



UNIVERSITY
of
GLASGOW

Glisson, W.B. and Welland, R. (2007) Web engineering security: essential elements. In, *The Second International Conference on Availability, Reliability and Security (ARES'07), 10-13 April 2007*, pages pp. 707-714, Vienna, Austria.

<http://eprints.gla.ac.uk/3486/>

Web Engineering Security: Essential Elements

William Bradley Glisson
University of Glasgow
glisson@dcs.gla.ac.uk

Ray Welland
University of Glasgow
ray@dcs.gla.ac.uk

Abstract

Security is an elusive target in today's high-speed and extremely complex, Web enabled, information rich business environment. This paper presents the idea that there are essential, basic organizational elements that need to be identified, defined and addressed before examining security aspects of a Web Engineering Development process. These elements are derived from empirical evidence based on a Web survey and supporting literature. This paper makes two contributions. The first contribution is the identification of the Web Engineering specific elements that need to be acknowledged and resolved prior to the assessment of a Web Engineering process from a security perspective. The second contribution is that these elements can be used to help guide Security Improvement Initiatives in Web Engineering.

1. Introduction

Fundamental components of the web engineering development environment include multidisciplinary involvement[6]; a complex, agile, time sensitive development environment[16]; a diverse end-user population[21] and a usability focused design[21].

It could be argued in today's Web engineering project environment that security should be included in this list. However, security is inherently not a part of 'Vanilla - Off the Shelf' Web engineering development processes and this inherent lack of security encourages environments that are susceptible to exploitation via potential breaches. These potential breaches translate into staggering corporate financial losses. The press is regularly inundated with a variety of security announcements validating these issues.

These announcements range from industry surveys[5, 12] reporting the trends and monetary losses, to application security breaches, to patch announcements. It is also important to recognize that potential security breaches are not limited to technical difficulties or process deficiencies. A recent ZDNET article published information on McAfee's misfortune detailing the fact

that a Deloitte external examiner left a back up CD in an airline seat pocket. The CD contained names, social security numbers, and stock information on thousands of past and present McAfee employees[7, 20]. This information complements a Deloitte 2005 statement indicating "it is clear that many security breaches are the result of human error or negligence resulting from weak operational practices"[5]. In order to improve human shortcomings, processes need to be developed and evolved so that they aid in the minimization of breaches due to human inadequacies.

These events drive the need to integrate security into the development process so that it provides an acceptable amount of risk mitigation, at an acceptable price, at a realistic user acceptance level while protecting the organization's information assets[8]. However, before you can effectively address the security needs of the business, there are essential elements that need to be acknowledged, addressed and resolved. These elements have been identified in a recent Web survey conducted over the summer of 2005[11].

2. Relevant Work

Technical solutions abound in the security arena and they are proposed and disproved on a regular basis. Relevant security articles exist on an array of topics that focus on improving specific aspects of security. The articles in this area range from security requirements [29], to security risk [31], to the Common Criteria [25], to the establishment of Security Criteria for Web Application Development[9].

Viega's article [29] on security requirements examines a critical area in establishing appropriate security. However, the article does not go into the aspects of these requirements and their cohesiveness with organizational compatibility. It also does not discuss foundation issues that need to be acknowledge and addressed before the security requirements are captured.

Wang's article inspects risk at various levels in the application along with the effects on quality factors [31]. However, the paper does not tackle organizational foundation issues that need to be addressed before

security can be implemented successfully, effectively and continually.

Literature is replete with articles that describe the implementation of a general Security Improvement Approach (SIA); however, they have the same issues. Articles by Taylor and McGraw [27], and McGraw[19] provide generic information that is not specific to Web Engineering and they fail to address underlying organizational issues that affect the ability of an organization to efficiently and effectively integrate security into the development process.

The Common Criteria (CC) attempts to fuse an assortment of international standards into a set of evaluation criteria to be utilized against information technology products[25]. The CC's biggest obstacle is the fact that one of the defining characteristics of a Web Engineering process is short development life cycles[18]. Short development life cycles do not coincide with the fact that the CC process is "Labor Intensive" consuming numerous weeks and months[25].

Recent research produced the Security Criteria for Web Application Development (SCWAD)[9] which broadens the focus of the security examination specifically in the area of Web Engineering processes. SCWAD has been proposed to assess the security applicability of an existing Web engineering process and to provide guidance to Security Improvement Initiatives (SII)[9]. SCWAD specifically recognizes six essential security criteria for evaluating web engineering methodologies [9].

The Web survey discussed in this paper contributes the identification of five essential security elements that need to be acknowledged and addressed prior to a Security Improvement Initiative (SII) being conducted in an organization. Essential element identification is based on apparent organizational deficiencies identified in the survey and relevant supporting literature. These same elements can also be used to help guide current SIIs in Web Engineering.

3. Survey Analysis

The point of the survey was to attempt to determine how security is realistically perceived and implemented in industry during Web application development.

3.1 Methodology

The Web survey was validated by two different individuals in the financial industry. The first individual is a technical lead for a major financial institution in the United States and the second individual is a Security Specialist for a financial institution in the United Kingdom.

The approach taken with the web survey was really more of a qualitative approach than a quantitative approach. Due to the fact that the survey was basically capturing current / past information, Zerkowicz and Wallace categorized this approach as a historical "Lessons Learned" approach to software engineering experimentation[33]. This historical "Lessons Learned" approach is used to identify trends. The benefit to this approach is that it is a low cost solution to acquiring data. One of the drawbacks is that it "cannot be used for statistically validating the results"[33]. Another drawback is that it is difficult to replicate, with comparable results, due to variances in the participants and mitigating issues that affect interviewee opinions. There is also a lack of control, in Web surveys, over the validity of the respondents and their answers.

Even though the survey was carefully designed in the beginning with the majority of the questions having a specific answer[22], the sample size was relatively small, (fifty-three initial respondents) coupled with a high number of respondents who did not complete all of the sections (eighteen), which severely detracts from any statistical data that could be derived from the survey results.

The majority of the respondents were acquired through e-mail request. The e-mail request was initiated through the British Computing Society in Glasgow. This request helped to target professionals in the industry. The balance, of the respondents, was acquired via communication with colleges, i.e., word of mouth. The reduced sample size in the various areas helped support the initial qualitative approach to the implementation of the survey instrument. Hence, the point of the survey was not to argue the validity of the sample size, the coverage area, or the incomplete survey responses[13]. In academia, there has been a great deal of debate over the demographic groups that have access to the internet, why individuals do not complete surveys, and the best presentation design for web surveys.

This survey endeavored to determine the responder's opinion[24] and acquire practical information regarding his or her experience with security and development methodologies. The Web provided the vehicle with the broadest industrial coverage, with the least cost and risk to organizations while providing information on trends in the industry. Other approaches such as gathering log data will not indicate where security is in the development process and interviews are very time consuming and costly to all parties.

3.2 Demographics

The initial questions were used to determine the interviewee's current role in the development process and to determine the overall size of the organization. The

titles indicated that the interviewees were experienced IT professionals. Out of the initial fifty-three valid respondents who participated in the survey, forty-one of the respondents, to the web survey, were from the United Kingdom. The balance of the respondents consisted of seven from Jordan, one from France, one from Japan, and three from the United States. The options for the size of the respondent's organization and their responses are detailed in Table 1. Fifty-three respondents participated in the survey; however, only thirty-five respondents provided input for all of the sections.

Table 1. Organization size

Categories	Size	Responses
1	0 - 500	28
2	500 - 1,000	4
3	1,000 - 5,000	9
4	5,000 - 10,000	3
5	10,000 - 50,000	5
6	50,000 - 100,000	2
7	100,000 or More	2

Although the specific industry was not captured in the survey, this result in the first category supports the idea that a lot of web development companies are small companies.

4. Results

As expected, the number of respondents decreased as the survey progressed from internet, to intranet to extranet questions. Out of the total number of respondents, fifty-one indicated that they have an internet; thirty-two indicated that they have an intranet and twelve indicated that they have an extranet.

It should be noted that most of the respondents represent small businesses. The majority of the respondent's organizations have internet sites. The break down of the type of application development process implemented by the various organizations is shown in Table 2 – Application Development Process.

The traditional systems development process appears to remain very prevalent in industry Web development. The responses that included some form of the traditional development process appeared in five out of the thirteen responses for internet development and eight out of the thirteen for intranet development and four out of six responses for extranet development. Oddly enough, none of the respondents indicated that they use both agile and traditional processes depending on the nature of the project.

This implies that the organizations involved in the survey are either all or nothing when implementing a development process. This result supports previous application development research findings where specific organizations have taken a “one size fits all

approach”[16]. One of the development process response options was “In-House”. In retrospect, it would have been interesting to have the individuals taking the survey explain their “In-House” approach at this point. This would have given some insight into the foundation of some of the customized development processes currently used in industry.

Table 2. Application development process

	<u>1</u>	<u>2</u>	<u>3</u>	<u>4</u>	<u>5</u>	<u>6</u>
Internet	2	3	2	0	6	13
Intranet	1	6	2	0	4	13
Extranet	0	2	2	0	2	6

Table 2 - Key

- 1 – Agile Development Process (Extreme Programming, DSDM)
- 2 – Traditional Systems Development Processes (Water Fall Approach, Spiral Model)
- 3 – A process that is a combination of Traditional and Agile Development Processes
- 4 – Use both Agile and Traditional process depending on the nature of the project.
- 5 – In-House
- 6 – Total Number of Respondents

An interesting point is that the data did not totally reflect expectations where the methodology and the size of the company were considered in the internet development process. The expectation was that the small companies would be using agile approaches and large companies would be using some form of a traditional approach. There is a category six company using an agile approach, two companies in category one using a traditional approach and one using an in-house approach. As the survey progressed to the intranet development questions, the number of companies using a traditional systems approach doubles to six companies. Two of these companies are in category one, three are in category five and one is in category seven. There were no agile answers to the extranet development question. As expected, there were no companies in category one that responded to having an extranet.

It is encouraging that seventeen of the respondents indicated that they have a defined application internet development process; however, nineteen out of thirty-six respondents indicated that they did not. At this point in the survey, the idea was to determine the existence of a defined process within an organization and not the specifics of the process. One issue that did surface through analysis is the question of a defined vs. implicit development process. An alternative set of questions would have been to ask if participants had an implicit development process and to have expanded on exactly what that entailed.

It is worth noting that there were more positive answers to the question asking about the existence of a

defined application development process for intranet and extranet applications. The same question, posed about the internet, yielded more negative responses. It should be noted that out of the six respondents who have a defined extranet application development process, five of the respondents have all three forms of Web application development processes defined. Hence, the trend indicates that organizations with a defined extranet process are more likely to have defined processes for internets and intranets. The high-level application development process results are summarized in Table 3 – Defined Application Development Process.

Table 3. Defined application development process

Question	YES	NO	DNK*	Respondents
Internet	14	19	3	36
Intranet	13	11	3	27
Extranet	6	4	1	11

*DNK: Do Not Know

There were thirty-five responses to a question about the organization having a defined application development internet *security* process. Out of the thirty-five responses, seventeen indicated that they have an internet application development security process, while fourteen indicated that they did not and four indicated that they “Do Not Know”.

The expectation was that there would have been more responses that had a defined internet application development process than a defined internet security process. On that same line of thought, another expectation also would have been for the respondents who answered positively to the defined application development process question to be the same as the respondents in the defined application development *security* process question.

In other words, the organizations that have an application development process would have been expected to have a security development process. A detailed examination reveals that there were seven responders who confirmed having a defined security development process but who also did not indicate positively that they have a defined application development process. This result, however, was neither logical nor expected from the survey.

The organizational demographics for the seven respondents who have a security process and do not have a defined development process indicates that these respondents are from relatively small organizations. The data are summarized in table 4 – Security Process & No Defined Application Development Process.

Table 4. Security process & no defined application development process

0-500	5
1,000 – 5,000	1
5,000 – 10,000	1

The results of the organizational demographics of the ten respondents that had both a defined application development process and an internet security process were as expected. The results were spread out across the respondent categories. This information is summarized in table 5 – Security Process & A Defined Application Development Process.

Table 5. Security process & a defined application development process

0-500	3
500 – 1,000	2
1,000 – 5,000	2
5,000 – 10,000	0
10,000 – 50,000	1
50,000 – 100,000	2
100,000 or More	0

The survey did indicate that security is being substantially recognized “During the initial design phase” for internet, intranet, and extranet development. This is an excellent indicator that security is starting to be included at the beginning of the development process. To what depth security is being addressed in the design phase is still open to investigation.

The survey then attempted to determine the phases that were included in the security process, whether there is an individual responsible for ensuring that the security process is followed and if there is any job related impact for not following the security process. The specifics that the survey revealed, in reference to the organizations that claimed to have defined application development security processes, are summarized in Table 6 – Security Process Information.

The table reveals that the weakest phase is the feedback phase. Most of the organizations that responded indicated there was an individual on the team who is responsible for insuring that the intranet security process is followed, but there was a drop in positive responses to the question inquiring about a job related impact for not following the intranet security process.

It is also worth noting that twenty-three of the respondents felt that their organizations considered security to be “Very Important” in its internet, intranet, and extranet applications. However, the number of “Very Important” responses fell to sixteen when asked how important security is within the development process. Organizations appear to be contributing to the security education of their employees. Thirty seven respondents indicated that they take any actions to educate employees about computer security. The survey did not attempt to define this information to determine the type of security education that was being distributed in organizations. The education numbers compared with the perception of importance indicates that there still appears to be a gap between understanding security and actually doing something about security in the development process.

This observation is also supported by the fact that out of a potential thirty-five respondents that completed the survey only seventeen have an internet security process.

Table 6. Security process information

Phases	Internet	Intranet	Extranet
Total Respondents	17	13	5
Risk Analysis	12	6	3
Security Requirements	14	9	5
Security Design	13	9	5
Controlled Implementation	14	7	5
Testing	12	5	4
Feedback	9	6	5
Employees Follow Security Process	14	9	5
Individual Responsible for Insuring Security Process is followed	15	9	5
Job Impact for not following the Security Process	4	5	3

Only nineteen (one more than half of the respondents) gave a positive answer to the question of the organization having a disaster recovery plan that includes the applications in the security design requirements. Only half of the nineteen responses indicated that the organization had tested the disaster recovery plan through execution.

5. Web Engineering Security Missing Element

Viega stated the issues well in the statement “The problem is, building secure software is not easy” [30]. The survey attempts to gain an understanding of the current role security plays in the Web application development process in industry. Since the survey specifically targeted Web application development the information derived from the results is targeted in the same area. That is not to say that the information may or may not be relevant in other areas of application development, but that the research conducted specifically inquired about Web application development processes.

In doing so, the survey identifies several elements that organizations appear to be failing to address. These identified elements need to be stressed when considering a Security Improvement Initiative (SII) for Web development projects. The detailed analysis of the information presented in this paper is reported in the *Web*

Survey Technical Report [11]. The five essential elements identified in this survey are as follows:

1. Web Application Development Methodology
2. Web Security Development Process Definition
3. End Users Feedback
4. Implement & Test Disaster Recovery Plans
5. Job Related Impact

5.1 Web Application Development Methodology

Before security can be addressed in an organization’s Web application development process, there needs to be an application development methodology in use within the organization. This methodology can be either implicit or explicit, though it is recommended that the development process be explicit. An explicit development methodology helps encourage understanding among existing employees and can be used to help foster new employee training. The point supported by the survey is that there needs to be a Web application development methodology within the organization, regardless of approach. A web development methodology also helps to provide structure to the complex, agile, time sensitive development environment. The survey responses indicated that there is the possibility that environments exist that claim to have a security process and no application development process.

This result initiates several queries. The natural questions include: was the survey too strict in asking for a defined documented process; are there organizations that do not have implicit or explicit development environment; and are there potential discrepancies on the definition of security among the participating parties? These concerns are valid observations to note and warrant a discussion in their own right. Regardless of the outcome of those discussions, security can not be implemented into a development environment that does not exist. Hence, the identification of the Web application development process (even if it is implicit) is a critical starting point when trying to integrate security into a development environment.

5.2 Web Security Development Process Definition

The discrepancy in the responses around the questions concerning a defined application development process and a defined application development internet security process indicates that there is possibly some confusion over the definition of an internet security process in the industry. In general, most of the respondents indicated that the phases of the security development process were present. This indication naturally leads one to suspect that the respondents could have simply added a security checklist to a small piece of a traditional process and called it a security development process.

This discrepancy naturally leads to a discussion about terminology. Terminology in various environments has the potential to have multiple meanings. As Anderson indicated, reality is a complex environment in the real world[1]. Different organizations will require “some combination of user authentication, transaction integrity and accountability, fault-tolerance, message secrecy and covertness”[1].

In order to cut down on possible confusion and to ensure that everyone is communicating properly, organizations should define:

- What security means to the business
- What it means to a web application
- What it means in the development process
- What a Web Engineering Security development process entails.

Defining this information naturally supports the Web engineering criteria for a usability focused design. For the purposes of this discussion, security should be defined in terms of Confidentiality, Integrity and Availability also known as the CIA[23]. Security, in terms of a web application, means that the information resources are suitably protected in terms of the CIA and that the level of protection is based on acceptable risk and appropriate end-user requirements. Security in the development process means integrating appropriate security measures into the existing development process in order to produce a more secure end-product. A Web Engineering Security process should include security information that is present in the Web Engineering Security (WES) Methodology[10]. Clearly defining the Web security development process will encourage clearer communication among employees and help with future employee training.

5.3 End-User Feedback

The survey noted that there was a lack of end-user feedback in the internet, intranet and extranet development processes. If a development process does not attempt to acquire feedback from the end users, this could signal potentially large problems with the development process alignment with the needs of the business. Strong support for end-user participation, in Web application development, has been previously indicated in a journal article by McDonald and Welland[17].

This lack of feedback has a direct impact on the potential effectiveness of a security solution. Actual end-users, not surrogate end-users, need to be used in the testing of the application. End-users will perform operations, submit data, and interpret instructions in ways that the development team, the business team or the technical staff within an organization could never dream! This is also true from a security perspective.

End-users should be observed and consulted for information on the effectiveness of the implemented security solution. Observing employees has the potential to reveal security issues and application problems that could be manipulated into contributing to a security breach.

It could be argued that employees are not always forthcoming with information, especially if the lack of security or the potential security vulnerability either does not directly affect their duties or actually helps them to accomplish their assigned task. This indicates that “users often disable or ignore security to get their work done”[3]. The opposite could also be argued in that employees may not be aware that they are creating security problems through a lack of knowledge, general education and training. Hence, a multiple stream approach consisting of end-user involvement in testing, end-user observation, and end-user consultation is recommended when working with end-users.

The concept of involving end-users in the security aspect of the application development process is not a new concept. Saltzer and Schroeder categorized “Psychological Acceptability” as one of eight “useful principles that can guide the design and contribute to an implementation without security flaws”[26].

Saltzer’s and Schroeder’s viewpoint was from the perspective of minimizing mistakes through the human interface design which is a valid point, but it does not specifically address end-user involvement in testing or observation of the end-user during testing. Existing research[3, 26] coupled with the results of the survey discussed in this paper strengthens the case for an organization to seek end-user feedback from a security perspective.

5.4 Implement & Test Disaster Recovery Plans

Nineteen of the thirty-seven respondents indicated that they have a disaster recovery plan that includes the individual applications. When asked if the organization has tested the disaster recovery plan by execution within the past twelve months the number fell to ten. Testing the disaster recovery plan implies that the plan is relatively up-to-date and is functional as of the last execution. Hence, the survey is really saying that there were ten out of a potential thirty-seven organizations that have an up-to-date, tested and functional disaster recovery plan.

This information concurs with an AT&T “survey of more than 1,200 businesses conducted from January to August, 2005; (where) nearly 40 percent stated that business continuity planning was not a priority”[2].

Security is really a risk management game in today’s society [30]. In today’s Web enabled environment disruptions are measured in minutes, not hours[14]. When it comes to risk, organizations have to make hard

decisions on exactly how much risk it is willing to accept and exactly how much money it is willing to spend to achieve the agreed upon level of security [8].

The logical progression, once the risk and cost decisions have been made, is to address the need for a disaster recovery plan. There are a multitude of reasons for developing and implementing a disaster recovery plan. These reasons not only include the obvious technical attacks on an organization's Web site, as reported by The Open Web Application Security Project (OWASP) [28], but also natural disasters and terrorist attacks. These possibilities have been blatantly exhibited over the past year or so and include: The Asian Tsunami; Hurricane Katrina; Madrid Bombings[4]; Terrorist bombing in London; and The Hemel Hempstead Oil Depot Fire[15].

These events stress the need for organizations to have and test a disaster recovery plan. If the organization does not have a disaster recovery plan, then it is difficult to develop a cost effective secure design solution for a Web application.

5.5 Job Related Impact

The survey revealed that the majority of the organizations do not have a job related impact for not following the security development process. There needs to be a job related impact associated with security process compliancy. Employees need to understand that there is a job related impact for not following organizational processes. This becomes even more important when considering security.

One solution would be to provide positive and negative reinforcement. The idea is to reward individuals that adhere to the security process. An example would be to provide monetary rewards to programmers based on the amount of secure code they produce, not the total amount of code that they generate. On the other side of this issue, there needs to be repercussions for individuals who do not follow the organization's security development process. Another idea that has surfaced is to tie security to the employees yearly evaluation [32].

Web application development takes place in a fast paced environment where business reputations, market shares, financial opportunities and losses are at risk daily. This increased performance pressure supports the business need for increased job related impact measures in secure Web application development.

6. Conclusion

The issues covered in this paper have been lightly discussed, in some form or variation, as solitary issues of importance during application development; however, they have never been viewed as a group of criteria for

secure Web application development. Realistically, the outcome of this survey presents the foundations for additional research on common sense solutions in the area of Web Engineering security processes.

The results from the Web survey have identified five elements that should be examined prior to any Security Improvement Initiative (SII) being conducted. The basic principle is that there appears to be fundamental issues with industrial Web application development that need to be addressed. The survey indicates that the elements listed in section five appear to be problem areas and warrant additional research. This does not mean that the list is exhaustive or conclusive or that these elements are mandatory for an organization to function. However, their presence will potentially improve the results of the SII and/or provide a less resistant path to SII identified areas that need improvement. This information can also be used to identify problem areas in SII's that are currently under construction.

An interesting topic to examine after conducting any survey is lessons learned. More specifically, if you could repeat the survey, would you repeat the survey in the same manner? The answer is "No". The survey should be divided into three separate surveys, one survey each for the internet, intranet and extranet. The restructure is based on the fact that several participants dropped out of the survey and that participants who did not pay close attention to the questions thought they were answering the same questions repeatedly. When, in reality, they were answering the same types of questions for the various forms of the net.

Future work in this area should include an attempt to drill down into the various interpretations of the definition of security among an assortment of organizations. It should also attempt to acquire more detailed information on an organization's in-house development process approaches to security and examine implicit approaches to security and their effectiveness in 'real-world' environments. Additional areas of interest that the survey did not explore would include: any interdependencies between the essential elements and the actual and/or perceived Return on Investment (ROI) for the individual stages of the development life cycle and specific ROI for security within each stage of the life cycle.

7. References

- [1] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. 2001, New York: John Wiley & Sons, Inc.
- [2] AT&T, *AT&T Study Finds U.S. Businesses Unprepared For Disaster*. 2005, AT&T
<http://www.att.com/news/2005/09/12-2>.

- [3] D. Balfanz, et al., *In search of usable security: five lessons from the field*. Security & Privacy Magazine, IEEE, 2004. 2(5): p. 19-24.
- [4] CNN, *Massacre in Madrid, Madrid bombings: One Year on*. 2006, CNN.com
<http://www.cnn.com/SPECIALS/2004/madrid.bombing/>.
- [5] Deloitte, *2005 Global Security Survey*. 2005, Deloitte Touché Tohmatsu: London. p. 1-44.
- [6] Y. Deshpande and S. Hansen, *Web Engineering: Creating a Discipline among Disciplines*. Multimedia, IEEE, 2001. 8(2): p. 82-87.
- [7] J. Evers, *Auditor loses McAfee employee data*. 2006, ZDNet News http://news.zdnet.com/2100-1009_22-6042544.html.
- [8] W.B. Glisson, L.M. Glisson, and R. Welland. *Web Development Evolution: The Business Perspective on Security*. in *Thirty-Fifth Annual Western Decision Sciences Institute*. 2006. Hawaii: Western Decision Sciences Institute <http://wdsinet.org/>.
- [9] W.B. Glisson, A. McDonald, and R. Welland. *Web Engineering Security: A Practitioner's Perspective*. in *International Conference on Web Engineering*. 2006. Palo Alto, California: Springer <http://www-conf.slac.stanford.edu/icwe06/default.htm>.
- [10] W.B. Glisson and R. Welland. *Web Development Evolution: The Assimilation of Web Engineering Security*. in *3rd Latin American Web Congress*. 2005. Buenos Aires - Argentina: IEEE CS Press
<http://www.ing.unlpam.edu.ar/laweb05/cfp.html>.
- [11] W.B. Glisson and R. Welland, *Web Survey Technical Report*. 2007.
- [12] L.A. Gordon, et al., *2005 CSI/FBI Computer Crime Survey*, in *Tenth Annual*. 2005, Computer Security Institute. p. 25.
- [13] H. Gunn, *Web-based Surveys: Changing the Survey Process*. c2002, <http://www.firstmonday.org/>
http://www.firstmonday.org/issues/issue7_12/gunn/#author.
- [14] IBM Global Services, *Business Continuity: New risks, new imperatives and a new approach*. 1999, IBM Global Services: Somers, NY <http://www-935.ibm.com/services/us/index.wss/summary/bcrs/a1000475?entxt=a1000388>.
- [15] T. Jones and J. Holden, *Disaster recovery: no more excuses*. 2005, Computer Business Review Online http://www.computerbusinessreview.com/article_feature.asp?guid=D82839BB-8BD7-4C94-B06E-BF0B27968B6A.
- [16] A. McDonald, *The Agile Web Engineering (AWE) Process*, Ph.D. Thesis, in *Department of Computing Science*. 2004, University of Glasgow: Glasgow.
- [17] A. McDonald and R. Welland, *Agile Web Engineering (AWE) Process: Perceptions within a Fortune 500 Financial Services Company*. Journal of Web Engineering, 2005. 4(4): p. 283-312.
- [18] A. McDonald and R. Welland. *Evaluation of Commercial Web Engineering Processes*. in *Fourth International Conference on Web Engineering, ICWE 2004, LNCS 3140*. 2004: ICWE <http://www.dcs.gla.ac.uk/~andrew/icwe2004.pdf>.
- [19] G. McGraw, *Software security*, in *IEEE Security & Privacy*. 2004. p. 80-83.
- [20] R. McMillan, *Auditor Loses Data on Thousands of McAfee Employees*. 2006, PC WORLD <http://www.pcworld.com/resource/article/0,aid,124870,pg,1,RSS,RSS,00,asp>.
- [21] S. Murugesan, et al. *A New Discipline for Development of Web-based Systems*. in *Proceedings of the 1999 International Conference Software Engineering*. 1999 http://ieeexplore.ieee.org/xpl/abs_free.jsp?arnumber=841085.
- [22] J. Neil, *Qualitative versus Quantitative Research: Key Points in a Classic Debate*, wilderdom.com
<http://www.wilderdom.com/research/QualitativeVersusQuantitativeResearch.html>.
- [23] C.P. Pfleeger and S.L. Pfleeger, *Security in Computing*. Third Edition ed. 2003, Upper Saddle River, NJ: Prentice Hall.
- [24] D.W. Reed, *The Scientific Method*, Department of Horticultural Sciences TexasA&M University <http://generalhorticulture.tamu.edu/LearningCommunity/ScientificMethod.htm>.
- [25] B. Rothke, *A Look at the Common Criteria*, in *Information Security Management Handbook*, H.F. Tipton and M. Krause, Editors. 2004, Auerbach: Boca Raton. p. 969-977.
- [26] J.H. Saltzer and M.D. Schroeder, *The Protection of Information in Computer Systems*. 1975, University of Virginia, Department of Computer Science
<http://www.cs.virginia.edu/~evans/cs551/saltzer/>.
- [27] D. Taylor and G. McGraw, *Adopting a software security improvement program*, in *IEEE Security & Privacy*. 2005. p. 88-91.
- [28] The Open Web Application Security Project (OWASP), *The Ten Most Critical Web Application Security Vulnerabilities*. 2004, The Open Web Application Security Project <http://www.owasp.org/index.jsp>.
- [29] J. Viega. *Building Security Requirements with CLASP*. in *International Conference on Software Engineering*. 2005. St. Louis, Missouri: ACM Press New York, NY, USA
<http://portal.acm.org/citation.cfm?id=1083200.1083207>.
- [30] J. Viega and B. McGraw, *Building Secure Software*. 2005, Boston: Addison-Wesley.
- [31] H. Wang and C. Wang, *Taxonomy of security considerations and software quality*. Communications of the ACM, 2003. 46(6): p. 75-78.
- [32] J.O. Wylder, *Towards Enforcing Security Policy: Encouraging Personal Accountability for Corporate Information Security Policy*, in *Information Security Management Handbook*, H.F. Tipton and M. Krause, Editors. 2004, Auerbach Publications. p. 945-952.
- [33] M. Zelkowitz and D. Wallace, *Experimental Models for Validating Technology*. IEEE Computer, 1998. 31(5): p. 23-31.