AMCIS 2015 Puerto Rico Paper Submission Information Security: Modeling the Unconscious Mind

Full Papers

Dr. Humayun Zafar
Kennesaw State University
hzafar@kennesaw.edu

Dr. Neale Martin
Sublime Behavior
nm@sublimebehavior.com

Abstract

We focus on the impact of individual habits of people on information security. More specifically, we ascertain the difference between conscious and unconscious errors in security breaches. Over the years, buzz words such as neuro-IS have come up, yet none have identified in a succinct manner, how issues pertaining to the human brain can be addressed.

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 IS managers tasked with information security (InfoSec) — many breaches occur when users are not consciously aware of what they are doing. Unconscious behavior can defeat the best efforts of security experts, meaning all of the security protocols in the world are powerless in the face of a stressed out worker. According to Microsoft's Security Intelligence report, 44.8% of vulnerabilities result from user action such as clicking a link, or being tricked into installing malware (Microsoft, 2011). The expense of breaches continues to escalate, with costs per incident totaling more than $7 million plus damaged reputations and loss of customer trust. Because of this, it is not a surprise that information security has attracted increased corporate attention. Security breach incidents not only cause a loss of customer goodwill and trust; but also have serious regulatory implications. Lewis (Lewis, 2003) concluded that human error accounted for over 65% of data breach incidents resulting in economic loss. Schultz (Schultz, 2005) referred to information security as being primarily a people problem – since technology is designed and managed by people, leaving opportunities for human error. Otto et al. (Otto, Antón, & Baumer, 2007) stated that an important measure put in place by Choice Point after a breach was aimed at addressing the problem of high error rates in customer records. Yet, even with numerous technical (firewalls, anti-virus, anti-spyware etc.) and non-technical (security education, training, and awareness) measures, the rate at which security breaches occur due to human error continue to trend upward. Our purpose is to identify a potential reason for this that has been largely overlooked in the literature. Based on our research, which we highlight in the next section, we contend that the answer lies in addressing the difference between conscious and unconscious errors in security breaches. This issue needs to be developed for any meaningful modeling. Unconscious habits form the center of human behavior, yet are largely underestimated and misunderstood. We adapt the Martin-Morich (Martin & Morich, 2011) model of behavior to information security.

Literature Review

Because users interact with information systems on a regular basis in their business 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 & 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. 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. Deterrent and preventive methods have a positive impact on information security effectiveness, but severity of the deterrence method does not (Kankanhalli, Teo, Tan, & Wei, 2003). Contrary to what is proposed by GDT, organizations with a high number of deterrent measures have higher incidents of insider abuse (Lee, Lee , & Yoo, 2004), indicating a significant negative relation between deterrent measures and insider abuse.

Prior studies have also focused on employee compliance to security policies. 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, Siponen, & Mahmood, 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 & 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.

There are a number of problems with the authors' approach to modeling IS that conflict with behavioral psychology that we will briefly address before introducing the Martin-Morich model. Pahnila et al. make a semantic error, confusing negative reinforcement with punishment. Reinforcement is any feedback that occurs after a behavior that makes that behavior more likely to occur in the future (Baker, Piper, McCarthy, Majeskie, & Fiore, 2004). A negative reinforcement is the removal of an aversive that occurs after a behavior, such as the silencing of an alarm clock by hitting a button. Positive reinforcement is a reward that occurs after a behavior. Punishment is any feedback that occurs after a behavior that makes the behavior less likely to occur. Positive punishment adds an aversive, while negative punishment takes away something that is perceived positively, such as taking away a favorite toy in response to a child's complaining.

In the authors' conceptualization, behavior can be made habitual "through making it mandatory initially or introducing rewards and other incentives." Feedback mechanisms facilitate habit formation by communicating to the unconscious mind a relationship between a behavior and a consequence. Incentives are offered before a behavior, and therefore do not directly influence habit formation.

Another structural problem of the model is the linkage between attitude, intention, and behavior. The literature suggests that attitude and intention only weakly predict behavior. One large meta-analysis showed that the correlation between attitude and behavior is less than 0.3. The linkage between intention and behavior is less than 0.5.

Pahnila et al. include habit in their model, but misapply the concept within their hypothesis.

H7. Habits affect an employee's intention to comply with IS security policies.

As a 'habit is unconscious or automatic behavior, as opposed to intentions or conscious behavior,' according to the authors, a habit by definition cannot affect an employee's intention to comply.

It is our contention that unconscious, habitual behavior is responsible for a large portion of InfoSec errors in ways that ultimately bypass most security policies, processes and procedures. In the next

section, we present a model based on our improved understanding of the roles of conscious and unconscious in terms of behavior that relates to InfoSec.

Model

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 InfoSec 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 the policies to users should be sufficient to obtain compliance. Yet, we will argue that 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.

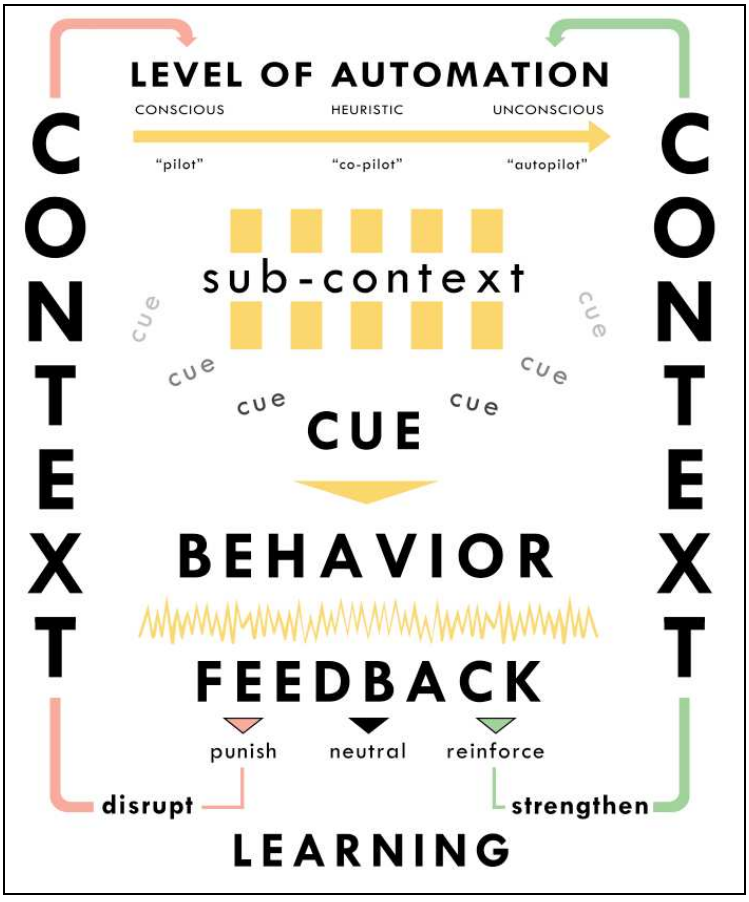

Figure 1: Martin- Morich Model of Consumer Behavior

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 prepotent, quick to activate, do not require conscious intervention, and are persistent (Wood & Neal, 2009). The 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.

We will explicate the model from the top down for convenience.

Level of Habit Formation

Behavior is the culmination of a complex interplay between conscious and unconscious mental processes. The 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.

It is important to understand the intensity of the habitual behavior under study to comprehend the risk profile for violating InfoSec policy 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…."[1] It is this laziness that causes the conscious mind to shift familiar tasks to the unconscious mind as quickly as possible.

A good InfoSec 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 (Forrester estimates between 25% and 40% of calls) is forgotten passwords (estimated by Gartner to cost $22 per call[2]).

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.

---

[1] Kahneman, Daniel, Thinking Fast and Slow; Farra, Straus and Giroux, New York

[2] "Automated Password Resets Cut IT Service Desk Costs. Gartner.

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 InfoSec 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.

Context

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 & Willison, 2009), employees in a highly contextualized environment may at times leave their workstations unattended to stroll around the office. However, if the computer is unlocked, it could provide an attacker with an opportunity to launch an attack.

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 a text message. 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.

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[3]. Unconscious pairing of actions and feedback train the unconscious mind outside of conscious mind control.

This important distinction, between educating the conscious mind and training the unconscious mind, must become imbedded in our approach to information and network security. It is not enough for users to know what they are supposed to do consciously; they must be trained sufficiently so that the unconscious mind operating on autopilot will do the right thing reliably.

An example of this process is learning to use a computer mouse. The movement of the hand creates an immediate movement of the cursor. The unconscious brain rapidly adapts because the cause effect is exact and instantaneous. In an innovative experiment[4], researchers programmed a mouse to move opposite of the way it was moved and then had subjects use the mouse while their hand and forearm were screened from view. After a few minutes of getting used to this arrangement, subjects perceived that their movements were in the same direction as the mouse, though they were actually moving in the opposite direction.

The closer in time a feedback is to a behavior, the more powerful the feedback, be it reinforcing or punishing. The more intense the feedback, the more impactful it is to habit formation. The more consistent a feedback is to a behavior, the more it leads to habit formation.

Strengthening Loop

When a dynamic situation links a behavior, a cue, and reinforcing feedback, it leads to habit formation. The more repetitions, the more unconscious and automatic the behavior becomes.

Disrupting Loop

Disruptions cause the conscious mind to attend to a situation. Disruptions can occur at any point of the behavioral cycle. For example, a new context or sub-context might emerge that would tweak behaviors, such as a new backup system or accessing an application from a smartphone that had been accessed from a desktop or laptop. Cues and feedbacks can similarly change in ways that disrupt automatic responses and creates a conscious evaluation. Even behaviors that are highly habitual can be disrupted if there is a breakdown across the dynamic chain of events.

Next Steps

Our next step is to setup an experiment at an organization. Based on preliminary work and research, we have realized that organizations may be better served if employee training pertaining to security also focuses on habits. For that reason the experiment will include at least two groups. The first group will include individuals who have been trained through traditional means. The second group will consist of people who have gone through habit training. We are going to carry out pre and post tests that last one month each in which employees will randomly be asked to complete tasks that may result in unsafe behavior.

Conclusion

InfoSec is an extremely diverse topic. It encompasses managerial and technical controls to protect assets from all sorts of threats, while also managing risks associated with information usage. However, there is an aspect of InfoSec that is often overlooked, which is ascertaining the difference between conscious and unconscious errors in security breaches. In 2010, an estimated $6 billion cost was incurred from stolen laptops, many of them thoughtlessly left in cars, coffee shops, or unlocked offices (Perolroth, 2011). This number does not represent the financial impact of reputation loss.

---

[3] Kandel, Eric In Search of Memory, pg. 199. W.W. Norton Company NY, NY.

[4] Bedford, F.L. *Of Computer Mice and Men*. Current Psychology of Cognition, 13, 405-426.

A modern day business, especially a large one, puts employees in an environment where they form habits that unintentionally lend themselves to InfoSec breaches. It is this portion of InfoSec research that needs to be further explored, understood, and designed for if the discipline is to address its most basic function.

References

Baker, T. B., Piper, M. E., McCarthy, D. E., Majeskie, M. R., & Fiore, M. C. (2004). Addiction motivation reformulated: an affective processing model of negative reinforcement. *Psychological review, 111*(1), 33-51.

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*(2), 139-154.

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*(6), 707-718.

Lewis, J. (2003). Cyber terror: Missing in action. *Knowledge, Technology & Policy, 16*(2), 34-41.

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.

Microsoft. (2011). Microsoft Security Intelligence Report Retrieved December 14, 2011, from http://www.microsoft.com/security/sir/default.aspx

Otto, P. N., Antón, A. I., & Baumer, D. L. (2007). The choicepoint dilemma: How data brokers should handle the privacy of personal information. *IEEE Security & Privacy, 5*(5), 15-23.

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.

Perolroth, N. (2011). Digital Data on Patients Raises Risk of Breaches Retrieved April 2, 2012, from http://www.nytimes.com/2011/12/19/technology/as-patient-records-are-digitized-data-breaches-are-on-the-rise.html

Schultz, E. (2005). The human factor in security. *Computers & Security, 24*(6), 425-426.

Sneha, S., & Varshney, U. (2009). Enabling ubiquitous patient monitoring: Model, decision protocols, opportunities and challenges. *Decision Support Systems, 46*(3), 606-619.

Straub , D. W. (1990). Effective IS Security. *Information Systems Research, 1*(3), 255-276.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems, 18*(2), 101-105.

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.