Eating the Forbidden Fruit: Human Curiosity Entices Data Breaches

Emergent Research Forum (ERF)

Dustin Ormond
Creighton University
DustinOrmond@creighton.edu

Hwee-Joo Kam
University of Tampa
hkam@ut.edu

Philip Menard
University of South Alabama
pmenard@southalabama.edu

Abstract

Data breaches across various industries infer that human curiosity has a powerful influence on information security behaviors. Drawing on Human Curiosity Theory, this study seeks to determine the impact that human curiosity has on information security policy violations despite the existence of training programs to increase information security awareness, the sanctions for violating information system policies, and the costs far exceeding the benefits associated with an information security violation. This study explores how human curiosity leads to data breaches by focusing on the innate desire of knowledge acquisition and the aversive emotional state resulting from knowledge deprivation. This leads to the two main objectives of this study: (1) identify and propose security countermeasures to curb insider curiosity and prevent data breaches and (2) present how Human Curiosity Theory challenges the notions of both General Deterrence Theory and Rational Choice Theory.

Keywords

Curiosity, data breaches, deterrence, rational choice

Introduction

Although curiosity leads to discovery and breakthroughs in scientific achievement (Loewenstein, 1994), it is not without drawbacks. A survey conducted by the German academics at Black Hat 2016 revealed that 34% of users clicked on a suspicious link due to curiosity (Benenson, Zinaida Gassmann, Freya Landwirth, 2016) regardless of information security awareness (ISA). Additionally, curiosity has led to unauthorized access and data breaches. For example, staff members in Orlando Regional Medical Center succumbed to curiosity and illegally accessed medical records of Pulse survivors, provoking anger and outrage in the LGBT Center of Central Florida (Grant, 2016). In 2017, a caregiver in the St. Charles healthcare system gained unauthorized access of 2,459 patients' records citing curiosity as the reason (Spurr, 2017).

We argue that human curiosity, stemmed from a *"cognitively induced deprivation"* of knowledge (Loewenstein, 1994), may overshadow perceived sanctions associated with security violation. General Deterrence Theory (GDT) posits that perceived sanctions on information systems (IS) misuse should deter IS abuse and security violations (D'Arcy, Hovav, & Galletta, 2009). For example, to foster HIPAA compliance, healthcare organizations have warned employees of sanctions for non-compliant behaviors. However, as new data breaches continue to hit the news, evidence suggests that perceived sanctions on IS misuse may not be enough. Prior studies have successfully examined neutralization as a reason for noncompliant actions (Barlow, Warkentin, Ormond, & Dennis, 2013, 2018; Siponen & Vance, 2010). A competing factor that has received less attention is that employees may succumb to their relentless *curiosity* such that they are aroused with an innate desire of knowledge acquisition in order to resolve puzzling objects (Berlyne, 1954).

We further suggest that human curiosity poses an anomaly for Rational Choice Theory (RCT), which proposes that employees' decisions of complying with an information security policy (ISP) are based upon perceived cost of non-compliance and perceived benefit of compliance (Bulgurcu, Cavusoglu, & Benbasat, 2010; Scott, 1999). Despite the perceived cost of violating ISP (in which the likelihood of getting caught and receiving severe disciplinary actions is high) and the perceived benefits of unauthorized data access (in which the gratification of learning the "secret" fades away rather quickly), some employees choose to violate ISP due to the insatiable thirst of curiosity. In the face of severe ramifications and long-term consequences of violating ISP, employees continue to violate ISP even for the brief moment of experiencing such fleeting rewards. Hence, our research questions (RQs) are:

RQ1: How does human curiosity overcome the perceived sanctions on IS misuse and the perceived cost of non-compliance to result in data breaches?

RQ2: What are the security countermeasures that could curb insider curiosity to bolster information security protection?

This study contributes to information security (InfoSec) research in the following ways. First, this study introduces Human Curiosity Theory to the InfoSec research and presents how this theory challenges GDT and RCT in the context of information security protection. Second, this study provides viable suggestions to curb employee's curiosity that will lead to unauthorized data access. Finally, this study is organized as follows. First, we present literature review. This is followed by theoretical framework. Next, we present conclusion and future research.

Literature Review

We integrate General Deterrence Theory and Human Curiosity Theory to determine what strengthens and/or weakens one's resolve to comply with information security polies.

General Deterrence Theory

Deterrence theory states that "*if punishment is severe, certain, and swift, a rational person will measure the gains and losses before engaging in crime and will be deterred from violating the law if the loss is greater than the gain*" (Onwudiwe, Odo, & Onyeozili, 2005). This statement emphasizes three components of deterrence theory that all focus on deterring abuse or noncompliance: perceived sanction severity, perceived sanction certainty, and perceived sanction celerity (D'Arcy & Herath, 2011; D'Arcy et al., 2009; Onwudiwe et al., 2005; Straub & Welke, 1998). Perceived sanction severity pertains to the strength of the punishment if an individual were caught, perceived sanction certainty pertains to the likelihood an individual will be caught, and perceived sanction celerity pertains to the speed an individual will be caught. However, even with the existence of deterrence mechanisms, IS abuse still occurs.

Human Curiosity Theory

One reason for violating ISP may be for sheer curiosity. There are several different schools of thought about human curiosity. A prior study proposes that human curiosity is evoked by novel stimuli, in which its novelty is distinctive based on individuals' previous experiences (Berlyne, 1960). On the other hand, Berlyne (1954) suggested that human curiosity pertains to epistemic curiosity, which is aroused by thematic probes (i.e., cue stimuli) and driven by conflict reduction activities, such as knowledge acquisition. In this context, conflict refers to something that is "*strange, unusual, and puzzling*" (Berlyne, 1954, pg. 184). Additionally, curiosity is superficial in the sense that it can arise, change focus, or end abruptly (Loewenstein, 1994), often competing with and even negating rational choice. RCT states that individuals weigh the costs and benefits before acting; only when the benefits exceed the costs will they engage in a certain behavior (Tversky & Kahneman, 1981; Westland, 1997). Curiosity has no rationality behind its motivations and behavior other than to fill a knowledge gap.

Curious individuals have an intrinsically motivated desire for information which is comparable to the same motivational intensity of a passion (Loewenstein, 1994). Early research examined curiosity as a feeling-of-interest or very pleasurable emotional experiences (Litman & Jimerson, 2004). However, subsequent research indicates that curiosity may be associated with a feeling-of-deprivation (Litman & Jimerson, 2004) or unpleasant feelings as a result of the uncertainty due to lack of desired knowledge (Litman, 2005;

Loewenstein, 1994). This form of curiosity often leads to tension, frustration, and dissatisfaction leading individuals with a wanting or need to know (Berridge, 1999; Berridge & Robinson, 1998). Curiosity as a feeling-of-deprivation stimulates more intense experiences than that of curiosity as a feeling-of-interest (Litman & Jimerson, 2004). In essence, curiosity at its best will lead to scientific inquiry; conversely, it may lead to investigating the actions and circumstances of others, even without proper authorization, in order to overcome boredom or eliminate uncertainty or ignorance (Litman & Jimerson, 2004; Loewenstein, 1994). In our research, we adopt Lowenstein's (1994) conceptualization of curiosity, composed of perceptions of deprivation and interest, and apply it to the InfoSec context through an integration with GDT.

Theoretical Framework

Based on this literature review, we propose the research model illustrated in Figure 1. The model proposes a framework to explain compliance while examining the moderating effects of curiosity on deterrence.

D'Arcy, Hovav, & Galletta (2009) posited that sanctions prohibit computer misuse. More specifically, perceived severity of sanctions denotes the degree of punishment (D'Arcy et al., 2009) related to ISP violation. Additionally, sanction certainty refers to is the probability of being punished (D'Arcy et al., 2009). Drawing on GDT, individuals will refrain from violating ISP given a high degree of sanction severity and sanction certainty (D'Arcy et al., 2009). That is, a high degree of sanction severity and sanction certainty promote ISP compliance. Therefore, we propose:

H1a: Perceptions of sanction severity are positively associated with ISP compliance.

H1b: Perceptions of sanction certainty are positively associated with ISP compliance.

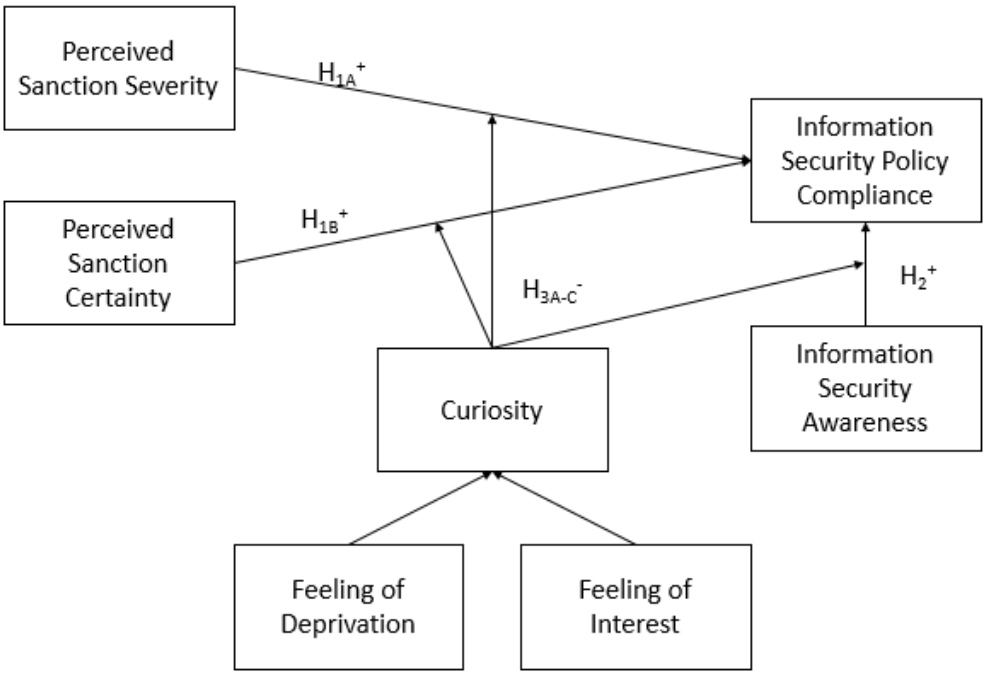

Figure 1: Research Model

Information security awareness (ISA) training also cultivates positive behaviors toward information security (Albrechtsen & Hovden, 2010). Bulgurcu, Cavusoglu and Benbasat (2010) have empirically demonstrated that ISA shapes attitudes in support of ISP compliance. Moreover, making individuals aware of the sanctions encourages individuals to comply with ISP (D'Arcy et al., 2009). We then hypothesize,

H2: Employees with higher levels of information security awareness are more likely to comply with ISP.

Loewenstein (1994) proposed that curiosity could be aroused by a feeling of deprivation and a feeling of interest. Curiosity as a feeling of deprivation (CFD) refers to an urge of seeking new information followed by feelings of tension and uncertainty (Loewenstein, 1994). To ease tension, individual explore their options to obtain information. Overall, CFD suggests aversive feeling of uncertainty and negative reinforcement of explorative behavior (Litman & Jimerson, 2004). On the other hand, curiosity as a feeling of interest (CFI) has a positive impact on explorative behavior, creating pleasure through stimulation. CFI is stimulated when individuals recognize the promising pleasure of learning new things (Loewenstein, 1994).

In essence, curiosity is evoked by a perceived gap of information and understanding (Loewenstein, 1994). Because curiosity provokes information seeking (Litman & Jimerson, 2004; Loewenstein, 1994), we assert that curious employees will ignore perceived sanctions to gain access to sensitive data that they are not authorized to view. Employees may illegally access sensitive data for pleasure and to alleviate tensions associated with deprivation of knowledge. Even a highly regulated industry such as healthcare, which is mandated to raise ISA among their employees and inform their employees of possible sanctions associated with security violation, experiences ISP violations because of human curiosity (Grant, 2016). We then propose:

H3a: Curious employees are more likely to disregard the severity of sanctions and violate ISP.

H3b: Curious employees are more likely to disregard the certainty of sanctions and violate ISP.

H3c: Curious employees are more likely to disregard the training and education of information security awareness and violate ISP.

Conclusion and Future

In the context of perceived sanctions and rational choices, this study examines the effect of human curiosity on ISP compliance. We argue that human curiosity may overshadow perceived sanctions associated with ISP violation and perceived cost of compliance/non-compliance based on RCT. Real-life cases in the healthcare industry suggest that some individuals will still violate ISP despite mandatory training of patients' information security and privacy (Grant, 2016). This study contributes to the InfoSec literature in the following ways. First, we challenge the notion of GDT to propose that human curiosity may be a powerful source to undermine ISP compliance. Second, this study provides viable suggestions to curb employee's curiosity that will lead to unauthorized data access. In the near future, we will collect data and conduct data analysis.

REFERENCES

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers and Security*, *29*(4), 432–445.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security*, *39*(Part B), 145–159.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2018). Don't even think about it! The effects of anti-neutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems*, forthcoming.

Benenson, Zinaida Gassmann, Freya Landwirth, R. (2016). Exploiting curiosity and context: How to make people click on a dangerous link despite their security awareness. Retrieved from https://paper.seebug.org/papers/Security Conf/Blackhat/2016/us-16-Benenson-Exploiting-Curiosity-And-Context-How-To-Make-People-Click-On-A-Dangerous-Link-Despite-Their-Security-Awareness-wp.pdf

Berlyne, D. E. (1954). A theory of human curiosity. *British Journal of Psychology*, *45*(3), 180–191.

Berlyne, D. E. (1960). *Conflict, Arousal, and Curiosity*. New York, NY: McGraw-Hill Book.

Berridge, K. C. (1999). Pleasure, pain, desire, and dread: Hidden core processes of emotion. In D. Kahneman, E. Diener, & N. Schwarz (Eds.), *Well-being: The foundations of hedonic psychology* (pp. 525–557). New York, NY: Russell Sage Foundation.

Berridge, K. C., & Robinson, T. E. (1998). What is the role of dopamine in reward: Hedonic impact, reward learning, or incentive salience? *Brain Research Reviews*, *28*(3), 309–369.

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.

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*(6), 643–658.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98.

Grant, M. (2016). ORMC Blames "Personal Curiosity" for Pulse Survivor Data Breach. Retrieved May 22, 2017, from http://www.wesh.com/article/ormc-blames-personal-curiosity-for-pulse-survivor-data-breach-1/4451797

Litman, J. A. (2005). Curiosity and the pleasures of learning: Wanting and liking new information. *Cognition and Emotion*, *19*(6), 793–814.

Litman, J. A., & Jimerson, T. L. (2004). The measurement of curiosity as a feeling of deprivation. *Journal of Personality Assessment*, *82*(2), 147–157.

Loewenstein, G. (1994). The psychology of curiosity: A review and reinterpretation. *Psychological Bulletin*, *116*(1), 75–98.

Onwudiwe, I. D., Odo, J., & Onyeozili, E. C. (2005). Deterrence theory. In *Encyclopedia of Prisons & Correctional Facilities* (Vol. 1, pp. 233–237). Sage Publications.

Scott, J. (1999). Rational choice theory. In G. Browning, A. Halcli, & F. Webster (Eds.), *Understanding contemporary society: Theories of the present*. Thousand Oaks, CA: SAGE.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487–502.

Spurr, K. (2017). St. Charles: 2,500 patient records accessed in privacy breach. Retrieved May 22, 2017, from http://www.bendbulletin.com/localstate/5157042-151/st-charles-2500-patient-records-accessed-in-privacy

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, *22*(4), 441–469.

Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science*, *211*(4481), 453–458.

Westland, C. (1997). A rational choice model of computer and network crime. *International Journal of Electronic Commerce*, *1*(2), 109–126.