WEB DEVELOPMENT EVOLUTION: THE BUSINESS PERSPECTIVE ON SECURITY

William Bradley Glisson, Department of Computing Science, University of Glasgow, 17Lilybank Gardens, Glasgow G12 8QQ, Scotland, 0141-330-4256, glisson@dcs.gla.ac.uk
L. Milton Glisson, School of Business and Economics, North Carolina A & T State University, Greensboro, NC 27411, USA, 336-334-7846 Ext. 6004, glissonm@ncat.edu
Ray Welland, Department of Computing Science, University of Glasgow, 17Lilybank Gardens, Glasgow G12 8QQ, Scotland, 0141-330-4256, Scotland, ray@dcs.gla.ac.uk

ABSTRACT

Protection of data, information, and knowledge is a hot topic in today's business environment. Societal, legislative and consumer pressures are forcing companies to examine business strategies, modify processes and acknowledge security to accept and defend accountability. Research indicates that a significant portion of the financial losses is due to straight forward software design errors. Security should be addressed throughout the application development process via an independent methodology containing customizable components. The methodology is designed to integrate with an organization's existing software development processes while providing structure to implement secure applications, helping companies mitigate hard and soft costs.

INTRODUCTION

Some of the most precious commodities in today's business environment include data, information and knowledge. Management of the data asset is becoming increasingly challenging as the world progressively utilizes the World Wide Web to conduct business. It has been said that "one man's data can be another man's knowledge, and vice versa, depending on context".[40] Once data is collected through a Web enabled application, then the challenge morphs into information and knowledge management as businesses take advantage of the Internet, intranets, extranets, and wireless connections to their networks. As Ralph Basham, the Director of the Secret Service put it "Information is the world's new currency; information has value".[20] This point is reinforced by Thomas A. Stewart when he wrote in The Wealth of Knowledge "Knowledge is what we buy, sell, and do".[40] "Knowledge management involves capturing, classifying, evaluating, retrieving and sharing all of a company's information assets in a way that provides context for effective decisions and actions"[14]. As strategic alliances and partnerships develop, it will become increasingly necessary for a company's information and knowledge to be available to all parties in the appropriate forms, at the appropriate place and time.[14] The main conduit for this transfer of knowledge, information and data is the Web. A major management issue that has become increasingly visible in today's Web market place is the security of an organization's data, information, and knowledge assets.

Security failures cost companies staggering amounts of money and have become a global epidemic that affects everyone in the world of e-business. There are several factors that contribute to an organization's security cost. The cost associated with application development is one of those factors. An article published in Secure Business Quarterly titled "*Tangible ROI through Secure Software Engineering*" (Fourth Quarter of 2001) states that "one dollar required to resolve an issue during the design phase grows into 60 to 100 dollars to resolve the same issue after the application has shipped".[23] They also indicate that the return on investment (ROI) can be as high as 21 percent when examined during the

design phase.[23] Even if the security flaw is not caught until the test phase, Gartner estimates that the cost to fix a "security vulnerability during testing to be less than 2 percent of the cost of removing it from a production system".[35]

Competitive market pressure is forcing businesses to improve application functionality and time to market in the web development environment. This atmosphere has encouraged research in development methodologies in the area of Web Engineering. Web Engineering is "the application of systematic, disciplined and quantifiable approaches to development, operation, and maintenance of Web-based applications".[10, 11] Web Engineering methodologies do not make any direct references to security, hence today's web applications face major security problems.[17]

The purpose of this paper is to discuss the business incentive for implementing security from an organizational point of view and examines, from a business perspective, a possible solution to security issues during application development through the use of the Web Engineering Security (WES) Methodology.

BUSINESS INCENTIVE

The 2004 CSI/FBI Computer Crime and Security Survey estimates losses from internet security breaches in the US to have exceeded $141 million within the last year.[18] The PricewaterhouseCoopers (PWC) information security breaches survey estimates that the average cost, for a large company's most serious security breach, is around $220 thousand.[37, 43] The survey indicates that organizations experience an average of fifteen breaches per year.[37] It also estimates that one-third of the breaches are serious breaches involving significant cost.[37] The PWC survey also indicates that security problems are on the rise in the United Kingdom and that malicious attacks are the primary culprits.[37] A deeper analysis of the surveys indicates that Internet probing is significantly increasing. [37] It also indicates that there are problems with web site defacement, misuse of public web applications, unauthorized access, insider net abuse, denial of service attacks and viruses. [18] This information demonstrates that there are individuals actively looking for software vulnerabilities on the web. This point is reinforced by testimony from Robert F. Decay, Director, Information Security Issues indicating that patch management is critical in mitigating cyber vulnerabilities.[6] According to the same report, the number of security vulnerabilities reported is increasing and attacks are becoming automated. [6] Software security encompasses more than encryption and password maintenance. The ability to defend against software attacks, in the long run, will need to come from "more rigorous software engineering practices, better tools and technologies".[6]

According to Deloitte & Touche's *2004 Global Security Survey*, the number of systems being compromised in the financial sector is on the rise and attacks are increasing.[7, 8] Now, either more companies are being more forthcoming with information, or more systems are being compromised, or possibly both. The truth of the matter is that we really do not know the exact number of systems that are truly being compromised. Most companies do not want this information made public for a variety of reasons. For example, they do not want to admit, from a reputation standpoint, that their systems have been compromised; they do not want to endure the expense necessary to rectify the problem; they do not know how to fix the problem or, even worse, they are not even aware that their systems have been compromised.

These issues can be summarized in terms of the economical cost. Since bad news sells in today's press environment, companies do not want to sustain damage to their reputations or lose public good will

which would translate into soft cost. Soft cost, also referred to in the accounting profession as indirect cost, in this instance refers to costs that are hard to quantify economically.[44] In opposition, hard cost, also referred to in the accounting profession as direct cost, refers to cost that are easily quantifiable.[44] There is some research that provides validity to company fears in terms of hard cost i.e., stock price. Telang and Wattal's research indicates that a software vendor loses, on average, approximately 0.6% of their stock price per vulnerability announcement.[42] It is only when their security issues start to seriously interrupt business or application functionality that they will admit to having a problem. Another possible reason for not wanting to admit to security breaches on the Internet is to minimize the chance of copy cat attacks on their systems until the issue has been resolved and patched.

As the World Wide Web continues to become an integral part of everyday life, the demands for secure web applications in the business world will continue to grow. This societal pressure is being felt in the corporate environment through U.S. legislation such as the Economic Espionage Act of 1996 (EEA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Graham-Leach-Bliley Act of 1999, and the Sarbanes-Oxley Act which was passed into law in July of 2002.[4, 22, 46] The EEA is the first law that explicitly makes the theft of commercial trade secrets a federal crime.[9, 22] HIPAA is concerned with disclosure and transmission of healthcare information.[38] The Graham-Leach-Bliley Act focuses on how financial organizations use and distribute a customer's personal information.[5] The Sarbanes-Oxley Act was originally designed to help restore confidence in publicly traded financial companies by making the chief executive officers and chief financial officers personally responsible for validating financial information.[26] However, the wording in the law has a broader reach than just the financial world. The law (Sarbanes-Oxley) states that company CEOs and CFOs establish and maintain proper "internal controls".[26, 46] This means that by signing off on the validity of the data within the system they are also signing off on its security.[26] The legislative story continues to evolve. Recently, a ninety-one page bill was introduced in the Senate by Senator Patrick Leahy and Senator Arlen Specter.[29] The proposal is reported to be the most aggressive "regulation-oriented" bill to date containing "an avalanche of new rules for corporate data security and stiff penalties for information burglars".[29] This naturally opens the door to question the definition of a secure system.

SECURITY

Security means more than implementing encryption, Secure Socket Layer (SSL), firewalls, creating and maintaining secure networks, the use of digital certificates, the different technologies used for authentication and authorization or intrusion detection systems.[12, 13] In-depth discussions on these topics and research into their improvement are occurring on a daily basis. However, a system's security is not determined solely by the technology that is implemented. A secure system to one organization may not meet another organization's definition of security. The definition of a secure system to a large financial organization will differ from that of a small local business, such as a law firm's web site. For the purposes of this dialogue we will define a secure system in terms of confidentiality, integrity and availability. The system should protect confidentiality by limiting admission to the appropriate individuals.[36] The integrity of the system should be maintained by only allowing modifications to be conducted by the appropriate individuals and within established guidelines.[36] The availability of the system is defined by providing access to the appropriate parties at designated times.[36] The decision that an organization has to address is how much risk is it willing to accept and at what financial cost. The policy, procedures, standards, and technical controls that are developed and implemented will define the systems confidentiality, integrity and availability. This collaborative approach defines the overall security of the system within a business.

The new focus on security through legislation, which is forcing accountability and responsibility, is encouraging security to become a major factor in the new evolution of the business strategy. This overall change in the business strategy can even be seen within Microsoft when Bill Gates announced the corporate shift towards "Trustworthy Computing" in January of 2002.[24] This business strategy interaction will continually need to be accounted for in the development of new applications. As Alan Zeichick, Conference Chairman of the Software Security Summit, phrased it, "Software is vulnerable! Enterprises have spent millions of dollars installing network firewalls and Virtual Private Networks, but the real danger is in poorly written applications".[3]

BUSINESS STRATEGY

Due to the obvious cost advantages, the legislative pressure, pressure from news organizations, and demand from the customer, security is evolving into an issue that needs to be addressed in an organization's businesses strategy. The business strategy encompasses all of the information about the overall business that ranges from defining the scope of the business, to establishing the business models, to broad marketing strategies, to the establishment of processes and policies, to the acquisition and distribution of information and to the overall approach to technology within the organization.[15]
Business strategy can be examined from the corporate, the business, and the operational point of view.[27] The corporate level strategy is the high level strategy that details the organization's purpose and scope.[27] The business level strategy deals with the competition in individual markets including market segmentation, market positioning, industry analysis, and brand value.[27] The operational strategy is concerned with the implementation aspect of the business which would include optimising web site design, hardware requirements and utilization and software requirements.[27]

Legal pressure is pushing security up to the corporate strategy level. Chief Executive Officers and Chief financial Officers are potentially being held accountable for the security of their applications. From a corporate perspective, this provides a champion. Champions are critical in the corporate environment in order to implement and sustain corporate cultural changes. Realistically, high level champions within the organization are more likely to succeed in changing and sustaining changes to corporate cultures. From a corporate perspective, security needs to be viewed as a collective organizational problem. Increased security should translate into increased communication among co-workers. Increased communication should facilitate a more in-depth understanding of the business which contributes to a better working environment, ultimately affecting the organization's bottom line.

From a business strategy standpoint, companies on the web need to understand that the web site is their front door to the world. They need to strive to develop brand awareness, creative marketing advertisements, and develop an environment that capitalizes on the customer's experience. The customer will make decisions about repeat business with a company based on their total experience. This includes, as Rick Freedman put it, "Delivering on the Click".[15] Companies have to outline the performance standards that they are going to provide and follow through with an effective, efficient and secure value chain while providing appropriate customer service capabilities. This basically follows the old adage "Say what you are going to do and do what you said"! Always remembering that competitors are only a click away! If customers perceive that their data is not safe and secure, this can result in lost customers, lost future revenue, lost market advantage and possibly monetary reparation.

The tightly integrated web theory does place a great deal of power in the hands of the customer from a business model point of view.[14] "Overall, the business environment continues to become more inter-connected. Traditional boundaries between organizations are eroding."[37] A customer logs onto a web

site and places an order for one widget. Real time update notifies the supplier and updates his inventory; the supplier's system then updates the manufacturer's system, and the manufacturer's system then updates the raw material supplier's system. This gives everyone in the supply chain the ability to adjust their inventories very quickly in response to demand which, in turn, severely reduces costs. This tight integration, from a security view point, opens the door to a multitude of problems if an attack is successful in compromising one of the linked systems. On the other hand, as organizations become compliant, there will undoubtedly be attempts to market this value added position. An in-depth examination of the effects of security on the individual components of an organization's business model is out of the scope of this paper. The purpose of this section is to acknowledge the fact that pressure from legislation, competitors, the press and customers will force organizations to acknowledge security as part of the business strategy.

If it appeared at all, security would traditionally have fallen under the operational strategy. Unfortunately, there appears to be a lack of understanding on how to protect application code as it is developed.[28] A recent survey conducted by BZ Research substantiates this idea. Of the BZ survey respondents, "55.9 percent blamed poor programming practices" for the number of vulnerabilities in software applications.[47] The next logical question is: how does a business protect itself and capitalize on software application development in order to gain a competitive advantage for their business. A possible solution, to security issues, during application development, is the integration of an independent flexible Web Engineering Security (WES) methodology with customizable components.

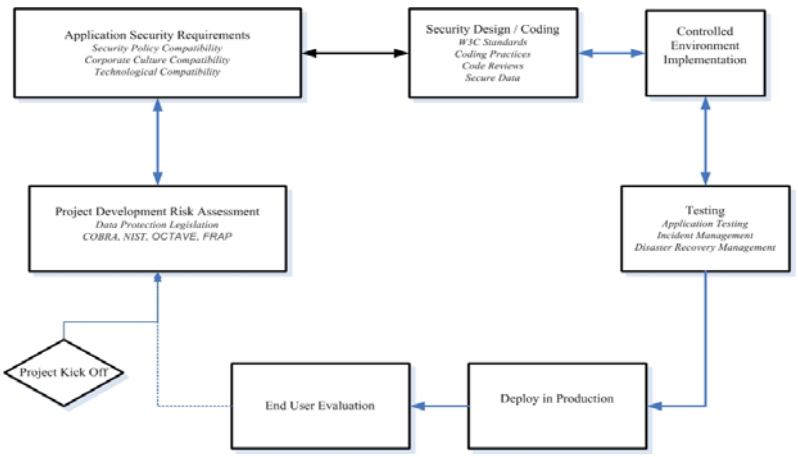
DEVELOPMENT METHODOLOGY

As discussed in the 3rd Latin American Web Congress proceedings, the foundation of the Web Engineering Security (WES) methodology is built on the principles of good communication, employee education, and cultural support.[17]

The principle of good communication is a critical component of the methodology, as it is needed to assure solution compatibility within the development team and within the organization.[17] Communication with the end user is needed to acquire the appropriate application requirements.[17] End user and technical employees need to be educated on the importance of security and the potential impact on the organization.[17] This education should include various types of technical attacks and social engineering attacks.[17, 31] Security needs to be viewed in the application development process as "everybody's problem".[17, 19] The cultural support needs to originate and be continually fostered by upper management.

The WES methodology, shown in Figure 1, is designed to complement an organization's current methodology, while providing guidance to the development process from a security perspective. The WES methodology starts with a Project Development Risk Assessment; then goes to Application Security Requirements; to Security Design / Coding; to Controlled Environment Implementation; to Testing; to Deploy in Production and the last step is to End User Evaluation. It should be noted that the stakeholders involved in each section will depend on the structure of the organization. In general, the stakeholders in the Project Development Risk Assessment will be the technical staff, which could include technical managers, application developers and security personnel, once they have been initially notified by the business unit of the potential project.

FIGURE 1 - WES METHODOLOGY



By conducting a **Project Development Risk Assessment**, the business and the information technology group can analyze each stage of the development by identifying the associated risk. This step provides an opportunity for the organization's development team to understand the application from a risk point of view and helps to generate applicable questions to address the application security requirements phase. Depending on the size of the organization and the market requirements, both the governmental and commercial perspectives, the risk analysis can be used to help identify known risks, point out new risks and ensure that these risks are acceptable. Depending on the needs of the organization, this can be either a very formal process or a very informal process. If it is a formal process, then the advantage for management is that it presents a clear understanding of the risks before a substantial investment is made in the development of the web application. The disadvantage of a highly formalized process is that it can slow down the development process. In reality, there will be a lot of cross-over communication between the Project Development Risk Assessment stage and the Application Security Requirements stage. Informal processes tend to be faster in nature but, by nature, introduce more risk through a potential lack of environmental and risk understanding.

The **Application Security Requirements** phase allows the development team to make a specific effort to acquire the security requirements thorough effective communication with the end user. Hence, the stakeholders involved in this stage would probably include the business unit and the technical staff. They should coordinate these requirements with the organization's security compatibility. The security compatibility encompasses several important issues that include security policies, standards, baselines, procedures, guidelines,[25] the corporate culture and existing technology. Policies, standards, baselines, procedures, and guidelines can assist in large organizations to provide cohesiveness within the organization. "The goal of an information security policy is to maintain the integrity, confidentiality and availability of information resources."[22] In smaller organizations, where it is not mandatory through regulation, they can be implicit to the organization. The policy provides the "what" and the standards, baseline, procedures and guidelines provide the "how".[21] They can work in concert to support the organization from a security perspective.

Corporate culture needs to take everything into account, ranging from employee security awareness programs, to employee education on social engineering attacks (discussed below), to recognition of organizational norms. Corporations need to educate the application end user employees and their development staff in terms of security. They also need to remind employees periodically about security policies, standards, baselines, procedures, and guidelines. One approach to this is to make the issue important to the employee by integrating it into their annual evaluation.[45] This will not solve all of an organization's security problems; however, it does provide a practice avenue for encouraging good security practices.[45]

Technical solutions alone will not provide protection against the human element. They will not provide protection against an end user who reveals his/her passwords, users who circumvent security to complete a specific task, or insider attacks.[13] When it comes to information security "the human factor is truly security's weakest link".[31] This fact has spawned an area of warfare in the business world know as social engineering. Social engineering attacks take place when an outsider or insider observes an organization, gathers information and makes necessary business contacts under the premise of a legitimate purpose in order to gather information.[31] This information is then used to acquire more information until the intruder has acquired something of value.[31] The same tactics can be used by a current employee to gain unauthorized privileges. Company employees need to be educated on the existence of social engineering attacks and how to identify them and prevent these attacks from occurring.[31]

The perception of security, and its importance to the business, needs to be effectively communicated at an employee level. If the employees do not place a great deal of importance on security and they regularly post passwords on screens or in accessible areas, trade passwords with colleagues, or grant system access to outside vendors, then they are creating a security risk for the company. Technological acceptance of corporate norms is when a solution has been implemented in the environment, becomes accepted and then becomes expected. If an organization has implemented a single sign-on solution for several of the existing applications then it would be reasonable for employees to expect new applications to take advantage of this technology. The justification for complying with this expectation or going against the grain needs to be examined and justified to the employees. Otherwise, employees could start to circumvent security when it suits their needs.

Existing technology needs to be examined from two view points; a compatibility point of view and a value added point of view. When an application is being proposed, the solution needs to be compatible with the existing infrastructure in the organization. Does the technical expertise exist in the organization to write the application in the proposed language? Does the hardware infrastructure support the new applications? Is the existing code repository compatible with the new development of the new application? There are both hard and soft costs associated with these types of questions that need to be taken into consideration when considering any new application development. Technology needs to be examined from a value added point of view. Whether you subscribe to individual aspects or to all of the "value configuration(s)" which include the value chain, the value shop and the value network, one of the goals of the organization is to provide added value regardless of the product or service that is being offered.[1] Technology is a major contributor to this goal in today's market place. Hence, when examining the validity in developing a new application, the organization should be asking how this will help them add value to their organization.

This information then allows the technical architect, in the **Security Design / Coding** phase, to pick the most appropriate technical controls from a design, risk and cost perspective. Once the high level design decisions have been made, then the coding takes place. The programmers should take into consideration coding standards, good coding practices, code reviews and appropriate security measures. Encouraging programmers to adhere to coding standards and to pursue good coding practices will increase the code readability which will inherently improve software maintenance. This improvement should be felt in both enhancement maintenance and patch maintenance. It has been estimated that maintenance accounts for an average of 60% of an application's software expense.[16] In reality, "better software engineering development leads to more maintenance, not less".[16] If an application meets the needs of a particular market, then the application will be enhanced through the addition of new features and improved functionality. Patch maintenance is another area that is critical to defending against cyber

vulnerabilities.[6] Any improvement in an organization's software maintenance capabilities translates into long term savings.

Code reviews ensure that the code is doing what it is suppose to do, decrease errors in the code and ensure that more than one person understands the application. The implementation of the type of code review is up to the individual organization. Code reviews can encompass everything from pair programming, to design reviews, to manual reviews of code after it has been written. It is up to the organization to decide the best avenue for implementation. Hence, the organization is not dependent on a single employee for modifications and support of a specific application. Applying appropriate security measures will help ensure data security and security consistency throughout the application.

Depending on the needs of the organization, the **Controlled Environment Implementation** can be as complex as implementing it into an environment that mirrors the production environment or it can be as simple as running the application on a desktop.[17] The goal of the environment is to minimize surprises. Basically, this phase allows the developers to test the application's compatibility with the operating system and interfacing programs before application testing and a production release.

Testing takes place from both the developer and the end user perspective. Programmers should be running their own battery of tests when the code is conceived. Again, it should be stressed that the methodology is designed to work in conjunction with existing organizational tools and processes. If the organization already has an investment in automated testing tools, they should be used in this stage to augment the testing process. The end users should be writing test scripts and actively interfacing with the application to ensure that the program is performing accordingly.

Within the area of new application development there is evidence to support the value of early integration of security into the development methodology. The National Institute of Standards and Technology (NIST) estimates that "93% of reported vulnerabilities are software vulnerabilities".[34] The Organization for Internet Safety (OIS) publishes Guidelines for Security Vulnerabilities Reporting and Response. In this document, they define a security vulnerability as "a flaw within a software system that can cause it to work contrary to its documented design and could be exploited to cause the system to violate its documented security policy".[17, 33] Hence, any flaws in the system design or application coding can potentially lead to security vulnerabilities.[17] The Open Web Application Security Project (OWASP) provides an excellent listing of the top ten vulnerabilities in Web Applications.[32] The (OWASP) list complements information discussed in the previous articles the "Top Web application security problems identified" and "The Bugs Stop Here" which were published in 2003.[2, 30] Only after testing has been completed should the application be moved into production.

After the application's **Deployed in Production**, end user feedback on the security of the application is mandatory. **End User Evaluation** is critical from the standpoint of security. An efficient and effective response to application security breaches is mandatory to web based business survival. If end users are circumventing the applications security in order to make their lives easier or perform their jobs in a timely manner, then these issues need to be investigated and resolved.[17] If the application has been compromised due to a flaw in the design or the code, then the security issue needs to be addressed, realistically, as rapidly as possible. If the application is not secure, businesses run the possibility that the application will be abused, corporate credibility lost, and financial consequences incurred.

After the process has been customized for needs of a specific business, then it can be documented so that it can be replicated for future projects. Depending on the needs of the organization, this can also serve

as an audit trail. The amount of documentation implemented will depend on the needs of the particular organization. A financial institution, due to regulations, will probably have to provide detailed documentation of their processes. In contrast, a small local business will probably document only the bare necessities in order to conduct business.

RELEVANT WORK

Among several papers, two specific examples have recognized the importance of security in the business environment. Secure Software, Inc. has produced a white paper titled "Why Application Security is the New Business Imperative – and How to Achieve It".[39] The WES methodology agrees with several points made within the paper such as the real solution to security is a "software development process that explicitly incorporates application security"; "remediating software security problems after the fact is expensive and time consuming"; "robust testing"; the process should be "repeatable and auditable".[39]

The white paper, "A Good Defense", published by the Center for Digital Government makes an excellent point in that information security is rapidly becoming "a cost of doing business".[41] This paper produces an excellent summary of the potential costs associated with several of the viruses that have been introduced into the Web environment over the years. The paper cites the cost claimed by various states and cities, as examples, and gives a good breakdown of categories that will bear the burden of an attack from a monetary point of view. The paper also gives good advice in reference to strengthening security in the future, but it does not drill down to the level of application development.

CONCLUSION

Addressing security consistently, cohesively and effectively is a difficult and complex task. There is no magical solution or a single solution to all of an organization's security issues. As pressure continues to escalate, in reference to application security through legislation and dissatisfied customers, not following a web application development methodology that specifically addresses security is an expensive and dangerous strategy for any business. Outside research indicates that it is cost effective to address security flaws during development. In theory, the implementation of WES should translate into a higher return on investment (ROI) for the company and help improve application and application feature time to market through constant and consistent security testing during application development. The implementation of security during the development process should positively impact application maintenance as well as helping to improve the overall profit for the organization. Security, from a business point of view, has become a critical issue in today's web enabled society. The question is not whether an attack will happen to an organization's web site, but when, and how will it be handled? The best approach to security, from a web development point of view, is to address security issues upfront in the design of the web application, mitigating both soft and hard costs.

The next step in the research is to conduct case studies in industry. The purpose of the case studies is three fold. First, case studies will provide additional information for the continual development of the WES methodology so that it is complementary to existing Web application development processes and, yet, retains flexibility through customizable components. The second contribution from the case studies will be to determine, from a practitioner's perspective, the compatibility of the WES with both traditional and agile Web development methodologies. The third advantage is that it will create a setting that will test the theory from a business perspective. This approach provides a 'real world' indication of the practicality of the WES methodology solution.

REFERENCES

[1] Afuah, A. and Tucci, C. L., *Internet Business Models and Strategies, Second Edition*. International Edition ed. c2003, Boston: MacGraw-Hill. 121-139.

[2] Berinato, S., *The Bugs Stop Here*, in *CIO*. c2003.

[3] BZ Media, IT Professionals Guard Against Disaster at First Annual Software Security Summit. 12/06/2005. http://www.bzmedia.com/pr/pr20041123.htm

[4] Clancy, H., ISS Service Helps Users Comply With Fed Laws. April 11, 2004. http://www.crn.com/sections/breakingnews/breakingnews.jhtml;jsessionid=SATRZS0JDIIZ2QSNDBCCKH0CJUMEKJVN?articleId=44585&_requestid=475222

[5] Consumer Privacy Guide, Financial Modernization Act (Gramm-Leach-Bliley Act). April 11, 2005. http://www.consumerprivacyguide.org/law/glb.shtml

[6] Dacey, R. F., *INFORMATION SECURITY Effective Patch Management is Critical to Mitigating Software Vulnerabilities*, in *Testimony Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House Committee on Government Reform*. c2003, United States General Accounting Office.

[7] Deloitte, *2004 Global Security Survey*. c2004: London. p. 1-36.

[8] Deloitte, Security Attacks On IT Systems More Than Double, According to Respondents of Deloitte & Touche LLP's Global Financial Services Survey. April 11, 2005. http://www.deloitte.com/dtt/press_release/0,1014,sid%253D2283%2526cid%253D50024,00.html

[9] Department of Justice USA, Computer Crime and Intellectual Property Section (CCIPS). 12/06/2005. http://www.usdoj.gov/criminal/cybercrime/ipmanual/08ipma.htm#VIII.C.3.

[10] Deshpande, Y. *Web Engineering Curriculum: A Case Study of an Evolving Framework*. in *Web Enginering 4th international conference, ICE 2004*. c2004. Munich, Germany.

[11] Deshpande, Y., Murugesan, S., Ginige, A., Hansen, S., Schwabe, D., Gaedke, M. and White, B., *Web Engineering*. Journal of Web Engineering, c2002. **1**(No. 1): p. 3-17.

[12] Dickson, J. B., *Web applications have become IT's next security battleground*. San Antonio Business Journal, c2004.

[13] Ellis, J. and Speed, T., *The internet security guidebook: from planning to deployment*, (ed). Carrasco, E. c2001., San Diego: Academic Press. 1-320.

[14] Fingar, P. and Aronica, R., *The Death of "e" and the Birth of the Real New Economy: Business Models, Technologies and Strategies for the 21st Century*. c2001, Tampa, Florida USA: Meghan-Kiffer Press. 82.

[15] Freedman, R., *The econsultant : guiding clients to Net success*. c2001., San Francisco :: Jossey-Bass/Pfeiffer,. xviii, 254 p. :.

[16] Glass, R. L., *Facts and Fallacies of Software Engineering*. c2003, Boston, USA: Addison-Wesley.

[17] Glisson, W. B. and Welland, R. *Web Development Evolution: The Assimilation of Web Engineering Security*. in *3rd Latin American Web Congress*. c2005. Buenos Aires - Argentina: IEEE CS Press.

[18] Gordon, L. A., Loeb, M. P., Lucyshyn, W. and Richardson, R., *2004 CSI/FBI Computer Crime Security Survey*. c2004, Computer Security Institute. p. 2-18.

[19] Graff, M. G. and Wyk, K. R. v., *Secure Coding Principles & Practices*, (ed). Russell, D. c2003, Sebastopol, CA: O'Reilly & Associates Inc. 1-183.

[20] Gross, G., Secret Service head calls for cybersecurity cooperation. 20/05/2005. http://www.computerworld.com/securitytopics/security/story/0,10801,101820,00.html?SKC=security-101820

[21] Hansche, S., Berti, J. and Hare, C., *Official (ISC)2 Guide to the CISSP Exam*. c2004, Boca Raton: Auerbach Publications.

[22] Hare, C., *Policy Development*, in *Information Security Managment Handbook*, Tipton, H.F. and Krause, M., (eds). c2004, Auerbach Publications: Boca Raton. p. 925-943.
[23] Hoo, K. S., Sudbury, A. W. and Jaquith, A. R., *Tangible ROI through Secure Software Engineering.* Secure Business Quarterly, c2001. **1**(2).
[24] Hopper, D. I. and Bridis, T., Information Security News: Microsoft announces corporate strategy shift toward security and privacy. July 1, 2005. http://seclists.org/lists/isn/2002/Jan/0092.html
[25] Howard, P. D., *The Security Policy life Cycle: Functions and Responsibilities*, in *Information Security Managment Handbook*, Tipton, H.F. and Krause, M., (eds). c2004, Auerbach Publications: Boca Raton.
[26] Hurley, E., Security and Sarbanes-Oxley. April 11, 2005. http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci929451,00.html
[27] Jelassi, T., *Strategies for e-Business*. c2005, Harlow, England: Prentice Hall.
[28] Lee, Y. L., Software Security at the Summit. 09/06/2005. http://www.sdtimes.com/article/story-20050301-12.html
[29] McCullagh, D., Senators propose sweeping data-security bill. July 01, 2005. http://news.zdnet.com/2100-1009_22-5769156.html
[30] Mimoso, M. S., Top Web application security problems identified SearchSecurity.com. April 12, 2005. http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci873823,00.html?NewsEL=9.25
[31] Mitnick, K., *The art of deception : controlling the human element of security / Kevin D. Mitnick & William L. Simon.* c2002., Indianapolis, Ind.: Wiley. 352.
[32] Open Web Application Security Project, The Ten Most Critical Web Application Security Vulnerabilities. http://www.owasp.org/index.jsp
[33] Organization for Internet Safety, Guidelines for Security Vulnerability Reporting and Response. http://www.oisafety.org/guidelines/Guidelines%20for%20Security%20Vulnerability%20Reporting%20and%20Response%20V2.0.pdf
[34] Ounce Labs, *Weapons for the Hunt: Methods for Software Risk Assessment*. c2004, Ounce Labs, Inc. p. 1-14.
[35] Pescatore, J., *Sanctum Buy Shows Security Is Key to Application Development*. c2004, Gartner. p. 1-3.
[36] Pfleeger, C. P. and Pfleeger, S. L., *Security in Computing*. Third Edition ed. c2003, Upper Saddle River, NJ: Prentice Hall.
[37] PricewaterhouseCoopers, *The Information Security Breaches Survey 2004*. c2004, PricewaterhouseCoopers. p. 1-36.
[38] Public Law 104-191 104th Congress, Health Insurance Portability and Accountability Act of 1996. Aplril 11, 2005. http://aspe.hhs.gov/admnsimp/pl104191.htm
[39] Secure Software, *Why Application Security is the New Business Imperative - and How to Achieve It*. c2004, Secure Software: McLean, Virgina. p. 1-12.
[40] Stewart, T. A., *The Wealth of Knowledge*. c2001, London: Nicholas Brealey Publishing.
[41] Taylor, P. W., *A Good Defense Information Security as a Cost of Doing Business*. c2004, Center For Digital Government.
[42] Telang, R. and Wattal, S., Impact of Software Vulnerability Announcements on the Market Value of Software Vendors - An Empirical Investigation. April 11, 2005. http://ssrn.com/abstract=677427
[43] TranslatorCafe.com, Currency Converter. 13/05/2005. http://www.translatorscafe.com/cafe/tools.asp?pn=currency
[44] VentureLine, MBA Glossary. July 03, 2005. http://www.ventureline.com/glossary.asp
[45] Wylder, J. O., *Towards Enforcing Security Policy: Encouraging Personal Accountability for Corporate Information Security Policy*, in *Information Security Management Handbook*, Tipton, H.F. and Krause, M., (eds). c2004, Auerbach Publications. p. 945-952.
[46] Zameeruddin, R., The Sarbanes-Oxley Act of 2002: An Overview, Analysis, and Caveats. April 11, 2005. http://www.westga.edu/~bquest/2003/auditlaw.htm
[47] Zeichick, A., Security: More Than Good Programming. 06/19/2005. http://www.sdtimes.com/printArticle/story-20050515-04.html;jsessionid=7AD21FBBABFF38D6127F61B13A239D23