Detecting and Rectifying the Non-Malicious Insider Threat in a Healthcare Setting

Abstract

We were tasked by a global leader in healthcare to look into making the organization more secure by creating a training program that focused on employee habits. By adapting a model from consumer behavior to information security, we were able to find strong correlations between habit creation and security threats such as phishing, unauthorized cloud computing use, and password sharing. We were also able to ascertain that traditional security training and awareness programs need to move away from the "one-size" fits all technique to custom models that need to look at employee groups. This study extends literature in habit and information security.

Keywords: habit, information security, employee training

Introduction

Samantha needed to work on a large file at home. It was too big to email, so she absent-mindedly plugged a flash drive someone had left in the break room into her desktop's USB port. This was not an issue for her since she had used the flash drive plenty of times in the past. She had logged on with her password, and the company's email client was open. This simple act started a chain reaction, launching malware hidden on the flash drive that propagated by attaching a copy of the malignant code to every email she sent. Within hours, the corporate network was thoroughly compromised. This hypothetical vignette illustrates an important insight that eludes many Information Technology (IT) managers tasked with information security - many breaches occur when users are not consciously aware of what they are doing. Also, contrary to recent headlines, not all threats in the cyber realm are malicious in nature. According to a

Ponemon study, 70% of US survey respondents and 64% of German respondents stated that more security incidents were caused by unintentional mistakes rather than malicious acts (Ponemon, 2015). We contend that most of these unintentional mistakes are due to habitual behavior that promotes an automatic response. Previous research supports the idea that automated behavior results from the force of habit (Kim et al., 2005, Jasperson et al., 2005, Ouellette and Wood, 1998). However, this issue has not been investigated in information security in any context.

We were tasked by a global leader in healthcare, heretofore referred to as the Caregiver to assist with efforts to strengthen their internal security protocols based on identified threats, in light of threats at a time when information technology is increasing in scope, scale, and importance to all areas of medicine. A critical element of this effort based on our research was training the disparate groups of professionals that must coordinate their efforts to provide best-of-care standards that are the hallmark of this organization. Because a high percentage of security breaches are the result of automated behaviors, traditional information security education is not enough since it assumes that all decisions are made rationally. Automated decisions are made by the brain in an area that is considered to be unconscious (Martin and Morich, 2011). Also, because information technology continuously evolves, along with digital exploits, trying to keep the Caregiver's personnel up to date via classroom instruction would be too time consuming to be plausible. We content for the organization to achieve its information security goals, every member of the organization must be trained to automatically do the right the thing at the right time every time. Not only is it not necessary to educate staff on the complexities of information security, doing so would be counterproductive. The key

is to train all personnel individually based on their disciplines and their IT contexts to do the right procedure without having to consciously think about it. Based on our research, we contend that the answer may lie in addressing the difference between conscious and unconscious errors in security breaches. This issue needs to be developed for any meaningful modeling (Benbasat and Barki, 2007). Unconscious habits form the center of human behavior, yet are largely underestimated and misunderstood. We adapted the Martin-Morich (Martin and Morich, 2011) model of behavior, which is described later to information security to answer the following research question: Does unconscious behavior need to be changed to reduce the probability of non-malicious insider threats?

In the next few sections we provide a review of previous research in information security and habits, a description of the research model that we adapted to information security, description of the research site, development of measures, and results before concluding.

Literature Review

Because there is a paucity of information security research with respect to automated/habitual behavior, we have divided this section into two parts. The first presents relevant information security research that deals with employee compliance, whereas the second provides an overview of existing IS habit-based research.

Information Security

Because users interact with information systems on a regular basis in their organizational activities, how they use the systems and whether they follow established measures will ultimately determine the overall security of an organization's information systems. Fundamentally, traditional IS security has a "behavioral root" (Workman and

Gathegi, 2007) and is a subject of psychological and sociological actions of people. Most prior research in organizational IS security has dealt with success and failure of security policies using a deterrence approach (Chen et al., 2012, Straub and Nance, 1990, Cheng et al., 2013, Herath and Rao, 2009, Bulgurcu et al., 2010). General Deterrence Theory (GDT) has been used to investigate the effect of organizational deterrent measures on computer abuses by employees. Deterrent measures can reduce computer abuse by potential offenders if the risk of punishment is high (deterrent certainty) and penalties for violations are severe (deterrent severity) (Straub 1990). However, findings regarding the effectiveness of deterrence measures have been mixed (D'Arcy and Herath, 2011). Deterrent and preventive methods have a positive impact on information security effectiveness, but the severity of the deterrence method does not (Kankanhalli et al., 2003). Contrary to what is proposed by GDT, organizations with a high number of deterrent measures have higher incidents of insider abuse (Lee et al., 2004), indicating a significant negative relation between deterrent measures and insider abuse.

Prior studies have also focused on employee compliance to security policies (Vance et al., 2012). An Information Security Policy Compliance Model suggests that a user's intention to comply with security policies is influenced by user attitude toward complying. According to the authors, user attitudes and intentions are influenced by a mixture of negative and positive reinforcements (Pahnila et al., 2007). Examples of negative reinforcements according to Pahnila et al. (Pahnila et al., 2007) include sanctions, threat appraisal, coping appraisal, and normative beliefs and positive reinforcements include information quality of policies, facilitation conditions, and habits.

In a similar study, the antecedents of employee compliance with information security policy (ISP) of an organization were investigated (Sneha and Varshney, 2009). The study indicated that an employee's attitude positively influences an employee's intention to comply with the ISP. In addition, information security awareness significantly influenced an employee's attitude to comply with the ISP through the employee's beliefs.

Habit Research

IS research in this area mostly focuses on continuing IT use being an act that is driven by conscious (non-habitual) decision making (De Guinea and Markus, 2009). However, it also draws from literature in psychology and social psychology to posit that much of continuing IT use is habitual. The argument is that when IT use is habitual, it ceases to be guided by an individual's intentions (Thorngate, 1976). Habitual IT use behavior in IS has been defined as repeated behavioral sequences that are automatically triggered by cues in the environment (Cheung and Limayem, 2005, Limayem and Hirt, 2003, Limayem et al., 2007, Kim et al., 2005), and is considered to be a critical predictor of technology use (Kim and Malhotra, 2005). Limayem and Cheung (Limayem and Cheung, 2008) used a moderation perspective and illustrated that the predictive power of intention weakened with continued habitual behavior by individuals. Venkatesh, Thong, and Xu (Venkatesh et al., 2012) integrated habit into the unified theory of acceptance and use of technology (UTAUT) to complement the theory's focus on intentionality as the overarching mechanism and key driver of behavior. They modeled habit as having both a direct effect on use and an indirect effect through behavioral intention. Studies have used various proxies for habit. For example, Kim and Malhotra (Kim and Malhotra, 2005)

equated past use to habit. Limayem and Hirt (Limayem and Hirt, 2003) introduced a self-reflective measure of habitual IS use as a viable alternative to past use. Some have used a "response-frequency measure" to measure habitual tendencies toward the choice of a certain travel mode (Verplanken et al., 1994, Verplanken et al., 1997, Verplanken et al., 1998). In terms of their psychometric properties these measures have not been compared to each other. Benbasat and Barki (Benbasat and Barki, 2007) have called for more research in habit, while others have called for alternative theoretical mechanisms in predicting technology use to extend research in this area (Bagozzi, 2007).

Martin-Morich Model of Consumer Behavior Adapted to Information Security

Compelling research from diverse fields including neuroscience, cognitive, social and behavioral psychology, and behavioral economics, reveals that most human behavior is predominantly the result of unconscious mental processes. When a person is in a familiar situation doing repetitive tasks, behavior rapidly becomes automatic, not open to conscious control. This research challenges the conventional wisdom embedded in most models of human behavior that posit humans are rational agents making conscious decisions.

The impact of these research streams to information security is profound. At the core of all security assumptions is that users are capable of following directions that require conscious attention to behaviors performed in highly habitual settings. From this perspective, it seems logical to assume that explaining information security policies to users should be sufficient to obtain compliance. Yet, a high percentage of security breaches are caused by unconscious user behavior, which is immune to all appeals that rely on conscious mind attention and control. We propose adapting the Martin-Morich

model of consumer behavior (shown in Figure 1) to develop an improved approach to information security.

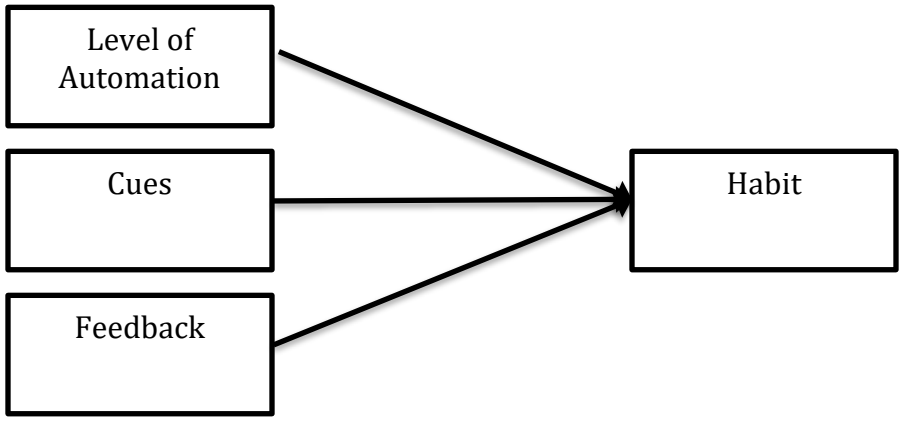

Figure 1: Martin-Morich Model

The Determinants of Habitual Behavior

Habits are automatic behaviors that are activated by cues in a stable context independent of goals and intentions. They are pre-potent, quick to activate, do not require conscious intervention, and are persistent (Wood and Neal, 2009). The Martin-Morich model posits a dynamic process where the conscious and unconscious minds both participate in guiding decisions and behavior. Decisions and behaviors that are made repeatedly in stable contexts become increasingly habitual. Decisions and behaviors that

are novel or occur in situations that are not familiar are more heavily influenced by the conscious mind. The model is designed to more closely reflect real world experiences where habitual behaviors can be disrupted by something that gets the attention of the conscious mind, and even highly complex behaviors can become habitual with sufficient repetitions.

Because the model describes a dynamic process, there is not a clear beginning or end. Behaviors under analysis might be new or ongoing for years. The model is designed to describe the process by which behavior becomes habitual over time and how it is possible to disrupt established habits.

In the next few sections we provide an explanation of the tenets of the model.

Level of Automation

Behavior is the culmination of a complex interplay between conscious and unconscious mental processes. The Martin-Morich model places behavior along a continuum of habit formation, with fully conscious behavior (pilot mode) on one end, and completely automatic behavior (autopilot mode) on the other. Between these extremes are heuristics (co-pilot mode) where simple rules govern behavior in familiar situations with multiple plausible behavioral responses. Contrary to human perception, most behavior is generated from the autopilot side of the spectrum (Verplanken et al., 2005).

It is important to understand the intensity of the habitual behavior under study to comprehend the risk profile for violating information security policies and procedures. Behavior that leads to high levels of habituation will inadvertently create greater security risks.

Pilot Mode

Pilot mode describes behaviors that are entirely or largely under the influence of the conscious mind. Pilot mode is engaged in novel situations where established behavioral repertoires do not exist and in situations that are highly important, highly salient, or highly risky.

To engage in conscious thought requires effort, and the conscious mind fatigues rapidly. This is a primary flaw in most security assumptions. There is a pervasive naïve presumption that users will follow security practices if they understand them, and if punishments are in place if they do not. “The defining feature of System 2 (the conscious mind) is that its operations are effortful, and one of its main characteristics is laziness….” (Kahneman, 2011). It is this laziness that causes the conscious mind to shift familiar tasks to the unconscious mind as quickly as possible.

A good information security example of this is passwords. Rules for passwords include not using the same password for multiple accounts and not using easy to remember passwords. In other words, passwords are designed to work against the way the brain works. Predictably, the most frequent calls to IT help lines is forgotten passwords (Witty and Brittain, 2004). Due to this reason, employees also have a tendency to share passwords in a team setting (Grosse and Upadhyay, 2013). However, that is due to not only the password being difficult to recall, but due to an element of trust that exists as being part of a team (Sasse et al., 2001).

Co-pilot

Co-pilot mode describes behaviors that have been repeated in stable environments but introduce conditional changes. For example, at the grocery store a shopper might develop a heuristic to stock up when a particular item goes on sale. Heuristics are quite

common in working with information systems as users develop shortcuts based on varying responses from programs, devices and other users. Most users receive a large volume of emails every day and unconsciously develop heuristics about which emails are responded to. For example, an employee may reply to an email in an order that is dependent on who sent it. An urgent email from a supervisor may dictate first response, whereas messages from unidentifiable resources may be deleted. In this scenario, an attacker may assume that an employee has certain heuristics, and therefore may create a message that spoofs a supervisor.

The conscious and unconscious minds work together to solve innumerable tasks throughout the day. Heuristics are simplified decision sets that can be described as the conscious mind intervening minimally to perform an action that is familiar. Heuristics also represent a threat to security because the conscious mind may not be sufficiently engaged to properly understand the security implications of a given behavior. For example, people in buildings that require badges to unlock doors might hold open the door for a woman, an elderly person, or someone with their hands full.

Autopilot

Autopilot mode represents behaviors that are repeated automatically without the need for conscious involvement. The transition from conscious to unconscious action can be seen in learning to type, where the conscious mind is at first heavily taxed, but quickly shifts learning of finger placement to the unconscious. The conscious mind thinks the word, the unconscious mind types. Once learned, the user's typing speed is negatively impacted by the intrusion of the conscious mind, as when a user looks at the keyboard.

Autopilot mode works outside of conscious awareness, and its workings are not available to conscious introspection. This means that a user may perform a behavior unknowingly that violates a policy that they understand and agree with. An example of this is Microsoft's Vista operating system. In attempting to make Vista more secure, the designers forced users to click an "allow" button before tasks that might open up the computer to intrusion. But the 'allow' button was activated for numerous routine permissions, causing acceptance to become unconscious. This new habit defeats the purpose and effectiveness of this information security solution.

The unconscious mind works automatically and effortlessly; a user cannot turn it off. This means to a large degree even when someone is consciously interacting with an information system, there is still a significant amount of information being processed by the unconscious mind. Often what the user might describe as a Pilot decision is simply the conscious mind accepting a decision presented by the habitual mind. Moreover, because the conscious mind requires will and effort, it exhausts rapidly. Expecting users to remain consciously vigilant in highly contextualized environments is unrealistic.

Habits form in stable contexts; situations that become familiar through unchanging repetition—like most workspaces. Established contexts signals the conscious brain that it does not have to pay attention; that routines that have worked before can be executed without conscious mind attention. Anyone who works in front of a computer screen for hours at a time, looking at the same programs, the same walls, sitting in the same chair for hours a day forms a uniquely powerful context. This is the central challenge to all efforts at information security; the very nature of working with PCs and programs puts people in highly habit-forming contexts. Considering that one of the

greatest threats an organization faces is from insiders (Warkentin and Willison, 2009), employees in a highly contextualized environment may be so used to sharing their passwords with team mates, that may inadvertently share it with someone who they initially may not have trusted. Password sharing continues to be a serious issue even though security education and training campaigns are carried out by organizations on a regular basis (Whitty et al., 2015).

Based on the concept of level of automation, we posit the following:

H1: Password sharing in a highly contextualized group environment will result in creation of a habit.

Cues

Cues are stimuli that have become triggers of habitual behavior in contextualized situations. The human brain is inundated with millions of stimuli, the vast majority of which are not processed by the conscious mind. However, when a behavior becomes closely associated with a context, specific stimuli become cues that trigger that behavior, such as responding instantly to an email. Cues are often built into information systems to create a desired behavior, such as a distinct sound to alert the user that a task needs to be performed. Once users become trained to automatically respond to a cue, they may respond to that cue inappropriately. A common example of this would be to absent-mindedly click on a link (Benenson et al., 2015) that could be a part of a phishing campaign. However, as explained in the autopilot section, it is the unconscious mind that is ultimately making that decision. Vishwanath et al. (Vishwanath et al., 2011) suggested that habitual patterns of IT interactions with high levels of email load influenced an individual's likelihood of being phished.

Therefore we posit:

H2: Phishing due to a high number of cues will result in creation of a habit.

Feedback

Feedback is anything that occurs after a behavior has the potential to be viewed as a consequence of that behavior. Outcomes that increase the likelihood that a behavior will be repeated are termed reinforcing. Those that make a behavior less likely to occur are termed punishing. This is how the unconscious mind learns, by associating an act with a result. The closer in time between action and feedback, the more powerful the association (Kandel, 2008). Generally speaking the purpose of security policies is to ensure compliance via a feedback mechanism (Warkentin et al., 2011). Though this technique has worked in the past, in the mobile cloud computing environment information security compliance continues to be a major concern (Kaufman, 2009). Velte et al. (Velte et al., 2009) specified the ease of working in the cloud computing environment due to a plethora of applications (Velte et al., 2009). However, in an organization setting regardless of convenience, security of mobile based cloud applications is a concern (Rittinghouse and Ransome, 2009). Delays between a request and feedback can be especially problematic as it would impact the user experience and later use of applications. (Tsai et al., 2009). The role of habit in this setting was highlighted by Venkatesh et al. (Venkatesh et al., 2000) who found that, after 3 months using an IS, the only significant predictor of later use was prior use; other factors were insignificant. It has also been stated that there is a correlation between ease of use of a system and habit formation (Burton-Jones and Hubona, 2006).

Therefore we posit:

H3: Cloud service technologies with adequate feedback mechanisms will result in creation of a habit of continued use.

We had an opportunity to test our model at a large healthcare facility. A description of the site is presented in the next section.

Research Site, Training Program Development, and Challenges

Caregiver is considered a leader in the healthcare arena and is based in the United States. It employs over 2000 physicians and scientists, as well as over 40,000 staff. The employees are not only vast in number but are also widely distributed. The organization also spends over $100 million each year on research, and security education, training, and awareness is already embedded at the organization. However, it is planning to extend traditional information security techniques to the behavioral aspect that revolves around unconscious behavior. This reason along with the fact that Caregiver is considered to be a leader in healthcare makes it an appropriate site for our research.

The challenges in providing training for Caregiver's personnel and associates are legion. We interviewed the head of the information security division at Caregiver. According to him, clinical professionals from physicians and nurses to technicians and adjunct staff have little time for training, are not motivated to learn about information security, and have highly variable knowledge regarding information technology. Some of the other challenges according to the division head include the following:

1. Clinical professionals automatically prioritized patient care above information security.
2. Historically, healthcare has been a low priority for hackers due to a lack of standardized platforms that would make hacking profitable. Because of this,

information security has been seen as an IT function as opposed to a globally shared responsibility.

3. Caregiver has an extensive network of contractors and external vendors, as well as medical staff distributed around the world making training even more important while simultaneously more difficult to provide.
4. As a leading medical research organization and globally recognized leader in medical training, creation and sharing of information is paramount to progress

Conversely, according to the division head the need for information security in healthcare in general, and information security training specifically, is increasing in urgency. According to the division head federal regulations require adoption of standardized software platforms to exchange patient information that makes hacking healthcare providers inevitable.

The division head cited three cases of security breaches involving healthcare. The Anthem data breach exposed nearly 80 million customers' personal information, including names, birthdays and Social Security numbers (Mathews, 2015). Eleven million Premera Health Insurance records were accessed by hackers, exposing confidential information including Social Security numbers and patients' medical information (Vinton, 2015). Finally, hackers accessed the records of 4.5 million UCLA Health System patients, stealing names, medical records, Social Security numbers, health plan IDs, birthdays and physical addresses (Pagliery, 2015).

The division head concedes that information technology is increasingly part of patient care at Caregiver. Caregiver uses a proprietary Healthcare Information System (HIS) that integrates all aspects of patient care and administration. Digitization of patient

records facilitates diagnosis and treatment, but also requires Caregiver to implement broader IT solutions including the ability to store and retrieve large data files (SAN, NAS), high availability networks, and wireless networks. According to the division head, digital records provide a powerful incentive for hackers while simultaneously creating innumerable opportunities for security breaches. He further stated that extensive use of mobile devices enable doctors and other clinicians, as well as patients to readily access and share medical information. However, each device is one more potential entry point for hackers. Ubiquitous connectivity increase the likelihood that users will access secure information over insecure networks such as free Wi-Fi and home networks. Connected medical devices are now being implanted in patients that not only communicate back to medical care givers, but are also programmable.

The division head also mentioned that Caregiver is aware that hacking is a global enterprise and patient information is a lucrative commodity. Medical records are going for a high multiple above financial records alone, with estimates according to the division head going from $20 to $50 per patient account. Hospitals and other health systems are far behind retail and financial institutions in prevention, training, and reporting. This aspect of healthcare has gained traction over the past few years (Thompson, 2014). It was further stated that health-care companies lacked many of the basic protections that security experts would expect in a company's network, e.g. encryption. Also, according to the division head the trend of pushing sensitive data outside of an organization's protected environment via cloud computing, mobile identity and access, and the Internet of Things (IoT) demands that security be pushed closer to the actual data. This presents a serious challenge to Caregiver's information security division. Many of the most

devastating data breaches are not from sophisticated hackers using state of the art attacks, but from simple exploits that rely on all-too-common user error (Liginlal et al., 2009).

Finally, the division head stated that at the core of the relationship between patients and healthcare providers is trust, and central to trust is confidentiality. Exposing a patient's medical records not only creates the nightmare of identify theft and the potential of insurance fraud, but the possible release of confidential health information which could disrupt patient willingness to share information with healthcare providers.

Training Program Development and Research Method

In order to design a successful information security training program for Caregiver, we used a three-phase approach.

Phase One: Assessment

In the first phase we worked closely with Caregiver's information security team to understand the organization's current approach to information security including secure network access, encryption, password policies, and biometrics. All training had to be customized to support current Caregiver policies regarding security. According to the head of Caregiver's information security division, the organization recognizes that some of the main information security threats it faces include phishing, use of unauthorized cloud services (e.g. Dropbox instead of proprietary encrypted one), and password sharing. Not surprisingly, previous literature in IS and complementary fields has commented on the importance of addressing these domains of information security (Wright and Marett, 2010, Vishwanath et al., 2011, Crossler et al., 2013, Takabi et al., 2010, Stanton et al., 2005, Ferreira et al., 2013, Zviran and Haga, 1999).

We also worked with various sub-organizations that received information security training to understand all of the contexts under which personnel engage in behavior that could lead to a data breach. We shadowed representatives from each group and performed interviews to better understand behavior. We wanted to diagnose the behavior to determine risks posed by unconscious and conscious processes. Within each context, we coordinated with Caregiver's information security group to determine appropriate information security behavior.

Phase Two: Develop Training Program

Our approach to training was based on educating participants on the principles and goals of information security, and repeating behaviors in context. The training program utilized a metaphorical framework that helped participants understand the why of information security without the need to understand the how or what of information security. Metaphor based training has proven to be successful (Lehto and Landry, 2012). The importance of using metaphors to create mental models in the field and its possible role in traditional research has also been discussed (Meyer, 1984, Mohammed et al., 2010). An analogy we used to explain why an encrypted cloud service should be used was training people to wash their hands to prevent the spread of disease without needing to explain germ theory. In the case of phishing the analogy was to incorporate a circle of trust. The circle had various layers, similar to an onion. The closer an individual to the center, the more trustworthy he or she was. If an email was from a person or organization that was distant from the center, then the employee should stop and think about the possible repercussions. In the case of password sharing, we asked the individuals to think about what they would do if someone asked for their ATM PIN.

The training combined a very short classroom session followed by behavior training in context. By repeating proper behavior in those situations identified from Phase One, critical neural pathways were created that activated automatically without the need for conscious thinking. The development of these neural pathways has been researched by Decety and Grezes (Decety and Grèzes, 1999).

Mindfulness training was included to train personnel when it was critical for them to consciously evaluate a situation from an information security perspective.

Phase Three: Implementation

Initial training was conducted on randomly selected groups within each department at Caregiver to test effectiveness within specific contexts and insure success of the behavioral approach. As already mentioned, we created customized training for employees. We had three groups: administrators (mostly managers), medical professionals (included physicians, physician assistants etc.) and staff (appointment coordinators, billing specialists etc.). Each one of these was randomly assigned to a treatment group (received behavioral training) and a control group (did not receive behavioral training). We also carried out pre- and post-tests for each group using a proprietary automated testing system. The tests dealt with phishing, use of unauthorized cloud services, and password sharing. Behavioral monitoring through technology is something that has not been extensively researched in IS (Crossler et al., 2013). However, the value of measuring actual behaviors instead of intentions has been noted in various studies (Anderson and Agarwal, 2010, Mahmood et al., 2010, Warkentin et al., 2012, Straub, 2009). In the next few sections we provide how the tests were carried out

at Caregiver. In some cases we were given data directly due to it being of a sensitive nature.

Phishing

We simulated two (one as a pre test and the other as a post test) targeted phishing campaigns based on an employee's classification. For example, a medical professional received an email asking them to click on a link that would purportedly take them to a website that had a listing of speakers from a major medical conference. Members of staff received an email that referred them to a website they could use to register for an advanced training session that would be paid for by Caregiver. Finally, the administrators were sent an email that asked them to go to a website that talked about upcoming updates to HIPAA (Health Insurance Portability and Accountability Act). In each case the testing system allowed us to not just monitor the number of clicks, but also trace it back to the user. We also had access to a listing of unique visitors.

Use of Unauthorized Cloud Services

According to the information security division, Caregiver subscribes to a proprietary cloud service that encrypts data. However, the division based on it's own monitoring system stated that only 20% of the employees use that service. Based on our research, the reasons for those included ease and intuitiveness of using alternatives such as Dropbox, compatibility and transferability of alternatives on various mobile and desktop platforms, the speed at which data could be accessed, and overall lack of familiarity with Caregiver's cloud service. Unlike phishing, for this portion of our study we had access to aggregated data of each user group that was provided to us by Caregiver.

Password Sharing

The current system used by Caregiver (HIS) implements single sign on technology. According to Caregiver, once again based on their own monitoring system, a high portion (45%) of their employees at some point share their credentials with other employees. This percentage is especially high in areas where health decisions supersede all others (e.g. critical care unit and ER). Based on training sessions some of the reasons cited for this included a new employee who did not have credentials for the system, an overall sense of trust in situations that required life or death decisions to be made, and a sense that nothing personal could be gained by having access to the HIS.

Habits and Security Threats

As a supplement to our work at Caregiver, we decided to look at existing literature that investigated habits, phishing, password sharing, and unauthorized cloud service use. We were able to adapt some of the measures (habits, phishing, and password sharing) that have appeared in the past. For unauthorized cloud service use we had to implement new measures based on existing research in cloud services adoption in the mobile and desktop environments (Botts et al., 2010, Doukas et al., 2010, Nkosi and Mekuria, 2010).

All items used the following response scale.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Table 1 shows the constructs that were used as part of the instrument development.

Table 1: Instrument Development

Constructs	**Measures**	**Sources**
Habit		
HA1	The use of HIS has become a habit for me	

HA2	I am addicted to using HIS	Adapted from Limayem and Hirt (Limayem and Hirt, 2003)
HA3	I must use HIS	
HA4	I don't even think twice before using HIS	
HA5	Using HIS has become natural to me	
Password Sharing		
PA1	I share my password with my team	Adapted from Stanton et al. (Stanton et al., 2005)
PA2	I share my password with another member of Caregiver	
PA3	I share my password with someone outside Caregiver	
Phishing		
PH1	There were suspicious words, phrases or sentences	Adapted from Sheng et al. (Sheng et al., 2007)
PH2	There were suspicious links	
PH3	There were grammatical or spelling errors in the e-mail	
PH4	The email contained pop-up boxes or attachments	
PH5	The email contained an air of urgency or a need to respond immediately	
PH6	The email asked for personal information	
Unauthorized Cloud Services Use		
CS1	Technology that adapts to mobility is important for me	
CS2	Current file sharing system is too cumbersome	
CS3	Current file sharing system is not functional	

The next section provides details of how we validated the survey, along with results of our pre- and post tests.

Results

The survey was first distributed to the information security division head at Caregiver. The reason for that was to ensure that the questions maintained anonymity of

the organization. For validation of the instrument we administered the survey at a comparable healthcare institution, which though was not the same size as Caregiver, it too participated in all areas Caregiver does but on a limited scale. 256 employees participated in the survey out of a total of 950.

We tested for convergent validity. Table 2 shows the loadings of the measures, as well as descriptive statistics of the measures. All measures fulfilled the recommended levels of composite reliability (0.70 or above) and average variance extracted (0.50 or above) (Fornell and Larcker, 1981).

Table 2: Psychometrics and Descriptive Statistics

Construct	Item	Loading	Mean	S.D.	t-value	Skewness	Kurtosis
Habit (CR = 0.91, AVE = 0.71)	HA1	0.81	4.22	1.07	30.22	-0.33	-0.21
	HA2	0.79	4.31	1.14	39.65	-0.56	0.45
	HA3	0.89	4.56	1.19	41.99	-0.53	0.42
	HA4	0.90	4.41	1.13	42.22	-0.58	0.60
	HA5	0.95	4.47	1.09	29.98	-0.41	0.49
Password Sharing (CR = 0.89, AVE = 0.76)	PA1	0.83	4.01	0.09	40.19	-0.21	0.25
	PA2	0.81	4.11	0.12	43.65	-0.24	0.30
	PA3	0.78	4.24	0.07	42.86	-0.20	0.24
Phishing (CR = 0.95, AVE = 0.75)	PH1	0.87	4.54	1.17	29.64	-0.33	-0.24
	PH2	0.93	4.64	1.10	29.87	-0.30	-0.21
	PH3	0.92	4.61	1.12	42.22	-0.32	-0.19
	PH4	0.95	4.62	1.19	41.09	-0.29	-0.20
	PH5	0.90	4.55	1.15	41.18	-0.35	-0.28

	PH6	0.88	4.51	1.16	40.20	-0.29	-0.18
Unauthorized Cloud Services Use (CR = 0.72, AVE = 0.55)	CS1	0.71	4.45	1.40	10.90	-0.90	0.29
	CS2	0.72	4.09	1.37	11.32	-0.83	0.24
	CS3	0.74	3.29	1.41	12.99	-0.76	0.30

NB: CR = composite reliability; AVE = average variance extracted

We also tested for discriminant validity, which was verified because the square root of the average variance extracted for each construct was higher than the correlations between it and all of the other constructs. Table 3 shows the results.

Table 3: Squared root of average variance extracted and correlation

	HA	PA	PH	CS
Habit (HA)	0.84			
Password Sharing (PA)	0.72	0.87		
Phishing (PH)	0.63	0.53	0.87	
Unauthorized Cloud Services Use (CS)	0.34	0.42	0.19	0.74

Overall, we were able to provide satisfactory support for reliability, convergent validity, and discriminant validity of the instrument.

Figure 2 presents the PLS results with explanatory powers, estimated path coefficients (significant paths indicated with an asterisk), and associated t-value of the paths.

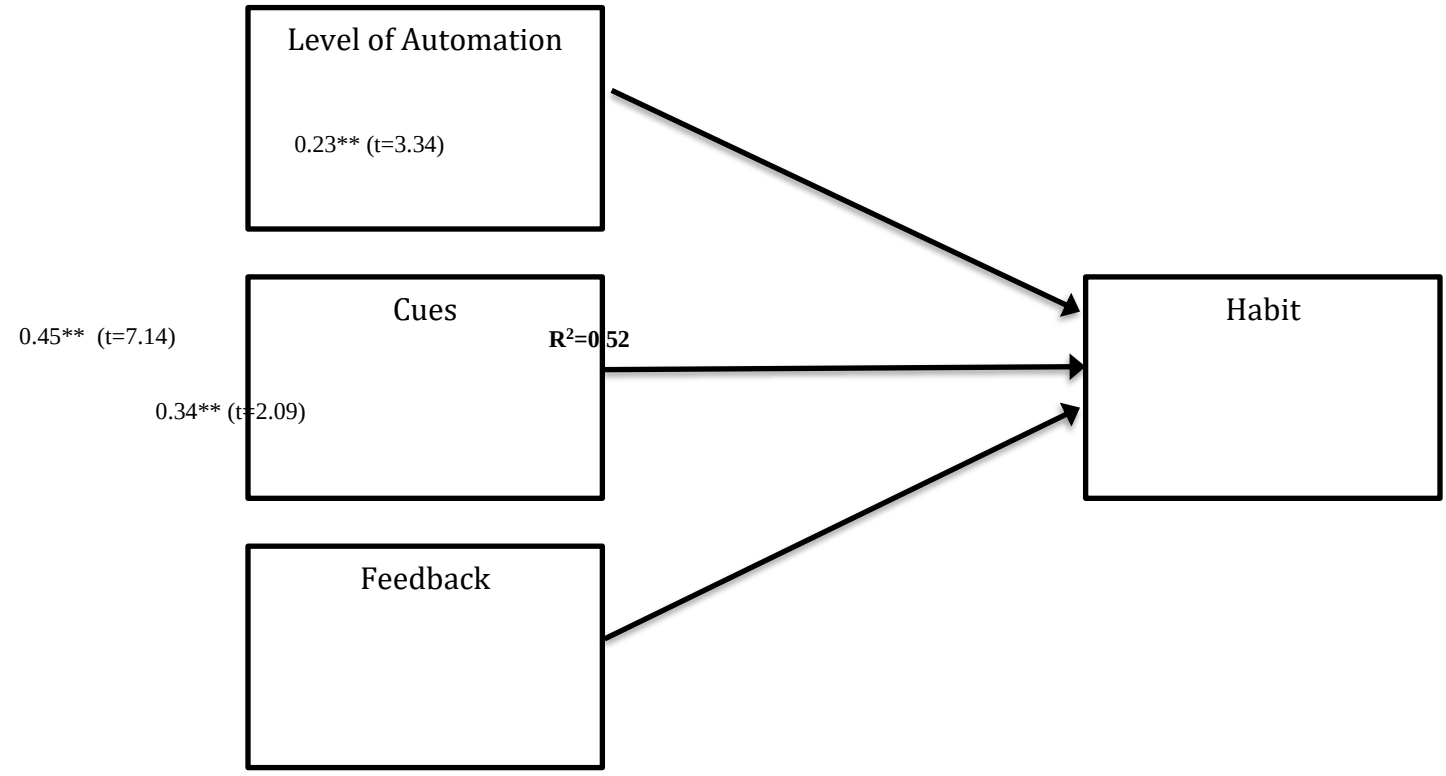

Figure 2: Results of PLS Analysis

Bootstrapping resampling procedure was used for significance testing of all paths. All hypothesized paths (H1, H2, and H3) in the research model were found to be statistically significant. Level of automation, cues, and feedback had a significant impact on habit, with path coefficients of 0.23, 0.45, and 0.34 respectively. The three constructs accounted for 52% of the variance in habit.

Next we provide results of the pre- and post-tests along with the survey parts of our study.

The pre-test window covered three weeks. The post-test window was the same time frame. A total of 343 employees were a part of the pre- and post-tests. The initial number was 345, however 2 were unable to complete because they left Caregiver. Table 4 provides details of the participants of the study.

Table 4: Study Participants

	Medical Professionals (MP)	Staff (ST)	Administrators (AD)
Male	59	76	25
Female	47	125	11
Total	106	201	36

180 participants received habit-based training (treatment group), with the rest (163) relying solely on the basic training that Caregiver provides to all its employees every two years (control group). Table 5 shows the breakdown of employees based on treatment and control groups.

Table 5: Group Totals

	MP	ST	AD
Treatment Group	54	100	19
Control Group	52	101	17

Table 6 presents an overview of the treatment and control groups using chi squared tests. The first value in each cell represents the total number of employees for which we were able to capture instances of either phishing, password sharing and unauthorized cloud service usage. The second value represents the expected cell totals, which is followed by the chi-square statistic for each cell.

	Threats	Pre-test			Post-test		
		MP	ST	AD	MP	ST	AD

Treatment Group (total 180)	**Phishing**	49 (42.37) [1.04]	64 (50.29) [3.74]	9 (7.58) [0.26]	21 (27.63) [1.59]	19 (32.71) [5.75]	4 (5.42) [0.37]
	Password Sharing	40 (31.96) [2.02]	53 (38.35) [5.60]	1 (0.53) [0.42]	18 (26.04) [2.48]	9 (23.65) [9.07]	0 (0.47) [0.47]
	Cloud Service	48 (40.45) [1.41]	78 (60.69) [4.94]	7 (5.79) [0.25]	23 (30.55) [1.86]	21 (38.31) [7.82]	2 (3.21) [0.46]
Control Group (total 143)	**Phishing**	43 (49.63) [0.89]	59 (72.71) [2.58]	12 (13.42) [0.15]	39 (32.37) [1.36]	61 (47.29) [3.97]*	11 (9.58) [0.21]
	Password Sharing	41 (49.04) [1.32]	67 (81.65) [2.63]	8 (8.47) [0.03]	48 (39.96) [1.62]	65 (50.35) [4.26]	8 (7.53) [0.03]
	Cloud Service	50 (57.55) [0.99]	82 (99.31) [3.02]	2 (3.21) [0.46]	51 (43.45) [1.31]	80 (62.69) [4.78]	3 (1.79) [0.83]

Table 6: Pre and Post Test Results

After comparing each threat instance's pre- and post test scores against each group (treatment against control) we get the following chi statistics (Table 7):

Table 7: Chi-Square Statistics

	MP	ST	AD
Phishing	4.87*	16.04*	0.99
Password Sharing	7.44*	21.56*	0.94
Cloud Service	5.57*	20.56*	2.00

* significant at $p<0.05$

Based on these results, we can see that habit based training positively impacted medical professionals and staff in their adherence to information security policies and controls as they relate to phishing, password sharing, and unauthorized cloud service access at Caregiver. The same cannot be said for administrators. Though we saw a slight variation in raw numbers, we simply did not have enough administrators in our sample that could participate.

Discussion of Results at Caregiver

We had an opportunity to discuss our results with executives at Caregiver. They provided us with unique perspectives that just showed how far healthcare has come. These are not only relevant to Caregiver, but to all healthcare organizations as well. Information technology has expanded geometrically at Caregiver over the past two decades with the advent of digital/electronic patient records (EMR and EHR), advanced imaging technologies (MRI, PET Scan, etc.), broadband networks (wired and wireless), and device technologies (flat panel monitors, laptops, smartphones, and tablets). These advances have put tremendous pressure on IT departments that must develop networks and data storage to not only handle massive data files, but also to make the information readily and easily accessible to a wide range of authorized users across an ever increasing range of devices. In addition, new communications technologies also continue apace with text, social media, and thousands of apps fundamentally changing how patients and healthcare providers interact.

Each advance in information technology that can be used for healthcare creates a potential problem for Caregiver from the perspective of information security. Based on our research at Caregiver we believe information gains value when it is relevant, reliable, accurate, timely, rich, fast, easy to access, easy to use, cheap, customizable, and secure. Unfortunately, the easier it is to access and use information, the more difficult it is to secure it. Where IT department at the Caregiver used to centrally control security, the new architecture is massively distributed where BYOD (bring your own device) has become standard operating procedure. The reflex to download a patient report at a local coffee shop's free Wi-Fi while grabbing a cappuccino can easily override hours of information security education. This insight into behavior helps explain why such a high

percentage of Caregiver's personnel clicked on a phishing email exploit even though they had all gone through security education, training, and awareness session once every two years.

Implications and Conclusion

As shown in this study, any behavior that is repeated in similar contexts will become habitual. Habits are automatic behaviors that operate outside of conscious awareness. They occur within contexts, where cues trigger behavior without requiring conscious thought. Habits are efficient and pre-potent—more powerful than other types of thoughts. And this is why most information security education at times fails to adequately change behavior that leads to breaches, identify theft, and loss of critical data files.

The value of information is automatically prioritized based on the dynamics of any given situation—doctors will consciously violate information security to help a patient, but will also unconsciously violate it when tired, stressed, or preoccupied without any malicious intent. In fact, the unintentional exposure of sensitive information is almost 83% higher for healthcare organizations than for other industries overall (Filkins, 2014). Nurses, technicians, administrators, and contractors experience variations of these challenges with the same outcome—unintentional violations of information security policies and procedures, which account for roughly half of all data breaches. For both the practitioner and researcher this means that security training and awareness programs need to be customized for groups. The habits that are formed in varied contextualized environments by doctors are different from nurses. Habit based research as stated

previously continues to be underrepresented. We believe that needs to change in order to further the agenda of information security in general, and healthcare in particular.

References

Anderson, C. L. & Agarwal, R. 2010. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly,* 34**,** 613-643.

Bagozzi, R. P. 2007. The Legacy of the Technology Acceptance Model and a Proposal for a Paradigm Shift. *Journal of the Association for Information Systems,* 8**,** 244-254.

Benbasat, I. & Barki, H. 2007. Quo vadis TAM? *Journal of the Association for Information Systems,* 8**,** 211-218.

Benenson, Z., Lenzini, G., Oliveira, D., Parkin, S. & Uebelacker, S. Maybe Poor Johnny Really Cannot Encrypt-The Case for a Complexity Theory for Usable Security. Proc. of the New Security Paradigm Workshop, 2015.

Botts, N., Thoms, B., Noamani, A. & Horan, T. A. Cloud computing architectures for the underserved: Public health cyberinfrastructures through a network of healthatms. System Sciences (HICSS), 2010 43rd Hawaii International Conference on, 2010. IEEE, 1-10.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly,* 34**,** 523-548.

Burton-Jones, A. & Hubona, G. S. 2006. The mediation of external variables in the technology acceptance model. *Information & Management,* 43**,** 706-717.

Chen, Y., Ramamurthy, K. & Wen, K.-W. 2012. Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems,* 29**,** 157-188.

Cheng, L., Li, Y., Li, W., Holm, E. & Zhai, Q. 2013. Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *computers & security,* 39**,** 447-459.

Cheung, C. & Limayem, M. 2005. The role of habit in information systems continuance: examining the evolving relationship between intention and usage. *ICIS 2005 Proceedings***,** 471-482.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M. & Baskerville, R. 2013. Future directions for behavioral information security research. *computers & security,* 32**,** 90-101.

D'arcy, J. & Herath, T. 2011. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems,* 20**,** 643-658.

De Guinea, A. O. & Markus, M. L. 2009. Why break the habit of a lifetime? Rethinking the roles of intention, habit, and emotion in continuing information technology use. *Mis Quarterly,* 33**,** 433-444.

Decety, J. & Grèzes, J. 1999. Neural mechanisms subserving the perception of human actions. *Trends in cognitive sciences,* 3**,** 172-178.

Doukas, C., Pliakas, T. & Maglogiannis, I. Mobile healthcare information management utilizing Cloud Computing and Android OS. Engineering in Medicine and

Biology Society (EMBC), 2010 Annual International Conference of the IEEE, 2010. IEEE, 1037-1040.

Ferreira, A., Correia, R., Chadwick, D., Santos, H. M., Gomes, R., Reis, D. & Antunes, L. 2013. Password sharing and how to reduce it. *IT Policy and Ethics: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications.*

Filkins, B. 2014. *New Threats Drive Improved Practices: State of Cybersecurity in Health Care Organizations* [Online]. Available: http://www.sans.org/reading-room/whitepapers/analyst/threats-drive-improved-practices-state-cybersecurity-health-care-organizations-35652 [Accessed September 27 2015].

Fornell, C. & Larcker, D. 1981. Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of Marketing Research,* 18**,** 382-388.

Grosse, E. & Upadhyay, M. 2013. Authentication at scale. *Security & Privacy, IEEE,* 11**,** 15-22.

Herath, T. & Rao, H. R. 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems,* 18**,** 106-125.

Jasperson, J., Carter, P. E. & Zmud, R. W. 2005. A Comprehensive Conceptualization of the Post-Adoptive Behaviors Associated with IT-Enabled Work Systems. *MIS Quarterly,* 29**,** 15.

Kahneman, D. 2011. *Thinking, fast and slow,* New York, Macmillan.

Kandel, E. 2008. *In search of memory,* Oregon Health and Science University.

Kankanhalli, A., Teo, H. H., Tan, B. C. Y. & Wei, K. K. 2003. An integrative study of information systems security effectiveness. *International Journal of Information Management,* 23**,** 139-154.

Kaufman, L. M. 2009. Data security in the world of cloud computing. *Security & Privacy, IEEE,* 7**,** 61-64.

Kim, S. S. & Malhotra, N. K. 2005. A longitudinal model of continued IS use: An integrative view of four mechanisms underlying postadoption phenomena. *Management Science,* 51**,** 741-755.

Kim, S. S., Malhotra, N. K. & Narasimhan, S. 2005. Research note—two competing perspectives on automatic use: A theoretical and empirical comparison. *Information Systems Research,* 16**,** 418-432.

Lee, S. M., Lee , S. G. & Yoo, S. 2004. An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management,* 41**,** 707-718.

Lehto, M. R. & Landry, S. J. 2012. *Introduction to human factors and ergonomics for engineers*, Crc Press.

Liginlal, D., Sim, I. & Khansa, L. 2009. How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security,* 28**,** 215-228.

Limayem, M. & Cheung, C. M. 2008. Understanding information systems continuance: The case of Internet-based learning technologies. *Information & management,* 45**,** 227-232.

Limayem, M. & Hirt, S. G. 2003. Force of habit and information systems usage: Theory and initial validation. *Journal of the Association for Information Systems,* 4**,** 65-97.

Limayem, M., Hirt, S. G. & Cheung, C. M. 2007. How habit limits the predictive power of intention: the case of information systems continuance. *MIS Quarterly,* 31**,** 705-737.

Mahmood, M. A., Siponen, M., Straub, D., Rao, H. R. & Raghu, T. 2010. Moving toward black hat research in information systems security: an editorial introduction to the special issue. *MIS Quarterly,* 34**,** 431-433.

Martin, N. & Morich, K. 2011. Unconscious mental processes in consumer choice: Toward a new model of consumer behavior. *Journal of Brand Management,* 18**,** 483-505.

Mathews, A. 2015. *Anthem: Hacked Database Included 78.8 Million People* [Online]. The Wall Street Journal. Available: http://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364 [Accessed September 25 2015].

Meyer, A. D. 1984. Mingling decision making metaphors. *Academy of Management Review,* 9**,** 6-17.

Mohammed, S., Ferzandi, L. & Hamilton, K. 2010. Metaphor no more: A 15-year review of the team mental model construct. *Journal of Management,* 36**,** 876-910.

Nkosi, M. & Mekuria, F. Cloud computing for enhanced mobile health applications. Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on, 2010. IEEE, 629-633.

Ouellette, J. A. & Wood, W. 1998. Habit and intention in everyday life: the multiple processes by which past behavior predicts future behavior. *Psychological bulletin,* 124**,** 54-74.

Pagliery, J. 2015. *UCLA Health hacked, 4.5 million victims* [Online]. CNN. Available: http://money.cnn.com/2015/07/17/technology/ucla-health-hack/ [Accessed September 24 2015].

Pahnila, S., Siponen, M. & Mahmood, A. Employees' Behavior Towards IS Security Policy Compliance. 40th Hawaii International Conference on System Sciences, 2007. 156b.

Ponemon. 2015. *The Unintentional Insider Risk in United States and German Organizations* [Online]. Available: http://www.raytheoncyber.com/spotlight/ponemon/pdfs/3P-Report-UnintentionalInsiderResearchReport-Ponemon.pdf [Accessed September 15 2015].

Rittinghouse, J. W. & Ransome, J. F. 2009. *Cloud computing: implementation, management, and security,* UK, CRC press.

Sasse, M. A., Brostoff, S. & Weirich, D. 2001. Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal,* 19**,** 122-131.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J. & Nunge, E. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. Proceedings of the 3rd symposium on Usable privacy and security, 2007. ACM, 88-99.

Sneha, S. & Varshney, U. 2009. Enabling ubiquitous patient monitoring: Model, decision protocols, opportunities and challenges. *Decision Support Systems,* 46**,** 606-619.

Stanton, J. M., Stam, K. R., Mastrangelo, P. & Jolton, J. 2005. Analysis of end user security behaviors. *Computers & Security,* 24**,** 124-133.

Straub, D. Black hat, white hat studies in information security. Keynote Presentation of the 1st IFIP 8.2 Security Conference, 2009 Cape Town, South Africa.

Straub , D. W. 1990. Effective IS Security. *Information Systems Research,* 1**,** 255-276.

Straub, D. W. & Nance, W. D. 1990. Discovering and disciplining computer abuse in organizations: a field study. *MIS Quarterly,* 14**,** 45-60.

Takabi, H., Joshi, J. B. & Ahn, G.-J. 2010. Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy,* 8**,** 24-31.

Thompson, C. 2014. *Hackers are coming after your medical records* [Online]. CNBC. Available: http://www.cnbc.com/2014/05/29/hackers-are-coming-after-your-medical-records.html?__source=ft&par=ft [Accessed September 24 2015].

Thorngate, W. 1976. Must we always think before we act? *Personality and Social Psychology Bulletin,* 2**,** 31-35.

Tsai, J. Y., Kelley, P., Drielsma, P., Cranor, L. F., Hong, J. & Sadeh, N. Who's viewed you?: the impact of feedback in a mobile location-sharing application. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2009 California, US. ACM, 47-58.

Vance, A., Siponen, M. & Pahnila, S. 2012. Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management,* 49**,** 190-198.

Velte, T., Velte, A. & Elsenpeter, R. 2009. *Cloud computing, a practical approach,* NY, McGraw-Hill, Inc.

Venkatesh, V., Morris, M. G. & Ackerman, P. L. 2000. A longitudinal field investigation of gender differences in individual technology adoption decision-making processes. *Organizational behavior and human decision processes,* 83**,** 33-60.

Venkatesh, V., Thong, J. Y. & Xu, X. 2012. Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Quarterly,* 36**,** 157-178.

Verplanken, B., Aarts, H., Knippenberg, A. & Knippenberg, C. 1994. Attitude versus general habit: antecedents of travel mode Choice1. *Journal of Applied Social Psychology,* 24**,** 285-300.

Verplanken, B., Aarts, H. & Van Knippenberg, A. 1997. Habit, information acquisition, and the process of making travel mode choices. *European Journal of Social Psychology,* 27**,** 539-560.

Verplanken, B., Aarts, H., Van Knippenberg, A. & Moonen, A. 1998. Habit versus planned behaviour: A field experiment. *The British Journal of Social Psychology,* 37**,** 111-128.

Verplanken, B., Myrbakk, V. & Rudi, E. 2005. The measurement of habit. *In:* BETSCH, T. & HABERSTROH, S. (eds.) *The routines of decision making.* NJ.

Vinton, K. 2015. *Premera Blue Cross Breach May Have Exposed 11 Million Customers' Medical And Financial Data* [Online]. Forbes. Available: http://www.forbes.com/sites/katevinton/2015/03/17/11-million-customers-

medical-and-financial-data-may-have-been-exposed-in-premera-blue-cross-breach/ [Accessed September 25 2015].

Vishwanath, A., Herath, T., Chen, R., Wang, J. & Rao, H. R. 2011. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems,* 51**,** 576-586.

Warkentin, M., Johnston, A. C. & Shropshire, J. 2011. The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems,* 20**,** 267-284.

Warkentin, M., Straub, D. & Malimage, K. Measuring secure behavior: A research commentary. Annual Symposium on Information Assurance & Secure Knowledge Management, 2012 Albany, NY. Citeseer, 5-6.

Warkentin, M. & Willison, R. 2009. Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems,* 18**,** 101-105.

Whitty, M., Doodson, J., Creese, S. & Hodges, D. 2015. Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. *Cyberpsychology, Behavior, and Social Networking,* 18**,** 3-7.

Witty, R. & Brittain, K. 2004. Automated password reset can cut IT service desk costs. *Gartner Report*.

Wood, W. & Neal, D. T. 2009. The habitual consumer. *Journal of Consumer Psychology,* 19**,** 579-592.

Workman, M. & Gathegi, J. 2007. Punishment and ethics deterrents: A study of insider security contravention. *Journal of the American Society for Information Science and Technology,* 58**,** 212-222.

Wright, R. T. & Marett, K. 2010. The influence of experiential and dispositional factors in phishing: an empirical investigation of the deceived. *Journal of Management Information Systems,* 27**,** 273-303.

Zviran, M. & Haga, W. J. 1999. Password security: an empirical study. *Journal of Management Information Systems,* 15**,** 161-185.