Evaluating Employee Intentions to Comply with Password Security Policies and Procedures for a Public Hospital EMR System

Queen Esther Booker

Minnesota State University, Mankato, 150 Morris Hall, Mankato, MN 56001
Phone: (507) 389-2445 Fax: (507) 389-5497
queen.booker@mnsu.edu

Carl M. Rebman, Jr.

University of San Diego, Alcala West, Coronado 212, San Diego, CA 92110
Phone: (619) 260-4135 Fax: (619) 260-7611
carlr@sandiego.edu

Fred L. Kitchens

Ball State University, Department of Information Systems and Operations Management, WB203, Muncie, IN 47304
Phone: (765) 285-5305 Fax: (765) 285-5117
fkitchens@bsu.edu

ABSTRACT

Digital assets have become a major asset for corporations. Protecting these assets could mean the difference between customer confidence and customer concern. Thus, understanding employee attitudes toward compliance security policies and procedures is important to understanding additional steps in risk management an organization must undertake to ensure maximizing the security of its digital assets. This paper follows the a three year analysis of a hospital's survey collection of compliance analysis using the Spitzmuller and Stanton Employee Security Compliance Survey adapted for analyzing passwords and email usage. The interest in the data collection was specifically for password attitudes. The email usage data was collected as validation for the results and to not bias the results for password attitudes.

INTRODUCTION

Long Beach Memorial is one of a small percentage of hospitals in the country with a fully integrated electronic medical records (EMR) system, well ahead of the national deadline established in the federal stimulus plan. Hospitals have been slow to adopting EMR systems due to concerns about patient privacy and information loss due to unauthorized access by employees and non employees alike. However, thanks to federal stimulus package of 2009, physicians will each receive a maximum of $44,000 over the course of five years from the Centers for Medicare

and Medicaid Services (CMS); beginning in 2011, if they implement and use a certified EMR in their facilities in a meaningful way. In addition, hospitals and healthcare providers that do not implement CCHIT-certified EMRs by 2014 will have their Medicare reimbursement rates cut by up to 3 percent beginning in 2015. The U.S. Congressional Budget Office (CBO) estimates these incentives will persuade nearly 90 percent of U.S. physicians to use EMRs over the next 10 years.

According to a study published by the New England Journal of Medicine in March, 2009, only 1.5 percent of acute-care hospitals have implemented a fully integrated EMR, and only 8 percent have a basic EMR in place (Steinbrook, 2009). Putting paper records into an electronic system does not come without concerns. One of the biggest is the worry that a patient's privacy and security could be at risk due to the amount of personal medical information involved. With the massive amount of personal patient information involved in an EMR, doctors and administrators alike emphasize the importance of ensuring that security features are put into place. EMR software should be capable of prohibiting access to certain parts of the record to unauthorized users.

But like many organizations, hospitals have users who must use EMR systems who are not technologically savvy. Many physicians lack basic computer skills, such as using e-mail and the Internet. This sentiment was echoed by a Boston area hospital that is implementing an EMR system. Their desire was to minimize the risk by developing trainings, policies and procedures that would inform as well as maximize adherence to behaviors to protect patient privacy with the data. Particular areas of concern were using and changing passwords, not downloading patient data to desktops, laptops, external drives or entering or extracting data on non secure communications protocols. (Steinbrook, 2009)

Their concern about potential employee resistance to the possible policies and procedures was also echoed in Leo’s story. He said that resistance from physicians and staff members lacking basic IT skills is a cause for concern. A recent report by the National Center for Health Statistics, found that only 38.4 percent of physicians reported using full or partial EMRs. "Though this number is on the rise, many physicians are hesitant to adopt because they worry that it might take more time to input patient data into a computer as opposed to documenting it on paper," he adds. This resistance could lead doctors to entrust the data entry to someone without the proper authority to access the system.

Researchers have found that some employees dislike technology policies and distrust monitoring systems, and some even actively thwart their organization’s use of these systems by altering monitoring equipment/software or by avoiding monitored areas (Nussbaum & du Rivage, 1986; Stanton, 2000, 2002; Stanton & Weiss, 2000, Spitzmuller & Stanton, 2006). Others simply do not comply with company policies. If employees succeed in circumventing systems, then the security technology and policies provide little of its intended value. The effectiveness of organizational monitoring techniques, and policies, then, depends on employees’ willingness to comply with their use. Insights into employees’ intentions to comply with policies or circumvent monitoring tools are helpful in promoting effective use of these technologies.

The literature suggests that barriers to acceptance of security devices can be grouped into the following categories: organizational commitment, physical invasiveness, information invasiveness, ease of use, privacy, and the perceived level of benefit from the device (Spitzmuller and Stanton, 2006; James et al, 2006; Deane, Barrelle, Henderson, & Mahar, 1995; Liu & Silverman, 2001; Woodward, 1997). Recent studies that focus primarily on security related concerns include the study by James et al (2006) that investigated the intention to use biometric devices, the study by Spitzmuller and Stanton (2006) that investigated the intention to thwart monitoring systems related to email, and a study by Booker and Kitchens (2007) that considered user acceptance with risk perception.

The objective of this study is to examine and compare attitudinal changes antecedents of compliance and resistance with organizationally-imposed policies and monitoring systems over time. The managers assumed that the resistance to password policies particularly related to the implementation of the EMR system would be very high by all employees but as training, employee engagement in the system implementation and engagement in the policy setting progressed, the attitudes would become more positive. The study utilized a Likert-type scale survey designed to study the user behavior toward email monitoring and password security policies and technologies and the intention to use these devices, with the data providing insight into possible barriers to adoption of general security technologies. The data was collected in January 2007, January 2008, and January 2009. The managers used the 2007 data as a beginning benchmark as to what the hospital was facing and the latter two years were used to measure improvements or setbacks based on results from the survey results.

The next section provides a brief discussion on planned behavior and the framework for the study. Section 3 discusses the methodology used to test the proposed model and Section 4 presents the results. Section 5 provides conclusion and directions for future research.

BACKGROUND

The theory of planned behavior (TpB) has during recent years become one of the most widely used theories to explain and predict human behavior. TpB has been applied to a variety of behaviors related to computer technology, with the most popular being the technology adoption model used to determine ease of use and perceived usability of various technologies (Davies, 1986). TpB is an extension of the theory of reasoned action. In TpB, perceived behavioral control is theorized to be an additional determinant of intention and behavior (Ajzen 1991). TpB is a theory of predicting intentions based attitudes, beliefs, social norms, intentions, volitional control, and behavior. Volitional control served as a moderator variable: given a certain level of intentions, a behavior would more likely occur in situations where the behavior was under the control of the actor.

TpB frameworks have application to the study of compliance and resistance pertaining to security technologies. Employees may hold certain beliefs and may form attitudes about organizational policies, monitoring and surveillance based on these beliefs. In turn, intentions to comply or resist may relate to attitudes as well as social norms about these behaviors. For example, Loch and Conger (1996) applied the theory of planned behavior to employees' use of computers in organizations, and found that attitudes and social norms predicted intentions to

misuse the organization's computers. Their study thus supported the utility of the theory in predicting behavioral intentions with reference to uses of technology in organizations. Spizmuller and Stanton (2006) applied the theory to behavior of employee's mitigation or lack of compliance with email monitoring and, too, found attitudes and social norms as prediction of intention to not comply.

RESEARCH METHODOLOGY

This study was related to the implementation of a password policy related to the automated medical records system. The security technology was passwords that were expected to be changed every six months and had to include a special character, upper and lowercase letters and at least two numbers. The password security policy was that no one was to share their password with anyone under any circumstance. Although the password access created a new layer of barriers to managing patient care, the study expected to find improvement in attitudes over time especially since the managers engaged in proven change management techniques, e.g., training, engaging the users in the implementation of the new system, engaging employees in the writing of the policies through a series of open forums and feedback session, and replacing retiring staff with employees with proven technology skills. Using TpB the following hypotheses were formulated related to the use of the password security policies and technologies:

H1a: Employee attitudes toward following the password policies would significantly improve from year 1 to year 2.

H1b: Employee attitudes toward following the password policies would significantly improve from year 2 to year 3.

H2a: Employee attitudes toward the organization would move significantly closer to a rules-based organization from a caring based organization from year 1 to year 2.

H2b: Employee attitudes toward the organization would move significantly closer to a rules-based organization from a caring based organization from year 2 to year 3.

The survey was sent to each employee via mail with a self addressed stamped envelope to return to an outside security company. The purpose of the paper system was to address the lack of technology skills among many employees and to encourage return of the surveys. The survey was given to employees the first week of January and employees were asked to return them by January 30 in 2007, 2008, and 2009. Participation was voluntary and anonymous although employees were asked to complete how long they had worked at the hospital in order to separate the responses from recently employed users who had not participated in previous year studies. Table 1 shows the number of usable surveys returned. Usable surveys were defined as surveys by current employees who have been with the organization for at least one year and a half years for year 2, and for employees who have been with the organization for at least 2 and a half years for year 3. Usable was also defined as surveys that were completed in full with no missing data. All usable surveys for year 1 were used.

Table 1. Number of Respondents by Year and Job Category

	Year 1	Year 2	Year 3
Total Usable Surveys	905	945	841

Outcome variables in this study were intentions to comply with or resist overall security policies and technologies and then with questions specific to passwords. The intention questions for the study were developed according to the strategy described by Ajzen and Fishbein (1980). Item content was derived previous studies on technology adoption and acceptance based on research from Spitzmuller and Stanton (2006), and Booker and Kitchen (2007). These sources provided input regarding which items were important regarding intentions. After developing the list of questions for the survey, the outcome variables were the following:

Outcome Variable Description
Organization has a rules culture
Organization has a caring culture
Attitude towards password security policies
Attitude towards password security technologies
Accept password security policies
Accept password security technologies
Avoid password security policies
Avoid password security technologies
Manipulate password security policies
Manipulate password security technologies
Complain about password security policies
Complain about password security technologies

DESCRIPTIVE STATISTICS

Table 2 lists the range, mean and standard deviation for each of the factors analyzed in the study for Year 1, Table 3 lists the descriptive statistics for Year 2, and Table 3 lists the descriptive statistics for Year 3. Recall the Likert-scale for the survey was a 5 point scale, with one being strongly disagree and 5 being strongly agree. In general, the respondents were comfortable with public policies on security and tended to have a positive attitude towards to general organizational security policies and technologies. These results were consistent across all three years and are consistent with results from previous studies.

Table 2. Mean and Standard Deviations for Study Variables for Years 1, 2 and 3

	Year 1 (N=905)		Year 2 (N=945)		Year 3 (N=841)	
Study Variable	***Mean***	***Std. Dev.***	***Mean***	***Std. Dev.***	***Mean***	***Std. Dev.***
Organization has a rules culture	2.43	1.1	3.03	1.42	3.5	1.13
Organization has a caring culture	4	0.82	2.92	1.39	2.96	1.43
Attitude towards password security policies	2.94	1.42	2.92	1.38	2.55	1.12

Attitude towards password security technologies	2.98	1.42	3.03	1.42	2.45	1.13
Accept password security policies	2.95	1.4	3.06	1.45	2.49	1.13
Accept password security technologies	2.97	1.42	2.92	1.39	2.52	1.14
Avoid password security policies	3.08	1.41	3.04	1.38	3.49	1.15
Avoid password security technologies	2.95	1.4	3.04	1.46	3.51	1.12
Manipulate password security policies	2.96	1.4	2.95	1.41	3.46	1.11
Manipulate password security technologies	3	1.39	2.98	1.44	3.53	1.15
Complain about password security policies	2.98	1.4	2.95	1.4	3.51	1.1
Complain about password security technologies	2.98	1.42	2.96	1.46	3.54	1.13

RESULTS

Recall that the questions were asked on a Likert scale of 1 to 5 where 1 was strongly disagree, 5 was strongly agree, and 3 was neutral. Without checking for significance, as the years progressed, current employees started on average as neutral and became less neutral and more likely to disagree with the password policies and technologies and more likely to manipulate and avoid them if possible in subsequent years. Full results are available upon request.

A compare means test was run for year 1 and year 2, and again for year 2 and year 3. Full results are available from the authors but the variables in question were attitudes towards password policies and attitudes of caring versus a rules based organization. The results for year 1 and year 2 are shown in Table 3.

Table 3. Significance between variables of interest and Year 1 and Year 2

	F	Sig.
Organization has a rules culture	*63.26571*	*0.00*
Organization has a caring culture	*320.3978*	*0.00*
Attitude towards password security policies	1.564503	0.21
Attitude towards password security technologies	0.035417	0.85
Accept password security policies	*4.106439*	*0.04*
Accept password security technologies	0.831284	0.36
Avoid password security policies	3.069479	0.08
Avoid password security technologies	3.334332	0.07
Manipulate password security policies	0.053452	0.82
Manipulate password security technologies	2.095138	0.15
Complain about password security policies	0.441839	0.51
Complain about password security	1.892655	0.17

technologies		

Note that the only variables with a significant difference using the compare means tests were organization has a rules culture, organization has a caring culture, and accept password security policies. Reviewing the actual means, respondents from year 1 moved from disagree to neutral in year 2 regarding the hospital having a rules culture. Respondents from year 1 leaned towards agreeing that the hospital had a caring culture to a less than neutral response in year 2. For year 2 and year 3, another compare means test was run on the same variables. The results are shown in Table 4.

Table 4. Significance between variables of interest and Year 2 and Year 3

	F	Sig.
Organization has a rules culture	42.11	0.00
Organization has a caring culture	1.62	0.20
Attitude towards password security policies	31.02	0.00
Attitude towards password security technologies	40.30	0.00
Accept password security policies	66.33	0.00
Accept password security technologies	30.29	0.00
Avoid password security policies	17.73	0.00
Avoid password security technologies	71.77	0.00
Manipulate password security policies	49.83	0.00
Manipulate password security technologies	45.37	0.00
Complain about password security policies	52.54	0.00
Complain about password security technologies	60.39	0.00

With the exception of attitudinal changes towards being a caring organization, all of the means tests were significant at or below the .05 level. The means for year 2 and year 3 for the variables of interest are shown in Table 5.

Table 5. Comparison of Means between Year 2 and Year 3

	Year 2	Year 3
Study Variable	Mean	Mean
Organization has a rules culture	3.03	3.5
Organization has a caring culture	2.92	2.96
Attitude towards password security policies	2.92	2.55
Attitude towards password security technologies	3.03	2.45
Accept password security policies	3.06	2.49
Accept password security technologies	2.92	2.52
Avoid password security policies	3.04	3.49
Avoid password security technologies	3.04	3.51

Manipulate password security policies	2.95	3.46
Manipulate password security technologies	2.98	3.53
Complain about password security policies	2.95	3.51
Complain about password security technologies	2.96	3.54

As the results indicate, the employees moved towards an attitude that the organization was becoming more rules based but maintained that it was still a caring organization. They also moved towards disagreeing with the password policies, and showing increasing attitudes of avoiding and manipulating the password security policies and procedures.

Again the hypotheses for the study were:
H1a: Employee attitudes toward following the password policies would significantly improve from year 1 to year 2.

H1b: Employee attitudes toward following the password policies would significantly improve from year 2 to year 3.

H2a: Employee attitudes toward the organization would move significantly closer to a rules-based organization from a caring based organization from year 1 to year 2.

H2b: Employee attitudes toward the organization would move significantly closer to a rules-based organization from a caring based organization from year 2 to year 3.

For hypothesis H1a, employee attitudes towards password policies did not improve significantly for years 1 and 2 so we reject H1a. For hypothesis H1b, employee attitudes did not improve significantly; instead they declined significantly so we reject hypothesis H1b. For hypotheses H2a and H2b, employee attitudes did not move from caring although attitudes did adjust more towards considering the hospital more rules based. Therefore all of the initial hypotheses must be rejected.

CONCLUSIONS AND FUTURE RESEARCH

Although the results led to the rejection of the hypotheses, significant information was learned from the data. The first was that the organization could move towards being more rules based without sacrificing its reputation for being a caring organization. However, the survey results do indicate that the attitudes towards avoiding and manipulating the password system to be troublesome. It was these similar attitudes that created an environment that lead to the theft of prescription medicines from a major hospital in Tucson, Arizona (see Booker and Johnson, 2005). The next step is to develop a further analysis to determine if those who must meet Sarbanes Oxley and HIPAA requirements share these attitudes or if the attitudes are primarily those who do not have to access the system frequently. There will also be another survey collected in 2010, and there are similar studies from eleven other hospitals for the same time periods that can be analyzed to determine if these results are common or an anomaly.

REFERENCES

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50, 1–33.

Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behavior. Englewood Cliffs: Prentice-Hall.

Booker, Q. & Kitchens, F. L. (2007). Predicting Employee Intention to Comply with Organizational Security Policies and Procedures Factoring Risk Perception. Proceedings of the 2007 Security Conference.

Booker, Q. E. & Johnson, A. (2005). A Study in Implementing a Neural Network Model to Assess Unauthorized Attempts to a County Hospital's Physical Computer Systems. Proceedings of the International Association of Business and Public Administration Disciplines Conference.

James, T., Pirim, T., Boswell, K., Reithel, B., & Barkhi, R. (2006) Determining the Intention to Use Biometric Devices: An Application and Extension of the Technology Acceptance Model. Journal of Organizational and End User Computing. Hershey: Jul-Sep 2006. 18 (3) 3, 1-24

Loch, K. D., & Conger, S. (1996). Evaluating ethical decision-making and computer use. Communications of the ACM, 39(7), 74–83.

Nussbaum, K., & du Rivage, V. (1986). Computer monitoring: Mismanagement by remote control. Business and Society Review, 56, 16–20.

Spitzmuller, C. & Stanton J. M. (2006). Examining employee compliance with organizational surveillance and monitoring, Journal of Occupational and Organizational Psychology, 79, 245–272

Stanton, J. M. (2000). Reactions to employee performance monitoring: Framework, review, and research directions. Human Performance, 13, 85–113.

Stanton, J. M. (2002). Information technology and privacy: A boundary management perspective. In S. Clarke, E. Coakes, G. Hunter, & A. Wenn (Eds.), Socio-technical and human cognition elements of information systems (pp. 79–103). London: Idea Group.

Stanton, J. M., & Weiss, E. M. (2000). Electronic monitoring in their own words: An exploratory study of employees' experiences with new types of surveillance. Computers in Human Behavior, 16, 423–440.

Steinbrook, R. (2009). Health Care and the American Recovery and Reinvestment Act. The New England Journal of Medicine, 360 (11), 1057-1060.