AIS Transactions on Human-Computer Interaction

Volume 9 | Issue 1 Article 4

3-30-2017

Toward a More Secure HRIS: The Role of HCI and Unconscious Behavior

Humayun Zafar
Kennesaw State University, hzafar@kennesaw.edu

Adriane B. Randolph
Kennesaw State University, arandol3@kennesaw.edu

Neale Martin
Sublime Behavior

Recommended Citation

Zafar, H., Randolph, A. B., & Martin, N. (2017). Toward a More Secure HRIS: The Role of HCI and Unconscious Behavior. *AIS Transactions on Human-Computer Interaction, 9*(1), 59-74. Retrieved from https://aisel.aisnet.org/thci/vol9/iss1/4
DOI:

Transactions on Human – Computer Interaction

Theory & Review Paper

Toward a More Secure HRIS: The Role of HCI and Unconscious Behavior

Humayun Zafar
Kennesaw State University, USA
hzafar@kennesaw.edu

Adriane B. Randolph
Kennesaw State University, USA

Neale Martin
Sublime Behavior, USA

Abstract:

By design, human resource information systems (HRIS) hold confidential and sensitive information. Therefore, one needs to ensure the security of these systems from unintentional mistakes that may compromise such information. Current systems design and training procedures of HRIS unintentionally help reinforce unsecure behaviors that result in non-malicious security breaches. Measures to improve security through design and training may only occur by breaking the use/impact cycle that individuals have habitually formed. Using strong contexts and cues allow trainers to interrupt individuals' habits. Then, they have the opportunity to enforce the repetition of the desired behavior. This paper introduces a model of habit formation from consumer behavior that one may apply to HRIS.

Keywords: Security, Privacy, Human Resource Management.

The manuscript was received 12/13/2015 and was with the authors 5 months for 4 revisions.

1 Introduction

Organizations have increasingly begun to use human resource information systems (HRIS) to capture, store, and use data about their employees. A HRIS is "a system used to acquire, store...analyze...and distribute information regarding an organization's human resources" (Kavanagh, Thite, & Johnson, 2015, p. 17). HRIS also include the interaction of people, policies, procedures, and data to manage the HR function (Hendrickson, 2003). As such, HRIS include a great deal of sensitive and confidential data about employees (e.g. social security numbers, medical data, bank account data, salaries, domestic partner benefits, employment test scores, and performance evaluations) (DeSanctis, 1986; Kovach & Cathcart, 1999). The more employee information in each data record, the more valuable the record becomes for malicious agents. For that reason, aggregated data from HRIS are designed to be shared among only an appropriate, approved audience, and system features are designed to help force good practices. Thus, the risk of a security breach presents significant challenges for human resources and employees. Organizations can be liable for identity theft caused by these data breaches and employees can be stigmatized if negative personal data leaks.

For this reason, organizations need to protect their employee data as effectively, if not more, as their other corporate data. Several studies have focused on how to educate employees and to develop more effective and secure acceptable use policies (CITES). Despite this, a high number of serious security breaches continue to plague organizations (Ponemon, 2012). Thus, clearly, one should consider other factors such as interface design and unconscious employee behavior as well.

Right or wrong, humans' repeated behaviors guide them. What one chooses to focus on and do over and again soon fades to something innate and unconsciously executed. Unconscious habits form the center of human behavior (which holds true in our personal and professional lives, for trivial and non-trivial tasks, and for secure and unsecure behaviors. Yet we have largely underestimated and misunderstood such habits (Martin, 2008). Organizations hope to ingrain correct, secure behaviors in their employees through policy and education, but these procedures may be contrary to unsecure behaviors they repetitively reinforce. Thus, a favored quote by professor and historian, Will Durant, has more salience: "We are what we repeatedly do. Excellence, then, is not an act, but a habit.". Here, we may relax the notion of "excellence" and instead be satisfied with "correct, secure behavior" by employees.

Traditional research in human-computer interaction (HCI) has examined the design and usability components of technology as intended rather than the use/impact cycle (Zhang & Li, 2005). The use/impact cycle concerns how individuals and organizations actually use technology and the related impact they have on them. By under-emphasizing the use/impact cycle of technology, researchers have predominantly ignored the impact that unconscious behavior may have. In this work, we present a behavioral model, along with propositions that build on existing theory, to guide future research in this area. We expressly examine secure and unsecure behaviors in the context of HRIS due to their criticality in organizations.

The paper proceeds as follows. In Section 2, we discuss the importance of privacy and security for employee data and how organizations have responded to security concerns. In Section 3, we review existing research in the areas of security and habit-based research and the consciousness of behavioral intention in HCI. In Section 4, we present our research framework, which builds on the Martin-Morich model of consumer behavior (Martin & Morich, 2011). In Section 5, we discuss determinants of habitual behavior and present a series of propositions guide future research. In Section 6, we discuss the results and, in Section 7, conclude the paper.

2 Background

Given the growing concern about identity theft and the security of employee data in HRIS, some states in the US (e.g., Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Missouri, South Carolina, and Washington) have passed privacy laws that require organizations to adopt reasonable security practices to prevent unauthorized access to personal data (National Conference of State Legislatures, 2015). Despite these new laws, in one survey, 43 percent of businesses confessed that they did not put any new security solutions in place to prevent the inadvertent release or access to employee data, and almost half of them did not change any internal policies to ensure that data were secure (Ponemon, 2012). A clear example of this practice is when the Office of Personnel Management (OPM) experienced a data breach that exposed millions of records (Eng, 2015).

According to another study, almost 40 percent of all security breaches in organizations are non-malicious in nature and typically result from complacency or negligence (PRNewsWire, 2014). As for why, it may be possible that non-malicious behavior is closely tied to cues from the interface (both software and hardware) and the nature of the interaction that employees have with HRIS; it is possible that the interface and technology interaction contribute to complacency in employees. A particular result of such interaction is the use of weak passwords, a major culprit of security breaches (Ives, Walsh, & Schneider, 2004; Zviran & Haga, 1999). As systems grow more complex, HRIS password requirements grow in terms of strength and incorporation of non-meaningful items. Unfortunately, employees may find it more natural to continue using weak passwords.

From a human-computer interaction (HCI) perspective, recalling a strong password is a tough task (Grawemeyer & Johnson, 2011). Essentially, information security relies on designing solutions that work diametrically opposite to the way employees' brains work naturally. It is important to avoid unaided recall wherever possible because it places a burden on a person's cognitive load and ability to perform (Sweller, 1994). As a result of this cognitive overload, an employee may default to some unconscious behavior that ultimately results in an error or security breach.

Though employees receive education on proper procedures and HRIS systems feature conscientious design features, employees still engage in unconscious behaviors that are unsecure. For example, employees who are logged into HRIS may absentmindedly plug unauthorized USB drives into their computers and, thus, cause a chain reaction that leaks sensitive employee data without realizing it. In another common example, due to stringent HRIS password requirements, employees may write passwords on a piece of paper stuck on the side of their monitors. Thus, unconscious behavior can defeat the best efforts of security and design experts. In other words, all of the security protocols in the world are powerless in the face of a stressed-out worker (Bandyopadhyay, Mykytyn, & Mykytyn, 1999; Greitzer & Frincke, 2010).

We consider unconscious behaviors here as synonymous with habitual behaviors because something done repeatedly becomes ingrained (Verplanken & Van Knippenberg, 1998). Once that behavior becomes habitual, deliberate intentions have less impact to the point of irrelevance (Triandis, 1979). Thus, HRIS are particularly prone to creating habit-based security risks at the individual or enterprise level based for several reasons:

1. HRIS contain the type of information that employees are likely to access from multiple devices and locations.
    - Employees access these systems when dealing with various life events (i.e., births/deaths) and often do so away from the work setting.
    - The frequency of accessing data from various networks will likely create routines that will lead to habitual behavior.
2. HRIS contain the type of information that employees often access under stressful conditions.
    - Personal information is needed immediately after an accident or when an employee's loved one is ill or injured.
3. HRIS passwords are typically complicated.
    - Complexity increases the likelihood that employees will write their passwords on a piece of paper or store them electronically on their computer or phone.
    - Employees need aids to reduce cognitive load.
4. Many HRIS functions are done routinely, which creates habitual behavior.
    - Employees execute habits without the need for conscious-level processing, which increases the likelihood of unsecure behavior (e.g., clicking on a link simply because that is what the user is used to doing).
    - Attempts to force employees into conscious-level processing may create frustration and compensatory behavior outside of information-security measures.

Further, by combining information from multiple databases and applications, a breach in one system is likely to create a breach in all systems and, thus, elevate an organization's risk.

3 Literature Review

This section comprises two parts. The first part presents relevant IS security and habit-based research. The second part references HCI literature regarding design-related behaviors and conscious and unconscious behavior.

3.1 Security and Habit Research

Since HRIS 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 HRIS. Fundamentally, traditional security research has a "behavioral root" (Workman & Gathegi, 2007) and is a subject of psychological and sociological actions of people. Most prior research in traditional organizational IS security—which is relevant to HRIS —has dealt with the success and failure of security policies by using a deterrence approach (Bulgurcu, Cavusoglu, & Benbasat, 2010; Chen, Ramamurthy, & Wen, 2012; Cheng, Li, Li, Holm, & Zhai, 2013; Herath & Rao, 2009; Straub & Nance, 1990).

A limited amount of work has investigated HRIS security. Zafar, Clark, and Ko (2011) looked at differences in perception between management and staff about HR security risk management in two companies. They found statistically significant differences in one of the companies and state that an organization's HR, information technology (IT), and executive branches need to effectively collaborate. Noting this gap, researchers have begun to develop conceptual frameworks of both a managerial and technical nature to enhance this field (Lippert & Swiercz, 2005; Noor & Razali, 2011; Zafar, 2013).

Habit-based research in IS mostly focuses on continuing technology use as an act that conscious (non-habitual) decision making drives (De Guinea & Markus, 2009). However, habit research also draws from literature in psychology to posit that much of continuing technology use is habitual. The argument is that, when technology use is habitual, an individual's intentions ceases to guide it (Thorngate, 1976).

Research has identified habitual IT use behavior in IS as repeated behavioral sequences that are automatically triggered by cues in the environment (Cheung & Limayem, 2005; Kim, Malhotra, & Narasimhan, 2005; Limayem & Hirt, 2003; Limayem, Hirt, & Cheung, 2007) and considered it to be a critical predictor of technology use (Kim & Malhotra, 2005). Using a moderation perspective, Limayem and Cheung (2008) illustrated that the predictive power of intention weakened with continued habitual behavior by individuals. Venkatesh, Thong, and Xu (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.

Research has also pointed to the role habits play when warnings users ignore warnings or routinely acknowledge notifications. For example, users click through half of all Secure Sockets Layer warnings in less than two seconds, which is consistent with warning fatigue (Akhawe & Felt, 2013). Further, employees' brains stop registering the novelty of security notifications due to the routine nature of clicking on similarly presented notifications over time (Anderson et al., 2015; Anderson, Vance, Kirwan, Eargle, & Jenkins, 2016). Research has also investigated the concept of warning and alert fatigue in clinical settings, which demonstrates the widespread applicability of habit formation (Kesselheim, Cresswell, Phansalkar, Bates, & Sheikh, 2011).

Studies have used various proxies for habit. For example, Kim and Malhotra (2005) equated past use to habit. 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" for habitual tendencies toward the choice of a certain travel mode (Verplanken, Aarts, Knippenberg, & Knippenberg, 1994; Verplanken, Aarts, & Van Knippenberg, 1997; Verplanken, Aarts, Van Knippenberg, & Moonen, 1998). In terms of their psychometric properties, research has not compared these measures to each other. Benbasat and Barki (2007) have called for more research on habit, while others have called for alternative theoretical mechanisms in predicting technology use to extend research in this area (Bagozzi, 2007).

Researchers have also investigated the interplay between compliance and habits. High propensity for compliance has been associated with high degree of security. Vance, Siponen, and Pahnila (2012) integrated habit with protection motivation theory (PMT) to explain compliance. The authors concluded that habitual compliance with security policies strongly reinforced the cognitive processes theorized by PMT. Interestingly, due to its general nature, other researchers who have investigated vulnerability and

severity in relation to compliance with security policies have used PMT (Herath & Rao, 2009; Johnston & Warkentin, 2010; Pahnila, Siponen, & Mahmood, 2007).

3.2 Consciousness of Behavioral Intention in HCI

Behavioral intention is often the focus of HCI as well. Researchers focus on where the user intends to move or what the user intends to select as captured in purposive and functional computing (Shneiderman & Plaisant, 2005; Yoo, 2010). They encourage designers to match the user's mental model of behavioral intention with what one expects from a system's layout, affordances, and responsiveness (Preece, Sharp, & Rogers, 2015). This recommended match implies that users can consciously access their mental maps and is reflected in popular elicitation techniques such as "talk aloud" and interviews. Thus, HCI questions have largely reflected the measurement tools available. Further, the field suggests that we may get closer to a match by incorporating users into the design process on the front end as with user-participation and user-centered design (Iivari, Treiblmaier, & Galletta, 2012) or by including system training on the back end (Santhanam, Yi, Sasidharan, & Park, 2013).

Increasingly, the field is appreciating the impact of unconscious processing on design assessment and individual performance with a system. Human-computer interaction researchers have examined aesthetics, emotion, and mood in conjunction with system use where they have found positive associations to enhance performance and perceptions (Cyr, Head, & Ivanov, 2006; Loiacono & Djamasbi, 2010). In addition, the neuro-information systems (neuroIS) subfield has shown the benefits of using neurophysiological tools and techniques to complement traditional psychometric tools to reflect unconscious processing (Dimoka et al., 2012; Riedl, Davis, & Hevner, 2014; Tams, Hill, Ortiz de Guinea, Thatcher, & Grover, 2014). The adoption of neuroscience-based tools into the IS field is still rather nascent and relegated to a limited community with access and knowledge of these tools. The knowledge, however, is accessible to all through the results of behavioral and social science research.

Overall, traditional HCI frameworks have largely considered interaction from a perspective of new use rather than integrated behavior, and we need a shift in paradigms as our interaction types have shifted (Lyytinen, 2010). With new use, individuals have not yet formed habit, which resides at the conscious level of mental processing. However, technology use is pervasive in our organizational and personal lives, and we must better appreciate how our unconscious, habitual behaviors affect our system use. In Section 4, we offer a model for application in the IS field for understanding habit and HRIS interaction.

4 Proposed Framework

Compelling research from diverse fields including neuroscience; cognitive, social and behavioral psychology; and behavioral economics reveals that most human behavior predominantly results from unconscious mental processes. When a person is in a familiar situation doing repetitive tasks, behavior rapidly becomes automatic and less open to conscious control. This research challenges the conventional wisdom embedded in most models of human behavior that posit humans are rational agents who make conscious decisions (Martin, 2008; Martin & Morich, 2011; Wood & Neal, 2009).

The impact of these research streams to HRIS security is profound. All security assumptions at their core assume that employees can follow directions that require conscious attention to behaviors performed in highly habitual settings. From this perspective, it seems logical to assume that explaining the policies to employees should be sufficient to obtain compliance. Yet, we argue that unconscious employee behavior causes a high percentage of security breaches, which is immune to all appeals that rely on conscious mind attention and control. We propose adapting the Martin-Morich model of consumer behavior (Martin & Morich, 2011) shown in Figure 1 to model employee consumption of HRIS. Such a model serves as a basis for understanding how we may develop an improved approach to HRIS information security achieved through more-informed interface design and training.

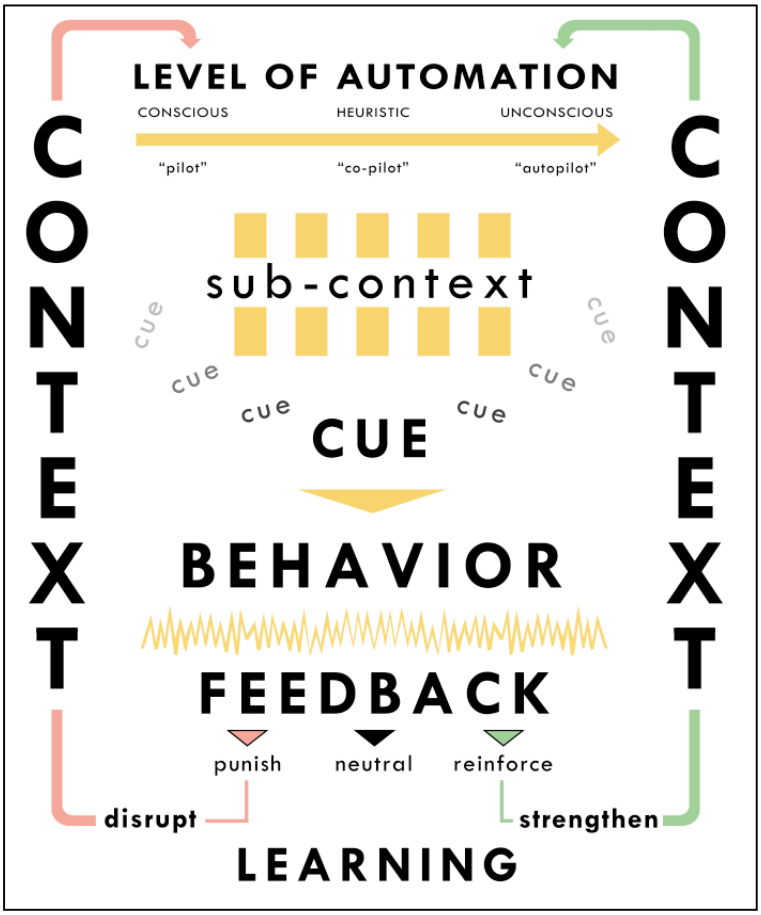

Figure 1. Martin-Morich Model of Consumer Behavior

We elect the Martin-Morich (2011) model over alternatives such as Lewin's (1972) three-step model for change. Lewin assumes that organizations operate in a stable state and that most of the projects undertaken are small scale in nature (Burnes, 2004). Cummings, Bridgman, and Brown (2016) further expand on the nature of Lewin's assumptions. Martin-Morich (2011), on the other hand, assume that individuals form true habits when they understand the complex sequence of cues, contexts, and feedback. Such complexity seems most reflective of IT contexts, which feature continuous change. Further, our proposed model incorporates newer insights gained about human behavior from social science research overlain with cognitive neuroscience.

5 The Determinants of Habitual Behavior

Habits are automatic behaviors that cues activate in a stable context independent of goals and intentions. They are quick to activate, do not require conscious intervention, and are persistent (Wood & Neal, 2009). Such behaviors are quite similar to the "system 1" thinking described by Kahneman (2003), who also supports the premise that an individual's cognitive response changes based on content and context. The proposed model posits a dynamic process where both the conscious and unconscious minds participate in guiding decisions and behavior. One's conscious mind more heavily influences decisions and behaviors that are novel or occur in unfamiliar situations. However, decisions and behaviors that one makes repeatedly in stable contexts become increasingly habitual. We designed the model to more closely reflect real-world experiences where something that gets the attention of the conscious mind can disrupt habitual behaviors and even highly complex behaviors can become habitual with sufficient repetitions.

Training is a common method to raise consciousness of proper security measures in an organization (Bulgurcu et al., 2010). For a new employee, training presents an unfamiliar situation in which to consciously practice sound security procedures. It is logical to think that employees may then repeat these sound security procedures and, thus, make the correct behavior habitual. However, one can see an

example of how habits can instead sabotage information security training in spear-phishing where emails and other message forms use specific information about an individual to trick people into lowering their guard and compromise a system (Hong, 2012).

While employees consciously know that they should not click on suspicious emails but are tired or stressed, they are likely to automatically click on an email that looks normal. For example, the OPM data breach exposed personal information on more than 21 million people, including information on people who were included in background checks but never became federal employees (Eng, 2015). One could use this information to design spear-phishing attacks that could easily defeat the reliance on an employee's conscious-level vigilance. Administrators of HRIS would be high-priority targets due to their access to the most valuable personnel data.

5.1 Strength of Habit

According to the Martin-Morich model (Martin & Morich, 2011), behaviors occur along a continuum of consciousness from primarily conscious to primarily unconscious (see Figure 1). The following describes each of three modes experienced along this continuum.

"Pilot" mode: novel situations focus the conscious mind's attention as do situations perceived as unusual or risky (e.g., a good example is when employees need to learn a new or updated software program). Conscious processing takes effort (Kahneman, 2003). As with passwords, tasks that require significant amounts of conscious effort routinely encourage employees to find shortcuts or workarounds to relieve their cognitive load (Sweller, 1994).

The two most popular passwords in 2014, unchanged from the several years prior, were "123456" and "password" (Condliffe, 2015). Websites and applications that require eight character passwords with at least one capitalization, one number, and one special character (i.e., passwords specifically hard for the human brain to remember or "strong" passwords) force employees to create password lists on their computers or write them down on a piece of paper.

"Co-pilot" mode: individuals who periodically encounter situations in which they can choose a decision among a small set of alternatives often develop heuristic processing. For example, employees often have annual decisions to make regarding contributions to retirement plans or charitable giving or selecting a healthcare plan. Rather than fully consciously evaluate each option, employees are likely to develop an informal rule that guides behavior, such as choosing the option recommended by the employer or simply electing the same plan options as the previous year.

"Autopilot" mode: behaviors that individuals repeat in similar situations create automatic habits that they execute without the need for conscious level goals, intentions, or oversight. Even complex behavior, if repeated enough times, will become habitual. Experts in an area develop a type of "neural efficiency" in which they exhibit lower activation levels and more concentrated areas of brain function (Neubauer & Fink, 2009). This neural efficiency allows streamlined thinking as with Kahneman's (2003) "system 2"; habits make behavior highly efficient and allow one to multitask in a way that cannot happen with conscious behavior. Because conscious processing takes effort and does not allow for multitasking, shifting behavior to habits is critical to efficiency. For example, employees often use their email systems as an informal filing system storing not only emails but also attachments. A similar set of habits have emerged around using multiple devices to access corporate email with mobile phones and tablets used unthinkingly to access and send emails (Cecchinato, Cox, & Bird, 2015).

Therefore, we posit:

> **P1**: One can enhance HRIS security by incorporating design and implementation practices that focus on the unconscious part of the behavioral spectrum.

5.2 Context and Cue

Habits form when one repeats a behavior in a similar situation, which becomes a context linking behavior to particular tasks that one needs to do (see Figure 1). The unconscious mind determines contexts based on perceptions of familiarity. Contexts can be very narrow (e.g., only making online purchases from a home computer) or broad (e.g., purchasing online from a mobile phone across any network). Once one creates a context, it provides the framework in which the habit functions. Most HRIS security training programs recommend that one look for clues such as misspellings or unusual requests to click on a link to

detect malicious emails. Malicious emails can potentially allow privileged information to leak to non-authorized sources, which amounts to trying to create a new context for employees: a malicious email context. It is easy to see why this education fails because individual do not encounter malicious emails in a stable situation. Indeed, the sender is trying very hard to make the email look like it belongs to the employee's familiar context.

Once an individual creates a habit in a context, a cue can activate it. Cues can be crafted to launch a behavior, such as the beep or vibration that signals an incoming text, or can form organically, such as the smell of fresh popcorn. The cue launches the behavior automatically, which eliminates the need for conscious processing to initiate behavior. Unintentional HRIS security lapses often happen when something cues a routine behavior as perhaps one learned in training in what appears to be a normal context.

Therefore, we posit:

P2: One can enhance HRIS security by designing systems that create strong contexts and cues.

5.3 Behavior and Feedback

Behavior goes through the same process as habit formation. Novel situations create new behaviors that conscious intention often guides. With repetitions over time, the behavior comes under the control of unconscious systems. This process is accelerated by reinforcing feedback and retarded by punishing feedback. HRIS security training assumes that education or information will lead to correct behavior and induce learning. However, as the model illustrates, the dynamic process of behaviors repeated over time leads to mental efficiency via transference of those behaviors to unconscious control. Such unconscious control cannot be overcome

Therefore, we posit:

P3: One can enhance HRIS security by focusing on repeating correct behavior as part of the HRIS training process.

The final sections describe implications for practitioners and researchers for how to incorporate desired behaviors into unconscious control via enhanced systems design and revised training procedures. Although with humans there will always be unexpected responses, employees working with HRIS should generally follow the Martin-Morich model (2011) for their behavior. Thus, if we hope to effect changes in behavior, we must break the use/impact cycle that individuals have habitually formed. Using strong contexts and cues allow one to interrupt others' habits. Then, one has the opportunity to enforce the repetition of desired behavior.

6 Discussion

Researchers wishing to undertake this agenda may design studies that incorporate more traditional psychometric tools, neurophysiological tools, or both. Inherently, a study will be longitudinal in nature to allow for the repetition of desired behavior to occur. During the pre- and post-tests participants, one may observe and survey participants and record their neurophysiological responses. However, we must note that, in recording neurophysiological responses, one creates a new context for the participant that will not mimic an everyday situation; most individuals do not conduct business wearing an electrode cap that records their brainwaves or have an eye-tracking device incorporated into their laptop to monitor the diameter of their pupils

After one administers a pre-test, training would begin. One should present and repeat different scenarios. During behavioral repetition, to reinforce desired behavior, one should provide strong cues alongside feedback for correct and incorrect behavior. For example, research has extended reinforcement used in "clicker training" with animals to humans (Pryor, 2009). For example, one could have a chime or click sound when a participant correctly indicates suspicion of an email with a suspicious URL in it versus no sound if the participant indicates nothing is amiss. The opposite would happen for a legitimate email. This repeated process would help reinforce desired action in the face of activities that threaten security when interacting with HRIS.

Practical implications of this work encourage managers to incorporate such repeated drills into training procedures that consider preferred actions in light of different security scenarios. One could also

incorporate stronger cues into HRIS to counteract risky behavior. Once practitioners appreciate the need to modify existing systems design and training procedures to counteract unconscious behavior, they will reinforce desired security behaviors and significantly reduce the risk undesired behaviors can have.

Such examinations have begun under a bourgeoning “neurosecurity” subfield (Anderson et al., 2015). This subfield of IS security research borrows knowledge from cognitive neuroscience as the Martin-Morich (2011) model presented here does. In proposing the Martin-Morich model, we help extend existing habit-based research in IS security with that in consumer behavior to help improve the security of HRIS.

7 Conclusion

Unconscious habits form the center of human behavior, yet research largely underestimates and misunderstands them. 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 percent of American survey respondents and 64 percent of German respondents stated that unintentional mistakes caused more security incidents than malicious acts (Ponemon, 2015). The study also considers the security, education, training, and awareness (SETA) programs that organizations have implemented. We contend that most unintentional mistakes result from habitual behavior that promotes an automatic response. Previous research supports the idea that automated behavior results from the force of habit (Jasperson, Carter, & Zmud, 2005; Kim et al., 2005; Ouellette & Wood, 1998). However, no one has investigated this issue in HRIS and HCI in any context. To better address this issue, we provide a framework that others can use in the future to investigate the role unconscious habits may play in the security of a HRIS.

References

Akhawe, D., & Felt, A. P. (2013). *Alice in warningland: A large-scale field study of browser security warning effectiveness.* Paper presented at the 22nd USENIX Security Symposium.

Anderson, B. B., Kirwan, C. B., Jenkins, J. L., Eargle, D., Howard, S., & Vance, A. (2015). *How polymorphic warnings reduce habituation in the brain: Insights from an fMRI study.* In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*.

Anderson, B. B., Vance, A., Kirwan, C. B., Eargle, D., & Jenkins, J. L. (2016). How users perceive and respond to security messages: A neuroIS research agenda and empirical study. *European Journal of Information Systems*, *25*(4), 364-390.

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*(4), 244-254.

Bandyopadhyay, K., Mykytyn, P. P., & Mykytyn, K. (1999). A framework for integrated risk management in information technology. *Management Decision, 37*(5), 437-445.

Benbasat, I., & Barki, H. (2007). Quo vadis TAM? *Journal of the Association for Information Systems, 8*(4), 211-218.

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*(3), 523-548.

Burnes, B. (2004). Kurt Lewin and the planned approach to change: A re-appraisal. *Journal of Management Studies, 41*(6), 977-1002.

Cecchinato, M. E., Cox, A. L., & Bird, J. (2015). *Working 9-5? Professional differences in email and boundary management practices. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*.

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems, 29*(3), 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*(B), 447-459.

Cheung, C., & Limayem, M. (2005). The role of habit in information systems continuance: examining the evolving relationship between intention and usage. In *Proceedings of the International Conference on Information Systems* (pp. 471-482).

Condliffe, J. (2015). The 25 most popular passwords of 2014: We're all doomed. *Gozmodo.* Retrieved from http://gizmodo.com/the-25-most-popular-passwords-of-2014-were-all-doomed-1680596951

Cummings, S., Bridgman, T., & Brown, K. G. (2016). Unfreezing change as three steps: Rethinking Kurt Lewin's legacy for change management. *Human Relations, 69*(1), 33-60.

Cyr, D., Head, M., & Ivanov, A. (2006). Design aesthetics leading to m-loyalty in mobile commerce. *Information & Management, 43*(8), 950-963.

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*(3), 433-444.

DeSanctis, G. (1986). Human resource information systems: A current assessment. *MIS Quarterly, 10*(1), 15-27.

Dimoka, A., Banker, R. D., Benbasat, I., Davis, F. D., Dennis, A. R., & Gefen, D. (2012). On the use of neurophysiological tools in IS research: Developing a research agenda for neuroIS. *MIS Quarterly, 36*(3), 679-702.

Eng, J. (2015). OPM hack: Government finally starts notifying 21.5 million victims. *NBC News.* Retrieved from http://www.nbcnews.com/tech/security/opm-hack-government-finally-starts-notifying-21-5-million-victims-n437126

Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with Computers, 23*(3), 256-267.

Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation. In C. W. Probst, J. Hunker, M. Bishop, & D. Gollmann (Eds.), *Insider threats in cyber security* (vol. 49, pp. 85-113). Berlin: Springer.

Hendrickson, A. R. (2003). Human resource information systems: Backbone technology of contemporary human resources. *Journal of Labor Research, 24*(3), 382-394.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM, 55*(1), 74-81.

Iivari, N., Treiblmaier, H., & Galletta, D. F. (2012). Introduction to the AIS THCI special issue on user participation/centeredness in new, challenging IS contexts. *AIS Transactions on Human-Computer Interaction, 4*(2), 44-50.

Ives, B., Walsh, K. R., & Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM, 47*(4), 75-78.

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*(3), 15.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549-566.

Kahneman, D. (2003). Maps of bounded rationality: Psychology for behavioral economics. *American economic review, 93*(5), 1449-1475.

Kavanagh, M. J., Thite, M., & Johnson, R. D. (Eds.). (2015). *Human resource information systems: Basics, applications, and future directions* (3rd ed.). Thousand Oaks, CA: Sage.

Kesselheim, A. S., Cresswell, K., Phansalkar, S., Bates, D. W., & Sheikh, A. (2011). Clinical decision support systems could be modified to reduce “alert fatigue” while still minimizing the risk of litigation. *Health Affairs, 30*(12), 2310-2317.

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*(5), 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*(4), 418-432.

Kovach, K., & Cathcart, C. (1999). Human resource information systems (HRIS): Providing business with rapid data access, information exchange and strategic advantage. *Public Personnel Management, 28*(2), 275-282.

Lewin, K. (1972). Frontiers in group dynamics: Concept, Method and reality in social equilibria and social change. *Human Relations, 1*(1), 5-41.

Limayem, M., & Cheung, C. M. (2008). Understanding information systems continuance: The case of Internet-based learning technologies. *Information & Management, 45*(4), 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*(1), 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*(4), 705-737.

Lippert, S. K., & Swiercz, P. M. (2005). Human resource information systems (HRIS) and technology trust. *Journal of Information Science, 31*(5), 340-353.

Loiacono, E., & Djamasbi, S. (2010). Moods and their relevance to systems usage models within organizations: an extended framework. *AIS Transactions on Human-Computer Interaction, 2*(2), 55-72.

Lyytinen, K. (2010). HCI research: Future directions that matter. *AIS Transactions on Human-Computer Interaction, 2*(2), 22-25.

Martin, N. (2008). *Habit: The 95% of behavior marketers ignore*. Upper Saddle River, NJ: Ft Press.

Martin, N., & Morich, K. (2011). Unconscious mental processes in consumer choice: Toward a new model of consumer behavior. *Journal of Brand Management, 18*(7), 483-505.

Neubauer, A. C., & Fink, A. (2009). Intelligence and neural efficiency. *Neuroscience & Biobehavioral Reviews, 33*(7), 1004-1023.

Noor, M. M., & Razali, R. (2011). *Human resources information systems (HRIS) for military domain-a conceptual framework.* Paper presented at the International Conference on Electrical Engineering and Informatics.

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*(1), 54-74.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Employees' behavior towards IS security policy compliance.* Paper presented at the 40th Hawaii International Conference on System Sciences.

Ponemon. (2012). 2012 *Business banking trust study*. Retrieved from http://info.guardianananalytics.com/rs/guardianananalytics/images/2012_Business_Banking_Trust_Study_Exec_Summary.pdf

Ponemon. (2015). The unintentional insider risk in United States and German organizations. Retrieved from http://www.raytheoncyber.com/spotlight/ponemon/pdfs/3P-Report-UnintentionalInsiderResearchReport-Ponemon.pdf

Preece, J., Sharp, H., & Rogers, Y. (2015). *Interaction design—beyond human-computer interaction*. NY: John Wiley & Sons.

National Conference of State Legislatures. (2015). Privacy protections in state constitutions. Retrieved from http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx

PRNewsWire. (2014). *Leading cause of data security breaches are due to insiders, not outsiders*. Retrieved from http://www.prnewswire.com/news-releases/leading-cause-of-data-security-breaches-are-due-to-insiders-not-outsiders-54002222.html

Pryor, K. (2009). *Reaching the animal mind: Clicker training and what it teaches us about all animals*. New York: Simon and Schuster.

Riedl, R., Davis, F. D., & Hevner, A. R. (2014). Towards a neuroIS research methodology: Intensifying the discussion on methods, tools, and measurement. *Journal of the Association for Information Systems, 15*(10), 1-10.

Santhanam, R., Yi, M. Y., Sasidharan, S., & Park, S.-H. (2013). Toward an integrative understanding of information technology training research across information systems and human-computer interaction: A comprehensive review. *AIS Transactions on Human-Computer Interaction, 5*(3), 134-156.

Shneiderman, B., & Plaisant, C. (2005). *Designing the user interface*. New York: Pearson.

Straub, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly, 14*(1), 45-60.

Sweller, J. (1994). Cognitive load theory, learning difficulty, and instructional design. *Learning and Instruction, 4*(4), 295-312.

Tams, S., Hill, K., Ortiz de Guinea, A., Thatcher, J., & Grover, V. (2014). NeuroIS—alternative or complement to existing methods? Illustrating the holistic effects of neuroscience and self-reported

data in the context of technostress research. *Journal of the Association for Information Systems, 15*(10), 723-753.

Thorngate, W. (1976). Must we always think before we act? *Personality and Social Psychology Bulletin, 2*(1), 31-35.

Triandis, H. C. (1979). *Values, attitudes, and interpersonal behavior.* Paper presented at the Nebraska Symposium on Motivation.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(3), 190-198.

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*(1), 157-178.

Verplanken, B., Aarts, H., Knippenberg, A., & Knippenberg, C. (1994). Attitude versus general habit: Antecedents of travel mode choice. *Journal of Applied Social Psychology, 24*(4), 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*(5), 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., & Van Knippenberg, A. (1998). Predicting behavior from actions in the past: Repeated decision making or a matter of habit. *Journal of Applied Social Psychology, 28*(15), 1355-1374.

Wood, W., & Neal, D. T. (2009). The habitual consumer. *Journal of Consumer Psychology, 19*(4), 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*(2), 212-222.

Yoo, Y. (2010). Computing in everyday life: A call for research on experiential computing. *MIS Quarterly, 34*(2), 213-231.

Zafar, H. (2013). Human resource information systems: Information security concerns for organizations. *Human Resource Management Review, 23*(1), 105-113.

Zafar, H., Clark, J. G., & Ko, M. S. (2011). An exploration of human resource management information systems security. *Journal of Emerging Knowledge on Emerging Markets, 3*(1), 1-28.

Zhang, P., & Li, N. (2005). The intellectual development of human-computer interaction research: A critical assessment of the MIS literature (1990-2002). *Journal of the Association for Information Systems, 6*(11), 227-292.

Zviran, M., & Haga, W. J. (1999). Password security: An empirical study. *Journal of Management Information Systems, 15*(4), 161-185.

About the Authors

Humayun Zafar is an Associate Professor of Information Security and Assurance in the Department of Information Systems at Kennesaw State University. He received his doctorate from the University of Texas at San Antonio in 2010. His research interests include organizational security risk management, network security, and organizational performance. His work has appeared in journals such as *Communications of the Association for Information Systems*, *Human Resource Management Review*, *Information Resources Management Journal*, *Information Systems Frontiers*, *Journal of Global Information Technology Management*, and *Journal of Information Privacy and Security*. He has also presented at academic and practitioner conferences such as the *Americas Conference on Information Systems*, *Hawaii International Conference on System Sciences*, *Mobility Live*!, and *SuperNova South*.

Adriane Randolph is the founder and executive director of the BrainLab and an Associate Professor of Information Systems in the Michael J. Coles College of Business at Kennesaw State University. She earned a Ph.D. in Computer Information Systems from Georgia State University and a B.S. in Systems Engineering with Distinction from the University of Virginia. Her research of over fourteen years focuses on brain-computer interface systems which allow for non-muscularly controlled assistive technologies and reflect varying cognitive states. Other research interests include human-computer interaction and neuro-information systems. She has been featured as a speaker for multiple TEDx events and was invited to be an original Google Glass Explorer. She has published manuscripts in the *International Journal of Human-Computer Interaction* and the *ACM Transactions on Accessible Computing*. Prior to academia, she worked for Accenture implementing change management and human performance tools in the federal government sector.

Neale Martin, PhD is founder and CEO of Sublime Behavior Marketing and author of Habit: the 95% of behavior marketers ignore and Mirages, Oases, and Roadkill on the Information Highway. He is former Professor of Innovation for Coles College of Management at Kennesaw State University. He received his doctorate from the Scheller School of Management, Georgia Institute of Technology. His work has appeared in *Journal of Brand Management*, and *Journal of Public Management and Social Policy*. He has also presented at marketing and brand conferences around the world.

Transactions on Human – Computer Interaction