Priming Security Behavior: A Study Based on Self-Concept Maintenance Theory

Emergent Research Forum

Nic DePaula
University at Albany
ndepaula@albany.edu

Sanjay Goel
University at Albany
goel@albany.edu

Abstract

We develop a proposal to test the role of priming and self-concept maintenance theory in an information security context. Self-concept maintenance theory proposes that ethical behavior is influenced by two particular mechanisms: attention to standards and categorization. Attention to standards refers to the extent to which individuals are cognizant about their moral standards; categorization refers to how an individual classifies a situation in terms of the ethical dilemma it poses. Through controlled experiments we propose to test the effects of these mechanisms on how individuals respond to an intellectual property infringement scenario and whether or not they commit a security policy violation. The studies employ conscious and subconscious primes and are tested under distinct conditions, namely when participants are being monitored and when having different sets of performance goals. In a discussion we also note the importance of understanding the ethics of manipulating employee behavior through this type of activity.

Keywords

Priming, security behavior, self-concept maintenance, moral standards

Introduction

Threats to information security come in many forms, from deliberate policy violations to compromises to intellectual property. In this proposal we consider the role of ethical priming and self-concept maintenance in affecting two types of security behavior: policy compliance and intellectual property infringement. Self-concept maintenance theory (SCM), as proposed by Mazar et al. (2008) and Welsh and Ordonez (2014), provides a useful framework to explain how individuals behave in situations that may pose an ethical dilemma. SCM posits that the likelihood that an individual will commit a dishonest act depends on the degree to which she becomes mindful of her moral standards. Moreover, SCM points to the fact that many situations are ethically ambiguous and that the categorization of a situation as ethical or not may also be affected by attention to moral standards. We test the effects of priming in activating moral standards, the categorization of ethical situations and how these processes ultimately affect security behavior. Given the degree to which monitoring is present in organizations and the role of performance goals in affecting ethical behavior we also consider the effects of these conditions in our study.

We see a variety of benefits of this approach. Studies in information security policy compliance have found conflicting evidence about the role of sanctions in improving security behavior or intention to comply with security policies; recent research has shown that “soft” factors like norms and emotions are more effective in predicting compliance to information security (Sommestad et al. 2014). Addressing and expanding on the role of these type of variables thus seems more productive. Secondly, many studies in the IS security field rely on self-reported behavior or constructs related to the intentions to comply with policies. Our study uses controlled experimental designs to identify how people respond to a hypothetical scenario and how they actually behave during an experiment. Ultimately, there are practical benefits for information security management. If priming is an effective mechanism to reduce information security infringement it may be successfully deployed in organizations. However, we also note the dangers of this type of activity in organizations as they may lead to a hyperbolic and unhealthy manipulation of employee behavior.
Literature Review

General deterrence theory (GDT) adopts the position that individuals conduct a cost benefit analysis prior to performing a deviant action, calculating the certainty, severity and celerity of the sanctions for the act (Gibbs 1975). Similarly, protection motivation theory (PMT) states that individuals in a risky situation undertake a threat-appraisal process, involving an evaluation of the severity and susceptibility of the risk, and a coping appraisal, involving an evaluation of self-efficacy, response efficacy and outcome value (Johnston et al. 2015). GDT and PMT have been extensively used to study computer abuse and security policy violations (e.g. Herath and Rao 2009a; Siponen et al. 2006). Although at one time the most prevalent framework, the literature suggests inconsistent and contradictory findings about the role of deterrence in information security (D’Arcy and Herath 2011; Hu et al. 2011). In the seminal paper of Siponen and Vance (2010), sanctions were found to be nonsignificant in the presence of neutralization, as people justify or rationalize their behavior through a set of techniques, such as denying the injury, the responsibility or assuming necessity for the action in their intention to violate a policy. Other studies in this context have found that intrinsic factors such as “perceived legitimacy” and “value congruence” are significant predictors of policy compliance while sanctions were not (Son 2011). The role of moral reasoning to explain security policy compliance has also been found significant (Myyry et al. 2009). All of these studies point to the importance of social norms and self-evaluation in explaining information security behavior.

Self-Concept Maintenance Theory

Self-concept maintenance (SCM) theory asserts that individuals will engage or avoid to engage in dishonest actions based on the effects of the action on their self-concept (Mazar et al. 2008). It asserts that for deviant or unethical actions individuals will balance their potential gains with an evaluation of their self-image. The importance of self-image was recognized in the work on neutralization (Piquero et al. 2005). Although in the study of Siponen and Vance (2010) informal sanctions (namely shame) was found to be nonsignificant in the presence of neutralization techniques, the importance of one’s self-concept is not removed from the theoretical explanation. In fact, the process of neutralization itself assumes that the neutralization techniques applied are carried out in order to maintain a positive self-image (Piquero et al. 2005).

SCM proposes two mechanisms that affect the likelihood that a dishonest act will be committed: attention to standards and categorization. Attention to standards refers to the degree to which one becomes mindful of one’s own moral standards. Since individuals are not always attentive to their own standards, reminding them has an effect on their behavior. This was demonstrated in an experiment by Mazar et al. (2008) in which a group were asked to write the Ten Commandments prior to taking a test where they could potentially cheat. Individuals who wrote the Ten Commandments cheated significantly less than individuals who were asked to simply remember book titles. Categorization refers to the process of classifying a situation as posing an ethical dilemma. This process is important since the ethicality of certain situations is often ambiguous, and the categorization is malleable. For example, taking data without permission from an organization sometimes may seem proper whereas taking money of the same value without permission may never be so. It has been found that attention to standards leads to a more conservative categorization of an ethically ambiguous situation, making it more difficult for individuals to deliberately rationalize their actions as they see fit (Welsh and Ordonez 2014).

Conscious and Subconscious Primes

Priming refers to a recent or frequent stimulus that is provided to an individual that has an effect on their subsequent behavior (Higgins et al. 1985). In the study of Mazar et al. (2008) the attention to standards are activated through a conscious prime, a message that explicitly refers to moral standards. Welsh and Ordonez (2014) expanded this framework by using subconscious primes in activating moral standards, where the moral nature of the content was not apparently obvious. We believe that identifying the effectiveness of subconscious primes may be particularly important in an information security context as users could be less averse to receiving the prime, thus becoming a more prevalent tactic for information security managers. We thus test these processes in an intellectual property infringement scenario:

H1a: Individuals primed with subconscious ethical content will have moral standards activated.
H1b: Individuals primed with subconscious ethical content are more likely to categorize an ethically ambiguous intellectual property infringement scenario as unethical.

Welsh and Ordonez (2014) also find that conscious priming was a stronger predictor for activating moral standards than subconscious primes. This is useful in so far as there may be a need to balance the use conscious primes with users’ aversion to security warnings. We thus test the following:

H1c: Ethical conscious primes are more likely to lead to a categorization of an ethically ambiguous intellectual property infringement as unethical, compared to subconscious primes.

**Monitoring and Behavior**

Monitoring of individuals is a standard practice in many organizations, and, ipso facto, it allows for policy violations to be detected. But do they actually reduce the amount of violations? Empirical findings are mixed. D’Arcy and Hovav (2007) found that monitoring had no effect on behavioral intention for IS misuse whereas Herath and Rao (2009) found that increased certainty of being detected had a significant and positive effect on individuals intention to comply with information security policies. In our experimental design we test the interaction of monitoring and priming. Welsh and Ordonez (2014) found that when individuals were not monitored, priming was effective in reducing cheating behavior, but the priming had no significant effect when individuals were monitored. This hypothesis would be especially important for organizations as they seek to understand the interacting effects of priming when monitoring is also taking place. We thus test the following hypotheses in the context of security policy violations:

H2a. Conscious ethical priming will decrease the likelihood that people will carry out a security policy violation when not monitored.

H2b. Conscious ethical priming will have no significant effect on security policy violation behavior when individuals are monitored.

**Effects of Performance Goals**

Although goal setting in organizations has long been shown to improve task performance, recent evidence points to how certain types of performance goals lead to improper organizational behavior (Ordoñez and Welsh 2015). Studies have shown that specific performance goals can lead people to take more risks (Larrick et al. 2009), be more deceptive (Poortvliet et al. 2011) and cheat more (Schweitzer et al. 2004). Barsky (2008) explained this phenomenon by suggesting that high cognitive loads from attention to the performance goals inhibits considerations of the wrongfulness of the acts. Based on this understanding, Welsh and Ordonez (2014) have shown that individuals do commit more unethical behavior when they have high performance goals, but also that activating standards in people’s minds reduces unethical behavior in these contexts. We have not found studies examining how performance goals directly affect security behavior. We believe this to be an important addition to security behavior research as performance goals have become such an integral part of organizational processes. We thus test the following hypotheses:

H3a. Individuals will commit more security policy violations when they have high performance goals in comparison to when they have “do your best” goals.

H3b. Conscious ethical priming will reduce policy violations when individuals have high performance goals.

**Study Design**

**Studies 1 and 2 – Intellectual Property Infringement**

Studies 1 and 2 will be controlled experimental designs with college participants. In study 1 participants will be randomly assigned to two treatment groups of conscious (ethical and neutral) primes. Study 2 is identical except the treatment groups will have subconscious primes. In each group, subsequent to receiving the prime, participants will be asked to read an intellectual property infringement scenario where illegal downloading of torrents or streaming of videos without paying is presented in an ethically ambiguous way.

*Dependent variables:* (a) activated standards, and (b) categorization. Activated standards will be measured via a *moral identity* scale that has been shown to be effective in identifying changes in moral self-concept.
Information security research, however, should further encourage organizations to understand policy implications. For study 4, in order to develop the ethics of employees and the field of business ethics (e.g. Moore 2000), the ethics of employers and the organization itself should be considered to have violated the security policy. As other studies cited here have shown individuals are affected by a number of contingent factors, including conditions imposed by the organization and the number of times the website was accessed. Since we will host the malicious website, we will be able to identify the IP addresses (the individuals) and the number of times the website was accessed.

Independent variables: (a) conscious and (b) subconscious ethical primes. Following the example of Mazar et al. (2008) our conscious ethical prime is a text reminder about a set of moral standards. Conscious primes are assumed to directly activate standards, therefore conscious primes will not be used to test activated standards. As in the work of Welsh and Ordonez (2014), the unconscious prime will consist of an unscrambling task in which participants will be asked to create grammatically correct phrases with words with moral references (e.g. “donated Mary charity to” to “Mary donated to charity”). A simplified conceptual model of the tested variable relationships are presented in figure 1 below.

![Conceptual Models for Studies 1 and 2 (left) & 3 and 4 (right)](image)

**Studies 3 and 4 – Security Policy Violation**

Studies 3 and 4 will also employ controlled experiments with college students. We will employ two 2 X 2 designs where ethical and neutral primes are given under monitored and unmonitored conditions in study 3, and under two sets of performance goals in study 4. In order for participants to understand policy violations we will first carry out lessons about what constitutes a security policy violation and the effects they can have for the students and the class. In each group individuals will first receive the prime, and then be led to a variety of browsing and research tasks. During this process, individuals will be presented with enticing links to a fake-malicious website created by the researchers.

Dependent variable: (a) access to malicious website. Individuals who go to the malicious website will be considered to have violated the security policy. Since we will host the malicious website, we will be able to identify the IP addresses (the individuals) and the number of times the website was accessed.

Independent variables: (a) monitoring, (b) primes, (c) performance goals. The primes for these studies will be the same as in studies 1 and 2. For study 3, one primed group (ethical) will be told their actions are being monitored. No such message will be given to the two unmonitored groups. For study 4, in order to distinguish the performance goals, individuals will be asked to solve a challenging number of web searching tasks in order to receive rewards from the study. This will be the high goals group. The “do-your-best” group will simply be asked to solve as many problems as possible.

**Discussion**

Information security research has elaborated on the *insider threat* problem and how actions of individuals may show their malicious intentions prior to major improprieties (e.g. Willison and Warkentin 2013). While our work supports research for this type of problem, and security efforts distinct from formal sanctions, it also complicates the idea of identifying potential information security offenders. As other studies cited here have shown individuals are affected by a number of contingent factors, including conditions imposed by the organizations themselves. Moreover, while the ethics of employees are often studied in the information security context, the ethics of employers in monitoring and manipulating employee behavior are not. Priming may be a benign and effective mechanism in order to stray individuals away from improprieties. However, this should in no way endorse abusive control or management psychopathy, a harmful problem for organizations (Boddy et al. 2015). The ethics of employee monitoring techniques has been addressed in the field of business ethics (e.g. Moore 2000). Information security research, however, should further develop the ethics of information security management activities in order to produce an understanding of unethical and pernicious manipulation of employees.
REFERENCES


