Secure Web Application Development and Global Regulation

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

L. Milton Glisson
N. C. A&T State University
glissonm@ncat.edu

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

Abstract

The World Wide Web (WWW) has been predominantly responsible for instigating radical paradigm transformations in today's global information rich civilizations. Many societies have basic operational economical components that depend on Web enabled systems in order to support daily commercial activities. The acceptance of E-commerce as a valid channel for conducting business coupled with societal integration and dependence on Web enabled technology has instigated the development of local, national, and global efforts to regulate criminal activities on the World Wide Web. This paper makes two contributions. The first contribution is the high-level review of the United States and United Kingdom legislation that has developed from the escalation and integration of the World Wide Web into society. The second contribution is the support for the idea that legislative compatibility, in concert with an organization's policy compatibility, needs to be acknowledged in secure Web application development methodologies.

1. Introduction

The World Wide Web (WWW) has been predominantly responsible for instigating radical paradigm transformations in today's global information rich civilizations. Many societies have basic operational economical components such as health care, government agencies, and financial services that depend on Web enabled systems in order to support daily commercial activities. E-commerce has achieved global acceptance as a valid channel for conducting business. Researchers predict revenue results from e-commerce activities in 2005 will be in the trillions of dollars[21]. The money spent on e-commerce applications to support this new revenue stream is in the billions. The criticality of the Web can also be demonstrated via organizational budgeting practices. The percentage of an organizations total information technology budget that is designated to e-business initiatives has increased from 17.5 % in 2001, to 19.3% in 2002, to 20.3 % in 2003 [27]. E-business continues to grow in significance in today's business environment. The economic, legal and societal interest in the e-business growth has created a demand for a more secure Web enabled business environment. Despite the critical role that security plays in the potential growth of e-commerce, reports are repeatedly produced by CSI/FBI [15], Deloitte [9] and PricewaterhouseCoopers [39] illuminating the fact that security breaches continue to cost organizations billions of dollars yearly.

The cost associated with security breaches coupled with society's dependence on the Web, and the issue of national security has prompted nations to introduce governance through legislation. This paper supports the idea that legislative compatibility, in concert with an organization's policy compatibility, needs to be acknowledged in secure Web application development methodologies.

2. Threat from the Internet

Several years ago (1996) in Chicago, an EmergencyNet News (ENN) Service news bulletin indicated that, according to reports from the Defence Investigative Service, the Internet was one of the fastest growing areas of intelligence gathering by foreign governments and potential enemies of the United States and her allies. At that particular time, it was believed that foreign entities were using the "net" extensively to gather military and commercial information and to practice the art of spreading disinformation. These contacts often identified themselves as sales agents, consultants, or representatives of other countries and even suggested that he or she was working for a "friendly" government or military agency[43]. There have been numerous contacts made via the Internet to American defence contractors, software producers, and related industries, all of which have been directed toward proprietary or sensitive information, schematics, blueprints and other proprietary information about the targeted companies or their products.

Another subterfuge involves using e-mail to engage in "social engineering" with company employees and

attempting to establish friendships with employees, which could prove beneficial to more traditional espionage methods[43]. Virtually everyone is familiar with these methods, but they are still being used and, most importantly, they are still working!

A new technique was developed in 2002. International terrorists began using the Internet to extort money from financial institutions, prompting at least some of those institutions to adopt appeasement policies. In other words, banks, brokerage houses, and investment firms in both the United States and the United Kingdom have paid off criminals who threatened to attack their computer systems, according to a report in the Times of London. At that time, it was indicated that terrorists had amassed upwards of 400 million pounds worldwide by issuing threats that they would destroy the computer systems of companies who did not meet their monetary demands[42].

Money was transferred to offshore bank accounts by financial organizations in London. The terrorists removed the money within minutes of its arrival. In three of the cases, the blackmail was for 10 million pounds. The fourth victim paid 12.5 million pounds. In these kinds of cases, banks are prone to keep the incidents quiet because of fear of loss of public confidence and the fear of copycat crimes by others[42].

These financial extortionists have become known as Cyber Terrorists. London is not by itself. At InfoWarCon in Montreal, Canada, in 1996, Steve Macko indicated that he had identified up to 43 financial institutions in Europe and the United States that had suffered organized financial attacks; a situation which he described as ". . .an example of Class III Information Warfare"[29]. According to the Emergency Net NEWS (ENN), the London Sunday Times, has learned that British and American Law enforcement agencies have investigated numerous "attacks" on financial institutions in London and New York since 1993. One of the major problems is that the crimes are carried out globally but law enforcement agencies stop at each other's border[29].

In each case, the extortionists threatened to crash the computer system of the company. They also demonstrated that they had the knowledge and capability to render the company's computer systems useless. According to the National Security Agency (NSA), they have penetrated computer systems using what are referred to as "Logic Bombs," which can be detonated remotely, electromagnetic pulses and "high emission radio frequency guns" which can blow a devastating electronic pulse through the computer systems[29]. This electronic invasion completely destroys any information inside the computer. To add insult to injury, the terrorists leave encrypted messages, which by pass the highest security levels of the systems. One such message read "Now do you believe we can destroy your computers?"[29].

3. Information Warfare

As noted by Kovacich, Alvin and Heidi Toffler identified three specific periods through which countries traverse that include the Agricultural Period, The Industrial Period and the Information Period[23]. As the twenty-first century opens, the majority of the world's nations are entering the information age. A side effect on the transition to the information age is that nations become system and information dependent.

Technology, computers and telecommunications systems are terms that are often used synonymously and because of the availability, power and low cost of the microprocessor; the world is in the process of building a Global Information Infrastructure (GII) [23]. This GII will carry the communications of individuals, business organizations, governments, and social sectors of all nations to every other sector and nation of the world. In years to come, GII will have the capacity to change cyber international borders, support or ignore cyber-economies, establish or destroy cyber markets, and change the concept of international relationships. The major conduit for the GII is naturally the World Wide Web. This makes web applications the expected targets for attacks. Confirming this trend, the U.S. Military has already begun graduating information warfare hackers to prepare for a new type of military action. You can be assured that other countries are taking similar steps for their own protection. But so are those in the world who would cause havoc[23].

4. Information Governance

Currently, companies in the economically advanced countries of the world are under significant pressure from government-mandated compliance requirements to implement new rules which put greater emphasis on how data is processed, managed and secured at virtually every level within the organization. These compliance mandates have the effect of forcing organizations to improve the management of volumes of information both created by the organization and received from global enterprises. The term "Information Governance" has moved to the forefront as a result of a combination of compliance regulations and market forces of globalization as companies attempt to manage a mountain of data that is being created on a daily basis[1].

The Aberdeen Group that conducted the benchmark study on Information Governance identified three performance levels and each group's level of performance:

1. Laggards (30%): This category identifies those enterprises whose practices are significantly behind the Industry Average.

2. Industry Average (50%): This category identifies those enterprises whose practices represent the average or norm.
3. Best in Class (20%): This category identifies those enterprises whose practices are significantly superior to the Industry Average[1].

It is interesting to note a couple of the specific findings of the Aberdeen Group's benchmark study such as:

1. Sixty-two percent (62%) of the companies indicated that compliance rules are a major Information Governance (IG) driver.
2. Forty-nine percent (49%) of the firms identified communication of information policies and procedures as a major 'pain-point' in advancing new governance strategies[1].

All of which is to say it is often necessary for new regulatory measures to have a requirement for compliance within the structure of the regulation and a penalty for non-compliance, which will force the individual firms to make a concerted effort to develop the necessary communication channels to deliver the information to the appropriate individuals.

To put this contest of "War" into perspective, Win Schwartau, defines three classes of information warfare: Class 1: personal information warfare, Class 2: corporate information warfare, and Class 3: global information warfare[41]. On the other hand: "The Computer Security Institute defines information warfare as, (d)istinct from "computer crime" because it implies an aggressive act on the part of one adversary – whether an individual, a competing organization or a rival government – against another in an ongoing struggle for hegemony in the marketplace or the political arena"[2].

Personal information warfare is probably best identified as the theft of your personal identity. Corporate information warfare is when the business entity loses market share, revenue, or products as a result of an attack from a competitor, which is not necessarily unlawful. Global information warfare takes place on a daily basis due to the high level of global competition among the world's leading corporations. Realistically, it is logical to assume that this warfare is probably conducted both legally and illegally.

5. US Legislation

Legislation exists in the US on both the Federal and the State levels. Since there are fifty states, covering the impact of all of individual state legislation is beyond the scope of this paper. However, the existence of the legislation needs to be acknowledged. An example of state legislation is the Minnesota Security Brach Disclosure Act. This act requires business to contact individuals when their personal data has been released to unauthorized parties due to a security breach[45].

Federal level executive orders / legislation that have affected the computer industry include the following:

- Electronic Communications Privacy Act - provided some of the foundations for investigating computer crimes[35].
- Federal Information Security Act (FISA) of 2002 - "requires each agency to inventory its major computer systems, to identify and provide appropriate security protections, and to develop, document, and implement an agency-wide information security program"[35].
- Executive order - National Strategy to Secure Cyberspace - makes recommendation to network operators[35].
- Homeland Security Act of 2002 - provides authority to the Secretary of Homeland Security to develop Information systems to encourage the storage, analysis and exchange of information[35].
- Homeland Security Presidential Directive No. 7 (HSPD-7) - stresses the improvement of protecting US critical infrastructure[35].
- Cyber Security Research and Development Act - authorized the National Science Foundation to award funding for computer security related activities[35]
- Check Clearing for the 21st Century Act - enables banks to process checks electronically and provide substitute checks to customers[55].

As discussed in the *Web Development Evolution: The Business Perspective on Security* [13], societal pressure is encouraging the development of U.S. legislation. This legislation includes:

- The Economic Espionage Act of 1996 (EEA)
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- The Graham-Leach-Bliley Act of 1999
- The Sarbanes-Oxley Act which was passed into law in July of 2002[62]
- The Fair and Accurate Credit Transaction Act of 2003
- The Family Rights and Privacy Act (FERPA)
- Identity Theft Penalty Enhancement Act of 2004.

The EEA was the first law that explicitly makes the theft of commercial trade secrets a federal crime[10, 13, 19]. The Act defined information in very broad terms which includes storage of information in intangible forms like that of a document on a computer[10, 13]. The EEA was liberal in how it defined "the phrase 'obtaining information' which includes merely reading it"[10, 13]. Possible penalties for violating the EEA range from fines, to imprisonment, to forfeiture of any property used to commit or facilitate the crime[5, 13, 19].

HIPAA is concerned with disclosure and transmission of healthcare information[7]. The Graham-Leach-Bliley Act focuses on how financial organizations use and distribute a customer's personal information[13, 17]. The Sarbanes-Oxley (SOX) Act was 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[13, 20]. However, the wording in the law has a broader reach than just the financial industry. The law (Sarbanes-Oxley) states that company CEOs and CFOs establish and maintain proper "internal controls"[13, 20, 62]. This means that by signing off on the validity of the data within the system they are also signing off on its security[13, 20]. It is important to note that this is only applicable in situations where the data can have a material impact on the organization's financial results[62].

FERPA protects the privacy of student records[54] and The Identity Theft Penalty Enhancement Act introduces stricter penalties for identity theft[36]. The legislative story continues to evolve. A ninety-one page bill was introduced in the Senate by Senator Patrick Leahy and Senator Arlen Specter[31]. The proposal is an aggressive "regulation-oriented" bill containing "an avalanche of new rules for corporate data security and stiff penalties for information burglars"[31]. The motivation for the legislation is the result of a series of high profile security problems[31].

6. US Legislation with International Impact

It should be noted that the SOX Act has an international impact. "It is significant to note that – in contrast to the traditional accommodation provided under the Securities Exchange Commission (SEC) and national exchange rules for listed non-U.S. companies – the requirements of the Act apply to all foreign private issuers:

- that have securities, including American Depositary Receipts ("ADRs"), registered under section 12 of the Securities Exchange Act of 1934;
- that are required to file reports under section 13(a) or 15(d) of the Securities Exchange Act (including all European companies filing Form 20-F); or
- that have filed a registration statement that has not yet become effective (under the Securities Act of 1933) and that have not been withdrawn"[30].

This translates into the Act being applicable to non-US companies that are registered with the SEC with a few exceptions. Other acts that have international impact include:

- Electronic Signatures Act - grants electronic contracts the same weight as paper contracts[56].
- The Computer Fraud Act of 1984 - dealt with computer violations to government computers[63].
- The National Information Infrastructure Protection Act of 1996 amended the Computer Fraud Act of 1986 [53] - expanded the legal reach to include non-government computers making unauthorized access to computer, not in the same state, a federal crime[63].
- The USA Patriot Act of 2001 - greatly expands the US government's capabilities to legally intercept a multitude of communications including communications relating to computer fraud and abuse[38].
- The US Safe Harbor Act - an agreement that allows US companies conducting business in the EU to conform to EU data protection laws[44].

7. UK Legal Issues

The purpose of this section is to acknowledge the legal pressures that are mounting through the introduction of legislation throughout the world in response to computer crimes and acknowledge the importance of a stable cyber space. Cyber legislation still has many problems to address that include the common definitions on computer crimes, international relations, sovereignty and jurisdiction[60]. To win the war on cyber crime legislation must not only be enacted but enforced as well. Enforcement of legislation in computer crimes is very difficult due to an array of factors that include anonymity, global reach through multiple jurisdictions, and the retention and preservation of evidence[24]. Additional factors include resources, technical knowledge, and the speed at which technology develops on the web, coupled with the need to counteract emerging problems[33].

The authorities need to have the resources to pursue cyber crimes; they need to have the employees with the proper technical knowledge to work on the cases and to ensure the accuracy of the data that is being presented in courts. A classic example is a breached server. Standard server activity includes log updates like access logs, error logs, and script logs. The logs are being modified via the system as it supports its everyday functions. As a general rule, courts do not like modified evidence. If the server modified the evidence the logical question that follows this line of thought is did the intruder alter the logs during the breach? In addition to these concerns, there is the need for properly trained professionals to capture this information without alteration or destruction and reasonably quickly from the time of the security breach. All of these issues from both the legislative and the enforcement perspective affect the ability of a government to prosecute computer crimes.

The cyber community is international by the very nature of the net. Hence, cyber crime is an international issue that affects all cyber citizens. This means that the US is not the only country that is concerned with cyber crime. Several countries have created legislation to address issues that have developed though the expansion of the net. Some of the legislation for forty-four different countries is listed in a report by Stein Schjolberg[40].

The United Kingdom laws that have impacted technology include the following:

- The Theft Act 1968 - applicable to fraud
- The Forgery and Counterfeiting Act 1981 - applicable to obscene materials
- The Criminal Damage Act 1977 - applicable to physical damage of computers
- The Protection of Children Act 1978 - applicable to child pornography
- The Telecommunications Act 1984
- The Public Order Act 1986 - applicable to racist materials
- The Criminal Justice Act 1988
- The Malicious Communications Act 1988 [50]
- The Copyright, Designs and Patents Act 1988
- The Computer Misuse Act of 1990
- The Criminal Justice and Public Order Act 1994
- The Data Protection Act of 1998
- Regulation of Investigatory Powers Act(RIP) 2000 [51]
- Electronic Communications Act 2000 [48]
- The Telecommunications Regulations 2000 [52]
- The Electronic Signatures Regulations 2002 [49].

Several of the Acts listed above are mentioned on the Civil Society Internet Rights project Web page[4]. All of the Acts listed above have influenced the application legality of Information Communication Technology. Four commonly examined laws when discussing computer crimes and the World Wide Web include:

- The Telecommunications Act 1984
- The Computer Misuse Act of 1990
- The Data Protection Act of 1998
- Regulation of Investigatory Powers Act (RIP) 2000.

The Telecommunications Act makes it a criminal act to transmit obscene materials via a telecommunications network or to deceive a licensed telecommunications service. The Act defines a telecommunication network broadly enough to include internet traffic[34].

In August of 1990, the Computer Misuse Act became law in the United Kingdom. The Act is concerned with three specific offences: unauthorised access to computer material; unauthorised access with intent to commit or facilitate commission of further offences; and unauthorised modification of computer material[46].

As with any act, there are always possibilities for amendments. Tom Harris proposed an amendment to The Computer Misuse Act of 1990 that would clearly criminalise interference with computer systems via denial of service attacks and significantly lengthen the maximum imprisonment terms for offences for unauthorized access and unauthorized modification [3]. The idea is to use the increased prison times as a deterrent for future crimes and increase extradition for violations of the law[26]. The reasoning behind the need to increase the prison time is to bring into line prison terms with that of other countries that were part of the Convention of Cyber-crime and make the crime serious enough to warrant extradition[61].

The Data Protection Act specifically addresses offences concerned with unauthorised procurement and / or processing of data[34]. An interesting point in the Data Protection Act is where a proven offence has taken place and the wording referencing the liability within corporate bodies in section sixty-one which states that “any person who was purporting to act in any such capacity, he as well as the body corporate shall be guilty of that offence and be liable to be proceeded against and punished accordingly”[47].

The Regulation of Investigatory Powers Act (RIP) 2000 deals with two major points. These points include the interception of data and the relinquishing of encryption keys. This means that the UK government can compel Internet Service Providers (ISP) to copy its traffic and divert this information to a government location for analysis. It also means that individuals holding encryption keys can be subject to prosecution for non-disclosure and for notifying any one that they have been served with a disclosure notice[16, 34, 51].

8. International Legal Forum

The importance of cyber space is voiced in the US report *The National Strategy to Secure Cyberspace* via the statement that, in regards to the nation’s critical infrastructure, “Cyberspace is their nervous system — the control system of our country” and that “the healthy functioning of cyberspace is essential to our economy and our national security”[58]. International support for this perspective is visible through efforts attempting to address computer crime which include agreements by the G8 nations [22], the Mutual Legal Assistance Treaties (MILAT)[57], the European Union border controls (Interpol) and United Nations (UN) recommendations[6, 18].

A major event taken on the international level occurred on November of 2001 when twenty-two European countries along with Japan, Canada, South Africa and the US signed the Cyber-crime treaty[37] also referenced as the Convention on Cyber-crime. The treaty is unique in that it is “the first international treaty on crimes committed via the Internet and other computer networks”[8]. The treaty "addresses an important problem: the difficulties law enforcement has in purs(u)ing criminals across national borders, something that is common in Internet crime"[25]. The Cybercrime treaty was put into force in July of 2004 (which required five ratifications including a minimum of three member countries) and address activities like “infringements of copyright, computer-related fraud, child pornography and violations of network security”[8]. Since then it has been

amended to include "an Additional Protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offence"[8]. Realistically, this means that "the Convention addresses issues of substantive and procedural criminal law, which member states are obliged to take measures to implement in national law, as well as issues of international co-operation"[61].

Along with international efforts to address cyber-crime governance there are several organizations that attempt to track and provide assistance with computer crime issues. These organizations include the Computer Emergency Response Team (CERT) at Carnegie Mellon, the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University, the Computer Incident Advisory Capability (CIAC) with the US Department of Energy, BugTraq which provides information on security vulnerabilities[18] and the Computer Crime Research Center.

9. Secure Web Application Development Methodologies

The support for legislative compatibility acknowledgement in secure application development process is constructed through the individual sections of this paper. The industry surveys discussed in section one indicates that the cost associated with security breaches is high. The estimated budgets discussed in the same section provide an estimated gauge on the importance of Web technology to today's businesses. The ease with which information is available on the net and the international obtainability is discussed in section two. The fact that organizations use this information to their advantage (in information warfare) is highlighted in sections three and four. The legislation discussed in the previous sections demonstrates the growing need to be aware of (global) internet legislation in the development process.

Gartner refers to the information security process as "The newest and least-mature lens added to the resources of the information security officer"[12]. The article also states that "focus(ing) on process maturity can improve the quality of work and the efficiency with which it is accomplished (and that) the ability to translate efficiency into cost savings makes process maturity an easily justified investment"[12]. In an article titled, *Software Security,* McGraw makes an excellent point stating that "we must figure out ways to build easier-to-defend code" and that the real problem "is poorly designed and implemented software"[32]. However, he does not discuss the legal impact for failing to build and implement more secure code; nor, does the article attempt to address organizational compatibility in the development process. Similar oversights occur in Comprehensive Lightweight Application Security Process (CLASP)[59], Microsoft's "Trustworthy Computing Security Development Lifecycle"[28], and "A methodology for secure software design"[11].

The Web Engineering Security (WES) methodology does acknowledge 'Organizational Compatibility' in the Security Requirements stage [14]. The WES methodology continues to break down organizational compatibility into Security Policy, Corporate Culture, and Technology Compatibility [14]. A sub-section of the security policy compatibility section is legal compatibility.

Examples of legal compatibility issues can be seen in information availability and information transmission. As discussed in section two, internet information is accessible to everyone. Does the amount of information that will be publicly available via an internet application comply with organizational policies, better yet, can it be used against the organization in any form of information warfare as discussed in section three? More importantly, does your Web enabled application violate any laws like the Data Protection Act of 1984 in the United Kingdom, via transmission of the data or storage of the data? If your application is passing information over the net and it is travelling via internet service providers, based in other countries, is there a legal violation of any type? Better yet, if the information is stored in another country what are the legal ramifications?

The results of this research brought about the expansion of the legal compatibility section within the WES methodology. The legal compatibility section now includes a check list of the US and UK legislation that applies to Web applications. The list is not exhaustive. The legal responsibility for the Web application still resides with the organization developing the application. The purpose behind the check list is to initiate a conversation over potentially relevant legalisation and to raise overall awareness on the subject.

The international ramifications to the use of Web enabled technology may be specific to individual countries such as the United Sates. Does your Web enabled system automatically e-mail order confirmations to customers in the United States? If so, has the organization considered the contractual obligations that this might create under the Electronic Signatures Act? The international impact is blatantly obvious with Sarbanes Oxley (SOX). If your business is listed on the Securities Exchange Commission (SEC), is your Web enabled system, which has a material impact on the organizations' financial results, secure according to Sarbanes Oxley (SOX) regulations?

The legal aspect of the project needs to be addressed early in the application development process as part of the secure application development methodology. This allows the organization to make a conscious decision as to whether to accept the risk the application introduces to

the business environment or to attempt to appropriately mitigate said risk.

10. Conclusion

Cyber-crime is a reality that cannot be ignored in today's global business environment. The ramifications from a financial perspective and a legal perspective are potentially enormous. Hence, Web application security needs to be incorporated into the entire development methodology. This includes upfront acknowledgement of the legal ramifications involved with the development and deployment of the Web applications. Effective security resolutions need to acknowledge the legal ramifications that the application introduces to the company and the attendant risks need to be mitigated.

The purpose behind this paper is not to debate the legislative or the legal enforcement challenges that computer crime presents. Nor is it to discuss the effectiveness of the current legislation or potential conflicts between legislation enacted in different countries.

The point is to acknowledge the increasing global legislation that is developing due to the growing impact of the World Wide Web on everyday life, on the business economical environments and the national importance. Economies continue to integrate with the Web to produce and/or provide goods and services. Societies continue to increase dependence on the Web to help provide basic operational economical components. This increasing dependency introduces potential national security risks. Therefore, societies are demanding a more secure World Wide Web which leads to the continued creation of new and refinement of existing security legislation. This security legislative growth potentially has world wide ripple effects on the global economy.

Our future research interest, in this area, is to examine the practicality and productivity of the processes and procedures implemented, by individual organizations, to address the legislative requirements that are being imposed on organizations.

Additional research should examine the practical effectiveness of international and domestic cyber legislation from a successful prosecution perspective, in respect to the deterrence of cyber crimes and the practical effects on the business environment. Research may also want to investigate any legislative conflicts between countries and the possible resolutions to any conflicts.

Acknowledgements: We would like to thank two security experts from a Global Fortune Five-hundred financial organization for their valuable input.

11. References

[1] A. Adamopoulos, *The Information Governance Benchmark Report*. 2006 http://www.aberdeen.com/summary/report/benchmark/RA_INFOGOV_AA_3291.asp.

[2] R.W. Aldrich, *The International Legal Implications of Information Warfare*. 1996. p. 4

[3] BBC, *Penalty plea on cyber criminals*. 2005, BBC http://news.bbc.co.uk/1/hi/uk_politics/4676169.stm.

[4] Civil Society Internet Rights Project (CSIR), *UK Internet Rights project: Fact Sheets: Computer crime*, internetrights.org.uk http://www.internetrights.org.uk/.

[5] M. Coblenz, *Federal Protection of Trade Secrets: The Economic Espionage Act of 1996*. c1997, Washington State Bar Association http://www.wsba.org/media/publications/barnews/archives/sep-97-federal.htm.

[6] Computer Crime Research Center Staff, *UN recommendations on fighting cybercrime*. 2005, Computer Crime Research Center http://www.crime-research.org/news/12.05.2005/1225/.

[7] P.L.-t. Congress, *HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996*. c1996, Congress: Washington http://aspe.hhs.gov/admnsimp/pl104191.htm.

[8] Council of Europe, *Convention on Cybercrime*. 2004, Council of Europe http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm.

[9] Deloitte, *2005 Global Security Survey*. 2005, Deloitte Touché Tohmatsu: London. p. 1-44.

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

[11] E.B. Fernandez. *A methodology for secure software design*. in *Procs. of the 2004 Intl. Symposium on Web Services and Applications (ISWS'04)*. 2004. Las Vegas, NV http://polaris.cse.fau.edu/~ed/EFLVSecSysDes1.pdf.

[12] Gartner Research, *Three Lenses Into Information Security*. 2006. p. 1-4.

[13] 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/.

[14] W.B. Glisson and R. Welland, *Web Engineering Security (WES) Technical Report*. 2007, University of Glasgow.

[15] L.A. Gordon, et al., *2005 CSI/FBIComputer Crime Survey*, in *Tenth Annual*. 2005, Computer Security Institute. p. 25.

[16] Guardian Unlimited, *The RIP Act*. 2000, Guardian Unlimited http://www.guardian.co.uk/theissues/article/0,6512,334007,00.html.

[17] C.P. Guide, *Financial Modernization Act (Gramm-Leach-Bliley Act)*. c2001, ConsumerPrivacyGuide.org http://www.consumerprivacyguide.org/law/glb.shtml.

[18] S. Hansche, J. Berti, and C. Hare, *Official (ISC)2 Guide to the CISSP Exam*. 2004, Boca Raton: Auerbach.

[19] C. Hare, *Policy Development*, in *Information Security Managment Handbook*, H.F.T.a.M. Krause, Editor. c2004, Auerbach Publications: Boca Raton. p. 925-943.

[20] E. Hurley, *Security and Sarbanes-Oxley*. c2003, SearchSecurity.com http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci929451,00.html.

[21] R.O.N. King, *E-Business Growth Demands Security Spending*. 2004, Web Hosting Industry Review http://www.thewhir.com/features/security-spending.cfm.

[22] W. Knight and J. Thorel, *G8 nations team up to fight cyber-crime*. 2000, ZDNet UK http://news.zdnet.co.uk/internet/security/0,39020375,2079018,00.htm.

[23] G.L. Kovacich, *Chapter 4-2-1: Information Warfare and the Information Systems Security Professional*, in *Handbook of Information Security Management: Policy, Standards, and Organization*, M. Krause and H.F. Tipton, Editors, CRC Press LLC.

[24] J. Landman, *Forensic Computing: An Introduction to the Principles and the Practical applications*. 2002, School of Computing and Mathematics, University of Western Sydney: Sydney, Australia. p. 15.

[25] R. Lemos, *International cybercrime treaty finalized*. 2001, CNET Networks http://news.com.com/2100-1001-268894.html.

[26] J. Leyden, *Enforcement is key to fighting cybercrime*. 2004, The Register http://www.theregister.co.uk/2004/07/02/cma_reform_analysis/.

[27] Line 56, *E-Business Spending now exceeds 20 percent of all I.T. expenditure*. 2003, Line56.com http://www.line56.com/articles/default.asp?NewsID=4888.

[28] S. Lipner. *The Trustworthy Computing Security Development Lifecycle*. in *2004 Annual Computer Security Applications Conference*. 2004. Tucson, Arizona: Annual Computer Security Applications Conference http://www.acsac.org/2004/papers/Lipner.pdf.

[29] S. Macko, *The Cyber Terrorists*. 1996, ENN: Emergency Net NEWS Service http://www.emergency.com/cybrterr.htm.

[30] Mayer, et al., *The Sarbanes-Oxley Act of 2002 and its Impact on European Companies*. 2002, Mayer, Brown, Rowe, and Maw: Washington, DC. p. 26.

[31] D. McCullagh, *Senators propose sweeping data-security bill*. c2005, ZDNet News http://news.zdnet.com/2100-1009_22-5769156.html.

[32] G. McGraw, *Software security*, in *IEEE Security & Privacy*. 2004. p. 80-83.

[33] R. McKemmish, *What is Forensic Computing?* 1999, Australian Institute of Criminology. p. 6.

[34] P. Mobbs, *Computer Crime The law on the misuse of computers and networks*. 2003, GreenNet Civil Society Internet Rights Project. http://www.internetrights.org.uk/briefings/irtb08-rev1-draft.pdf.

[35] J. Moteff, *Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directives*. 2004, Congressional Research Service [CRS]: Washington, DC. p. 16.

[36] Office of the Press Secretary, *President Bush Signs Identity Theft Penalty Enhancement Act*. 2004, US Government: Washington, DC http://www.whitehouse.gov/news/releases/2004/07/20040715-3.html.

[37] C.P. Pfleeger and S.L. Pfleeger, *Security in Computing*. Third Edition ed. 2003, Upper Saddle River, NJ: Prentice.

[38] R. Plesser, J. Halpert, and M. Cividanes, *Summary and Analysis of Key Sections of USA PATRIOT ACT of 2001*. 2001, Center for Democracy and Technology http://www.cdt.org/security/011031summary.shtml.

[39] PricewaterhouseCoopers, *The Information Security Breaches Survey 2004*. 2004, PricewaterhouseCoopers.

[40] S. Schjolberg, *The Legal Framework - Unauthorized Access to Computer Systems*. 2003, Moss District Court, Norway http://www.mosstingrett.no/info/legal.html.

[41] W. Schwartau, *Information Warfare: Cyberterrorism : Protecting Your Personal Security in the Electronic Age*. 2 ed. 1996, New York, NY: Thunder's Mouth Press. 768.

[42] D. Shelton, *Banks appease online terrorists,*. 1996 http://news.com.com/Banks+appease+online+terrorists/2100-1023_3-213603.html.

[43] C.L. Staten, *Warning; Internet Used by Foreign Intelligence Operatives,*. 2006, ENN: Emergency Net News Service http://www.emergency.com/net-warn.htm.

[44] G. Steinke, *Data privacy approaches from US and EU perspectives*. Telematics and Informatics, 2002. **19**(2): p. 193-200.

[45] The State of Minnesota, *H.F. No. 2121, 3rd Engrossment - 84th Legislative Session (2005-2006)*. 2005, Minnesota House of Representatives http://www.revisor.leg.state.mn.us.

[46] UK Parliament, *Computer Misuse Act 1990*. 1990, Queen's Printer of Acts of Parliament: London

[47] UK Parliament, *Data Protection Act 1998*. 1998, Controller of HMSO: London

[48] UK Parliament, *Electronic Communications Act 2000*. 2000, UK Government: London

[49] UK Parliament, *The Electronic Signatures Regulations 2002*. 2002, UK Government: London

[50] UK Parliament, *Malicious Communications Act 1988*. 1988, UK Government: London

[51] UK Parliament, *Regulation of Investigatory Powers Act 2000*. 2000, Queen's Printer of Acts of Parliament: London

[52] UK Parliament, *The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000*. 2000, UK Government: London

[53] United States Department of Justice, *Computer Crime Policy & Programs*, US Government: Washington, DC http://www.usdoj.gov/criminal/cybercrime/ccpolicy.html.

[54] US Department of Education, *The Family Educational Rights and Privacy Act (FERPA)*, http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

[55] US Government, *Check Clearing for the 21st Century Act*. 2003, The Federal Reserve Board: Washington, DC http://www.federalreserve.gov/paymentsystems/truncation/.

[56] US Government, *Electronic Signatures Act*. 2000, US Government: Washington http://www.ecsi.net/help/help_esig.html.

[57] US Government, *Mutual Legal Assistance Treaty Between the United States and Russia*. 2002, US Government: Washington, DC http://www.state.gov/r/pa/prs/ps/2002/7734.htm.

[58] US Government, *The National Strategy to Secure Cyberspace*. 2003, US Government: Washington. p. 76.

[59] J. Viega, *Security in the software development lifecycle*. 2004, IBM http://www-128.ibm.com/developerworks/rational/library/content/RationalEdge/oct04/viega/.

[60] I. Walden, *Crime and Security in Cyberspace*. Cambridge Review of International Affairs, 2005. **18**(1): p. 51-68.

[61] I. Walden, *Harmonising Computer Crime Laws in Europe*. Journal of Crime, Criminal Law and Criminal Justice, 2004. **12**(4): p. 321-336.

[62] R. Zameeruddin, *The Sarbanes-Oxley Act of 2002: An Overview, Analysis, and Caveats*. c2003, University of West Georgia http://www.westga.edu/~bquest/2003/auditlaw.htm.

[63] G.R. Zegarelli, *Computer Fraud and Abuse Act of 1986*, BookRags & Macmillan Science Library: Computer Sciences http://www.bookrags.com/research/computer-fraud-and-abuse-act-of-198-csci-01/.