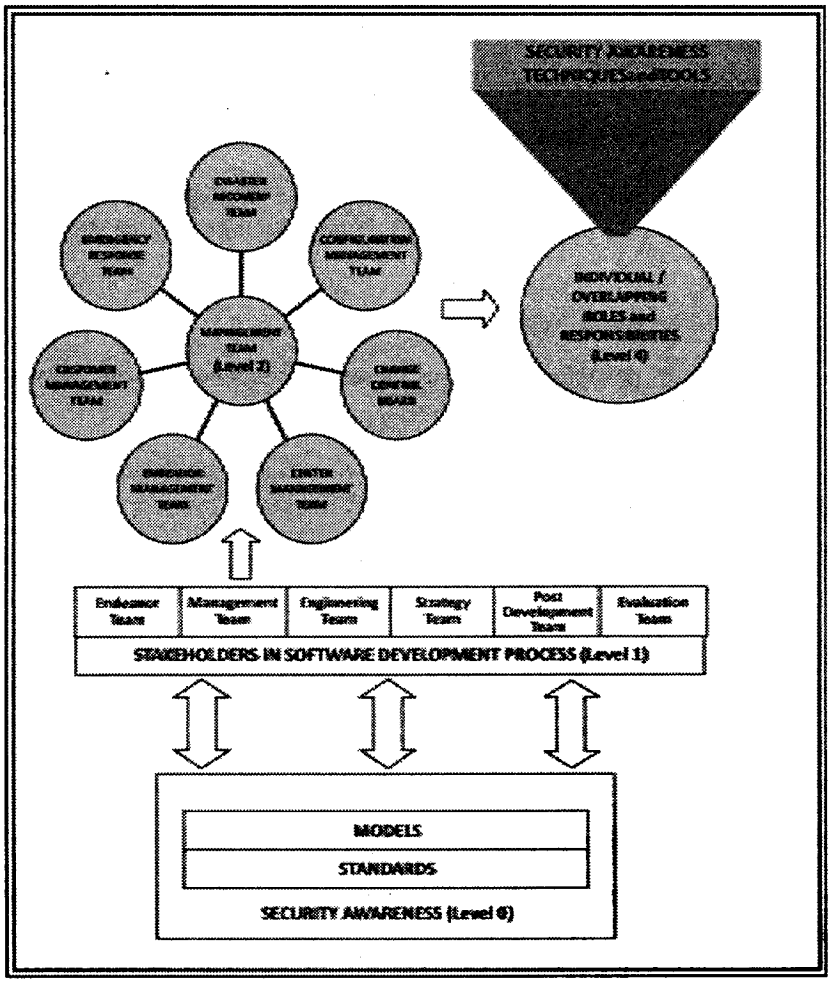
- Produces the various kinds of architecture work products, databases for one or more related systems/ applications
- Deploys a system or application to its production environments; produces and maintains one or more related environments and the hardware components of a system
- Performs most of the system and launch testing independently, without referring to the teams that developed the system or application
- Integrates the components of a system or application, responsible both for the productivity and quality metrics for an endeavor and for the methods and processes that are used on one or more endeavors
- Performs developer-independent quality engineering tasks on an endeavor, the primary requirements engineering tasks
- Supports reuse within a development, maintenance, or subcontractor organization
- Establishes and enforces the endeavor's security policies by performing the security engineering and security testing tasks

- Produces the software components of a system, application, or framework
- Provides training on one or more endeavors, and responsible for producing the user interfaces

The Postdevelopment team performs the following tasks:

- Manages the content of one or more systems or applications
- Performs the maintenance activity tasks on one or more systems or applications
- Keeps a data center and all of its applications and components functioning properly
- Keeps the list(s) of approved standard hardware and software products for the environments of an organization
- Performs the retirement tasks
- And staffs a contact center
- Provides support to the users of one or more systems or applications

The evaluation team performs one or more technical evaluations of the architecture work products,



configuration management work products, content management work products, content management process, database work product, deployment work product, environment work product, hardware design, implementation, and testing work products, integration work product, management work product, operations work product, application development requirements work, retirement work products, safety work products, and software design, implementation, and testing work products.

It is evident from the study and identification of various stakeholders of software development process that over a period of time with the increase in degree and complexity in software development process, many new teams and roles have evolved and the existing roles have been subcategorized into classified sub roles. Many new roles were introduced or existing roles were sub categorized to ease the degree and complexity factor of software development process. Individual roles and overlapping roles were distributed as per the requirements of the teams with proper demarcation of common and individual responsibilities. The management team here is worth mentioning because it plays an important role in the software security awareness framework.

Software Security Awareness Framework

The software security framework that we have proposed is based on management perspective of software development team. In the proposed framework, which depicted through a figure drawn below, level 0 includes various established standards and models of creating security awareness which forms the basis of our proposed framework. Level 0 coordinates with level 1 which includes various core teams of software development process. Further, since our paper focuses on the management perspective of security awareness, we have expended the core management team into 7 sub teams which form level 2. Level 2 further branches off into individual and overlapping roles of the 7 sub teams of core management team. Further, the security awareness tools and techniques like education/training program, awareness checklists, games and simulation, survey, tests, quiz, online community, industry/academia interaction, etc.

Conclusion and Future Work

In today's information age, systems are being attacked from varied sources and the magnitude of such attack is growing day by day. Research findings have shown that the biggest threat to a system is from an insider's attack rather than an outsider's. The extent of security concerns increases when an insider's access conspires with the skills of an outside attacker to endanger the complete system. Hence, a security framework for creating awareness with a management perspective should be designed and put into place. This could promote a sense of awareness among the employees (insider) of an organization regarding the security of the system and its implementation. This paper tried to present a critical review of some of the tangible research work on various methods of creating awareness among the employees taking into account the management angle. At the same time, a number of noteworthy research areas for further investigations in the concerned area are identified which include extending the proposed framework to include branched off sub teams and new roles of the core teams in addition to the management team. The paper will help the researchers who want to pursue their research in security awareness by providing a brief but complete review on the existing literature along with the current research topics. It will serve as a base paper for the researchers who will pursue the research topics through our paper. Future work may include the development of a concrete system for creating and promoting awareness with proper mapping of various core and sub teams with their internal and external roles with available techniques of creating awareness. Then, metrics may also be developed and applied to

the mapping for the quantification of the values. This in turn will contribute to increase the precision level of the mapping. This work will surely help the industry in implementing awareness among the employees from the management perspective which takes into account the core management team and its 7 sub teams.

Works Cited

Armerding, Taylor. "The 15 worst data security breaches of the 21st Century." 15 February 2012. Web.29 Apr 2013. <http://www.csoonline.com/article /700263/the-15-worst-data-security-breaches-of-the-21st-century>

Banerjee, C. et al. "Software Security Rules: SDLC Perspective." *International Journal of Computer Science and Information Security.* IJCSIS. USA (October 2009): 123-28. Web. 30 Apr 2013. < http://arxiv.org/abs/0911.0494>

Becker, J. et al. "Developing Maturity Models for IT Management – A Procedure Model and Its Application." *Business and Information Systems Engineering.* June 2009: 213-22. Web. 29 Apr 2013. <http://books.google.co.in/books?id=S8evz8GMI-QCandprintsec =frontcoveranddq=isbn:3642218423 andhl=enandsa=Xandei=FnN_UcD8IZHyrQe8ilHIDwandved=0CDIQ6AEwAA#v=onepageandqandf =false>

Beyer, Anja and Christiane Westendofr. "How to Establish Security Awareness in Schools." 177-86. Web. 30 Apr 2013. < link.springer.com/chapter/10.1007%2F978-3-8348-9363-5_17>

Banerjee, C. and S. K. Pandey "Research on Software Security Awareness: Problems and Prospects." ACM SIGSOFT SEN. September 2010. Web. 29 Apr 2013. <http://dl.acm.org/citation.cfm?doid= 1838687.1838709>

Cappelli, Dawn M. et al. "Insider Threats in the SDLC." 16/09/2012. *CSO Magazine.* Program. Software Engineering Institute. Carnegie Mellon University. Web. 29 Apr 2013. <www.cert.org/archive/pdf/sepg500.pdf>

"Computer Security." Web. 29 Apr 2013. <csrc.nist.gov/publications/nistpubs/800-50/NIST-P800-50.pdf>

Cyber Security Watch Survey. "Cybercrime Increasing Faster Than Some Company Defenses." *CSO Magazine.* The US Secret Service. Software Engineering Institute CERT. 25/09/2012. Carnegie Mellon University and Deloitte's Center for Security and Privacy Solutions. Web. 29 Apr 2013. <http://www.sei.cmu.edu/ newsitems/cyber_sec_watch _2010_ release.cfm>

Fung. Chun Che et al. "Raising Information Security Awareness in Digital Ecosystem with Games." 2008. pp 375-380. Web. 30 Apr 2013. <http://www.researchgate.net/publication /43980185_Raising_information_security_awareness_in_digital_ecosystem_with_games_-_a_pilot_study_in_Thailand>

Hacking and System Cracking. "Timeline of computer security hacker history." Web. 29 Apr 2013.<http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history>

Humphrey, Watts S."Introduction to the team software process." Addison-Wesley Publications. 2000. Web. 29 Apr 2013. <http://www.amazon.com/Introduction-Team-Software-Process-ebook/dp/B001FBFHD8?>

"InfoSec in the News." Security Awareness Incorporated. 15/09/2012. Web. 29 Apr 2013. <http://www.securityawareness.com/secnews.htm>

IT Blogs. "Toolbox for IT." Web. 29 Apr 2013. <http://it.toolbox.com/blogs/adventuresinsecurity/strengthen-security-with-an-effective-security-awareness-program-8707>

Kizza, Joseph Migga . "A Guide to Computer Network Security." *Springer.* 2008

McGraw, G. et al. "The building security in maturity model." Web. 29 Apr 2013. <http://www.bsi-mm.com/ .June 2009>

Olzak, Tom. "Strengthen Security with an Effective Security Awareness Program." 16/09/2012. Web. 29 Apr 2013. <http://adventuresinsecurity.com/Papers/Build_a_Security_ Awareness_Program.pdf>

Pandey, S. K. et al. "Recent Advances in SRE Research." *International Journal on Computer Science and Engineering.* 2010: 1079-85. Web. 29 Apr 2013. <www.enggjournals.com/ijcse/doc/IJCSE10-02-04-64.pdf?>

Paul, Mano. "Software Security: Being Secure in an Insecure World." 26/09/2012. The International Information Systems Security Certification Consortium. Web. 29 Apr 2013. <www.softwaremag.com/trk.cfm?uid=65>

---. "Software Security: Being Secure in an Insecure World." The International Information Systems. 26/09/2012. Web. 29 Apr 2013. < www.isc2.org/uploadedFiles/(ISC)2... /CSSLP_WhitePaper_3B.pdf?>

Sans. "Information Security Research." Web. 29 Apr 2013. <http://www.sans.org/about /sans.php>

---. "Policies." Web. 29 Apr 2013. <http://www.sandisk.com/media/226716/enisa-whitepaper.pdf>

Sarma, Anita et al. "A Comprehensive Evaluation of Workspace Awareness in Software Configuration Management Systems IEEE Symposium on Visual Languages and Human-Centric Computing." IEEE. 2007: 23-26. Web. 30 Apr 2013. <http://dl.acm.org/citation.cfm?id=1308296>

"Security Awareness." InfoSecurityLab. Web. 29 Apr 2013. <http://www.infosecuritylab.com>

"Security Awareness." Web. 29 Apr2013.<http://en.wikipedia.org/wiki/Security_awareness>

Smith, Allen M. et al. "Using Security Awareness to Combat the Advanced Persistent Threat." June 1-3. 2009. Alaska. Web. 30 Apr 2013. pp 64-70. <www.cisse.info/archives /category/12-papers?download=131...2009?>

Steven, John and Ken van Wyk "Essential Factors for Successful Software Security Awareness Training. Security and Privacy." Journal Sep-Oct 2006: 80-83. IEEE. Web. 30 Apr 2013. <http:// ieeexplore.ieee.org/xpl login.jsp?tp=andarnumber=1704791andurl= http%3A%2F%2 Fieeexplore.ieee.org%2Fxpls% 2Fabs_all.jsp%3Farnumber%3D1704791>

Talib, et al. "Secure Software Engineering: A New Teaching Perspective Based on the SWEBOK." *Interdisciplinary Journal of Information.* Knowledge and Management. 2010: 83-99. Web. 29 Apr 2013. <www.highbeam.com›Publications›Business journals?>

"Training and Awareness." Build Security In. Web. 29 Apr2013. <https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/training/256 -BSI.html>

Tsipenyuk K. "Seven Pernicious Kingdoms-A Taxonomy of Software Security Error". Nov-Dec 2005. Web. 29 Apr 2013. <http://cwe.mitre.org/documents/sources/SevenPernicious Kingdoms.pdf>