BRIDGING THE GAP BETWEEN COMPUTER SECURITY AND LEGAL REQUIREMENTS

CHRISTOPHER E. EVERETT*

Table of Contents

ABSTRACT

The security of computer systems is a critical issue to organizations. Business managers want to understand how the different security pieces of a computer system will help the bottom line of an organization. Information technology (IT) professionals, on the other hand, try to secure the systems using the limited time and money that is available in most technology budgets. Business managers and IT professionals need to understand each other's positions so that they can reach a compromise on the security aspects of an organization's computer system. The two sides can reach this compromise by analyzing the risks associated with the information maintained on a computer system versus the potential liability of a security breach. The corresponding security level can then be directly tied to the individualized needs of an organization. By working to bridge the gap between the two sides, business managers will know why security helps the bottom line of an organization and IT professionals will have the time and money to better secure the system.

* J.D. Candidate 2006, Nova Southestern University, Shepard Broad Law Center; B.S. in Computer Science and M.S. in Computer Science, Mississippi State University. The author wishes to thank: his wife, Dr. Christine R. Rutter, for all of her love and support throughout this process and the faculty of the Law Center, especially Professor Linda F. Harrison, for their support and guidance.

I. INTRODUCTION

It happens late at night across America more often then most business managers want to think about. The pager goes off alerting an information technology (IT) professional of a problem with the computer system. The IT professional has no choice but to check on the delicate balance of the system. Has the backup failed again, or is it another false alarm? The IT professional hopes that it is just another false alarm triggered by the rules of the system. As the IT professional logs into the system, the realization of what has happened breaks the silence of the night. The system has been hacked![1]

Although the described situation is fictional, the realization that a system has been hacked occurs on a daily basis.[2] After a computer system is hacked, the IT professional will at some point ask:

1) Have I failed in my duties? [3]
2) What could I have done to prevent this catastrophe?[4]
3) How can I convince the business managers that computer security helps the bottom line of the organization?
4) Will I lose my job?

This article is designed to answer the IT professional's third question:

- How can I convince the business managers that computer security helps the bottom line of the organization?

During the day-to-day routine, most IT professionals are worried about the technology of the system (i.e., "Will that new router fit into the network properly?" and "Will the new desktops allow for remote administration?") while business managers are more worried about the return on the investment of the technology (i.e., "Will that new router decrease the processing time of orders?" and "How will the new desktops increase productivity?"). One problem is that the business managers "may perceive that … security is something that the … [IT professionals] handle as part of their day-to-day activities" [5] or the business managers "may think that security is handled by the organization's firewall."[6] These perceptions are misguided and can be corrected through training and education to ensure that the business managers understand the measures necessary for a computer system to be secure.[7]

---

1. This scenario is fictional, but based on the author's experiences as an IT professional at numerous K-12 schools and small companies.

2. *See Software Engineering Institute*, CERT/CC Statistics 1988-2004, *at* http://www.cert.org/stats/cert_stats.html (last visited Feb. 17, 2005) [hereinafter CERT/CC Statistics].

3. An IT professional's worst nightmare is being hacked and not realizing it for several weeks or months.

4. The IT professional and business manager should keep in mind that "[a] fundamental fact in computer and network security is the impossibility of 100 percent assurance that a computer is *trusted*." William A. Arbaugh, *A Patch in Nine Saves Time?*, COMPUTER, June 2004, at 82.

5. Moira West-Brown, *Avoiding Trial-By-Fire Approach to Security Incidents*, CROSSTALK, Oct. 2000, *available at* http://www.stsc.hill.af.mil/crosstalk/2000/10/allen.html (last visited Feb. 17, 2005). The day-to-day activities of many IT professionals involve "basic support and operation of the vast amount of computing equipment in place." *Id.*

6. *Id.* "Firewalls may prevent some attacks, but cannot prevent all attack types; and, if not properly configured and monitored, they may still leave the organization open to a range of others." *Id.*

7. *See supra* note 4.

This difference in needs creates a split between the IT professionals and the business managers. While it is not always important that new desktops are delivered every three years, it is imperative that the computer systems are secure from threats.[8] Bridging the gap between the computer technology that the IT professionals want for the system and the computer technology that the business managers want to purchase for the system is challenging for even the most seasoned IT professional.

One way to bridge this gap between the parties is to confront both the technology aspects and business aspects of computer security. An IT professional can utilize the legal liability argument that stems from the information that is maintained on the computer system to give the business manager an argument for securing the computer system.[9] The business reasoning for securing the network turns on a utility argument that it will be cheaper to be proactive in the securing of the system, than having to pay for any loses and for attempting to secure the system after a breach.[10] The IT professional can determine the security drivers that fit the computer system that needs to be protected and decide what the minimal security level for the computer system needs to be.[11] The security level would be based on the utility analysis that will allow the organization to claim that it made reasonable efforts to protect the computer system from being hacked.

A. *Scope*

This article is designed for business managers, IT professionals, and attorneys. The article is designed to provide both a starting place to discuss the security measures that are needed to fulfill an organization's legal obligations and as a tool for justifications for security measures.[12] This article does not discuss under what legal theories an organization would be liable for a computer security breach, nor does this article discuss the pros and cons of those

---

8. There are many elements to computer security, but an important point is that "[c]omputer items must be protected only until they lose their value. They must be protected to a degree consistent with their value." CHARLES P. PFLEEGER, SECURITY IN COMPUTING 9 (2nd ed. 1999).

9. Decreasing the liability of information loses from an organization's computer system is imperative for business managers, because "[a] security incident can have a wide-ranging negative impact on a company's revenue streams, customer confidence, and public relations." MARK EGAN & TIM MATHER, THE EXECUTIVE GUIDE TO INFORMATION SECURITY: THREATS, CHALLENGES, AND SOLUTIONS 2 (2005).

10. "[A] *cost/benefit analysis* of network systems security is clearly important. The costs will be those of deploying and maintaining various defense mechanisms to protect a system or site against attacks, including the costs of any constraints on the system imposed by the defense mechanism." Soumyo D. Moitra & Suresh L. Konda, *The Survivability of Network Systems: An Empirical Analysis* 1, Technical Report CMU/SEI-2000-TR-021 (2000), *available at* http://www.cert.org/archive/pdf/00tr021.pdf (last visited Feb. 24, 2005). "The benefits will be those of increased survivability of the system or site" and as a direct result of the survivability a decrease in potential liability. *Id.*

11. "[S]ystems security professionals should assume that the legal system will come into play to compensate individuals and companies who can successfully allege and prove that there was some human error. For a successful defense, persuasive proof of extreme vigilance will be required … even when the latest and best in 'durable precautions' have been incorporated into network security." Fred Chris Smith, *Ethical Responsibilities and Legal Liabilities of Network Security Professionals*, 1997 PROC. OF THE 13TH ANN. COMPUTER SECURITY APPLICATIONS CONF. 239, 246.

12. This article is for organizations that maintain information on its computer systems whether for internal or external use, but this article does not cover any liability for military information since that type of information has a different set of requirements then non-military information.

different legal theories.[13] This article assumes that organizations will at some point in the future be held liable for failure to properly secure its computer systems, because "[t]he potential onslaught of claims arising from insecure computer systems is not a veiled threat, but more aptly a ripening promise."[14] This article covers not only the protection of an organization's own information, but information from other sources that an organization maintains on its computer systems.[15] By following the guidelines described in this article, an organization will be able to claim that they were attempting to fulfill their security obligations.[16]

B. *Overview*

Part I of this article began with an introduction of a day in the life of an IT professional that occurs across the world. Part I also discusses the limited scope of this article. Part II of this article discusses why computer systems should be secure. Part II also includes a discussion of the ever changing legal requirements for securing computer systems. Additionally, Part II includes an overview of the different types of risks involved with computer systems along with the relevant state and federal laws associated with the information.

Part III is an overview of the security drivers and the security levels that an organization should utilize in deciding how to protect the information maintained on its computer system. Part III then covers how the use of the utility analysis will resolve certain legal issues. Part IV demonstrates why the utilization of the utility analysis will work in practice to help business managers understand the potential liability issues regarding computer security and to help IT professionals give business reasons why an organization should invest in computer security.

---

13. There are numerous articles describing the different legal theories under which an organization may or may not be liable along with commentary about current and future laws regarding the different legal theories. *See, e.g.,* Nancy R. Mead, *Who is Liable for Insecure Systems?*, COMPUTER, July 2004, at 27; Ethan Preston & Paul Turner, *The Global Rise of a Duty to Disclose Information Security Breaches*, 22 J. MARSHALL J. COMPUTER & INFO. L. 457 (2004); Monica Vir, Note and Comment, *The Blame Game: Can Internet Service Providers Escape Liability for Semantic Attacks?*, 29 RUTGERS COMPUTER & TECH. L.J. 193 (2003); Erin Kenneally, *Duty and Liability for Negligent Internet Security*, ;LOGIN:, Dec. 2001, at 62; Sarah Faulkner, Comment, *Invasion of the Information Snatchers: Creating Liability for Corporations with Vulnerable Computer Networks*, 18 J. MARSHALL J. COMPUTER & INFO. L. 1019 (2000); David L. Gripman, Comment, *The Doors are Locked but the Thieves and Vandals are Still Getting In: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem*, 16 J. MARSHALL J. COMPUTER & INFO. L. 167 (1997); John Jay Fossett, *The Development of Negligence in Computer Law*, 14 N. KY. L. REV. 289 (1987).

14. Erin Kenneally, *The Byte Stops Here: Duty and Liability for Negligent Internet Security,* COMPUTER SECURITY J., vol. XVI 2000, at 1 [hereinafter Kenneally 2000]. There is a good indication that cases arising from insecure systems will hold an organization liable based on the liability of architects when buildings fail because of design defects, landlords for failing to "provide adequate security for criminal invasions against their tenants," and "medical causation claims by chemical exposure victims." *Id.* Although the issue of whether an organization could be held liable for a security breach has not been resolved. *See, e.g.,* Erin Kenneally, *Who's Liable for Insecure Networks?*, COMPUTER, June 2002, at 93; Kenneally 2000, *supra* note 14; Carl S. Kaplan, *Can Hacking Victims be Held Legally Liable?*, N.Y. TIMES, Aug. 24, 2001, *available at* http://www.nytimes.com/2001/08/24/technology/24CYBERLAW.html (last visited Feb. 24, 2005); Cheryl S. Massingale & A. Faye Borthick, *Risk Allocation for Computer System Security Breaches: Potential Liability for Providers of Computer Services*, 12 W. NEW ENG. L. REV. 167 (1990).

15. *See* LANCE ROSE, NETLAW: YOUR RIGHTS IN THE ONLINE WORLD 142 (1995).

16. The security drivers and security levels are designed to fulfill an organization's obligations under negligence theory. *See infra* Part III.

II. WHY SHOULD THE COMPUTER SYSTEM BE SECURED?

The goal of computer security is to maintain the confidentiality, integrity, availability, and accountability of the computer system and the information residing on the computer system.[17] The harder question is how much security is required to not only ensure these four items for an organization, but to ensure that liability is reduced for any lapses in the confidentiality, integrity, availability, or accountability of the computer system or information.[18]

The first issue is the legal standard that must be met to reduce the potential liability when there is a lapse in security. The legal standard is constantly in flux, but an understanding of the analysis behind the standard will allow both IT professionals and business managers to find a common ground for the needed security level of the organization. To calculate the legal standard, an organization must evaluate the types of risks that are associated with the information that is maintained on its computer system. Both IT professionals and business managers need to be aware of the different types of risk and work to reduce any legal exposure by working to ensure that the confidentiality, integrity, availability, and accountability of the computer system containing the information are not comprised.

A. *The Ever Changing Legal Requirements*

The question of how much security is required is related to the calculation of the probability of injury and the severity of the injury versus the burden of securing against the injury.[19] This calculation of injury versus burden is a utility type analysis.[20] For liability to be reduced, the burden of securing against the injury must not be less than the probability of injury multiplied by the severity of the injury.[21] The probability of injury is the likelihood that the

---

17. PFLEEGER, *supra* note 8, at 5; Butler W. Lampson, *Computer Security in the Real World*, COMPUTER, June 2004, at 37. "**Confidentiality** means that the assets of a computing system are accessible only by authorized parties. … **Integrity** means that assets are accessible only by authorized parties or only in authorized ways. … **Availability** means that assets are accessible to authorized parties." PFLEEGER, *supra* note 8, at 5. Accountability is "knowing who has had access to information or resources." Lampson, *supra* note 17, at 39.

18. The security of the computer system is also known as information security which is defined in the United States Code as:

> The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide--
> (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
> (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
> (C) availability, which means ensuring timely and reliable access to and use of information.

44 U.S.C. § 3542(b)(1) (2004). Section 3542(b)(1) gives definitions for integrity, confidentiality, and availability, but the loss of each is much simpler to define. "A loss of *confidentiality* is the unauthorized disclosure of information." STANDARDS FOR SECURITY CATEGORIZATION OF FEDERAL INFORMATION AND INFORMATION SYSTEMS, FIPS PUB 199, 2 (Nat'l Inst. of Standards and Tech. 2003). "A loss of *integrity* is the unauthorized modification or destruction of information." *Id.* "A loss of *availability* is the disruption of access to or use of information or an information system." *Id.*

19. United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947).

20. *See supra* Part I.

21. *Carroll Towing Co.*, 159 F.2d at 173. Stated "in algebraic terms: if the probability be called P; the injury, L; and the burden, B; liability depends upon whether B is less than L multiplied by P: i.e., whether B < PL." *Id.*

resulting injury will occur.[22] Since there is such a large number of reported attempted break-ins and the numbers are increasing, the likelihood that an organization will be hacked or at least attempted to be hacked into is high, although the exact probability depends on many organization-dependent factors.[23]

The next part of the calculation is the severity of the injury.[24] The severity of the injury is directly related to the type of information that an organization maintains on its computer system and the risk associated with maintaining that data. There are many types of risks associated with the different kinds of data on a computer system and the services provided by a computer system. Each of the risks has its own degree of danger associated with a loss or exposure.[25]

The last part of the calculation is the burden of securing against the injury.[26] Securing against the injury is "the burden of adequate precautions."[27] The necessary precautions is the part of the calculation that causes the disparity between what the IT professionals want to use to protect the computer system and what the business managers deem necessary to protect the computer system. Another dilemma with adequate precautions is that in the computer security field, the needed security precautions are always in flux. Thus, when utilizing the burden or utility analysis on the computer security level, an organization's legal requirements for protecting information is constantly changing.

B. *Types of Risks*

There are several types of information at risk including personal information, financial information, credit card information, healthcare information, and intellectual property. It is imperative that both IT professionals and business managers understand these types of risks and understand that "[p]ractical security balances the cost of protection and the risk of loss."[28] Thus, an organization should base its decisions on the level of protection based on the type of information that is stored on the computer system.

1. Personal Information

Personal information includes name, address, e-mail address, telephone number, social security number, and other types of information that can be used to identify a person.[29] Organizations should be aware that some states have legal requirements that organizations with

---

22. *Id.*
23. *See* CERT/CC Statistics, *supra* note 2.
24. *Carroll Towing Co.*, 159 F.2d at 173.
25. Some of the dangers include: 1) "Damage to information;" 2)"Disruption of information;" 3)"Theft of money;" 4)"Theft of information;" and 5)"Loss of privacy." Lampson, *supra* note 17, at 39.
26. *Carroll Towing Co.*, 159 F.2d at 173.
27. *Id.*
28. Lampson, *supra* note 17, at 38.
29. *See* CAL. CIV. CODE § 1798.80 (West 2005). Section 1798.80(e) defines personally information as:
"Personal information" means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information. *Id.*

personal information should protect the information by reasonable methods.[30] The disclosure of personal information maintained by an organization can also have other affects such as the mandatory disclosure of the security breach to the person(s) whose information was or could have been exposed during a security breach.[31] The importance of protecting personal information is paramount not only because of the negative publicity, but because of the increasing costs for consumers to recover from identity theft and the cost to businesses and financial institutions for the fraudulent charges attributed to identity theft.

One such security breach occurred when IKEA had to close "its online catalog order site … after a privacy breach made the personal information of tens of thousands of its customers available online."[32] The personal information included "names, addresses, phone numbers, and email addresses of customers who ordered IKEA catalogs."[33] Another security breach occurred when "Eli Lilly & Co. was fined and forced to enter into a 20-year consent decree with the FTC after it inadvertently exposed the e-mail addresses of hundreds of users of Prozac. The agreement with the FTC required broad changes to the firm's computer security practice."[34]

Although both the Eli Lilly & Co. and IKEA breaches seemingly stem from an inadvertent incorrect configuration of their computer systems that only disclosed basic contact information, other breaches do occur on systems that contain sensitive information such as social security numbers and birthdates. One break-in allowed a hacker "to view the names and social security numbers of 400" T-Mobile customers.[35] Another reported break-in occurred on a UC Berkeley computer "in which the hacker gained access to names, addresses, telephone numbers, social security numbers and birth dates of about 600,000" people.[36]

It is estimated that it costs an average of $500 in out-of-pocket expenses plus approximately 30 hours of time to handle the process of recovering from identity theft.[37] Thus, T-Mobile's break-in that compromised the personal information of 400 customers cost approximately $200,000 plus 12,000 hours of time if all of the 400 customers had to recover from identity theft.[38] The next level of break-in involves hundreds of thousands of people's

---

30. Section 1798.82(b) provides that "[a] business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." *Id.*

31. It should also be noted that since July 1, 2003, organizations doing business in California have to disclose any security breaches that affect private information of consumers in California to the consumers. § 1798.82. Although section 1798.82(f) gives the exception that personal information "does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records." *Id.* Thus, organizations do have some leeway when a security breach occurs regarding notification of the consumers.

32. Troy Wolverton, *IKEA Exposes Customer Information on Catalog Site*, CNET NEWS.COM, Sep. 6, 2000, *at* http://news.com.com/IKEA+exposes+customer+information+on+catalog+site/2100-1017_3-245372.html (last visited Feb. 24, 2005).

33. *Id.*

34. Jonathan Krim, *Firms Look to Limit Liability for Online Security Breaches*, WASH. POST, Mar. 5, 2004, at E01.

35. *Man Who Hacked into T-Mobile Pleads Guilty*, TechNewsWorld, Feb. 16, 2005, *at* http://www.technewsworld.com/story/40656.html (last visited Feb. 24, 2005) [hereinafter *T-Mobile Hacked*].

36. Susan B. Shor, *UC Berkeley Hack Not Unusual, Analyst Says*, TECHNEWSWORLD, Oct. 21, 2004, *at* http://www.technewsworld.com/story/37507.html (last visited Feb. 24, 2005).

37. Federal Trade Commission, *Identity Theft Survey Report*, Sept. 2003, at 7, *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf (last visited Mar. 4, 2005) [hereinafter *Identity Theft*].

38. *T-Mobile Hacked, supra* note 35.

personal information, which happened when the personal information of 600,000 people were obtained by a hacker from a UC Berkeley computer system.[39] If all of the 600,000 people had to recover from identity theft, then the cost of recovery would be approximately $300 million plus 18 million hours of time. Of course, not all of the personal information that is stolen leads to a person's identity being stolen, but the possibility of such a large amount of damages that could stem from a loss of personal information is substantial. In addition, a person whose personal information has been stolen has to remain on guard for the rest of his or her life to protect themselves from identity theft.[40] The cost to an individual for this lifelong vigilance is not easily calculated except for the definite loss of reputation to the organization that allowed the information to be stolen.

Another important reason for protecting personal information is the cost to businesses and financial institutions for the fraudulent charges related to identity theft. It is estimated that identity theft costs businesses and financial institutions $4,800 per identity theft victim.[41] For the T-Mobile break-in, the cost to businesses and financial institutions could be $1.9 million for the 400 victims,[42] while the UC Berkeley break-in cost to businesses and financial institutions could be $2.8 billion for the 600,000 victims.[43]

The large amounts for which an organization could be held liable could be devastating for an organization when placed in the burden analysis, especially if the organization did not take even the minimum precautions necessary to protect the information. Thus, if T-Mobile was held liable for the breach in its computer security, then its potential liability could extend to over $2 million while UC Berkeley's liability could extend to over $3 billion. These potentials for liability are dependent on the number of people whose identities are stolen from the personal information that was contained on the computer systems of the organizations, but the potential loss from 600,000 people attempting to recover damages would be daunting for any organization, especially if that organization could have provided adequate protection of the information.

2. Financial Information

Financial information includes both personal financial information for an individual and corporate financial information. In addition to the general types of damage that could occur from the release of private financial information, some financial information is also regulated by federal laws and regulations.[44] Protection of personal financial information by financial institutions is regulated by the Gramm-Leach-Bliley Act (GLBA) of 2001[45] while the protection of corporate financial information is regulated by the Sarbanes-Oxley Act of 2002.[46]

Under the GLBA, each "financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those

39. Shor, supra note 36.

40. *See ID Theft Victims Face Lifetime of Vigilance*, Feb. 24, 2005, *at* http://www.cnn.com/2005/TECH/02/24/choicepoint.victims.ap/ (last visited Mar. 4, 2005).

41. *Identity Theft*, supra note 37, at 7.

42. *T-Mobile Hacked, supra* note 35.

43. Shor, supra note 36.

44. This is only covering law and regulations in the United States and does not cover any foreign laws and regulations such as the European Data Protection Directive. *See, e.g.,* Preston & Turner, *supra* note 13.

45. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (2001).

46. Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (2002).

customers' nonpublic personal information."[47] In addition, federal agencies and regulators have to "establish appropriate standards for the financial institutions."[48] Under Sarbanes-Oxley, organizations have to establish and maintain "an adequate internal control structure and procedures for financial reporting."[49] Part of the challenge of having a proper internal control structure for finances is directly related to the challenge of maintaining information security.[50] Both of these acts put additional obligations on organizations to securely maintain financial information.

There are different types of security breaches that can occur regarding financial information. One type of break-in occurred in 1994 to Citibank when "a group of Russian hackers" stole $10 million by making illegal transfers.[51] Although Citibank eventually recovered $9.6 million of the stolen money, twenty of Citibank's top customers left citing poor computer security.[52] This type of break-in does not directly affect customer information but instead affects the long-term stability of the bank.

On a different side of computer security, a security breach that occurred because of human error happened in 2003 to Bank Rhode Island when "a laptop containing the names, addresses and social security numbers of about 43,000 customers was stolen from [the bank's] … principal data-processing provider."[53] Another more recent security breach happened in 2005 to Bank of America when "computer data tapes containing personal information on up to 1.2 million federal employees, including some members of the U.S. Senate" were lost.[54] "The lost data includes social security numbers and account information that could make customers of a federal government charge card program vulnerable to identity theft."[55] These breaches fall under the type of information that the GLBA is designed to protect. These types of breaches

---

47. 15 U.S.C. § 6801(a) (2005).

48. § 6801(b). The standards are:

> (1) to insure the security and confidentiality of customer records and information;
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. *Id.*

The federal agencies and authorities that have to establish the safeguards include Federal Trade Commission, the Board of Governors of the Federal Reserve System, the Board of Directors of the Federal Deposit Insurance Corporation, the Director of the Office of Thrift Supervision, the Securities and Exchange Commission, and the insurance authority of each state. § 6805(a).

49. 15 U.S.C. § 7262(a) (2005).

50. *See* EGAN & MATHER, *supra* note 9, at 19. Some of the challenges of a proper internal control structure include confidentiality, integrity, availability, and accountability which are the same challenges of any other computer security project. *See id.* In addition, "[s]ince the bulk of information in most companies is created, stored, transmitted and maintained electronically, one could logically conclude that IT shoulders a lion's share of the responsibility for Sarbanes-Oxley compliance." CipherTrust, *How Sarbanes-Oxley Affects Corporate Email Systems*, Oct. 21, 2004, *at* http://www.ciphertrust.com/resources/articles/articles/sox.php (last visited March 4, 2005).

51. Richard Behar et al., *Who's Reading your E-Mail? As the World Gets Networked, Spies, Rogue Employees, and Bored Teens are Invading Companies' Computers to Make Mischief, Steal Trade Secrets—Even Sabotage Careers*, FORTUNE, Feb. 3, 1997, at 56.

52. *Id.*

53. Lucas Mearian, *BankRI Customer Information Stolen Along with Laptop*, COMPUTERWORLD, Dec. 19, 2003, *at* http://www.computerworld.com/securitytopics/security/story/0,10801,88443,00.html (last visited Mar. 4, 2005).

54. *Bank of America Loses Customer Data*, MSNBC, Mar. 1, 2005, *at* http://www.msnbc.msn.com/id/7032779/ (last visited Mar. 4, 2005).

55. *Id.*

expose not only personal financial information to hackers, but also personal information to hackers. The personal information such as the Social Security numbers could be used for identity theft and the risk of such identity theft carries the same potential liability.[56]

The requirements on organizations to securely maintain information under the GLBA and Sarbanes-Oxley, the threat of negative publicity and lack of customer confidence in the organization, and the potential for the financial information about customers and the organization all contribute to the high level of risk involved with the maintenance of financial information. There are no estimates as to the potential liability risks involved with information that is protected under GLBA or Sarbanes-Oxley although there are potential criminal penalties involved with the failure to secure information required under Sarbanes-Oxley. It is also difficult to calculate the potential liability when other types of security breaches occur such as what happened to Citibank in 1994. Citibank was able to recover most of the stolen funds, but the damage to Citibank's reputation was not measurable. The potential liability for personal financial information can be calculated based on the potential identity theft that may occur.[57] Corporate financial information has many other potential pitfalls, because of the sensitive nature between competitors and the market.

Even though there is a lack of empirical data about the potential liability of most of the different types of financial information that may be stored on computer systems, all of the different types of financial information carry a significant risk to the maintainer of the information upon exposure. The risks vary from criminal penalties to money damages to the loss of customers. All of these risks are significant to the organization and should be utilized when calculating the potential liability for financial information stored on the organization's computer systems.

3. Credit and Debit Card Information

Credit and debit card information is unique from the other types of information that is at risk because the credit card companies have "zero-liability and other policies" that limit the loss of consumers. Credit and debit cards can also be replaced, since the card numbers are not permanently attached to an individual.[58] Over the years, there have been numerous reported incidents of credit card information thefts from organizations' computer systems. Some of these organizations include BJ's Wholesale Club[59] and Data Processors International.[60] The issue of securing credit card information is a major issue that should not be ignored by any organization - big or small.

One issue with the easy replacement of cards is that "[i]t generally costs banks $5 to $6 to replace … cards."[61] If the card issuers have to replace eight million cards,[62] someone is paying the $40 to $48 million for the new cards. So, the risk associated with credit and card information

---

56. *See supra* Part II.B.1.
57. *See supra* Part II.B.1.
58. *Hacker Breach Dents Confidence in Card Security*, ATM & DEBIT NEWS, Feb. 27, 2003, at 1.
59. Timothy C. Barmann, *Banks Cancel Debit Cards after BJ's Wholesale Club Warns of Theft*, PROVIDENCE JOURNAL, Mar. 16, 2004, *available at* 2004 WL 59429202.
60. *Hacker Breach Dents Confidence in Card Security*, *supra* note 58.
61. Barmann, *supra* note 59.
62. Eight million debit and credit car accounts where comprised by the Data Processors International security breach. *Hacker Breach Dents Confidence in Card Security*, *supra* note 58.

is not only the fraudulent use of the credit cards, but the cost of replacing all of the cards that were compromised.

The other major issue with credit card fraud is who ends up paying for all of the fraud. In some circumstances, the merchant ends up paying for the fraud while, in other circumstances, the bank issuing the card ends up paying.[63] An example of a merchant paying for the cost of fraud involves Expedia, which had to "record $4 to $6 million ... in third quarter losses to cover fraudulent credit card purchases made on its Web site" in 2000.[64] This cost is significant for the organizations that maintain credit card information on computer systems, because the use of stolen credit card information could cause widespread loss to merchants which could force the organization that did not maintain adequate security precautions on its computer systems to absorb the loss.

Overall, the cost of replacing credit and debit cards and the cost of the fraud to banks and merchants is significant. The cost for both the replacement of cards and the fraudulent charges can easily reach into the millions of dollars. While the banks and merchants currently cover most of these expenses, the burden could be shifted to any organization that allowed the loss of the card information. Thus, organizations that maintain credit card information should be aware of the risks involved with the exposure of the information and should work to minimize this risk, since the injury could cost millions of dollars.

4. Healthcare Information

Healthcare information has particular personal and financial value.[65] People have a significant interest in protecting their healthcare information to ensure that the information does not adversely affect their job, insurance rates, and other vital aspects of a person's life. A person's life could be negatively impacted if sensitive medical information was disclosed, such as the use of anti-depressants, anti-psychotic medication, or sleeping pills. There are many other medical treatments and conditions that could negatively impacted a person's life such as fertility treatments, attention deficit hyperactivity disorder, AIDS, cancer, STDs, sickle cell trait, pregnancy, drug rehabilitation, alcohol rehabilitation, and genetic markers that indicate potentially increased risk for diseases. These lists of medications, treatments, and conditions are just a few examples of some of the sensitive medical information that could be stored on an organization's computer system.

The disclosure of any of these medical issues could have widespread and long lasting affects on a person. If an organization does not take adequate precautions to protect healthcare information, then the organization runs the risk that the disclosure of the sensitive information could cause people to lose their jobs, have higher insurance rates, and personal distress. The injury upon disclosure of healthcare information is significant and should be calculated when determining the precautions that need to be taken to protect the information.

There are other issues surrounding the maintenance of healthcare information on an organization's computer systems. One issue is the regulation of the information by the Health

63. Randy Gainer, *A Cyberspace Perspective: Allocating the Risk of Loss for Bank Card Fraud on the Internet*, 15 J. MARSHALL J. COMPUTER & INFO. L. 39, 46 (1996).

64. Paul A. Greenberg, *Expedia Stung by Major Credit Card Fraud*, E-COMMERCE TIMES, March 2, 2000, *at* http://www.ecommercetimes.com/story/2638.html (last visited Mar. 4, 2005).

65. *See* Whalen v. Roe, 429 U.S. 589, 599 (1977).

Information Portability and Accountability Act (HIPAA) of 1996.[66] "To ensure the privacy and confidentiality of patient's medical records," HIPAA "institutes standards for the privacy of individually identifiable health information."[67] To protect the medical information, HIPAA provides for both civil and criminal punishments.[68] Thus, an organization not only has to be concerned with the negative affects to the person upon theft of any information, but also any consequences under HIPAA if the information is not protected.

5. Intellectual Property

There are several different forms of intellectual property that are at risk. These different forms include pending patent applications, trade secrets, copyrighted material, and other types of confidential materials maintained by organizations. "[I]n the corporate world where intellectual property is often the only thing separating competitors, it is cheaper and easier to steal information than to develop it."[69] It is important for all types of organizations to protect their intellectual property because the disclosure of an organization's intellectual property will give the competitors a significant advantage.

A major dilemma for many software companies occurs when their source code is stolen. In 2004, the source code that controls many of Cisco's routers and switches was stolen.[70] This theft is troubling for other organizations because Cisco has been buying "smaller firms that specialize in network security software."[71] So, if Cisco is unable to protect its intellectual property from computer security breaches, then other organizations will have to put in extra effort to protect their intellectual property. Another major problem for software companies is the illegal copying of the software. In some cases, groups "would obtain advance copies of computer programs not yet commercially available and circumvent the copyright protections embedded in the software."[72] The theft of source code and the theft of software programs that have not even been released are major risks for software companies.

Other industries also have to worry about the theft of intellectual property. Although some of the theft comes from published patents or from reverse engineering, some of the theft occurs from hackers breaking into organization's computer systems to steal intellectual property. The pharmaceutical industry worries about the theft of drug research while other industries such as the soft drink industry are concerned with the disclosure of its trade secrets. Considering that the estimated cost of research for a new drug is $450-$700 million, the risk of exposure to pharmaceutical companies is extreme.[73] Considering that the Coca-Cola Company had over $21 billion in revenue in 2004, the protection of its formulas as trade secrets is imperative for the

---

66. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

67. EGAN & MATHER, *supra* note 9, at 18.

68. *See* 42 U.S.C. § 1320d-5 (2005); 42 U.S.C. § 1320d-6.

69. Kennealy 2001, *supra* note 13, at 64.

70. Jay Lyman, *UK Suspect Arrested in Cisco Source Code Theft*, TECHNEWSWORLD, Sept. 20, 2004, *at* http://www.technewsworld.com/story/36787.html (last visited Mar. 4, 2005).

71. Keith Regan, *Cisco Probes Potential Source Code Leak*, E-COMMERCE TIMES, May 17, 2004, *at* http://www.technewsworld.com/story/33827.html (last visited Mar. 4, 2005).

72. U.S. Department of Justice, *Warwick Man is Sentenced for Software Privacy*, Apr. 23, 2004, *available at* http://www.usdoj.gov/criminal/cybercrime/russoSent.htm (last visited Mar. 5, 2005).

73. Network Science Corporation, *Drug Development: The Short Story*, *at* http://www.netsci.org/scgi-bin/Courseware/projector.pl?Course_num=course1&Filename=slide07.html (last visited Mar. 5, 2005).

company.[74] The pharmaceutical industry and soft drink industry are just a few of the many types of industries that should be careful about exposing their secrets.

The exposure of an organization's intellectual property can have significant risks to the organization. Technology, pharmaceutical, and soft drink organizations are just a few of the types of organizations that can be injured by the theft of intellectual property. The theft can range from salary information to designs for new products to cutting edge research. Basically, any type of sensitive information that an organization could store on a computer system could be stolen. The theft of intellectual property is a risk that organizations should minimize, because although there is not empirical evidence for intellectual property losses, the loss could range from negative publicity to the loss of a competitive edge to the loss of millions of dollars of research.

III. Lowering Legal Exposure by Analyzing Security Needs

The ability to lower the legal exposure of an organization can be accomplished by analyzing the security needs of the organization and protecting the information according to the individualized needs of the organization. The first part of the analysis is the determination of the security drivers of the organization. These security drivers are directly tied to the risks of the information that is maintained on the organization's computer systems. The next step is to determine the security level that the organization needs to maintain to provide adequate protection for the information. It is imperative that IT professionals and business managers understand the limitations of both the security drivers and the selection of a security level for an organization.

A. *Security Drivers*

One challenging aspect to the proper utilization of computer security is the selection of the correct security drivers. The security drivers are the risks associated with the information maintained on the organization's computer system. Both the IT professionals and the business managers should understand these security drivers; so that a proper determination of the needed security level for an organization can be determined that fits the individualized needs of the organization. The list of security drivers is not exclusive, but should be a starting place for the two sides when determining the computer security needed to reduce an organization's exposure to legal liability.

These security drivers are designed for the type of information that is maintained on an organization's computer systems and the methods of accessing the information. The security drivers do not cover the technical aspects of an organization's computer system, because the adequate precautions that are necessary to protect information that is at risk is not dependent on the technology that an organization has chosen to use, but is dependent on the risks involved with the injury that the information could cause if stolen.

The IT professionals and business managers should utilize the security drivers in Table 1 to choose the proper security level for an organization. There are many other drivers that either party may add based on the individualized needs of the organization. There are other types of

74. The Coca-Cola Company, *U.S. Securities and Exchange Commission Form 10-K*, Commission File No. 1-2217, at 4, *available at* http://www2.coca-cola.com/investors/pdfs/form_10K_2004.pdf (last visited Mar. 5, 2005).

information that has a large potential for injury and can be added to an organization's security driver list for consideration when determining the proper security level for the organization.

Table 1 - Security drivers[75]

Security Drivers	Risks
Sensitivity of Information	
Personal Information	The maintenance of personal information carries varying amounts of risk to the organization depending on the amount of information stored. A small amount of information has a minimal risk of injury while large amounts of information carry a high risk of injury.
Financial Information	The maintenance of financial information carries a high risk of injury regardless of the amount, because of the regulations that control the disclosure and control of financial information. In addition, the theft and exposure of financial information can cause organizations to lose customers.
Credit and Debit Card Information	The maintenance of credit card information has a lower risk of injury than other types of personal or financial information, since the credit and debit cards can be re-issued unlike other personal information. The risk can become significant when a large number of card information is maintained on the computer system, because of the cost of card replacement and fraud.
Healthcare Information	The maintenance of healthcare information has a high risk, because of potential injury that can occur to patients and the requirements under HIPAA for protecting the information.
Intellectual Property	The maintenance of intellectual property has a low to high risk depending on the nature of the information stored on the computer system. Some types of intellectual property have a low risk, because the injury upon theft is low while other types of intellectual property could devastate an organization.
Amount of Information	The more information that is maintained in general, the more injury that can occur. If the computer system only has the personal information for 100 people, then the injury is small compared to the injury that could occur from the theft of personal information for 600,000 people.
Information Access	
Internet	The risk of injury to any type of information is high when the information is accessed via the Internet, because of the 24/7 nature of the Internet.
Modem	The risk of injury to any type of information is nominal when the information is accessed via dial-up, because the IT professionals will be able to provide more security protections than via Internet access.
Wireless	The risk of injury to any type of information is high when the information is accessed via a wireless network, because of the inherent weak security in most wireless products. Note: the security drivers are designed to be independent of specific technology, but since wireless is becoming a method of access to large amounts of data, it is important to categorize the risk of this type of access.

75. *See, e.g., supra* Part II.B; EGAN & MATHER, *supra* note 9.

Intranet	The risk of injury to any type of information is moderate when the information is accessed via an organization's Intranet, because the risk of theft from internal users is significant.[76]
Users	
Internal	The risk of injury to any type of information is moderate when the information is only accessed by an organization's internal users, because of risk of theft from internal users is significant.[77]
Public	The risk of injury to any type of information is high when the information is accessed by the public, because public access means that the information could be disclosed inadvertently to the public or since the information is accessible to the public, the information could be hacked by any member of the public.
Type of System	
Business	The risk of injury for a business system varies according to the specific uses of the system.
Infrastructure	The risk of injury for an infrastructure system is high, because the system is part of the infrastructure.
Endanger Life	The risk of injury for a computer system that affects a life function is extremely high.
Endanger Environment	The risk of injury for a computer system that affects the environment is high.

B. *Security Level*

The classification of the computer security needed for an organization into a security level is a difficult task since every organization has slightly different requirements. Every organization has different requirements because "[s]ecurity doesn't exist in products and verbiage alone; it requires a process, people, policies, education, and technologies working together."[78] While bridging the gap between IT professionals and business managers, both sides should understand that "[s]tronger defenses will imply higher costs, and … [both sides] have to consider tradeoffs between security and costs, where costs could include possible functional limitations to the system."[79] But regardless of the potential cost, an analysis between the potential injury involved with the information maintained on the computer system and the burden for securing the computer system needs to be performed to determine the precautions that should be taken to protect the information.

---

76. *See* CSO Magazine, *2004 E-Crime Watch Survey: Summary of Findings*, at 14, *at* http://www.cert.org/archive/pdf/2004eCrimeWatchSummary.pdf (last visited Feb. 24, 2005) [hereinafter *2004 E-Crime*].

77. *See id.*

78. Robert K. Weiler, *Decision Support: You Can't Outsource Liability for Security*, INFORMATION WEEK, Aug. 26, 2002, *available at* http://www.informationweek.com/story/showArticle.jhtml?articleID=6502997 (last visited Feb. 22, 2005).

79. Moitra & Konda, *supra* note 10, at 2.

While analyzing the security drivers to determine the security level for an organization, the organization needs to address the issue that "[y]ou cannot protect everything equally."[80] It is important to understand that the computer system in an organization needs to be protected at a security level that is customized according to the security drivers that apply to the organization. When different types of information are maintained on a computer system, the different types can be protected according to the individualized risks of the information.

The security level for an organization has three major parts. These three parts are specification, implementation, and assurance.[81] The security level needs these three major parts along with the sub-parts because security cannot be accomplished by "products and verbiage alone."[82] Some business managers are under the false impression that the organization can buy a few security products and the computer system will be secure.[83] One problem with relying on a product to solve an organization's security issues is that "[e]ven a very moderately resourced attacker can break anything that's at all large and complex. There is nothing that can be done to stop this, so long as there are enough different security vulnerabilities to do statistics: different testers find different bugs."[84] Thus, relying on software alone will not solve the security issues of a computer system.[85]

Based on the security drivers, the IT professionals and business managers can reach a compromise on the security level required for an organization. The first step in determining the security level is to review the available security options. The next step is to determine how many and which options are worth the burden for the protection of the information. The determination should take sub-parts from each of the three major parts-specification, implementation, and assurance. Through the use of these three major parts, an organization will be more prepared to protect the information stored on its computer system.[86]

The different parts of a security level should combine to form both a holistic approach and defense-in-depth approach to computer security. The combination of specification, implementation, and assurance gives the security a holistic approach while the sub-parts of the specification, implementation, and assurance parts give the security the defense-in-depth aspect.

---

80. Julia Allen et al*., Improving the Security of Networked Systems*, CROSSTALK, Oct. 2000, *available at* http://www.stsc.hill.af.mil/crosstalk/2000/10/allen.html (last visited Feb. 17, 2005).

81. Lampson, *supra* note 17, at 38.

82. Weiler, *supra* note 78.

83. *See* David Geer, *Just How Secure are Security Products?*, COMPUTER, June 2004, at 14.

84. Ross Anderson, *Why Information Security is Hard: An Economic Perspective*, 2001 PROC. OF THE 17TH ANN. COMPUTER SECURITY APPLICATIONS CONF. 358, 362.

85. Although some business personal advocate putting the responsibility of computer system security breaches on the software companies that produced the software since the software had bugs. There are numerous theories of liability that are put forth for why software companies should be liable when their software products fail, but most software companies have been avoiding liability by the use of some form of liability waiver. *See, e.g.,* Daniel J. Ryan, *Two Views on Security Software Liability: Let the Legal System Decide*, IEEE SECURITY & PRIVACY, Jan./Feb. 2003, at 70; Carey Heckman, *Two Views on Security Software Liability: Using the Right Legal Tools*, IEEE SECURITY & PRIVACY, Jan./Feb. 2003, at 73; Nancy R. Mead, *International Liability Issues for Software Quality*, CMU/SEI-2003-SR-001, July 2003, *available at* http://www.cert.org/archive/pdf/03sr001.pdf (last visited Feb. 23, 2005); Kevin R. Pinkney, *Putting Blame Where Blame is due: Software Manufacturer and Customer Liability for Secuirty-Related Software Failure*, 13 ALB. L.J. SCI. & TECH. 43 (2002); Nancy J. Wahl, *Responsibility for Unreliable Software*, 1994 PROC. OF THE CONF. ON ETHICS IN THE COMPUTER AGE 175.

86. This article gives an overview of the sub-parts of the three major parts, but the details of the sub-parts are beyond the scope of this article. There are numerous other books and articles that go into detail about these sub-parts. *See infra* notes 87, 97, and 101.

Overall, the use of the different parts of the security level dependent on the needs of the organization will provide the appropriate security level for the organization.

1. Specification

The specification includes policies, standards, procedures, and guidelines.[87] "A policy … is a high-level statement of enterprise beliefs, goals, and objectives and the general means for their attainment for a specified subject area."[88] "Standards are mandatory requirements that support individual policies."[89] "Procedures are mandatory, step-by-step, detailed actions required to successfully complete a task."[90] "Guidelines are more general statements designed to achieve the policy's objectives but by providing a framework within which to implement procedures."[91] Depending on the risks to the organization, the use of the different types of specifications allow for the organization to better manage the security risks.

Proper policies are important in the implementation of computer security because without any policies, "the organization may be in greater danger of a breach of security, loss of competitive advantage, loss in customer confidence, or an increase in government interference. By implementing policies, the organization takes control of its destiny."[92] An information security policy is a short, non-technical document designed for the entire organization, while the IT security policy refers to broad technical decisions for the organization, but does not give technical details.[93] "The goal of an information security policy is to maintain the integrity, confidentiality, and availability of information resources."[94] Another type of policy that can be utilized is an inappropriate use policy which outlines the acceptable and unacceptable uses of an organization's computer system. There are numerous other types of polices that can be utilized to provide the proper level of protection for the information maintained on the organization's computer system and based on the security drivers, more research into the different types of policies may be necessary.[95]

"Standards define what is to be accomplished in specific terms."[96] Standards are important because they give guidance as to what is required and expected for the security environment. There are many types of standards that can be customized according to the individual needs of an organization. The standards include those developed by the National

---

87. *See, e.g.*, STEVE PURSER, A PRACTICAL GUIDE TO MANAGING INFORMATION SECURITY (2004); ERIC GREENBERG, MISSION-CRITICAL SECURITY PLANNER: WHEN HACKERS WON'T TAKE NO FOR AN ANSWER (2003); MAXIMUM SECURITY (3rd ed. 2001); THOMAS R. PELTIER, INFORMATION SECURITY POLICIES AND PROCEDURES: A PRACTITIONER'S REFERENCE (2nd ed. 2004); JOSEPH G. BOYCE & DAN W. JENNINGS, INFORMATION ASSURANCE: MANAGING ORGANIZATIONAL IT SECURITY RISKS (2002); *2004 E-Crime, supra* note 76, at 19-32.; JOHN CHIRILLO, HACK ATTACKS DENIED: A COMPLETE GUIDE TO NETWORK LOCKDOWN (2001); JAE K. SHIM ET AL., THE INTERNATIONAL HANDBOOK OF COMPUTER SECURITY (2000); National Institute of Standards and Technology, *An Introduction of Computer Security: The NIST Handbook* (1995), *at* http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf (last visited Mar. 4, 2005).

88. PELTIER, *supra* note 87, at 49.

89. *Id.*

90. *Id.*

91. *Id.*

92. *Id*. at 47.

93. PURSER, *supra* note 87, at 136-37.

94. PELTIER, *supra* note 87, at 47.

95. *See id.*

96. *Id.* at 114.

Institute of Standards and Technology, HIPAA requirements, and GLBA requirements. The standard used depends on the needs of the organization. Overall, the use of standards enables an organization to have a minimal base from which the entire organization can build the level of security that is required. Procedures and guidelines are important to an organization because they allow an organization to customize the needs and details of day-to-day operations to ensure that the level of security needed is met.

Overall, the use of policies, standards, procedures, and guidelines enables an organization to put into writing what needs to be protected and how the organization is going to protect that information. An organization should be aware that these specification documents are not static, but living documents that should be updated on a schedule to ensure that the documents support the current needs of the organization.

2. Implementation

Implementation includes desktop and server protection, network protection, training, data protection, and physical protection.[97] There are many parts to these categories for the proper implementation of an effective security level for an organization. When most business managers think about computer security, they think about the visible aspects of the implementation of computer security, but there are many hidden aspects of the implementation of computer security.

Desktop and server security has many integral parts including anti-virus, anti-spyware, patch management, authentication (including two-factor using biometrics, smart cards), security scanner, integrity-checking programs, role-based access control, and an intrusion detection system. Network security has many integral parts that have to work in unison to protect the network. These parts include firewalls (packet-filter, stateful inspection, and application gateway), virtual private networks, anti-virus scanning, content filtering, intrusion detection system, security scanners, and a system watcher. There are other parts to both desktop and server security and network security depending on the needs of the organization, but the listed parts are some of the more common. Although depending on the potential injury if the information is released, an organization should be aware of other types of security.

Training is important because "real-world systems are more than just technology, and if we want to secure them, we also must consider their nontechnological aspects."[98] User training is imperative not only for the use of the security mechanisms that protect the computer system, but also to prevent social engineering. One type of social engineering that has become widespread is phishing.[99] User training includes education and awareness programs and new employee security training. Another important aspect of training is training for IT professionals. The field of computer security is constantly changing and to ensure that an organization's computer system is properly protected, the IT professionals securing the computer system have to be properly trained (via conferences, training, and other educational materials).

---

97. *See, e.g.,* PURSER, *supra* note 87; JULIA H. ALLEN, THE CERT GUIDE TO SYSTEM AND NETWORK SECURITY PRACTICES (2001); MAXIMUM SECURITY, *supra* note 87; BOYCE & JENNINGS, *supra* note 87; SHIM ET AL., *supra* note 87; Anderson, supra note 84; *2004 E-Crime*, *supra* note 76.

98. S.W. Smith, *A Funny Thing Happened on the Way to the Marketplace*, IEEE SECURITY & PRIVACY, Nov./Dec. 2003, at 74.

99. Phishing is the use of "spam to direct their victims to Web sites designed by thieves to resemble legitimate e-commerce sites." Michele Delio, *IT Tackles Phishing*, INFOWORLD, Jan. 24, 2005, at 31.

Data protection includes encryption and electronic signatures. Encryption addresses the issue of confidentiality and electronic signatures address the use of authenticity and data integrity.[100] Other types of data protection include access controls on confidential data, encryption of critical data in transit, and encryption of critical data in storage. Physical protection includes electronic access control systems, badging systems, closed caption television, biometrics, and emission security.

Overall, the use of desktop and server protection, network protection, training, data protection, and physical protection helps an organization control the risk of injury from the theft of information maintained on its computer system. Not every type of security implementation is listed, because of the ever changing field of computer security.

3. Assurance

Assurance includes monitoring and auditing.[101] Monitoring includes employee monitoring, monitoring Internet connections, wireless monitoring, keystroke monitoring, intrusion detection system (monitored by humans and/or automated systems with built in alarms), and log management tools. Auditing includes storage and review of voice mail, employee/contractor background examinations, periodic risk assessments, transaction trial auditing, mandatory internal reporting of insider misuse/abuse, internal auditor, external auditor, regular security audits, periodic systems penetration testing, storage and review of computer files, storage and review of e-mail, use of "white hat" hackers, and polygraph examinations. The use of monitoring and auditing to protect the information stored on an organization's computer system provides part of the overall protection for the information.

C. *How will the analysis help computer security?*

The IT professional who is trying to figure out how to get the business manager to understand to what precautions are required to secure the computer system will benefit from this utility or burden analysis of the computer security issue.[102] The utility analysis is important because every organization is different, and the information that needs to be protected is different.

It is imperative that an organization perform this analysis and not rely solely on industry standards because "there are precautions so imperative that even their universal disregard will not excuse their omission."[103] "[I]ndustry standards are merely a minimal standard that may be considered" when determining liability and compliance with standards will not be the only factor in determining whether an organization is liable.[104] In addition, an organization should not rely

---

100. Emily M. Weitzenboeck, *Enterprise Security: Legal Challenges and Possible Solutions*, 2001 PROC. OF THE 10TH INT'L WORKSHOPS ON ENABLING TECHNOLOGIES: INFRASTRUCTURE FOR COLLABORATIVE ENTERPRISES 183, 185.

101. *See, e.g.,* PURSER, *supra* note 87; BOYCE & JENNINGS, *supra* note 87; SHIM ET AL., *supra* note 87; *2004 E-Crime*, *supra* note 76.

102. *See supra* Part II.A.

103. T.J. Hooper v. Northern Barge Corp., 60 F.2d 737, 740 (2d Cir. 1932).

104. Zacher v. Budd Co., 396 N.W.2d 122, 133 (S.D. 1986). Additionally, "[i]n determining whether conduct is negligent, the customs of the community, or of others under like circumstances, are factors to be taken into account, but are not controlling where a reasonable man would not follow them." RESTATEMENT (SECOND) OF TORTS § 295A.

on legislative enactments or administrative regulations as its only indication of the level of security required for its computer system.[105] Analyzing an organization's individual security needs and implementing those needs reduces the organization's potential liability by not relying on industry standards or regulations as the minimal level of computer security.

This individualized analysis also helps to reduce an organization's potential liability by embedding the research and education of new security tools into the security levels. Organizations cannot ignore new security tools simply because other organizations are not using the security tools, but must weigh the benefit of the security tool against the need for protection.[106] An analysis is designed to look at the individual characteristics of an organization and perform the burden analysis based on these characteristics to determine how active an organization needs to be in evaluating new security tools to determine if the tool is worth the burden of use to reduce the probability that the computer system will be hacked into.

Thus, this analysis of the risks to an organization will help provide a solution to reduce an organization's potential liability by individualizing the security level that the organization needs to maintain not based on an industry standard or regulation, but based on the individualized needs of the organization. These individualized needs are directly related to the type of information that the organization maintains and the probability that the information could be accessed by third parties versus the burden on the organization to secure the data. An IT professional can thus utilize this analysis to show the business managers of an organization the potential liability that may result by not providing adequate precautions for the security of the computer system.

IV. CONCLUSION

By analyzing the individual needs of an organization, the organization will be able to fulfill its duties and obligations to its customers and others that use or could be affected by the organization's computer system. Computer systems "have become such an integral part of America government and business that computer-related risks cannot be separated from national defense, general safety, health, business, and privacy risks."[107] Thus, organizations have a duty to ensure that the information maintained on its computer system is adequately protected.

An individualized analysis will help solve the legal problems by "[b]eing proactive about security [which] is critical to mitigating your security risk."[108] An organization that follows as many of the standards and guidelines about computer security[109] and takes the extra steps to calculate its computer security approach and customize the approach according to the specific needs of the organization will have taken the steps to adequately protect the information it

---

105. "Compliance with a legislative enactment or administrative regulation does not prevent a finding of negligence where a reasonable man would take additional precaution." RESTATEMENT (SECOND) OF TORTS § 288C. *See Zacher*, 396 N.W.2d at 133 (quoting Turner v. American General Corp., 392 A.2d 1005, 1007 (D.C. 1978)).

106. *See* ROSE, supra note 15, at 148. "This does not mean that the system operator should become a leader in testing out every possible new security tool. New tools of any kind are often unreliable or ineffective, and the system operator could actually decrease security if he or she implements new, unproven tools too quickly." *Id.*

107. Richard D. Pethia, Testimony before the House Committee on Government Reform, Subcommittee on Government Efficiency, Nov. 19, 2000, *available at* http://www.cert.org/congressional_testimony/pethia-11-02/Pethia_testimony_11-19-02.html (last visited Feb. 24, 2005).

108. West-Brown, *supra* note 5.

109. Organizations should be aware that blindly following standards developed by the industry will not protect a company from liability. *See Zacher*, 396 N.W.2d at 122.

maintains. The individualized computer security approach is of course only the first step in the process. The organization also has to implement the security plan and monitor the implementation. This holistic approach to computer security may help the organization escape liability and better yet, may decrease the number of computer security break-ins.

Even if the utilization of these measures protects the organization from legal liability, business managers should understand that "having good security measures in place will not prevent" the organization "from suffering computer security incidents."[110] Thus, the risks of maintaining information never completely disappears, but the legal liability may be reduced by using the methods described in this article.

110. West-Brown, *supra* note 5. "It is probably futile to hope for an *absolute* security for any network system." Moitra & Konda, *supra* note 10, at 1.