Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2009 Proceedings

Americas Conference on Information Systems (AMCIS)

2009

A Human Centered Framework for Information Security Management: A Healthcare Perspective

Hamid R. Nemati
University of North Carolina at Greensboro, nemati@uncg.edu

Mitchell Church
University of North Carolina at Greensboro, emchurch@uncg.edu

A Human Centered Framework for Information Security Management: A Healthcare Perspective

Hamid R. Nemati
ISOM Dept. UNCG
Nemati@uncg.edu

Mitchell Church
ISOM Dept. UNCG
emchurch@uncg.edu

ABSTRACT

Research on the human element of information security is fragmented at best. This paper presents a management framework for organizations in the health care industry who wish to improve their information security procedures in an effort to comply with HIPAA and other regulations. The emphasis is on securing an organization from internal threats by adequately educating employees and building an organizational culture where security initiatives are valued and respected. The premise of the paper is that a cultural approach is the only way to gain the versatile security environment needed to comply with regulations as vast and complex as HIPAA. We argue that this framework demands that empirical data be collected through careful industry research with health care providers so as to prove the real world value of its application.

Keywords

Information Security, Organizational Culture, Management Framework, Internal Threats,

INTRODUCTION

Organizational Information security has evolved over the last several decades. The emergence of new technologies has historically been the primary motivating factor. As distributed information systems continue to defy geographical borders, the traditional technological means of handling information systems has become less effective. Increasingly companies are finding their own internal employees to represent the greatest risk to information security and sensitive employee data. This is especially true in organizations covered by such regulations as HIPAA, where guidelines for exacting procedures to follow are carefully documented.

Research dealing with how to manage the human element of information security is fragmented at best. Research into securing systems from a managerial standpoint exists, though in most cases the research fails to go beyond traditional managerial and technical methods (Backhouse & Dhillon, 1996). While many have recognized the need for a security approach that understands the business process, and the role of the employee in protecting an organization, little research has been done on how to nurture this type of environment.

To combat threats targeted against organizations, there exists a need for a framework that goes beyond technology and manages threats from the standpoint of organizational culture (Adams & Sasse, 1999). In this paper, a framework is presented for managing the human element of an organizational information security in such a way as to maximize data security while at the same time increasing productivity. This is accomplished by seamlessly integrating security protocols and procedures with everyday organizational activities. The emphasis is on building an organizational culture in which the employee feels empowered and invested in the overall security mission of the corporation. As organizational procedures and policies are developed, they are incorporated into the framework in such a way that, over time, they become seamlessly integrated into the organizational culture through careful management and employee education. The end result is not only a more secure system, but an organization with a greater awareness of security threats and a deeper understanding of the measures organizations must employ to protect themselves.

A HEALTHCARE FOCUS

As an industry that receives more than average attention from regulators and consumers in regards to information security and privacy, the health care industry is particularly well-suited for a framework of this type. Specifically in the area of privacy and patient confidentiality, the industry has a long history. The foundations for the doctor patient privacy relationship extend back to Greek times and the Hippocratic oath; *"All that may come to my knowledge in the exercise of my*

profession . . . which ought not to be spread abroad, I will keep secret and will never reveal" (Dorland, 2007). This history has led to an increased sensitivity to issues of privacy than might not be present in other industries.

If anything, time and experience have taught us to hold issues pertaining to our individual health even closer to the chest. As the medical industry in this country has become more established, the confidential relationship between a doctor and a patient has been the subject of intense scrutiny. In fact, Moore argues that the health care industry is one of the few in which confidentiality truly exists, because *"While anyone may be liable for invading a person's privacy, only those with information derived from the special confidential relationship have a duty to maintain its confidentiality*"(Moore et al., 2007).

Today, the Health Insurance Privacy Protection Act (HIPAA) represents the most recent manifestation of these feelings held by our society. HIPAA is concerned primarily with the collection, storage, and handling of patient data in a way that maintains patient privacy. This is standardized through a series of regulations and requirements to which all health care providers are held accountable.

The origins of HIPAA stem from a desire to increase productivity by automating information flows within health care organizations, while at the same time preserving our society's views of privacy and confidentiality. In the time before its implementation, however, information technology was regularly compromising patient information. Hoffman attributes this exposure to a variety of factors. Some of these include the theft of computers containing sensitive data, hacking by outside attackers, inadvertent disclosure by authorized employees, or the malicious, intentional misuse of data (Hoffman & Podgurski, 2007). The number of patients affected can sometimes be staggering. In his book, "The Digital Person", Dan Solove claims that organizations have inadvertently posted patient psychological and sexual information online in insecure formats, and cites documented evidence that in one single attack hackers may have compromised over 230,000 patient records (Solove, 2006). As personal information becomes more electronic, our "digital dossiers" described by Solove become much more detailed and widely available ((Solove, 2006). Therefore the need to produce management and technological solutions to secure this information is paramount.

HIPAA represents a comparatively aggressive step on the part of the government to outline exactly how this should be undertaken. These regulations can expose health care organizations to litigation and severe financial repercussions should violations be reported. Because of this, these organizations are always struggling to find ways to lower their operating risk by implementing HIPAA in a cost-effective, efficient way.

Managing something like HIPAA is impossible to accomplish through technological means alone. Instead, the exposure it creates at all levels of the organization must be met with an equally broad program of education and effective management that encompasses each employee that may come into contact with patient information. For hospitals, this represents a large number of individuals. The sheer scope of the undertaking has created organizations that have already begun to feel the strain of meeting regulation requirements (Zieliński, Duplaga, & Ingram, 2006).

In addition to more regulation, many agree that the future will bring more rigid enforcement of the policies that already exist. A 2008 article in Healthcare magazine shows the trend in the number of reported HIPAA infractions and their investigations over the last several years. According to the report, the number of complaints continues to rise, "*from a total of 339 complaints investigated in 2003, to 2,466 complaints investigated in 2006",* which represents an increase of 627 percent ("Update," 2008).

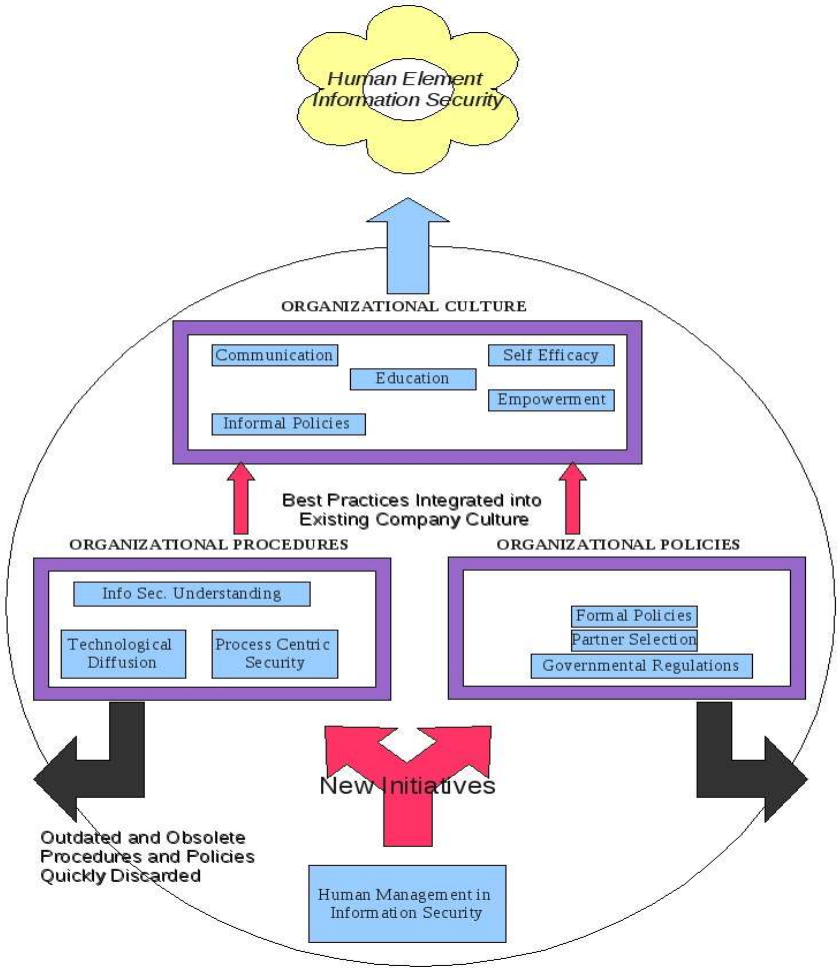
Currently, all this culminates in a health care industry that is more regulated than many other industries. A recent report by Chillmark research, a market research firm specializing in the health care industry, points to the debate over the proposed extension of HIPAA regulation to vendors of PHRs (Personal Health Records)[1]. PHR's are records maintained of all health related information on a person and may include past medications, surgeries, and any ailments diagnosed by physicians or other medical institutions. Proponents of extending this regulation point to the poor record of the PHR industry to provide standards for how information is to be kept and stored.

Extensions like these reflect the ever more prevalent concern our society shows toward privacy. While hospitals represent the initial locale for implementing this type of regulation, by spreading out into other industries that touch the health care industry directly and indirectly, HIPAA compliance will likely become a requirement for many more organizations. The advantage for these organizations is that the health care industry provides a context for planning for the future and making proactive information security decisions. This reflects the action currently being taken by some organizations such as the NAIC (National Association of Insurance Companies), who is stepping up information security

[1] http://chilmarkresearch.com/2008/05/05/why-extending-hipaa-to-phrs-is-not-a-good-idea/

protocols to bring their practices in line with those of legislation similar to HIPAA ("NAIC Wants Writers to Expand Privacy Notice.," 2003).

That's not to say that organizations are being forced to adopt HIPAA. In fact, some see it as an opportunity to gain an advantage over their competition. Davis points to the lessons learned when HIPAA compliance was made mandatory in 2005 for all covered entities and their partners, stating that "*Marketing opportunities are created anytime a service provider leaves a market environment".* Because many vendors were not explicitly forced to comply themselves, they had not considered the business impact of being unable to do business with organizations covered under HIPAA. Therefore "*HIPAA had the effect of forcing some providers out of the mix, thinning the field".* Davis further states that this in turn produced a competitive advantage as "*Suppliers able to provide HIPAA- compliant services found themselves in the enviable position of simply being there to fill the void"* (Davis, 2008). The impact on the relationships between HIPAA covered entities and those



they do business with is essential to this framework. For this reason advice is offered later for using good partner relationships to help strengthen security and alleviate the stress of a HIPAA implementation.

MANAGEMENT FRAMEWORK – ORGANIZATIONAL CULTURE AS THE KEY TO IS SUCCESS

With this framework the emphasis is on constantly improving the relationship between management of the organization and information security by working towards implementing security as an aspect of organizational culture. The framework can simply be broken down into three key components: Organizational culture, policies, and procedures.

Organizational culture represents all of the efforts of management to foster a culture that emphasizes education and employee empowerment to deliver effective information security. Organizational culture makes up the greatest part of the framework. We propose that only within an organizational culture is it possible to create an environment with the security and flexibility to handle the various threats stemming from internal employees. The organizational culture method uses education, information, empowerment and self-efficacy to create a sense of teamwork and pride among the employee base. This environment encourages employees to take credit for their own actions and help to secure the organization because it is the accepted course of action within the organization. Policies and procedures within our framework are viewed as those methods that are implemented with the intention of migrating towards integration with the company culture. For example, a new system may dictate a written policy that governs how the system is accessed, who has access, etc. This policy should be implemented with the expectation that it is only temporary, however, and at the same time, a procedure should be adopted that encourages education and training around the new system in such a way as to foster cultural elements that will eventually render the policy unnecessary. In this way, rather than being a weakness in the Information Assurance chain, the employees over time become the most versatile and effective security policy available.

Finally, organizational procedures deal with designing systems and security hardware and infrastructure for human users. As a result, the practice of technological diffusion becomes extremely important. By focusing on security from a business process standpoint, independent of technology, the organization is assuming a cultural view of their systems and security. During the design process of a system under this framework, great care should be given that everywhere possible technology is used to integrate security needs seamlessly and invisibly to the end user. This way, employees are never asked to do more than is absolutely necessary to protect the organization. This helps to foster the sense of teamwork and collaboration needed to create the proposed organizational culture. Additionally, it improves employee feelings of self-efficacy and empowerment.

There are many other reasons for emphasizing this cultural approach. It is flexible, cheap, and if implemented effectively, quite sufficient at providing security. Most importantly, it focuses on the human element of an organization. This is especially important as employees are increasingly targeted by hackers and outside threats. Through phishing attacks and social engineering, hackers continuously seek to exploit an uninformed employee base to compromise organizational integrity (Adams & Sasse, 1999).

Our society makes heavy use of similar methods when implementing its own security. Law enforcement operates heavily on the concept of social conditioning and the influence of deterrence to create a culture full of law-abiding citizens (Martin, 2007). Through these methods they achieve statistically low crime rates with a minimum of resources. This is the only realistic way to combat crime in a society like ours, because law enforcement lacks the resources to be everywhere at once, and therefore cannot physically prevent many crimes from happening. The common citizenry outnumbers law enforcement officials by a huge margin. There are simply too many people capable of committing too many crimes. Nevertheless, the presence of law enforcement and a fear of punishment can create an environment where individuals are deterred from committing crimes. This deterrence may stem from a fear of getting caught or from an aversion to the shame caused by being a criminal (Hogue, 1986). For many people, it also stems from a desire to simply do the right thing. These individuals in turn instill this same desire in their children, and thus a law-abiding society is capable of perpetuating itself.

Considering that this is the security method we choose for our everyday lives, it makes sense that these same concepts can be applied to implementing an information security framework. Because the environment we want to create is based more around prevention and positive reinforcement, educating and conditioning employees so that they are fully aware of the security risks posed by certain types of threats is essential. It is also beneficial for employees to have a complete understanding of the consequences of these threats should an attack occur; both threats to themselves and the corporation as a whole. Additionally, informal controls should reward and recognize employees who help foster this type of environment, as these are our "model citizens" who will hopefully spread their knowledge and expertise to other employees and allow our organization culture to propagate.

.

TECHNOLOGY IS NOT THE (FIRST) ANSWER:

For any security framework to have the flexibility and relevance needed for today's increasingly complex information technology industry, it must be founded on the principal that security is not simply a technology issue. This requires a shift of focus on the part of application developers and systems engineers. We've already seen what can go wrong with our earlier Internet example. Now we will explore the benefits of a systems design process that emphasizes security both early and often.

What does a security focused application look like? What problems can be identified and fixed when we consider

problems from the standpoint of security? Several best practices help us to answer these and other questions. For example, a security minded organization should create a culture that sees no potential security threat as too unlikely to worry about. Employees are identifying and discussing potential security problems, they are simply doing the work for the organization that would otherwise be done by those seeking to compromise the informational integrity of the organization. No threat is too small, or too inconceivable to worry about, at least in the design stage. Greg Day, a senior analyst for McAfee, says that cybercriminals do not discriminate based on size, and for them, no target is too small (Ashford, 2007). By approaching problems from a standpoint that does not include only technological solutions, companies can often gain a better understanding of their core business processes.

PROCESS-CENTRIC SECURITY:

Most everyone has by now heard Sun Tzu's famous lines in *The Art of War, "Therefore, I say: Know your enemy and know yourself; in a hundred battles, you will never be defeated"*. These words are quoted often enough in our society, and they apply very well to the concept of internet security, and most notably business processes. Modern organizations have many tools that know the enemy. These include firewalls, anti-virus software, and a variety of other technical control solutions. Much less common is an organization that truly knows itself, and can identify where it is weakest ("The future according to Simon.," 2003).

The trend to decentralize corporate data in an effort to improve productivity has not been without risk. According to an Ernst and Young Poll of 1,320 IT executives, 80% of organizations surveyed had experienced losses due to information breaches. More alarmingly, 70% of those who had lost money were not able to even quantify the amount of the loss (Violino, 1997).

The reason these losses are not noticed, not quantified, or certainly not prevented is that weak points are difficult to locate. This is especially true if an organization does not have a full understanding of its core business processes. Today, many business processes cross organizational and geographical boundaries, greatly adding to the number of potential threats to information assurance (Uhruski, Grochowski, & Schaefer, 2008). The most obvious threat associated with this is an increase in points of access. Far from the IT fortress of 20 years ago, businesses today have sensitive corporate data on thousands of laptops and desktops, all of which are often accessing remote servers constantly (Post & Kagan, 2003).

Health care industries frequently use this type of architecture. In a system like this, losing track of a couple entry points is easy (Violino, 1997). This is true especially when the security personnel have not been involved directly in the development of the processes used by the organization. Too often, hospitals establish these business processes, and look to secure them after the core functionality is already in place (Yau, Gong, Huang, Gao, & Zhu, 2008).

TECHNOLOGICAL DIFFUSION

The problem for organizations in the health care industry is to change the way employees view security. We have already discussed numerous ways in which an effective company culture can work towards this, but it is also important to understand that technology must do its part. This is accomplished through the concept of technological *diffusion*, which seeks to improve user acceptance by seamless integration of technology.

The goal of technological diffusion is simple and straightforward; to implement our security controls in such a way that it is invisible to the user (Hu, Chau, Liu Sheng, & Kar Yan Tam, 1999). In reality, however, this is no simple task. Fortunately empirical methods for gauging user acceptance of existing technologies exist. A direct correlation exists between user acceptance of security protocols and their effectiveness (Lallmahamood, 2007). A suitable goal then is the goal of implementation of a technical security architecture that encourages user compliance because it is simply easier to comply than not.

To apply this concept to a real world scenario, consider password policies in a typical organization. Many users memorize a handful of passwords for a variety of systems. These passwords need to be updated frequently, and often have byzantine requirements for what constitutes a valid password. Asking users to come up with and maintain multiple tough-to-crack passwords is unrealistic. If anything, this leads to users developing their own password system that helps them remember the passwords (Hu et al., 1999). This usually results in dictionary passwords or passwords with personal significant (Alsulaiman & El Saddik, 2008).

A better solution is to diffuse authentication technology down to one password, for an authentication server that controls access to other systems as needed. Researchers at the University of Austin, TX have already developed a Single

Password Protocol (SPP) that accomplishes this. The protocol consolidates authentication data into one password, but still provides security from phishing and other authentication related attacks (Gouda, Liu, Leung, & Alam, 2007).

The protection provided by SPP comes from two key features. First, a server never knows a user's password. Instead, hashing functions are used to create server-specific access tickets. These operate like movie tickets, in that they are good for one use only. This has the effect of constantly changing a user password, yet the actual user is saved the headache of remembering multiple logins, or constantly updating and changing server passwords. The technology is invisible to the user, and is therefore diffused to the point that password security policies become moot. Now that users are only required to maintain one password, this combined with an adequate informal policy designed around educating users of the importance and sanctity of that password provides a much more effective security environment.

Case Study #1:

Part of the research methodology involved in developing this framework consisted of interviews with hospital department managers at several institutions in the Piedmont-Triad area. The departments chosen for study were selected because of their role in the medical supply chain and their tendency to utilize information from a variety of departments for making medical decisions. For these reasons, our primary focus was on the radiology and emergency room job families.

These cases are meant primarily to underline the fact that technology cannot provide the level of security needed to maintain HIPAA compliance in health care organizations. Each of these cases has been selected because it represents a typical situation that could occur in any health care setting and results in a direct loss to the organization. All of these scenarios were provided by health care department managers during interviews for the purposes of this paper. All of the institutions we looked at were typical for their industry, meaning that they were necessarily fairly large operations, with significant information technology infrastructures. All of these institutions already had some system in place for monitoring HIPPA, rather through technological or managerial means, or some combination of the two. Nevertheless, in talking with employees and managers certain instances were uncovered which focused on the breakdown in HIPAA compliance resulting from the current methods employed. For the sake of brevity, here we only present one example of such a case.

One heath care organization had treated an individual for injuries related to a vehicle versus pedestrian accident that resulted in the death of the pedestrian. The resident, who was driving the vehicle involved in the incident, was identified as being a local television personality. Because of his notoriety within the community, several employees uninvolved in his care accessed his information within the organization's system out of simple curiosity and concern. As a result of this unauthorized access, information was leaked to the press regarding the patient's blood alcohol level.

As part of their HIPAA compliance program, this organization had implemented tracking software into their systems to maintain a record of all access attempts by personnel for a particular patient. In addition to this they had outlined a specific formal policy that called for strict disciplinary action in the event of unauthorized accesses. The hospital, therefore, had established two out of three controls within the security controls hierarchy; formal and technical controls.

Where the organization made a mistake however was in not adequately implementing informal controls in the form of employee education around the significance of HIPAA compliance. Employees may have had some knowledge of the penalty for unauthorized access of a patient record, but it is likely they had no knowledge of the tracking system that would allow such access attempts to be carefully monitored. The case resulted in the hospital's forced termination of more than ten key personnel as mandated by their own company policy.

This type of situation is exactly what our security framework is designed to prevent. By not adequately educating their personnel about the penalties for unauthorized access attempts, they are to blame for the expense associated with the firing, and subsequent hiring and training of new employees. This situation underlines the scope of the task of insuring HIPAA compliance within a large organization. It also spotlights the inadequacy of technical controls to deal with these types of problems. The employees affected had to have access to similar patient information to perform their basic job functions. The distinction here is a matter of context, and relevance to the duties a person is performing at any given time. Because of this, no technical control could have adequately prevented what happened.

Conclusions:

For organizations covered by HIPAA, and those organizations that want to look to the future of information security in a society that is increasingly concerned with privacy, information security is synonymous with management culture. Achieving compliance is less about any particular technology, and more about fostering a work environment that emphasizes education and awareness of security risks and company policies. This type of approach to security not only provides the

flexibility needed to combat today's threats, but it acknowledges the fact that today an organization's employees represent its softest target, and its greatest threat to information security.

Organizations seeking to create this type of culture must look at several areas of their organization. First, security discussions must happen frequently, and at all levels of a new system implementation. This implementation must also carefully consider automated activities from the standpoint of the business process. A process focused approach allows an organization to carefully consider each point of entry for a potential threat to identify and fortify weaknesses. As part of this, organizations must carefully consider the organizational culture of their partners, and look to outsource with organizations that share their company philosophy.

Every security decision that a company makes must come back to the issue of organizational culture. That means education, training, and above all, understanding. Even such security concerns as formal policies and new technology implementations must have a long term goal of seamlessly integrating with the established cultural environment. This means that policies and technical restrictions on access are constantly being reevaluated in the face of empirical data from employees, and outdated and redundant security protocols are removed, resulting in greater employee empowerment and productivity.

Finally, organizations must consider that technological diffusion is essential to achieving compliance with both outside regulations and internal security initiatives. The goal of this diffusion goes hand in hand with usability, and is designed to produce security systems that are easier to use than circumnavigate.

The research available attests to the strength and robustness of this framework in delivering high quality management for human information security. Further, the case studies provided here also underscore the need for a more effective means of educating and protecting employees and organizations from the liabilities that stem from ineffective efforts at HIPAA compliance. Therefore this framework justifies and demands further empirical analysis to prove its effectiveness in real world applications. The next step is to develop a system for measurably identifying when and how these framework components are applied in health care organizations, and what overall effectiveness is produced by their application. This may take the form of either hands on research together with health care management, or empirical surveys designed to measure employee awareness of HIPAA related issues and their risks to both individual employees and the organization at large.

REFERENCES

Adams, A., & Sasse, M. A. (1999). Users Are Not The Enemy. *Communications of the ACM*, *42*(12), 40-46.

Alsulaiman, F. A., & El Saddik, A. (2008). Three-Dimensional Password for More Secure Authentication. *IEEE Transactions on Instrumentation & Measurement*, *57*(9), 1929-1938. doi: 10.1109/TIM.2008.9 19905.

Ashford, W. (2007). Small businesses fail to recognize e-crime threat. *Computer Weekly*, 4.

Backhouse, J., & Dhillon, G. (1996). Structures of responsibility and security of information systems. *European Journal of Information Systems*, *5*(1), 2.

Davis, G. (2008). New Regulations Can Create Market Opportunities. *Marketing Health Services*, *28*(2), 40. doi: Article.

Dorland. (2007). *Dorland's Illustrated Medical Dictionary with CD-ROM* (31st ed., p. 2208). Saunders.

Gouda, M. G., Liu, A. X., Leung, L. M., & Alam, M. A. (2007). SPP: An anti-phishing single password protocol. *Computer Networks*, *51*(13), 3715-3726. doi: 10.1016/j.comnet.2007.03.007.

Hoffman, S., & Podgurski, A. (2007). Securing The HIPPA Security Rule. (cover story). *Journal of Internet Law*, *10*(8), 1-16.

HOGUE, A. R. (1986). *Origins Of The Common Law* (p. 287). Liberty Fund Inc.

Hu, P. J., Chau, P. Y. K., Liu Sheng, O. R., & Kar Yan Tam. (1999). Examining the Technology Acceptance Model Using Physician Acceptance of Telemedicine Technology. *Journal of Management Information Systems*, *16*(2), 91-112.

Lallmahamood, M. (2007). An Examination of Individual's Perceived Security and Privacy of the Internet in Malaysia and the Influence of This on Their Intention to Use E-Commerce: Using An Extension of the Technology Acceptance Model. *Journal of Internet Banking & Commerce*, *12*(3), 1-26.

Martin, J. (2007). *The English Legal System* (5th ed., p. 320). Hodder Arnold.

Moore, I. N., Snyder, S. L., Miller, C., An, A. Q., Blackford, J. U., Chuan Zhou, et al. (2007). Confidentiality And Privacy In Health Care From The Patient's Perspective: Does HIPAA Help? *Health Matrix: Journal of Law Medicine*, *17*(2), 215-272.

NAIC Wants Writers to Expand Privacy Notice. (2003). *Best's Review*, *103*(9), 12.

Post, G., & Kagan, A. (2003). Computer security and operating system updates. *Information & Software Technology*, *45*(8), 461. doi: 10.1016/S0950-5849(03)00016-8.

Solove, D. (2006). *The Digital Person: Technology and Privacy in the Information Age* (p. 290). NYU Press.

The future according to Simon. (2003). *Journal of Commerce (15307557)*, *4*(26), 27.

Uhruski, P., Grochowski, M., & Schaefer, R. (2008). A Two-Layer Agent-Based System For Large-Scale Distributed Computation. *Computational Intelligence*, *24*(3), 191-212.

Update: HIPAA Privacy and Security Rules. (2008). *Health Care Registration: The Newsletter for Health Care Registration Professionals*, *17*(7), 1-12.

Violino, B. (1997). Collapsing the fortress walls. *InformationWeek*, (635), 104.

Yau, S., Gong, H., Huang, D., Gao, W., & Zhu, L. (2008). Specification, decomposition and agent synthesis for situation-aware service-based systems. *Journal of Systems & Software*, *81*(10), 1663-1680.

Zieliński, K., Duplaga, M., & Ingram, D. (2006). *Information Technology Solutions for Healthcare*. Retrieved September 24, 2008, from http://dx.doi.org/10.1007/1-84628-141-5.