Understanding Cyber Security Perceptions Related to Information Risk in a Healthcare Setting

Derek J. Sedlack
Nova Southeastern University
sedlack@nova.edu

Abstract

Healthcare organizations are facing an information system expansion for efficiency, for effectiveness, and to enhance profitability. We cannot expect all healthcare employees to become information systems or security experts; however, human perceptions of risks and the identification of those risks require an organizational approach. A case study analysis of physicians practicing through a multi-million dollar healthcare organization is presented to better understand their group perceptions of risk relating to the organization's information strategy.

Keywords

Cyber security, information security strategy, risk, perceptions, information security, healthcare

Introduction

Healthcare organizations are facing an information system expansion for efficiency, for effectiveness, and to enhance profitability. Pressures increase from governance to secure big data (Hashem, Yaqoob, Anuar, Mokhtar, Gani, & Khan, 2015), respond to client demands for high quality service regardless of location (Azarm-Daigle, Kuziemsky, & Peyton, 2015), and appropriate finances to meet these demands (Wendel, O'Donohue, & Serratt, 2014).

Attempts to offset risks largely involve five decades of highly technical approaches (von Solms, 2000) such as encryption (Zhou, Cau, Dong, Xiong, & Vasilakos, 2015) or outsourcing to data centers that costs billions (DCSM, 2014) and only hope to keep pace with data adversaries (Hazari, Hargrave, & Clenney, 2008). Non-sensible work practices (Adams & Sasse, 1999) and a lack of expertise (Hazari et al., 2008; Rotvold, 2008) only enhance healthcare security challenges since ideal conditions have well informed employees that take an active role toward better securing information (Siponen, 2001).

We cannot expect all healthcare employees to become information systems or security experts; however, human perceptions of risks and the identification of those risks require an organizational approach (Islam & Dong, 2008). Electronic Medical Records (EMR) mandated by the government require information systems. Increasingly sophisticated diagnosis (Bayraktar, Karan, & Gümüşkaya, 2011) through expanding networks (Alemdar & Ersoy, 2010) require healthcare professionals to use increasingly sophisticated information systems. Different technology use through role or responsibility (Yoshioka, Yates, & Orlikowsk, 2002) shapes views, or frames of groups into distinct pockets (Bijker, 1987; Davidson, 2006; Vaast, 2007) that commonly lead to misidentified risk severity resulting in inaccurate tradeoffs relative to the organization.

In this research, a case study analysis of physicians practicing through a multi-million dollar healthcare organization was conducted to better understand their group perceptions of risk relating to the organization's information strategy. Interviews with the Chief Information Security Officer (CISO) were conducted in his office and follow-up discussions with physicians took place at their private practices or in a neutral setting. This study analyzed factors contributing to the overall information security posture of the healthcare organization since visiting physicians create, modify, and access healthcare privacy information, locally and remotely, that impacts the organization. Before beginning the case study, a thorough literature review was conducted and general questions were developed for interviews with practicing physicians.

Literature Review

The world generates information at a manic pace, especially in industries like Healthcare where data collection and storage are mandated. While some information systems are purposefully designed integrated information system components with adequate control, many are ad-hoc or built on legacy systems too expensive to completely replace, leaving costly security holes or risks that organizations have trouble adequately assessing (Williams, 2013). Sophisticated technical controls alone have not worked (Hazari, Hargrave, & Clenney, 2008) and researchers recommend behavioral aspects to provide better information security over technical approaches alone (Baskerville, 1993, 2003; Baskerville & Stage, 1996). Managing risk has numerous approaches (Alberts & Dorofee, 2002; Briand, et al., 1998; Courtney, 1977; Kallman, 2007; Peltier, 2001; Vidalis, 2003; Whitman, 2003) toward identifying and mitigating the weakest link (Ambrose, Seabright, & Schminke, 2002; Whitman, 2003); however, probability data is largely problematic (Baskerville, 1993) in contextualized form (Nonaka & Takeuchi, 1995), creating employee perception and business implementation voids.

Organizational information system and resource controls are required (Peltier, 2001), but the more vexing problem is understanding user behavior relating to IT threats (Liang & Xue, 2009) and user framed perceptions relating to information security (Flechais & Sasse, 2009). These frames may transform information security by user actions inconsistent with organizational expectations (von Solms, 2006) that weakens the overall security posture, including people and process deficiencies (Stewart, 2004). These salient, shifting frames diverge from organizational strategic designs from misuse through ignorance of intrinsic complexities (Siponen, 2001), political and social influences (Sanford & Bhattacherjee, 2008), tacked-on job responsibilities without adequate resources (Wei, Wang, & Ju, 2005), and/or management and worker power struggles (McGovern & Hicks, 2004). As Healthcare shifts from a societal not-for-profit benefit toward a revenue focused business, IS security strategy requires a more holistic approach (Johnston & Hale, 2009) including policies, practices, and procedures.

Physicians are presented with increasingly unreasonable or *not sensible* work practices, policies and procedures. They are asked by patients to instantly remember personal details including previous outcomes, medication lists from various sources (prescribed and homeopathic), and any relevant side-effects. Hospitals expect up-to-date medical skills regardless workloads that may include visitation and private practice. Insurance companies expect physicians to eliminate their risks while maintaining best practices related to patient health. When such expectations, including information security adherence, present as task completion obstacles, they will either be ignored or circumvented in trade for task completion (Adams and Sasse, 1999; Katos & Furnell, 2008). Alternatively, physicians are turning toward technology to replace core memorization, cross-referenced pharmaceutical charts, and colleague consultations. This reliance on technology demands a more security conscious behavior, supported by simple and clear policies and procedures (Bhagyavati & Hicks, 2003; Craig, 1993; Jones & Lipton, 1975), especially when physicians are responsible in numerous locations that maintain different policies and procedures – possibly with some in conflict.

Policy and procedural adherence do not guarantee appropriate behavior and the fabrication of sound protection mechanisms (Jones & Lipton, 1975) does not assure security. Security Education Training and Awareness (SETA) is an appropriate compliance mechanism (Choi, Kim, Goo, & Whitmore, 2008; Roper, Grau, and Fischer, 2006; Siponen, 2001), but it does not deter disgruntled or beleaguered employees (Ambrose, Seabright, & Schminke, 2002), or ensure comprehension. As increasingly sophisticated, invasive technologies are employed through Healthcare, finding enough appropriately trained/educated employees becomes challenging (Bacon & Tikekar, 2003), emphasizing how critical the structural reliance on a congruent information security strategy across differing frames; however, researchers struggle to identify a unified approach that accounts for employee turnover, incongruent professional training, varying competence levels, and other dynamic environmental conditions that negatively impact organizational information security effectiveness. This case study positions an alternative model that focused on information strategy to address the organizational risk gaps contributing to the billion dollar misappropriated data market.

Information Strategy

A focus on data-related strategy is emphasized in structural standards (Gunther, Jochen, Ivantysynova, & Ziekow, 2009) and prior research (Sedlack & Tejay, 2011) indicated an importance for healthcare organizations to not only design and implement an appropriate strategy relating to information, but ensuring that everyone understands and abides by the prescribed tenets. The security or securing of information is referred to throughout literature as information security. Information assurance is a belief that said information is secured. Information assurance through the securing/security of information cannot be accomplished without formal instruction, or strategy. As such, this paper will approach information strategy as a comprehensive approach toward the secure and assurance of data, at rest, stored, processed, or transmitted related to the organization in this study, understanding that each of these areas respectfully qualify as fully independent research fields.

Corporate Strategy

The Healthcare industry has transformed from a single visit, single source treatment, to the demand for mobile access to longitudinal records from both patient and provider (Thilakanathan, Chen, Nepal, Calvo, & Alem, 2014). Independent practices are shifting to branch offices with affiliations to hospitals or larger healthcare organizations with an emphasis on business solvency and performance management that mirrors techniques previously associated with corporate executives (Bergeron, 2005). The cost benefit and ubiquitous access to life-saving *cyberized* data through Cloud Computing has not been ignored by the Healthcare industry (Wang, Chen, & Zhang, 2015) and shifting data to a remote cite does not eliminate organizational HIPAA requirements. As information systems infiltrate oncology, radiology, and most other facets of health-related business, due to EMR compliance or efficiency, an increased importance is placed on managing risks related to information nature, use, and strategy through technology.

Healthcare Strategy

An increased focus on information availability (Alemdar & Ersoy, 2010) through untethered networks (Azarm-Daigle, Kuziemsky, & Peyton, 2015) to feed data-intensive applications (Chen & Zhang, 2014) means an increased demand from providers to treat patients and patients expect more comprehensive treatment. Thilakanathan, Chen, Nepal, Calvo, and Alem, (2014) argue that Healthcare mobile devices are increasing in popularity. Physicians expect instant access to data and patients demand safer care due to larger available data sets. These data sets of personally identifiable information (PII) and anonymized big data for diagnosis and treatment are not isolated to the local office, hospital, or regional center, but used to share and collaborate over cloud-computing environments inter-organizationally (Fabian, Ermakova, & Junghanns, 2015).

While there is discussion over data breach frequency (Edwards, Hofmeyr, & Forrest, 2015; Liu, Musen, & Chou, 2015), Healthcare data breaches cost yearly upwards of $55 billion and could point to an increasing attack sophistication (Edwards, Hofmeyr, & Forrest) such as the ransomware attack on Hollywood Presbyterian Medical Center that shut down information system functionality until hackers were paid a $17,000 bitcoin ransom from an initial $3.4M demand (Dvorak, 2016). Information systems designed to share information and protocols are largely of public construction through RFC, so how does an organization, specifically one responsible for human life, properly address information security and privacy concerns (Thilakanathan et al., 2014)?

Perceptions of Risk

While businesses always experience risk, this case study specifically focuses on how groups within organizations identify and interpret information risk through shared perceptions. Dynamic environments create incongruent perceptions (Giddens, 1984). Technological Frames of Reference (TFR) are an appropriate lens to study organizational incongruity (Davidson, 2006). Orlikowski and Gash (1994) found that Technological Frames of Reference (TFR) states member perceptions of organizational groups coalesce into similar views, even if those views are incongruent with the organization. Organizations commonly create and publish polices and expect employees to memorize and interpret them appropriately. When employees cannot remember policies or misremember them, strategic misalignment occurs. Translating policies directly into procedures may adhere to regulatory compliance like HIPAA, but it reduces customer value (Jensen & Potts, 2004) since compliance procedures may not align with customer expectations such as inhibiting their access to certain information. Information technology must be initially configured, but over time that configuration may become misaligned with business strategy. Employees trained to particular IT standards may not adequately interpret those standards to properly align with organizational information strategy. Employees are sometimes expected to purchase, maintain, and use their own devices (BYOD) within the organizational infrastructure. Employees need to be trained in the relative technologies to understand how to properly assess risk and act accordingly in the best interest of the patient and organization (Lerchey & Paras, 2000). If they are not properly trained or educated, daily use may become misaligned with organizational demands.

Employees that are over-exposed to risks may tune out (Adams & Sasse, 1999), but a lack of training may cause employee forgetfulness, misinterpretation, or disregard of real information risks, like broken authentication devices, weak passwords, or exposed confidential documentation. Many employees only intervene when risks appear severe (Stewart, 2004), like when a back door is left open or a non-employee asks for specific access to secured areas; however, what about leaving work unprotected at home or storing corporate data on an unprotected personal device? As physicians are asked to collect, store, analyze, and apply more patient data in increasingly mobile settings and patients demand higher quality care through healthcare information, their data and others, security and privacy of these electronic records become paramount (Fernandez-Aleman, Denor, Lozoya, & Toval, 2013).

Case Study

In order to understand perceptions of risk, we conducted interviews with several physicians with private practices and privileges at a large Healthcare organization in South Florida. As with many case-based analyses, these insights may not be representative. However, this sample is intended to provide a representative of similarly educated practitioners focused on delivering high quality care for their patients. The author anticipates the provided insights will prove helpful to researchers or practitioners studying information security gaps created by group perceptions related to risk.

This case study was conducted from May 2010 to May 2011. The participants are from one large organization in the Healthcare industry, identified here as Hospital One (pseudonyms are provided for anonymity). Hospital One has been in operation for more than 30 years and sustains more than 500 physicians and 1500 nurses and staff. Hospital One publically reported revenues of at least $100 million in 2010 and is part of a larger parent corporation with more than $2 billion in revenue for 2010, over 100 contributing hospitals, and 100 surgical centers. Time and resources limited this study to only Hospital One from the larger group. In structured interviews, physicians were asked about their perceptions of risk related to information. The author focused on the nature of IT, the use of IT, and IT strategy. The nature of IT relates to inherent risks. Inherent risk is defined independently of use or intention. IT use relates to handled risk. Handled risk related to the implementation, application, or non-use. IT strategy is the rationale behind purchase and/or implementation.

Case Hospital One

In this case study, physician perceptions of risk related to information are discussed. Hospital One uses infrastructure (technology) and formal policies to adhere to government HIPAA mandates to protect client and organizational data. The CEO and staff represent a formal security committee to oversee the steering committee for: policy creation and review, consultant audits, new or changing requirements, and compliance oversight. The CISO is responsible for security policy creation and maintenance, policy enforcement, and overall information security related activities. Physicians have private practices and visiting privileges at Hospital One. The physicians are responsible for oversight and implementation of all information security aspects, technical, formal, and informal, but must adhere to Hospital One mandates.

Remote Access

The CISO reported policy compliance the highest priority during this case study, but telling physicians that information security was important was frequently overtrumped with the saving of lives. The growing use of private physicians adhering to and understanding how their actions impacted Hospital One's organizational information security strategy was a growing concern for management and security staff. Private practices needed to transfer and utilize patient information in daily business: financial, personally identifying, descriptive, predictive, and prescriptive. Several years before this case study, Hospital One did not authenticate information access, internally or externally. Prior to the case study, Hospital One used single-factor authentication through keyfobs. It was not possible to assign specific fobs to physicians, limiting auditing and controls. Keyfob issues were only identified upon complaint due to loss or operating issue. During the case study, Hospital One transitioned from single-factor fobs to two-factor, integrated software authentication.

Policies

Hospital One maintained no less than 14 working formal information security policies at the time of study, including: access establishment, modification, and termination; assigned security responsibility; data backup; documentation standards; email use; encryption; media disposal; media re-use; password management; removable storage media; security training and awareness; general security; and workstation use and security policies. Hospital One identified strategic information incongruity when individual policies were technically followed and data loss still occurred.

The *removable storage media* and *encryption* policies were not combined to ensure data on removable storage media was encrypted during a form of *data backup* – transfer to Iron Mountain. Data was encrypted in-transit according to policy. The media were boxed and transferred to transport for archival according to policy, but the data or removable media were not encrypted. According to the CISO, some media were reported lost during transit, providing access to patient data to whoever obtained the media.

Corrective action was mandatory online training for related personnel to both understand and prove information policy congruency. Employees generally understood that reading the policy would ensure compliance, but the training discussed inherent risks associated with removable media and why it was important to consider risk outside one's immediate job description or during the completion of a single task. Physicians better understood how encryption worked and why Hospital One needed to encrypt data. Policies were also moved to a central portal online and linked using HTML hyperlinks. This allowed employees to quickly access new material or clarify cross-referenced policies for a more comprehensive overview of Hospital One information strategy.

The *workstation use* and *encryption* policies stated that communications between private practice and Hospital One must be encrypted. Since the remote access software used encryption, the policy was followed. The CISO reported that explicit audit tracking was available since physicians authenticated using blanket keyfobs. Loss of the keyfob meant expensive and time intensive replacement measures. Some fobs just stopped working. The CISO declared that solution as, "the fob that never went away". Once issued, fobs were never disabled due to a lack of associated accurate reporting. Physicians were reported to share fobs frequently with other physicians and staff, for convenience or due to fob theft/loss, making individual physician access tracking impossible.

Corrective action was a transition away from single-factor authentication (keyfob) to two-factor authentication (username + password). Physicians that lost their keyfob would frequently use a shared keyfob with other physicians. While the fob provided technical security and using the fob was in compliance with policies, physicians and their staff didn't understand why it was important for them to authenticate any time information was transferred or why they should not share credentials. Switching to integrated two-factor authentication corrected the inherent risks associated with shared fobs since physicians were less likely to share a password. Physicians also understood that unique credentials could be individually tracked and audited. While physicians know about HIPAA and understand it helps protect client data, few understood that Hospital One was required to track each transaction for direct accountability. When physicians were made aware that each change was tracked for audit as well as control and the associated HHS violation fines, they asked for an easy method to reset their password to remain in compliance. Forgotten passwords could be changed through the service desk, or a new authentication portal at minimal expense and inconvenience. If passwords were not used or were no longer viable through employment termination, an automated policy could disable access. The CISO reported an initial timeframe of 90 days based on historical employment records. A new sanction policy was created to provide clear and deliberate penalties for non-compliance.

The *workstation use* policy stated that only authorized users can access Hospital One systems. In private practice, physicians would logon in the morning and use that single authentication instance to commit transactions throughout the day. Even though the physician was responsible for policy compliance, it was not possible to determine who or when information was accessed remotely, only logon and logoff fob IDs and times.

Corrective action was implementing session inactivity timeouts of 90 seconds. Physicians demanded no timeouts because they needed access to financial and health-related information throughout the day and they were not previously bound by a session time requirement. Hospital One management discussed the strategic requirements of session timeouts with physicians. Times were variable and should reflect minimum times to complete required actions along with maximum idle times when physicians or staff were likely to leave a workstation unattended. Internal Hospital One stations were assigned 15 minute session timeouts due to potential public accessibility. Due to integration authentication credentials, Hospital One created shorter internal session timeouts consistent with high traffic areas and longer timeouts for more controlled, physician private practices.

Mobile Observation

One physician using their iPhone during follow-up discussions appeared to be accessing an application. The author asked if they used their phone to access protected medical data. The physician excitedly described a pharmaceutical application that not only saved them the time of looking up side-effects per patient, but could be directly tied to patient allergies and other prescriptions in the patient's exam room, at the hospital, or while they were otherwise away from traditional computer access. Additionally, any added medication would automatically cross-reference interrelated side-effects without the physician having to "memorize new drugs and side effects or incompatibilities that come out each month". The author asked if the information was ever incorrect, inaccurate, or could be purposefully misrepresented to the detriment of a patient. The physician appeared appalled at the notion and assured the researcher that the application was always up-to-date, accurate, and secure.

Unified Approach

While the researcher was not made aware of intent from Hospital One to request procedural congruence between the hospital and physician's private practice, the unified access method and conversion of static policies into Hyper-Linked, web-available forms demonstrated a shift toward more holistic compliance. Expansion of policies and/or procedures more readily available and consumable by an increasingly mobile society appears focused on compliance and comprehension over checkbox completion. Hospital One investment in training that can be inexpensively customized by role, responsibility, and learning modality will help ensure compliance with information security strategy.

Conclusion

The primary focus of Healthcare is not information security; however, an increasing reliance on information systems for primary and acute care was accentuated in the malware attack on Hollywood Presbyterian Medical Center, where even life support could have been shut down. Mobile data access becomes increasingly critical in a mobile society predicated on instant access for themselves and their service providers. A growing hunger for protected medical data to diagnose and remediate reduces an organization's ability to properly and effectively secure patient records, at rest or in use. An increasing reliance on immediate data in triage and surgery means a burdened reliance on information systems. While the lack of healthcare data could inhibit or deflect proper care, the lack of information systems in a technologically reliant system is equally damaging. This case study highlighted the importance of employees understanding appropriate technical capabilities and use to effectively support the organization's information security strategy. If the physician improperly uses the technology or increases organizational risk through improper configuration, complex information security measures may be readily circumvented.

Securing data appears to be an uphill battle and while it may be unreasonable to ask all Healthcare professionals to become information system or security experts, properly training them to perceive risks congruent with organizational strategy may reduce significant gaps that would serve to improve a structure's information security posture. When organizational members better understand technological capabilities and use them consistent with organizational information security strategy, applied information security improves. When members understand and discuss different technological approaches based on role and responsibility, information security alignment improves. When organizational groups/members are able to properly assess and respond to information risks congruent with organizational effectiveness, the information security strategy is supported.

Discussions

The independent nature of both academic and professional training will likely continue to separate the technically trained or savvy and those responsible for technical use, but lacking formal technical instruction or education. While it is unrealistic to expect all employees to become technically proficient with each tool, operating system, and security artifact briefly encountered, organizations should hire, train, and design information security strategies around organizational objectives. Additionally, when employees are better able to identify and assess information risks, reported risks increase thus increasingly the likelihood of mitigation.

Technological Frames of Reference has proven a useful research tool toward understanding individual and role-based perceptions of risk relating to information security strategy in this Healthcare setting. Expanding research to measure the effectiveness of strategic alignment or realignment is warranted. Understanding risk perceptions correlating to education, gender, or other demographics would allow researchers to design a more accurate framework and practitioners to continue improving their information security posture through training, workforce positioning, and/or hiring practices.

Similar research in additional industry settings: such as finance, manufacturing, telecommunications, and education would provide additional data toward designing a unified approach that could reduce billions in data losses annually. Other demographic or personal factors commonly associated within each industry may contribute to risk perception incongruity. Science would also benefit to understand if similar corrective actions in other fields/industries had similar results. Retail giant Target's data weakness was exposed through a vendor, unlikely to share aligned information security perceptions with Target, although the common interest of securing confidential data should be similar across all organizations in every industry and should serve as a warning to companies outsourcing services with access to any integrated infrastructure.

As the Internet of Things rapidly expands to meet insatiable customer demands for instant data, private data custodians like the Healthcare industry will feel increased pressure to secure technology specifically designed for insecure procedures. Information technology was designed to share information and is largely built on public requests for comments through working groups. Secure systems limit extensibility and increase access times through stricter access control measures and administration, increasing operational costs that reduce corporate investment returns. When users of technology better identify with the organization's information security strategy, employees or clients, both company and consumer benefit. Data breaches impacting younger information system users, like the Sony PlayStation breach, should be leveraged to inform and educate about information security strategy as much as admonish purposefully ineffective designs.

REFERENCES

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

Alberts, C., and Dorofee, A. 2002. *Managing Information Security Risks: The OCTAVE Approach*. Boston: Addison-Wesley Professional.

Alemdar, H. and Ersoy, C. 2010, October. Wireless Sensor Networks for Healthcare: A Survey. *Computer Networks, (54:15)*, pp. 2688-2710.

Ambrose, M. L., Seabright, M. A., and Schminke, M. 2002. Sabotage in the Workplace: The Role of Organizational Injustice. *Organizational Behavior and Human Decision Processes, (89:1)*, pp. 947-965.

Azarm-Daigle, M., Kuziemsky, C., and Peyton, L. 2015 A Review of Cross Organizational Healthcare Data Sharing. *Procedia Computer Science, 63*, 2015, pp. 425-432, ISSN 1877-0509.

Bacon, T., and Tikekar, R. 2003. Experiences with Developing a Computer Security Information Assurance Curriculum. *Journal of Computing Sciences in Colleges, (18:4)*, pp. 254-267.

Baskerville, R. L. 1993. Information Systems Security Design Methods: Implications for Information Systems Development. *ACM Computer Surveys, (25:4)*, pp. 375-414.

Baskerville, R. L. 2003. The LEO Principle: Perspectives on 50 Years of Business Computing. *The Journal of Strategic Information Systems, (12:4)*, pp. 255-263.

Baskerville, R. L., and Stage, J. 1996. Controlling Prototype Development Through Risk Analysis. *MIS Quarterly, (20:4)*, pp. 481-504.

Bayraktar, C., Karan, O., and Gümüşkaya, H. 2011. Diagnosing Internal Illnesses Using Pervasive Healthcare Computing and Neural Networks. *Procedia Computer Science, 3*, 584-588.

Bergeron, B. 2005. Performance Management in Small Practices. *The Journal of Medical Practice Management, (20:5)*, pp. 237-241.

Bhagyavati, and Hicks, G. 2003. A Basic Security Plan for a Generic Organization. *Journal of Computing Sciences in Colleges, (19:1)*, pp. 248-256.

Bijker, W. 1987. *The Social Construction of Bakelite: Toward a Theory of Invention*. Cambridge, MA: MIT Press.

Briand, L. C., Emam, K. E., and Bomarius, F. 1998. COBRA: A Hybrid Method for Software Cost Estimation, Benchmarking, and Risk Assessment. *Paper Presented at the Proceedings of the 20th International Conference on Software Engineering*, Kyoto, Japan.

Courtney, R. H. J. 1977. Security Risk Assessment in Electronic Data Processing Systems. *Paper Presented at the Proceedings of the June 13-16, 1977, National Computer Conferenc*e, Dallas, Texas.

Craig, J. 1993. Developing a computer use policy at the University of California at Berkeley. Paper presented at the *Proceedings of the 21st Annual ACM SIGUCCS conference on User services*, San Diego, California, United States.

Choi, N., Kim, D., Goo, J., and Whitmore, A. 2008. Knowing is Doing: An Empirical Validation of the Relationship Between Managerial Information Security Awareness and Action. *Information Management & Computer Security, (16:5)*, pp. 484-501.

"Data Center Security Market Expected to Reach $13.77 Billion by 2018." [DCSM] M2 PresswireFeb 07 2014. ProQuest. Web. 24 Feb. 2016.

Davidson, E. J. 2002. Technology Frames and Framing: A Socio-Cognitive Investigation of Requirements Determination. *MIS Quarterly, (26:4)*, pp. 329-358.

Dvorak, K. 2016 Feb. *California Hospital Pays Hackers $17K After Ransomware Attack*. FierceHealthIT. Retrieved from http://www.fiercehealthit.com/story/california-hospital-pays-hackers-17k-after-ransomware-attack/2016-02-18.

Edwards, B., Hofmeyr, S, and Forrest, S. 2015. Hype and Heavy Tails: A Closer Look at Data Breaches. *The 14th Annual Workshop on the Economics of Information Security*, June 22-23.

Fabian, B., Ermakova, T., and Junghanns, P. 2015). Collaborative and Secure Sharing of Healthcare Data in Multi-Clouds. *Information Systems, 48*, pp. 132-150.

Fernandez-Aleman, J. L., Senor, I. C., Lozoya, P. A., and Toval, A. 2013. Security and Privacy in Electronic Health Records: A Systematic Literature Review. *Journal of Biomedical Informatics, 46*, pp. 541-562.

Flechais, I., and Sasse, M. A. 2009. Stakeholder Involvement, Motivation, Responsibility, Communication: How to Design Usable Security in E-Science. *International Journal of Human-Computer Studies, (67:4)*, pp. 281-296.

Giddens, A. 1984. *The Constitution of Society: Outline of the Theory of Structure*. Berkeley, CA: University of California Press.

Gunther, O., Jochen, R., Ivantysynova, L., & Ziekow, H. 2009. IT Infrastructures in Manufacturing: Insights from Seven Case Studies. *Proceedings from the Fifteenth Americas Conference on Information Systems*, San Francisco, California, August 6-9.

Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U. 2015. The Rise of "Big Data" on Cloud Computing: Review and Open Research Issues. *Information Systems, (47:January)*, pp. 98-115.

Hazari, S., Hargrave, W., & Clenney, B. 2008. An Empirical Investigation of Factors Influencing Information Security Behavior. *Journal of Information Privacy & Security, (4:4)*, pp. 3-20.

Islam, S., and Dong, W. 2008. Human Factors in Software Security Risk Management. Paper presented at the *Proceedings of the first international workshop on leadership and management in software architecture*, Leipzig, Germany.

Jensen, C., and Potts, C. 2004. Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices. *Proceedings of the SIGCHI conference on human factors in computing systems*, 24-29 April, Vienna, Austria.

Johnston, A., and Hale, R. 2009. Improved Security Through Information Security Governance. *Communications of the ACM, (52:1)*, pp. 126-129.

Jones, A. K., and Lipton, R. J. 1975. The Enforcement of Security Policies for Computation. Paper presented at the *Proceedings of the fifth ACM symposium on operating systems principles*, Austin, Texas, United States. http://portal.acm.org/citation.cfm?id=806538#

Kallman, J. 2007. Identifying Risk. *Risk Management, (54:9)*, pp. 58-59.

Katos, V., and Furnell, S. 2008. When Security Causes its Own Type of Harm. *Computer Fraud & Security, 16*.

Lerchey, J. K., and Paras, C. J. 2000. Shaping a New Generation of Users: You Can Show Them the Policies, But You Can't Make Them Think. *Proceedings of the 28th Annual ACM SIGUCCS Conference on User Services: Building the Future* (pp. 158-161), Richmond, Virginia, United States.

Liang, H., and Xue, Y. 2009. Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly, (33:1)*, p. 71.

Liu, V. Musen, M. A., and Chou, T. 2015. Data Breaches of Protected Health Information in the United States. *The Journal of the American Medical Association, (313:14)*, pp. 1471-1473.

Mårtensson, P. and Lee, A. S. 2004. Dialogical Action Research at Omega Corporation. *MIS Quarterly, (28:3)*, pp. 507-536.

McGovern, T., and Hicks, C. 2004. How Political Processes Shaped the IT Adopted by a Small Make-to-Order Company: A Case Study in the Insulated Wire and Cable Industry. *Information & Management, (42:1)*, pp. 243-257.

Michael, J. B., Sibley, E. H., and Littleman, D. C. 1993. Integration of Formal and Heuristic Reasoning as a Basis for Testing and Debugging Computer Security Policy. *Proceedings on the 1992-1993 Workshop on New Security Paradigms* (pp. 69-75), Little Compton, Rhode Island, United States.

Nonaka, I., and Takeuchi, H. 1995. *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation*. New York: Oxford University Press.

Orlikowski, W. J., and Gash, D. C. 1994. Technological Frames: Making Sense of Information Technology in Organizations. *ACM Transactions on Information Systems, (12:2)*, pp. 174-208.

Peltier, T. R. 2001. *Information Security Risk Analysis*. Boca Raton, FL: Auerbach Publications, div. of CRC Press LLC.

Roper, C., Grau, J., and Fischer, L. 2006. *Security Education, Awareness, and Training: From Theory to Practice*. Burlington, MA: Butterworth-Heinemann.

Rotvold, G. 2008. How to Create a Security Culture in Your Organization. *Information Management Journal, (42:6)*, pp. 32-34,36-38. doi: 1601672801

Sanford, C., and Bhattacherjee, A. 2008. IT Implementation in a Developing Country Municipality: A Sociocognitive Analysis. *International Journal of Technology and Human Interaction, (4:3)*, pp. 68-93.

Sedlack, D. and Tejay, G. P. J. 2011. Improving Information Security Through Technological Frames of Reference. *Proceedings of the 13th Annual Conference of the Southern Association for Information Systems*, 25-26 Atlanta, GA, Paper 30.

Shah, A. H., Aziz, S. M., and Rahman, M. 2014. Review of Cyber-Physical System in Healthcare. *International Journal of Distributed Sensor Networks*, vol. 2014, Article ID 217415, 20 pages.

Siponen, M. T. 2001. Five Dimensions of Information Security Awareness. *ACM SIGCAS Computers and Society, (31:2)*, pp. 24-29. doi: 10.1145/503345.503348.

Stewart, A. 2004. On risk: Perception and Direction. *Computers & Security, (23:5)*, pp. 362-370.

Thilakanathan, D., Chen, S., Nepal, S., Calvo, R., and Alem, L. 2014. A Platform for Secure Monitoring and Sharing of Generic Health Data in the Cloud. *Future Generation Computer Systems, (35)*, pp. 102-113.

Wendel, J. O'Donohue, W., and Serratt, T. D. 2014. *Understanding Healthcare Economics; Managing Your Career in an Evolving Healthcare System*. Portland, OR:CRC Press.

Vaast, E. 2007. Danger is in the Eye of the Beholders: Social Representations of Information Systems security in healthcare. *The Journal of Strategic Information Systems, (16:2)*, pp. 130-152.

Vidalis, S. 2003. *A Critical Discussion of Risk and Threat Analysis Methods and Methodologies*. School of Computing Technical Report CS-04-03, School of Computing, University of Glamorgan, Wales, 20.

von Solms, B. 2000. Information Security -- The Third Wave? *Computers & Security, (19:7)*, pp. 615-620.

Wang, W., Chen, L., and Zhang, Q. 2015. Outsourcing High-Dimensional Healthcare Data to Cloud with Personalized Privacy Preservation. *Computer Networks, (88:9)*, 136-148.

Wei, H.-L., Wang, E. T. G., and Ju, P.-H. 2005. Understanding Misalignment and Cascading Change of ERP Implementation: A Stage View of Process Analysis. *European Journal of Information Systems: Including a special section on the pacific Asia conference, (14:4)*, pp. 324-334.

Whitman, M. 2003. Enemy at the Gate: Threats to Information Security. *Communications of the ACM, (46:8)*, pp. 91-95.

Williams, P. H. 2013. Information Security Governance: A Risk Assessment Approach to Health Information Systems Protection. *Studies in Health Technology and Informatics, 193*, pp. 186-206.

Yoshioka, T., Yates, J., and Orlikowsk, W. J. 2002. Community-based interpretive schemes: exploring the use of cyber meetings within a global organization. *Paper presented at the Proceedings of the 35th Annual Hawaii International Conference on Systems Science* (CD-ROM), Los Alamitos, CA.

Zhou, J., Cao, Z., Dong, X. Vasilakos, A. V. 2014. A Secure and Privacy-Preserving Key Management Scheme for Cloud-Assisted Wireless Body Area Network in M-Healthcare Social Networks. *Information Sciences, (314:1)*, pp. 255-276.