

Joanne Kuzma, University of Worcester, UK

Sue Barnes, University of Worcester, UK

Abstract: The rise of online commerce has brought about advantages for consumers wishing to research and purchase auto insurance from online agents, and the global market for this business is rising. However, along with benefits come issues related to security of auto insurance Web applications. Unsecured Web applications are a major problem with overall computer security, and can lead to problems with consumer trust. Government legal mandates and individual company technical solutions are two methods that are being used to attempt to mitigate this issue. This study analyzes 60 auto insurance Web sites in three Western European countries to determine the level of Web application security, and what types of vulnerabilities are common in the sites. It also reviews some technical and procedural methods firms can take to ease some of these problems.

1. Introduction

The rise of online auto insurance commerce has led to an increase in consumer usage of these sites as consumers realize many advantages. They are able to conduct research and purchase policies without having to physically visit an insurance agent. However, along with the advantages come issues that consumers must consider, such as Web-based security vulnerabilities with these sites. With daily news about security breaches and loss of personal data to hackers, consumers are becoming increasingly concerned about loss or misuse of their data. Consumer trust is a critical issue for online commerce, and high-profile security breaches highlight vulnerabilities to consumers, thus causing a potential loss in trust. Also, these vulnerabilities cause concern for firms, who can possibly lose business and profits when breaches occur.

In order to alleviate consumer concerns and ensure that systems are not breached, firms need to take a multi-phased approach to ensuring safe Web applications. Guarda (2008) indicates there are two factors that are needed to solve the issue of securing data and systems: laws and incorporation of legal principles into digital technology. Governments are enacting legislation requiring firms to better protect consumer data. In addition, technical solutions exist to mitigate Web vulnerability issues, but require constant vigilance and updates to software.

However, despite legal requirements and the abundance of technical solutions, fully protected Web applications appears to be rare, and firms are not adequately protecting consumers. This research analyzes 60 Western European insurance agency Web sites offering auto insurance using a software tool, N-Stalker. The study reviews a number of common Web application security vulnerabilities for each site and lists technical and managerial recommendations to better improve online security.

2. Framework for Web Security

2.1 Growth of Market

There has been an increase in global growth of the auto insurance market. Reportlinker.com (2008) quoted statistics from Datamonitor's Motor Insurance Guide which indicated the global motor insurance market grew by 2.2% in 2007 to reach a value of \$480.0 billion. They estimate the value will grow to \$537.4 billion in 2012, in spite of the recent worldwide recession. The online market is also growing. From 2007 to 2008, the number of U.S. auto policies purchased online increased from 2.1 million to 2.3 million, a 7 percent increase (Comscore.com, 2009).

The growth of online commerce has led to many positive advantages for consumers. First, the increased number of insurance firms has led to consumers being able to effectively research more products and services, and easier ability to perform cost comparisons. This therefore leads to increased competition and lower prices. Brown & Goolsbee (2002) performed a study showing that increasing Internet use leads to price reduction, and specifically online commerce has reduced the price of life insurance by 8 to 15 percent. Insurance firms themselves can benefit from doing business online. Research by Lee & Cata (2005) revealed that insurance firms receive more tangible and intangible benefits when they do substantial business through online commerce. Second, customers view other convenient features of online commerce in a positive light. This includes the ease of receiving quotes and ability to access the services 24x7.

With the advantages to online sites, it is easy to see why consumers are flocking to online commerce and the online insurance industry has seen a growth in business. However, even though the market is growing, consumers are aware of problems with this type of commerce and express concerns. The relationship between security of online Web sites and consumer trust in these sites is an issue that insurance agencies should consider in their security plans and development. Hoffman (et al, 1999) indicates that questionable security can be detrimental to online shopping, and if security concerns are raised too high, consumer trust erodes and the likelihood of online buying can decrease. Continual news articles on hacking attacks and loss of consumer data lead consumers to view safe online shopping with scepticism. Because merchants do not appear to police themselves and implement technical solutions, consumers are increasingly relying on government legal mandates to help protect their interest.

2.2 Legal Aspects

As technology advances, governments are increasingly enacting new legislation to ensure secure systems and protection of consumers' data, although the enactment is often reactive rather than proactive. Many European countries have laws that mandate data protection of records, and part of this process is to ensure secure computer systems through a variety of technical and procedural processes. However, it should be noted that laws throughout the world are inconsistent and it may be difficult for online consumers to discover what level of protection they have when using different online insurance sites.

In Spain, consumer data protection is constitutionally mandated through Article 18.4 of the Constitution (Office of Head of State, 1999). In April 2009, new regulations determined the array of security measures to be implemented by any processor of personal data along with fines to be implemented for any infringements (Sanchez, 2009). Ireland also has secure data protection legislation, its Data Protection Acts of 1988 and 2003. The Amendment SI 626 of 2001 interpret the nature of security measures required to demonstrate compliance and requires firms to ensure their staff are aware of security measures (Data Protection Commissioner Ireland, 2005). In the UK, the Data Protection Act of 1998 specifies the legal obligation that firms have to protect consumers' personal data and governs the technical responsibilities for data storage. Additional legislation was introduced in 2008 to enhance the law to include notification requirements for breaches and giving the UK Information Commissioner the power to conduct computer security audits (Castro-Edwards, 2008).

EU legislation provides for tight levels of data protection under the Data Protection Directive, (Robinson, et al, 2009). The directive 95/46/EC specifically mentions overall technology and security and states:

Member States ...must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. ...Measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected (Access to European Union Law, 1995).

2.3 Security Problems and Breaches

News articles about security breaches appear almost daily, showing that firms are not doing enough to protect their data and leaving their consumers' at risk. In 2009, Aviva Insurance reported a security breach putting UK customers at risk (Gross, 2009). In 2009, the UK Information Commissioner's Office found that insurance firm Amicus Legal was in breach of the Data Protection Act after the firm had personal information on 100,000 consumers was stolen (Young, 2009). In 2009, UK insurance agency Jubilee Managing Agency was found guilty of breaching the Data Protection Act when they compromised data of 2,100 clients (Flinders, 2009). Insurance firms are particularly vulnerable to data breaches because they have to keep many years of data to help them calculate insurance quotes and charges (Flinders, 2009).

2.4 Web Application Security

With the increase of online commerce, Web applications have become fertile ground for attackers attempting to penetrate systems and misuse private data. This leads to a concern among consumers that their data and systems can be at risk due to Web vulnerabilities. Web security firm, Cenzic (2009), indicates that during 2008, almost 80 percent of Web-related flaws were caused by Web application vulnerabilities with the three most common types being: a) SQL injection, b) Denial of Service and c) Cross-site Scripting.

The SANS™ Institute, a worldwide security organization, lists cross-site scripting, SQL injection and cross site forgery as major web vulnerabilities for 2007 (SANS Institute, 2009a). They indicate that cross site scripting (also known as XSS), is the most insidious and easily found Web application security issue. It can cause a variety of issues including defacement of Web sites, insertion of hostile content, phishing attacks and allowing hackers to take over a user's browser. SQL injections occur when user supplied data is intermingled with dynamic queries or poorly constructed stored procedures and allow attackers to create, read and update any arbitrary data available to the application. Cross site forgeries occur when malicious systems require legitimate users to execute commands without their consent, and is very difficult to prevent these vulnerabilities they and are becoming very common (SANS Institute, 2009a).

3. Methodology

The research was accomplished through completing an analysis of 60 European insurance sites to determine the most common Web security issues. The project consisted of four phases:

Choosing an online testing tool
Choosing a list of insurance sites to test
Running a software analysis
Analyzing the results

3.1 Choosing a Testing Tool

The first phase of this study was to choose a software testing tool to scan for Web vulnerabilities. Several criteria were part of the decision for choosing a product. First, because this testing would be done on the researcher's personal computer (PC), the software had to be able to be run on a Windows XP stand-alone machine. Second, due to budget constraints, the software cost needed to be kept under \$100, although preferably free-ware could be used. Third, the product had to have specific vulnerability testing to be able to scan Web sites, as opposed to common server-based scanning products. Several products were reviewed to see if they met the criteria including the following:

IBM's Rational AppScan – although this product had extensive vulnerability functions and options, its cost was \$15,500 (IBM, 2009), which was too high for this research.

Nessus, from Tenable Network Security, had very robust functionality, but testing of third-party sites required purchase of the ProfessionalFeed subscription, which costs \$1,200 (Tenable Network Security, 2009).

Security Auditor's Research Assistant (Sara), from Advanced Research Corporation could be installed on a PC, had sufficient functionality and was free (Advanced Research Corporation, 2009). However, the researcher had technical problems with the installation and there was no product documentation. Due to time constraints on researching the process, the product was not selected.

N-Stalker Web Application Security Scanner 2009 Free Edition was gratis and had sufficient functionality for testing as well as user documentation. After a successful download and review, this was chosen.

The free version of N-Stalker was able to test a large number of different Web application vulnerability issues including:

Cross-Site Script Injection

Web Server Infrastructure including Web Server, Platform, SSL encryption, HTTP Method discovery, Directory Brute-Force, HTTP protocol and other vulnerabilities

Web Signature Attacks including IIS, FrontPage, CGI Security, PHP Security, ASP Security, SANS Top 20 and other tests

Backup security check (N-Stalker, 2009)

In addition, the software was relatively easy to use and included reporting features available on screen and reports could be saved in PDF format. Figure 1 shows a screen print of an initial test after installation. The top portion of the figure shows a variety of scan options that can be utilized. The bottom portion is divided into three sections. The first is the 'Website Tree', which shows the various Web pages that have been tested for the site. The free version of N-Stalker will test up to 100 pages per site. This limitation was acceptable for this research study, but a company wishing to test their own site would want to purchase an upgrade that would test all pages within a Web site. The second column shows a variety of scanner events and will list the vulnerabilities, in this case there were three vulnerabilities from the scan: a) Microsoft .NET Framework vulnerability, b) Possible Backup file found and c) Old versions of Microsoft IIS. The third column shows scan

engine results and a column chart with the vulnerability statistics.

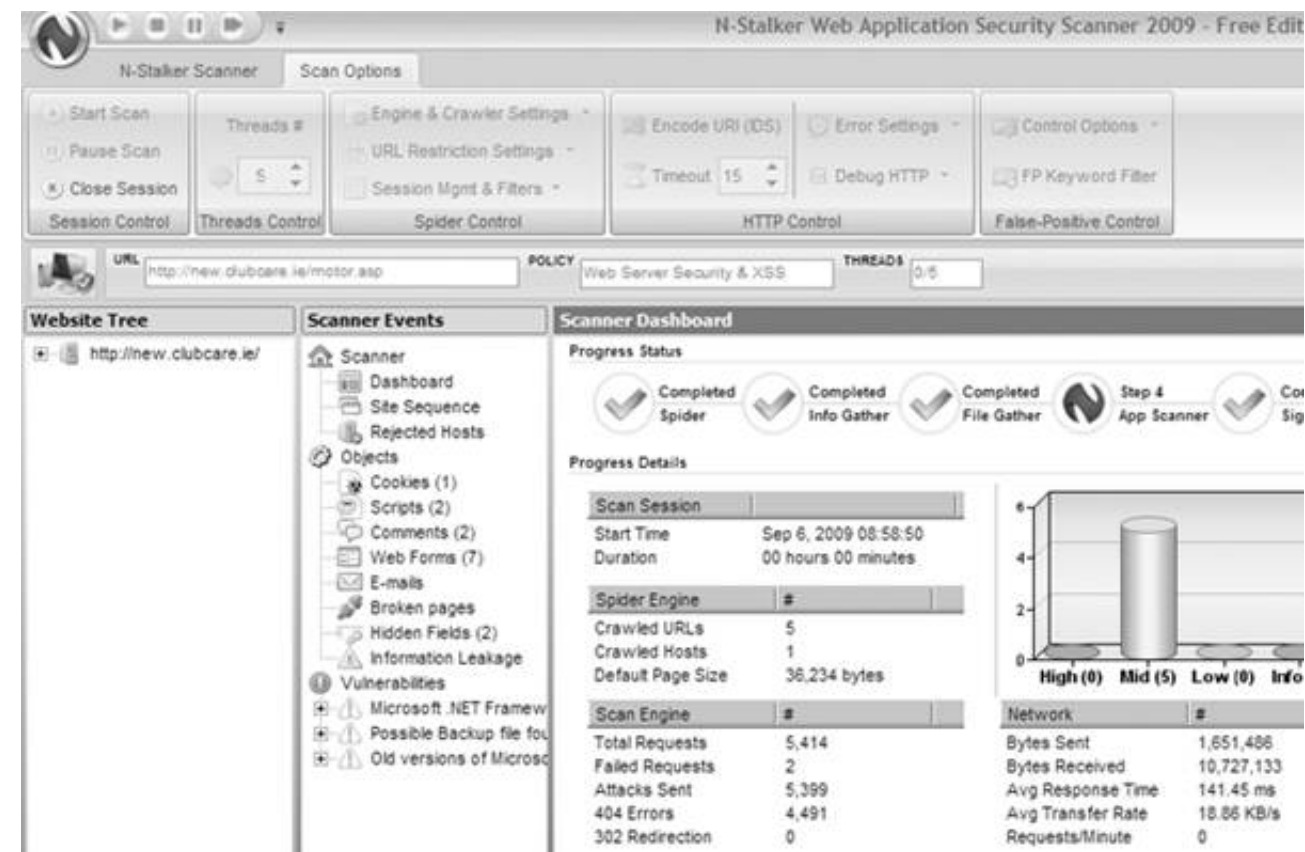


Figure 1: Screen print of N-Stalker testing report

3.2 Choosing Testing Sites

The second phase of this project was to choose several European countries and insurance agencies based in those countries. Due to the larger number of insurance agencies to be found in online searches for Western European countries compared to agencies from developing countries, it was decided to concentrate the search among three countries: a) UK, b) Spain and c) Ireland. After picking the three countries, the next step was to compile a list of insurance companies to test. Because there are many categories of insurance agents, it was decided to specialize on agents offering auto insurance quotes. Therefore, in order to compile a list of 20 agencies for each country, an advanced Google search was used with the main keywords 'UK auto insurance quote,' or 'Ireland auto insurance quote.'

Although thousands of Google results were displayed, only the top commercial sites were chosen. It was imperative that every site was reviewed to ensure it was a valid agency that sold auto insurance and that the agency was based in one of the three countries. Thus, 60 functional e-commerce insurance agent sites were each run and a vulnerability report produced for each.

3.3 Running the Software Analysis

For this study, the N-Stalker free software was downloaded and installed on a stand-alone personal computer. After opening the software, the research inserted the URL site name for one of the insurance sites into the Scan Wizard box. Although various security vulnerability scan types can be chosen, for this study the researcher chose to analyze cross site scripting and general Web server security. A scan was started and allowed to run. On average, a normal test run took 15 minutes, although the times varied from a few minutes up to 1.5 hours. All 60 insurance sites were tested over a one-week period.

A technical report was produced for each site listing the types and numbers of specific vulnerabilities. Each report was divided into several sections listing three levels of security vulnerability: a) high priority vulnerabilities, b) medium level vulnerabilities and c) informational issues.

High level – critical problems for web application security which could lead to a high risk of damage or potential of attacks. These issues should take precedence when setting a schedule for correction.

Medium – moderate ranked problems that could pose some level of risk to users of the web application. These need to be corrected, but after high-level issues are fixed.

Informational – messages that probably pose little or no issue of risk to users, but still should be analyzed by web developers in case any could lead to vulnerabilities.

For each level, specific error types could be found. For example, the specific error ‘old apache version may be susceptible to flaws’ would be listed under the ‘high’ level error section if this vulnerability was found for a specific insurance site. As each report was produced, the researcher recorded the specific vulnerability types and numbers into an Excel spreadsheet for future sorting and analysis.

4. Analysis of Results

Table 1 shows overall vulnerability testing results of 60 insurance agencies. The table is divided horizontally into three sections: high level errors, medium level errors and informational messages. The first row for each section shows the level of errors while the second details specific error statistics, including the total number of errors for each country, how many different types of errors, the number of sites without errors and the range of error types per site. The last three columns list the results of three countries: a) UK, b) Spain and c) Ireland.

There was a wide range of total errors and the specific error types for each country. Within the ‘high’ category, which relates to critical problems found in the site, the 20 UK sites had a total error count of 1455. Spain and Ireland had lower numbers of 16 and 50 respectively. There were 207 types of errors for the UK, while only 5 for Spain and 11 for Ireland. One area where the agencies did well was the number that did not contain any high level errors, 18 in the UK, 15 in Spain and 16 in Ireland. This means that the majority of sites did not contain critical issues. There was a wide range of the number of high level errors per site, ranging from zero to 206 in the UK, zero to five in Spain and zero to eight in Ireland. However, it should be noted that the results for one insurance agency in the

UK appeared to skew these results. The site egroup-insurance.co.uk had an overabundance of errors compared to all other sites. The Web site for this agency had different critical error types with a total of 1452 issues. This one site had so many issues that it did skew the UK results, making them look much worse than the results for the other countries. Without this site, the results for all countries would have been similar.

Results in the ‘medium’ level error category showed more sites containing issues at this intensity, along with more types of errors. The UK sites had 478 total errors while Spanish sites had 248 and Irish contained 240. The types of errors were 56 (UK), 15 (Spain), and 23 (Ireland). Most of the sites did possess medium intensity issues, and only four UK sites did not have them, while five Spanish sites and eight Irish sites were free of problems at this level. Similar to the problem raised with one site skewing results in the ‘high’ level category, the same issue was raised within the ‘medium’ level section. The UK insurance agency site egroup-insurance.co.uk had 51 different medium level types of errors with a total of 348 problems for these types, which was similar to the ‘high’ level categories in that it skewed the results to a much higher level. The range of error types for Spain and Ireland ranged from zero to 10, and zero to 16 respectively.

As Table 1 shows, there were two different types of informational warnings and most sites in all three countries did have one or the other of these informational cautions. There were a total of 122 warnings in UK sites, 87 in Spanish sites and 59 in Irish sites.

Table 1. Vulnerability Testing Results

	UK	Spain	Ireland
High Level			
Total errors	1455	16	50
Types of errors	207	5	11
Sites w/no errors	18	15	16
Range of errors	0-206	0-5	0-8
Medium Level			
Total errors	478	248	240
Types of errors	56	15	23
Sites w/no errors	4	5	8
Range of errors	0-50	0-10	0-16
Informational			
Total warnings	122	87	59
Types of warnings	1	2	1
Sites w/no warning	5	5	9
Range of warnings	0-1	0-2	0-1

Results in Table 2 show the most common error types for each vulnerability category: a) high, b) medium and c) informational. A wide range of different error types was compiled for high level (218 different types) and medium level (76 types). This study only shows the top four errors for the high and medium categories and the only two types found in the informational category. The most common informational warning, ‘Uncommon HTTP Methods supported,’ was recorded 260 times in 41 of the 60 sites, a sizable number.

Over one-third of the sites (26) contained the medium-level error “Old versions of Microsoft-IIS might be susceptible to security flaws.” Another common error in this category was ‘Possible backup file,’ which occurred in 20 sites with 126 occurrences. Cross site scripting issues were found in 13 sites (166 occurrences).

The total number of high-level errors was lower than the medium-based category, but still showed a significant presence. The most common issues were ‘old apache versions’ (9 sites), ‘old OpenSSL versions’ (5 sites) and ‘old mod_ssl versions’ (5 sites).

Table 2. Most Common Error Types

	UK Errors		Spain Errors		Ireland Errors		Total	
	Site	No.	Site	No.	Site	No.	Site	No.
High								
old apache vers may be susceptible to security flaws	1	1	5	5	3	3	9	9
Old OpenSSL version may be susceptible to security flaws	1	1	3	5	1	1	5	7
Old mod_ssl versions may be susceptible to security flaws	1	1	3	3	1	1	5	5
PHPLDAPAdmin 0.9.7 Welcome.PHP Multiple Vulnerabilities	1	21					1	21
Medium								
Old versions of Microsoft-IIS might be susceptible to security flaws	12	12	5	5	9	9	26	26
Possible Backup File Found	3	94	8	13	9	19	20	126
Possible Cross-Site Scripting and/or HTML injection found	4	13	4	43	5	110	13	166
File contains important information used by the FrontPage client			6	6	1	1	7	7
Informational								
Uncommon HTTP Methods supported	15	122	15	79	11	59	41	260
Directory Allows for File Listing			1	8			18	

5. Technical Implications

Results of this study show that Western European insurance agency Web sites have serious Web application vulnerabilities that can put consumers at risk. The presence of old software versions seems to be a common predicament throughout many of the sites, especially with Microsoft, apache and SSL product versions. Other ‘old versions’ types of errors did occur in the overall statistics, although not all were shown in table 2. A total of six different ‘old version’ errors occurred

in 51 different sites. There is a huge issue in computer security related to firms using outdated software and not applying software patches. Gerber (2008) states that a major problem of out-of-date software is that it can open the door to hackers. A recent study found that 90 percent of computers had old versions of software on them, potentially leading to vulnerabilities. Naraine (2003) quotes security studies that estimate up to 50 percent of all firms could be at risk due to unpatched and old software. He further indicates that part of the problem is due to the sheer amount of security information that they must keep track of on a daily basis, and updates often fall by the wayside. Cox (2002) also agrees this is an issue and states that developers often ‘install and forget,’ where they will install default software, but forget that it must be kept up-to-date to maintain security.

In order to fully protect their firms, it is imperative that new versions of software, upgrades and patches be consistently applied; otherwise the firms could open themselves to serious security vulnerabilities. Older versions of software could result in disclosure of sensitive information, and it is recommended that site operators install updated versions of software, such as the case of an older version of Apache issue (N-Stalker, 2009).

Two other major problems found in this study included a variety of injection and cross-site scripting vulnerabilities. There were 9 types of injection vulnerabilities, such as SQL injection, PHP script code and HTML code with 21 sites with these problems. Three different types of cross-site scripting errors were found in 14 sites. SANS Institute (2009a) indicates that cross-site scripting and SQL injection vulnerabilities are among the most common types of Web application issues. SANs (2009b) gives some advice on protecting against these problems, including having strong coding practices and using input validation methods to validate data before storing it. Injection flaws occur when interpreters are tricked into executing unintended commands. Protection can be followed by employing safe coding practices (SANS Institute, 2009c).

It should also be noted that one of the insurance Web sites contained in this study recently suffered a security breach. The UK Aviva Insurance Web site was included in this study and the results showed one medium error ‘Default Apache Manual/Documentation Found,’ and 12 informational messages. Between December 2008 and February 2009, the company had a data breach which affected 550 UK customers. The company representative indicated that they took steps to prevent future breaches and mentioned ‘Data breach is an industry wide issue, but one that we take very seriously’ (Gross, 2009). Although the breach in early 2009 was due to a malware attacks due to faulty hardware, this study does show Web vulnerabilities appearing in the software scan.

6. Design and Business Implications

Technical considerations and practices are a primary way to mitigate Web application vulnerabilities, but overall security needs to be expanded into a multi-dimensional approach. First, security is not just a technical problem to be left in the hands of Web developers and information systems experts. Secure systems should be a concern for management and should be considered a business issue. Poorly designed and unsecured systems can lead to a myriad of problems that could ultimately have a negative impact on business and profitability. A relationship between poor security and a negative impact on profitability has been established in research. A study by Ko and Dorantes (2006) on market reaction to breaches showed that breaches can have a short-term negative impact on a business.

Budget concerns remain a high concern of executives who are trying to effectively manage risk within tight budgets. A 2008 survey of executives in large firms

found that 53 percent said that their organizations allocated five percent or less of their overall Information Technology budget to information security (Richardson, 2008). He further explains that security managers now have to usually justify their security budgets in economic terms and indicate a return on investment (ROI). Economic rationalization of security now needs to be included within budget justification, and web application managers need to effectively convey costing justifications to upper management. The cost of not implementing security can cause financial problems for firms. In 2008, the average annual security loss reported by firms was \$300,000 (Richardson, 2008). In addition, breaches can result in loss of customer goodwill (Gezelter, 2004, p. 22.21). Thus, spending appropriate funds on effective security is essential to a firm's continued profitability.

There are several other managerial and procedural factors that management should consider to enhance their Web applications and overall computer security. First, Lampson (2004) suggests that firms enforce auditing and logging to protect against attackers. This will allow periodic review of the application in order to ensure higher levels of security. In fact, not only is this advisable, but in the UK, compliance audits are a part of the Data Protection Act (France, 2001). Management also needs to ensure that secure Web application development is taken seriously and that security is included within the development process. Managers and developers often take the approach that developing new applications as rapidly as possible, not integrating security into design and spending the least amount of money as possible is the most effective approach. However, this is a common problem and often leads to loss of secure applications. Moscaritolo (2009) indicates that most Web applications are vulnerable and security requirements are rarely considered in system design and development.

7. Conclusion

The research in this paper shows that most insurance Web sites in three Western European countries do not meet minimum security protection levels for online consumers. An average of 20 percent of sites contain critical vulnerabilities and 70 percent contain medium-level issues. This is an unacceptable level of protection, and users of sites should be concerned about the risk to their data and computer systems. Several types of vulnerabilities are consistently found on many sites, such as old versions of software, injection and cross-site scripting errors. These types of vulnerabilities are not only predominant in this study, but are common in ubiquitous Web applications in many industries. There are defined technical methods of protecting against these specific problems, and technical staff must become more diligent in promoting safe Web development. In addition, firms should realize that security is not only a technical concern, but is a multi-dimensional concern. Managerial and procedural factors should be reviewed, and firms need to realize that lack of security can have a negative impact on profitability.

Although this study concentrated on insurance Web application for three Western European countries, it could be further expanded in future studies to include analysis of the U.S., other European countries as well as developing countries. It may be especially beneficial to review sites in developing countries as there is a lack of research into security issues with their online insurance sites. In addition, the number of citizens using online agents for these countries will continue to grow, and the benefit of secure Web sites will be critical to their consumers.

References

- Access to European Union Law, (1995), "Directive 95/46/EC of the European Parliament and of the Council," Retrieved 1st of October, 2009 http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Directive&an_doc=1995&nu_doc=46
- Advanced Research Corporation (2009) "Security Auditor's Research Assistant", Retrieved 4th of October, 2009 <http://www-arc.com/sara/>.
- Brown, J. & Goolsbee, A. (2002) "Does the Internet Make Markets More Competitive? Evidence from the Life Insurance Industry," *Journal of Political Economy*, June 2002, 110(3), pp. 441-507.
- Castro-Edwards, J. (2008) "Data Protection: Where Are We Now?", *Journal of Database Marketing and Customer Strategy Management*, December 2008, Vol. 15, No. 4, pp. 285-292.
- Cenzic (2009) "Web Application Security Trends Report Q3-Q4, 2008", Retrieved 27 of September, 2009 http://www.cenzic.com/downloads/Cenzic_AppSecTrends_Q3-Q4-2008.pdf
- Comscore.com, (2009) "U.S. Auto Insurance Policies Purchased Online Up 7 Percent In 2008 Versus Year Ago Despite Soft Consumer Demand," April 2, 2009, Retrieved 1st of October, 2009 http://comscore.com/index.php//Press_Events/Press_Releases/2009/4/Auto_Insurance_Policies_Purchased_Online_Up_7_Percent
- Cox, M. (2002) "Apache Security Secrets: Revealed", *Proceedings of ApacheCon 2002*, Los Angeles, Ca. 2002. Retrieved 4th of October, 2009 <http://www.cgisecurity.com/webserver/apache/tu04-handout.pdf>.
- Data Protection Commissioner Ireland (2005), "Security Guidelines," Retrieved 21st of September, 2009 <http://www.dataprotection.ie/viewtxt.asp?DocID=29&StartDate=1+January+2009>
- Flinders, K. (2009) "Insurance firm breaches Data Protection Act," *Computerweekly*, Retrieved 1st of October, 2009 <http://www.computerweekly.com/Articles/2009/07/08/236818/insurance-firm-breaches-data-protection-act.htm>.
- France, E. (2001, June) "Data Protection Audit Manual", *Information Commissioner's Office*, Retrieved 11th of October, 2009 http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_complete_audit_guide.pdf
- Gerber, L. (2008) "Latest Studies Reveal The Dangers Of Using Out Of Date Software!", *PCINews.com*, Retrieved 1st of September, 2009 <http://www.pc1news.com/news/0444/latest-studies-reveal-the-dangers-of-using-out-of-date-software.html>.

Gezelter, R. (2002) "Protecting Web Sites" in *Computer Security Handbook*. Bosworth, S. & Kabay, M. (editors), John Wiley & Sons, NY.

Gross, G. (2009) "Batteries.com, Insurance Firm Report Data Breaches," IDG News Service. Retrieved 1st of September, 2009 http://www.csoonline.com/article/494086/Batteries.com_Insurance_Firm_Report_Data_Breaches.

Guarda, P. (2008) "Data Protection, Information Privacy, and Security Measures: an essay on the European and the Italian Legal Frameworks," *Cyberspaizo e dir.*, 2008, 65-92. Retrieved 1st of October, 2009 https://www.inf.unibz.it/courses/images/stories/2008_2009/dataprotection_securitymeasures_guarda.pdf.

Hoffman, D., Novak, T., & Peralta, M. (1999) "Building Consumer Trust Online," *Communications of the ACM*. 42(4), April 1999, pp. 80-85.

IBM (2009) "Web Application Security", Retrieved 1st of September, 2009 <http://www-01.ibm.com/software/rational/offerings/websecurity/webappsecurity.html>.

Ko, M., & Dorantes, C., (2006) "The Impact of Information Security Breaches on Financial Performance of the Breached Firms: An Empirical Investigation", *Journal of Information Technology Management*. 17(2), pp 13-22.

Lampson, B. (2004) "Computer Security in the Real World", *Computer*, 37(6), pp. 37-46.

Lee, S, & Cata, T. (2005), "Critical Success Factors of Web-Based E-Service: The Case of E-Insurance," *International Journal of E-Business Research*, 1 (3), pp. 21-40.

Moscaritolo, A. (2009) "Web apps account for 80 percent of internet vulnerabilities", *SC Magazine*. 2009, March 18. Retrieved 1st of October, 2009 <http://www.scmagazineus.com/Web-apps-account-for-80-percent-of-internet-vulnerabilities/article/129027/>.

Naraine, R. (2003) "When Patches Aren't Applied", *Cioupdate.com*, Retrieved 1st of October, 2009 <http://www.cioupdate.com/reports/article.php/2172051/When-Patches-Arent-Applied.htm>.

N-Stalker (2009) "N-Stalker Security Checks", Retrieved 15th of September, 2009 <http://nstalker.com/products/security-checks>

Office of Head of State (1999) "Organic Law 15/99 of 13 December 1999 on the Protection of Personal Data," Retrieved 1st of October, 2009 https://www.agpd.es/upload/Ley%20Org%20Elnica%2015-99_ingles.pdf.

Office of the Data Protection Commissioner, (2001), *Security Measures for Personal Data: A Guide to the New Data Protection Rules, European Communities (Data Protection) Regulations, 2001*, Retrieved 18th of September, 2009 <http://www.dataprotection.ie/viewdoc.asp?DocID=39>

Reportlinker.com (2008), "Motor Insurance: Global Industry Guide," November 2008, Retrieved 1st of September, 2009
<http://www.reportlinker.com/p099574/Motor-Insurance-Global-Industry-Guide.html>

Richardson, R. (2008), "2008 CSI Computer Crime & Security Survey", *Computer Security Institute*. Retrieved 1st of October, 2009
http://www.gocsi.com/forms/csi_survey.jhtml.

Robinson, N., Graux, H., Botterman, M. & Valeri, L. (2009) "EU Data Protection Directive: Summary", UK Information Commissioner's Office. May 2009.
Retrieved 1st of October, 2009
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive_summary.pdf.

Sanchez, J. (2009), "Spain: New Data Protection Rules," Mondaq.com, Retrieved 1st of October, 2009 <http://www.mondaq.com/article.asp?articleid=64912>.

SANS Institute (2009a) "SANS Top-20 2007 Security Risks (2007 Annual Update)", Retrieved 15th of September, 2009 <http://www.sans.org/top20/#s1>.

SANS Institute (2009b) "SANS Top-20 2007- Cross Site Scripting", Retrieved 15th of September, 2009 http://www.owasp.org/index.php/Top_10_2007-A1.

SANS Institute (2009c) "SANS Top-20 2007 – Injection Flaws", Retrieved 15th of September, 2009 http://www.owasp.org/index.php/Top_10_2007-A2.

Tenable Network Security (2009) "Nessus ProfessionalFeed", Retrieved 15th of September, 2009 <http://www.tenablesecurity.com/nessus/>.

Young, T. (2009) "Insurance firm breaches Data Protection Act," *Computing*, Retrieved 15th of September, 2009
<http://www.computing.co.uk/computing/news/2243798/amicus-legal-breaches>

Dolog, P., Schaefer, M. (2005). A Framework for Browsing and Manipulating and Maintaining Interoperable Learner Profiles, Proc. of UM2005 - 10th International Conference on User Modeling, July, 2005, Edinburgh, UK. Springer Verlag.

Cheetham, G. & Chivers, G. (2005). *Professions, Competence and Informal Learning*, Cheltenham:Edward Elgar Publishing.

Deerwester, S., Dumais, S.T., Furnas, G. W., Landauer, T. and Harshman, R. (1990).Indexing by latent semantic analysis. *Journal of the American Society for Information Science*, vol. 41, 391-407.

IMS Global Learning Consortium (2005). *IMS ePortfolios Specification*. Retrieved 1st of July, 2006 from <http://www.imsglobal.org/ep/index.html>