Cybersecurity: Role of Behavioral Training in Healthcare

Emergent Research Forum Papers

Humayun Zafar Ph.D.
Kennesaw State University
hzafar@kennesaw.edu

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.

Keywords (Required)

Training, cybersecurity, healthcare

Introduction

Many security 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. 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). 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. 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 believe that 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. 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 on habits, a description of the research model that we adapted to information security, description of the research site and some preliminary results.

Literature Review

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). 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), and is considered to be a critical predictor of technology use (Kim and Malhotra 2005). 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 (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" to measure habitual tendencies toward the choice of a certain travel mode (Verplanken et al. 1997). In terms of their psychometric properties these measures have not been compared to each other.

Martin-Morich Model of Consumer Behavior Adapted to Information Security

When a person is in a familiar situation doing repetitive tasks, behavior rapidly becomes automatic, not requiring conscious control (Martin and Morich 2011). 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.

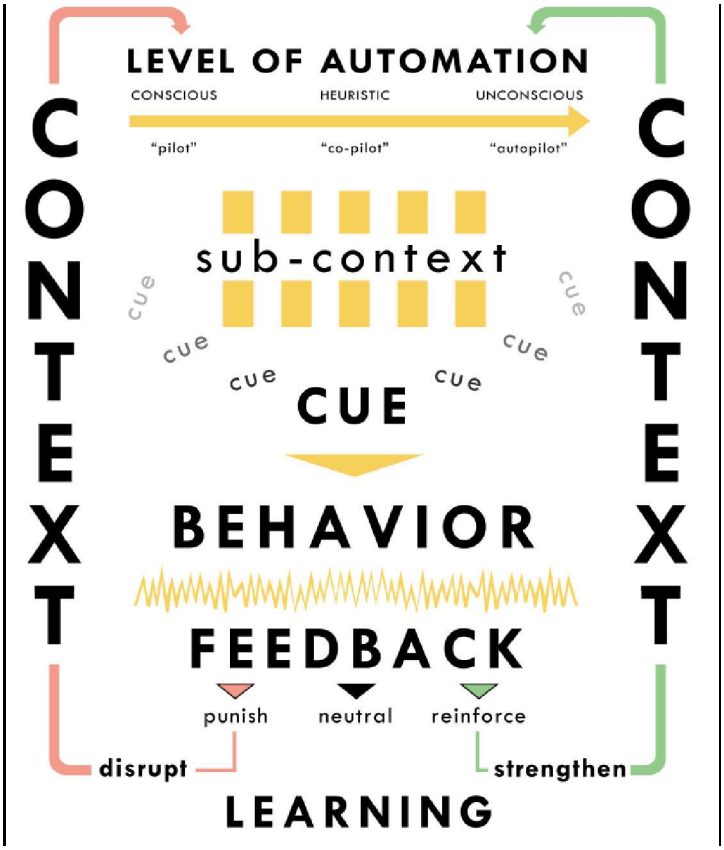

Figure 1: Martin-Morich Model Adapted for IT Security Threats

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. 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.

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.

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 (Ferreira et al. 2013; Wright and Marett 2010; Zviran and Haga 1999).

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.

Phase Three: Implementation

Initial training was conducted on randomly selected groups within each department at Caregiver to test effectiveness within specific contexts and ensure 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).

Table 1 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.

Table 1: Pre and Post Test Results

	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]

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

References

Benbasat, I., and Barki, H. 2007. "Quo Vadis Tam?," *Journal of the Association for Information Systems* (8:4), pp. 211-218.

Cheung, C., and Limayem, M. 2005. "The Role of Habit in Information Systems Continuance: Examining the Evolving Relationship between Intention and Usage," *ICIS 2005 Proceedings*:39), pp. 471-482.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research," *computers & security* (32), pp. 90-101.

De Guinea, A. O., and 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), pp. 433-444.

Ferreira, A., Correia, R., Chadwick, D., Santos, H. M., Gomes, R., Reis, D., and Antunes, L. 2013. "Password Sharing and How to Reduce It," in *It Policy and Ethics: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications*. pp. 22-42.

Kim, S. S., and Malhotra, N. K. 2005. "A Longitudinal Model of Continued Is Use: An Integrative View of Four Mechanisms Underlying Postadoption Phenomena," *Management Science* (51:5), pp. 741-755.

Kim, S. S., Malhotra, N. K., and Narasimhan, S. 2005. "Research Note—Two Competing Perspectives on Automatic Use: A Theoretical and Empirical Comparison," *Information Systems Research* (16:4), pp. 418-432.

Lehto, M. R., and Landry, S. J. 2012. *Introduction to Human Factors and Ergonomics for Engineers*, (2 ed.). Crc Press.

Limayem, M., and Cheung, C. M. 2008. "Understanding Information Systems Continuance: The Case of Internet-Based Learning Technologies," *Information & management* (45:4), pp. 227-232.

Limayem, M., and Hirt, S. G. 2003. "Force of Habit and Information Systems Usage: Theory and Initial Validation," *Journal of the Association for Information Systems* (4:1), pp. 65-97.

Martin, N., and Morich, K. 2011. "Unconscious Mental Processes in Consumer Choice: Toward a New Model of Consumer Behavior," *Journal of Brand Management* (18:7), pp. 483-505.

Meyer, A. D. 1984. "Mingling Decision Making Metaphors," *Academy of Management Review* (9:1), pp. 6-17.

Mohammed, S., Ferzandi, L., and Hamilton, K. 2010. "Metaphor No More: A 15-Year Review of the Team Mental Model Construct," *Journal of Management* (36:4), pp. 876-910.

Thorngate, W. 1976. "Must We Always Think before We Act?," *Personality and Social Psychology Bulletin* (2:1), pp. 31-35.

Venkatesh, V., Thong, J. Y., and Xu, X. 2012. "Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology," *MIS Quarterly* (36:1), pp. 157-178.

Verplanken, B., Aarts, H., and Van Knippenberg, A. 1997. "Habit, Information Acquisition, and the Process of Making Travel Mode Choices," *European Journal of Social Psychology* (27:5), pp. 539-560.

Wood, W., and Neal, D. T. 2009. "The Habitual Consumer," *Journal of Consumer Psychology* (19:4), pp. 579-592.

Wright, R. T., and Marett, K. 2010. "The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived," *Journal of Management Information Systems* (27:1), pp. 273-303.

Zviran, M., and Haga, W. J. 1999. "Password Security: An Empirical Study," *Journal of Management Information Systems* (15:4), pp. 161-185.