# INFORMATION SECURITY: AN ORGANIZATIONAL VIEW

**Sven Aelterman, Principal Consultant, Adduxis**

***ABSTRACT***

*This paper presents a model that can be used to assess information security at different levels in order to draw attention to the limited scope of information security in today's businesses. Most business and technology professionals restrict their approach to information security to technological means. Yet, many successful attacks use non-technological means to gain access to privileged information. Next, in order to present arguments for taking a broad view of information security, the legal environment is briefly reviewed. Finally, recommendations are made that will allow organizations to start implementing organizational information security programs based on the newly developed model.*

## INFORMATION SECURITY: THE COMMON VIEW

In 1990, Niederman, Brancheau & Wetherbe surveyed senior Information Systems (IS) executives to determine the key issues related to IS management that organizations would face in the 1990s. "Improving information security and control" ranked 19th, slightly more important than "Establishing effective disaster recovery capabilities." (Niederman, Brancheau & Wetherbe, 1990)

Information security has gained an increased level of attention since that research. Faults in software leading to disclosure of information at major companies have shown that no organization is safe from intruders. In addition to highly publicized cases, recent government regulation (including Sarbanes-Oxley, HIPAA[1] and California Senate Bill 1386) has also drawn attention to the importance of information security in the 21st century.

While this increased attention to information security is a positive trend, most technology and business professionals take a narrow approach when considering potential threats to the security of the information that is present in the organization. Most only consider the technological aspect of the puzzle. This is evidenced by two popular models of information security. One was developed by Microsoft (Figure 1) and another one by SPI Dynamics, a security research and consulting firm.

[1] Health Insurance Portability and Accountability Act of 1996. For more information, see Rouse & Liu (2004) and Rouse, Aelterman & Astone (2003).

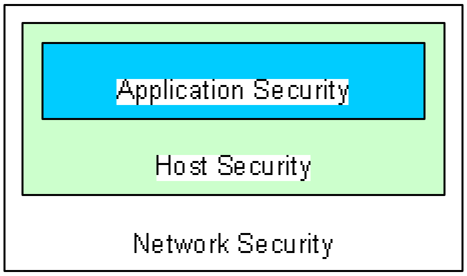

**Figure 1: Microsoft's security model**

Both models present three tiers of technology architecture where the technology infrastructure of an organization can be vulnerable to attack. These models are indeed valuable when it comes to understanding the risks that exist related to technology. Unfortunately, they present a narrow, technological picture. Vulnerabilities can also exist within the organization, in its policies, procedures, physical access security, and culture. This was illustrated especially well in the case study presented by Winkler and Dealy (1995). The case presents aggregated results of hackers attempting to gain unrestricted access to the information resources of financial institutions, using only non-technological methods. The test proved extremely successful and shows how vulnerable even financial institutions are.

The attempts were successful because the organizations were not prepared to deal with "social engineering." Infamous hacker Kevin Mitnick describes the social engineering process as trying "to make an emotional connection with the person on the [inside] to create a sense of trust […] and then exploiting it." (Lemos, 2000) Examples and possible countermeasures are presented in the Recommendations section of the paper. It is also important to note that according to the 2004 CSI/FBI Computer Crime and Security Survey 52% of respondents indicated that at least one attack originated inside the organization (Gordon, Loeb, Lucyshyn & Richardson, 2004). According to the 2004 E-Crime Watch survey (conducted by the United States Secret Service, CSO magazine and CERT), on average 28.6% of e-crimes or intrusions were caused by insiders (). (The differences in numbers are caused by differences in interpretations and statistical methods used.) It is easier for insiders to use social engineering, because they are more familiar with the inner workings of the organization.

While social engineering is not a new threat (it was, among others, heavily discussed by Winkler & Dealy (1995)), Mitnick experienced that no attention at all was paid to such security issues at the most attended security conference worldwide (Mitnick, 2001).

## THE ORGANIZATIONAL VIEW

In order to help organizations assess where vulnerabilities related to information security may exist, the following model is proposed. It builds on the previously presented Microsoft model and adds two tiers.

The first tier that was added to the model is the **Physical tier**. The Physical tier of information security is related to controlling physical access to the assets that hold the information. These assets can include file cabinets, archives, and server computers and storage devices. A thorough evaluation of the issues related to physical (or access) security is beyond the scope of this paper. For more information about physical security related to information systems, please see Blaze (2004) and Pagoria (2004).

The tier of interest in this paper is the **Organizational tier**. The model shows the organizational tier as all-encompassing. If the organization (to include policies, procedures, and culture) is vulnerable at this level, all other levels are affected.

While the inner three tiers of the model (Network, Host, and Application) are the domain of the organization's IT professionals (whether in-house or contractors), the responsibility of creating and enforcing organizational and physical security lies with all members of the organization. Inclusion of all members of the organization is an integral part of the model.

Finally, the model has added a "column" that runs through all layers named "Relationships Security." As used in this model, relationships security is the aspects of security related to doing business with partners, customers and suppliers (especially electronically, but certainly not limited to only e-business). The reason for this is that even if the organization has implemented all necessary precautions, business partners may not have. Information could still be disclosed or compromised through those third parties. The organization should take an active interest in the security efforts that are made by those third parties (customers, suppliers and partners). Seven percent of respondents to the 2004 E-Crime Watch survey indicated to have caused "Critical system disruption affecting customers & business partners" as a result of "insider network, data, or system intrusion."

The relationships security aspect has been added as a column through all five layers of the model because (a) third parties will have legitimate access to the organization's physical assets, network, computer equipment, and applications and (b) the organization should consult with third parties about their security initiatives that apply to all five layers.

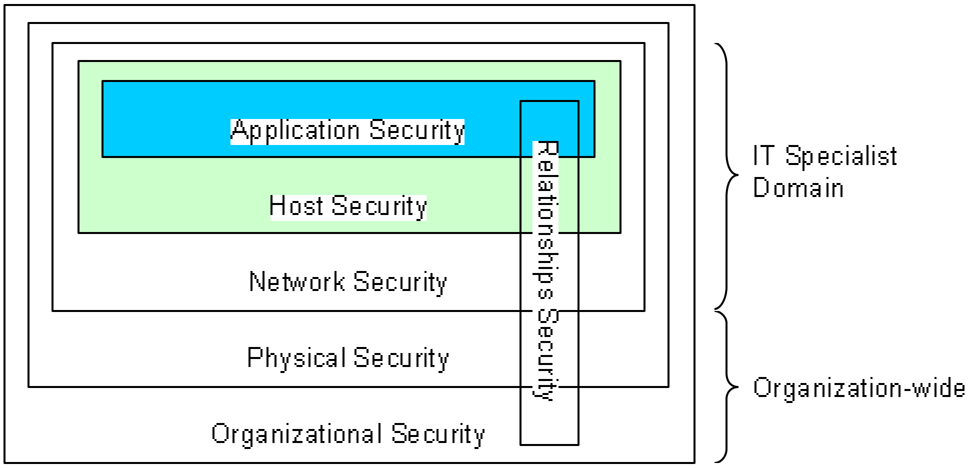

**Figure 2: Conceptual organizational view of information security.**

The modified model present above is not unlike the defense-in-depth conceptual model as illustrated by Microsoft. The model is shown below (Figure 3). It includes policies and procedures in its first layer and then physical security in its second layer. The remaining layers of the model are based on the OSI reference model for networking (Microsoft, 2003). Unfortunately, Microsoft fails to address any policies, procedures or physical security aspects.

Because the enhanced model presented in this paper (Figure 2) adds layers, it may be perceived as more elaborate and complex. If it is, there must be a greater return from using this model than using a merely technical model of information security.

This return comes from several factors. Today, the most important factor may very well be the legal environment. The previously mentioned laws include sections that deal specifically with information security. While a full overview of the information security legislation is outside the scope of this paper, it is interesting to briefly evaluate some of the ideas behind the legislation and the potential impact it may have on organizations.

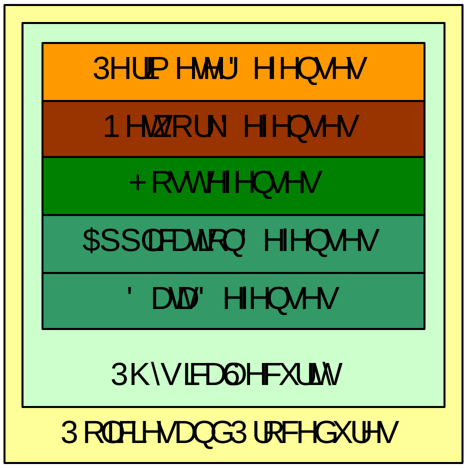

**Figure 3: Defense-in-dept conceptual model. Adapted from Microsoft (2003).**

## OVERVIEW OF THE LEGAL ENVIRONMENT

### Legislation

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) specifically includes administrative (akin to what is called organizational security in this paper) and physical security, as well as technological safeguards. Because of HIPAA, the healthcare industry has done the most to comply with regulations (Scalet, 2004). Compliance with HIPAA is enforced by the Department of Health and Human Services (HHS). Because it is not clear how the HHS will enforce many of the provisions in the Act yet, it is not possible to estimate the potential consequences of non-compliance. At this time, no fines have been levied.

The Gramm-Leach-Bliley Act of 1999 (GLBA) was enacted to ensure that financial institutions keep customer's confidential information secure. Financial institutions span a broad range of organizations: banks, insurance underwriters, but also universities if they offer, or are involved in providing, student loans. A section of the GLBA requires these organizations to have programs and policies in place to ensure the confidentiality of the information provided to them by customers.

The Sarbanes-Oxley Act specifically requires the documenting and auditing of security policies, which includes physical security, organizational information security, and technological security (Williams, 2003 and Stults, 2004). The Act is not specific in which "controls" are covered and should be audited. While the Act was specifically designed to ensure that financial statements of publicly traded organizations are accurate and reliable, the effects also impact the way these organizations store and access any data and information related to the creation and auditing of financial statements.

California Senate Bill 1386, also known as the Security Breach Notification Act, requires companies whose information systems have been compromised to notify their customers if certain data was lost. Requiring notification will allow consumers to be watchful for potential consequences of the information disclosure. It will however subject the organization to public scrutiny and the inevitable negative publicity associated with it. It is noteworthy that while the law already applies to any business interacting with California residents, federal legislation in the same vein has been proposed (Roberts, 2003).

Another California law, the California Online Privacy Protection Act of 2003, requires web site operators whose sites can interact with California residents to have clearly posted privacy policies. In addition, liability is imposed for both negligent and intentional violation of these policies. (Wolf, 2004) The success of an Internet-based attack against the organization's data stores can lead to liability claims if the organization did not take the necessary precautions.

## Enforcement

Many agencies are responsible for enforcing these laws, but the Federal Trade Commission (FTC) appears to be most involved. The FTC is involved because most online retailers and other organizations involved in e-commerce post statements on their sites stating that the information visitors provide will be kept secure. If breaches occur because common security practices are not in place, the FTC can determine that the organization does not employ reasonable caution when handling consumers' data (negligence) (Shenk, 2004).

A prime example occurred in late 2003, when Victoria's Secret agreed to pay a $50,000 fine and compensate online shoppers for information that was [inadvertently] disclosed on its website. But fines or restitution resulting from breaches of information security and the personal information that was exposed because of them can be more severe.

Not only can the monetary consequences be severe, so can the impact on the organization's reputation and future performance. In 2002, the FTC announced a settlement with Microsoft over its Passport service (used to identify users of its Hotmail and Messenger services, among others). The FTC found that Microsoft did not provide as much security for personally identifiable information as it claimed it did. The settlement includes a provision that Microsoft will submit to annual audits conducted by the FTC for the next 20 years (Arbogast & Smith, 2002).

The negative publicity associated with security breaches can have long-lasting effects. Imagine a successful online retailer experiencing a breach right before or during the Christmas shopping season. Its image will be tainted at least throughout that year's busiest and most profitable shopping month, potentially directing customers to competitors' sites. Disclosure of information breaches is now almost guaranteed, after the Security Breach Notification Act was enacted in California.

## THE IMPORTANCE OF THE ORGANIZATIONAL VIEW

One author asserts that information systems security can loose its usefulness if not used, misused or misinterpreted by end users (Siponen, 2000). Too often, end users today are not involved at all in issues relating to security. It is often the information technology department's responsibility to adequately secure computers and networks. The users must live with the consequences, which may include a decreased (even if only perceived) usefulness of computer systems.

The model presented in this paper calls for an inclusion of all members of the organization in implementing security practices. It is important to educate end users about the importance of information security. By doing so, their understanding of the importance of specific measures will increase. This is likely to lead to increased buy-in and increased use of the resources that are available, even with certain limitations. Specific recommendations regarding the training of technology staff and end-users can be found in the next section of this paper.

Taking an organizational view of information security is also important because it is tightly coupled to information systems. Information systems are no longer the departmental or functional "information islands" of yore. Now, information systems are an organization-wide resource. Therefore, it must be managed as such. Access to and control of information systems is the responsibility of the entire organization, not just of the technology department or of individual functional areas which manage their own information assets.

## INFORMATION SECURITY RECOMMENDATIONS

### Education

As mentioned above, information security must be treated as an organizational issue. All members of the organization must be involved. Training is the first step towards this involvement. Many training resources are available for technology staff, including seminars, courses, and certification tracks.

Security awareness training for end users is less common. To be effective, the end user training can be organized by the in-house technology staff, provided the necessary skills and knowledge is available. Training may include demonstrations of how technology resources can be abused if policies are not strictly adhered to, hands-on labs to ensure employees are familiar with the correct operation of software and hardware, and seminars outlining the organizational policies and possible employment consequences following violations of such policies.

For many organizations, the Computer Security Institute (CSI) can provide help. The CSI organizes seminars that provide attendees with practical guidelines to organizing workshops for employees. The Institute also provides a quarterly security newsletter that can be customized to include an organization's logo and column.

Higher education institutions can also play an important role. By better preparing information systems and computer science graduates, new professionals entering the workforce will already have an edge over the attacker: awareness. Most programs or courses focusing on security at this time do not include organizational policies and procedures, but instead focus on technology (for example, Grimaila & Kim (2002), Sanders (2003) and Stevens & Jamieson (2002)). Yet, examples of how the curriculum can be improved are also available (Kim & Surendran, 2002).

## Organizational Policies

The organizational policies should at a minimum include all of the following: prohibit user account or password sharing (or the sharing of any employee credentials, including badges), disallow[2] software installation by employees other than technology staff, and ensure that no passwords or sensitive information is written down. Furthermore, the organization should educate its members about common "social engineering" practices, which coerce people to release sensitive information to outsiders who present themselves as trustworthy.

Such exploits commonly involve the use of phones. It is imperative that phone operators, receptionists and secretaries are made aware of this abuse and are taught not to give out potentially sensitive information to an unverified person. Mitnick states that "if someone is making a request of a sensitive nature... and you don't personally know this person, then you have to call them back." (Gray, 2004)

Because hackers (whether they use technology-based attacks or social engineering) continuously "retool", it is important to ensure that the practices and procedures that have been established are reviewed on a regular basis. Much like it is necessary to keep computer software applications up to date to protect against newfound vulnerabilities, it is necessary to keep organizational "software" updated. The training that is offered to employees must be held at regular intervals (yearly at least) and must be updated to ensure accuracy and timeliness.

An often overlooked but important policy is the clean-desk policy. Suggested by Mitnick (Gray, 2004) and thoroughly discussed in Berinato & Tallman (2004), the goal of the clean-desk policy is to eliminate access to information by people who happen to be in the building or who have breached the physical building security and gained access to offices. It includes such practices as locking computer workstations and removing day planners from the desktop. It is also important to note that a physical security breach does not necessarily need to occur. Visitors, janitors and others who have permission to access the facilities may be able to obtain information they should not have access to, if a clean-desk policy is not in place and enforced.

Social engineering can also be facilitated from documents found in trash. Even documents that don't seem to contain confidential information prima facie may prove valuable in aiding an attacker. Such documents can include company phone books, organization charts, calendars, company letterhead, etc. In order for employees to be aware of the sensitivity of documents, Dolan (2004) suggests a data classification scheme. Each company document can be classified according to its level of confidentiality, which in his example ranges from Top Secret

[2] This should not only be a company policy, but should be enforced by the IT department through software settings.

to Public. Appropriate procedures can then be established to allow and disallow distribution and to govern proper destruction of these documents.

A problem similar to discarding old documents is the retiring of old computers. Many cases exist where organizations have donated or sold computer equipment that still contained sensitive information (Lunsford, Robbins, & Bizarro, 2004). Organizations must be aware that computer equipment's value goes well beyond the value of the hardware. Any computer equipment that can store data should be wiped clean by the IT department of the organization before being put up for auction or being donated.

Finally, it is also important that time is spent determining which employee groups must be allowed access to which information. By restricting access to only those employees who need the information to accomplish their job duties, the organization achieves two goals. First, the number of people who can potentially misuse (intentionally or unknowingly) the information is reduced. Secondly, the people who are privileged to access the protected information will be more aware of the fact that that information is indeed confidential. It may make them less inclined to share the information with people who would normally not have access to it.

Advice regarding the development of organizational security policy can be found in Baskerville & Siponen (2002). The authors present a model for developing a security policy for organizations based on the fact that each organization will require specific policies and that policy examples or templates are not appropriate.

### Organizational Culture

Perhaps the most important aspect in ensuring the long-term success of security initiatives is cultivating a company culture that encourages employees to follow the security guidelines strictly. Creating or changing company culture is notoriously difficult, and this paper will not discuss possible ways of achieving this. To an extent, recurrent training and continued upper management involvement may go a long way to achieve this goal. The ideal culture from a security perspective would be one where employees are wary of sharing data versus cooperative of requests for information from strangers.

### Relationships Security

In order to ensure that everyone who accesses information does so legitimately, companies must not only look inward, but also more and more outward. Recent trends in business, the advent of e-business especially, has caused increased information sharing between organizations. While this is beneficial, it adds complexity to the task of ensuring that information is kept confidential.

Organizations doing business exclusively or primarily with business customers can to an extent cooperate to create a secure environment in which information can be shared and kept confidential at the same time. Such cooperation can include sharing lists of employee permissions and access levels, exchanging security-related technology information, and creating standards for information security that all parties will adhere to. Such practices may prevent successful attacks from occurring because of inadequate security measures at either organization, and may also serve to increase trust between the organizations. Increased trust can then lead to a better business relationship.

Exactly which companies or organizations will be able to exercise control over other organizations may very well be determined by the same forces Michael Porter discussed in his classic work (Porter, 1979). Companies with bargaining power over their customers and/or suppliers may be able to enforce security standards, while weaker players may be forced to accept practices and standards imposed.

For organizations with many customers who interact using a business-2-consumer (B2C) web site (e.g. Amazon.com), exercising control over those customers' security practices is not feasible. Yet, in the B2C realm, businesses can do more to help consumers stay up-to-date and alert. Encouraging safe computing habits, enforcing strong passwords and other simple means can still be effective. It is important to note that if consumer accounts and passwords are misused to buy items using the consumer's credit card (which may have been stored by the online retailer), the merchant will be responsible for the fraudulent charges.

### Testing

For any policy or culture shift to be known to be effective, testing is required. However, testing security presents some challenges. It is important to find a security consulting firm that is both reliable and trustworthy. If the firm is not reliable, the organization could be left with a false sense of security. A firm that is not trustworthy may act unethically on the information it was able to obtain if the security measures prove ineffective.

Another challenge lies in the fact that someone is likely to lose face, no matter what the outcome is. If the attack is successful, the employees responsible for securing the organization's assets have failed. If the attack is unsuccessful and a later (real) attack succeeds, the security firm has lost its credibility.

While specific recommendations for dealing with these challenges are beyond the scope of this paper, it serves to illustrate that there are many more topics related to the non-technical aspect of information security remain to be researched and dealt with.

## CONCLUSION

It is important that organizations strike a balance between technology-based defenses and organizational policies and procedures against cyber- and other attacks. There is no doubt that technology will often become involved at one point during the process of an attack against the organization's information resources. Security tools such as firewalls, intrusion detection systems, and practices such as penetration testing should remain important components of a successful defense mechanism.

Yet, this paper illustrates how organizations can be vulnerable to non-technology based means of gaining access to information. The model presented in this paper expands upon existing models to allow an easy transition from a technology-only mindset into an organizational mindset. Implementing the procedures described in this paper, as part of a coordinated effort, will help avoid costly and embarrassing attacks.

## REFERENCES

Arbogast, B. & Smith, B. (2002). Q&A: Microsoft's agreement with the Federal Trade Commission on Passport. Press release. Retrieved on February 11, 2005 from http://www.microsoft.com/presspass/features/2002/aug02/08-08passport.asp

Baskerville, R. & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management*, *15* (5/6), 337-346. Retrieved on January 5, 2005 from Proquest.

Berinato, S. & Tallman, C. (2004). What's wrong with this picture? CSO Magazine, 3 (3). Retrieved on January 5, 2005 from http://www.csoonline.com/read/030104/desk.html

Blaze, M. (2004). Safecracking for the computer scientist. Retrieved on January 5, 2005 from http://www.crypto.com/papers/safelocks.pdf

Friedman, S. (2003). Building the ideal web hosting facility: A physical security perspective. Retrieved on January 5, 2005 from http://www.sans.org/rr/whitepapers/physcial/270.php

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, P. (2004). 2004 CSI/FBI Computer Crime and Security Survey. Retrieved on November 30, 2004 from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf

Gray, P. (2004). Social engineering: Don't be fooled. Technology & Business Magazine, May 2004. Retrieved on November 30, 2004 from http://www.zdnet.com.au/insight/security/0,39023764,39149146,00.htm

Grimaila, M. R. & Kim, I. (2002). An undergraduate business information security course and laboratory. *Journal of Information Systems Education*, *13* (3), 189-195. Retrieved on January 5, 2005 from Proquest.

Kim, K. & Surendran, K. (2002). Information security management curriculum design: A joint industry and academic effort. *Journal of Information Systems Education*, *13* (3), 227-235. Retrieved on January 5, 2005 from Proquest.

Lemos, R. (2000). Mitnick teaches 'social engineering'. *ZDNet News*, July 16, 2000. Retrieved on October 18, 2004 from http://zdnet.com.com/2100-11-522261.html?legacy=zdnn

Lunsford, D. L., Robbins, W. A., & Bizarro, P. A. (2004). Protecting information privacy when retiring old computers. *The CPA Journal*, *74* (7), 60. Retrieved on January 5, 2005 from Proquest.

Microsoft (2003). Security Content Overview. Retrieved on November 30, 2004 from http://download.microsoft.com/download/0/d/2/0d26f453-a3fe-4dfe-836e-a64f4daf8b43/Microsoft_Security_Content_Overview.pdf

Mitnick, K. (2001). My first RSA conference. SecurityFocus, Apr. 30, 2001. Retrieved on December 9, 2004 from http://www.securityfocus.com/news/199

Niederman, F., Brancheau, J. C. & Wetherbe, J. C. (1990). Information Systems Management Issues in the 1990s. Retrieved on November 30, 2004 from http://misrc.umn.edu/workingpapers/fullpapers/1991/9108.pdf

Pagoria, B. (2004). Implementing robust physical security: A lord of the rings. Retrieved on January 5, 2005 from http://www.sans.org/rr/whitepapers/physcial/1447.php

Porter, M. E. (1979). How competitive forces shape strategy. *Harvard Business Review, March-April 1979.* (reprint 79208)

Roberts, S. E. (2003). Liability for data leaks. *National Law Journal, 26* (4) 23. Retrieved on February 7, 2005 from LexisNexis.

Rouse, M. J., Aelterman, S. & Astone, M. (2003). The Health Insurance Portability and Accountability Act and its Impact on the Health Care Industry. *TSU System-Wide Business Symposium*, 2003. Retrieved on October 18, 2004 from http://scob.troyst.edu/Publications/ArticleView.aspx?PDFLink=/Publications/SIRHRC2003/2003SIRHRC/HIPAA.pdf&ArticleID=HIPAA

Rouse, M. J. & Liu, C. (2004). Healthcare Industry's Move Towards E-Commerce and Challenges Ahead. *TSU System-Wide Business Symposium*, 2004. Retrieved on October 18, 2004 from http://scob.troyst.edu/Publications/Archives.aspx

Sanders, A. D. (2003). Teaching tip: Utilizing simple hacking techniques to teach system security and hacker identification. *Journal of Information Systems Education, 14* (1), 5. Retrieved on January 5, 2005 from Proquest.

Scalet, S. D. (2004). Managing HIPAA's pain. *CSO Magazine, 3* (4). Retrieved on January 5, 2005 from http://www.csoonline.com/read/040104/hippa.html

Shenk, S. B. M. (2004). A patch in time saves nine: Liability risks for unpatched software. *Corporate Counsellor, 18* (11) 3. Retrieved on February 7, 2005 from LexisNexis.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8* (1), 31-41. Retrieved on November 30, 2004 from http://oasis.oulu.fi/publications/imcs080100-ms.pdf

Stevens, K. J. & Jamieson, R. (2002). A popular postgraduate information systems security course. *Journal of Information Systems Education, 13* (3), 219-226. Retrieved on January 5, 2005 from Proquest.

Stults, G. (2004). An overview of Sarbanes-Oxley for the information security professional. Retrieved on January 5, 2005 from http://www.sans.org/rr/whitepapers/legal/1426.php

Williams, F. (2003). Sarbanes, Oxley and you. *CSO Magazine, 2* (10). Retrieved on January 5, 2005 from http://www.csoonline.com/read/100103/index.html

Winkler, I. S. & Dealy, B. (1995). Information security technology? … Don't rely on it. A case study in social engineering. Retrieved on December 8, 2004 from http://oncampus.richmond.edu/~dszajda/classes/cs395_computer_security/Fall_2004/papers/winkler_social_engineering.pdf

Wolf, C. (2004). California's new online privacy policy has nationwide implications. *Journal of Internet Law, 7* (7), 3-9. Retrieved on February 7, 2005 from Infotrac.