Information Systems Security

ISSN: 1065-898X (Print) 1934-869X (Online) Journal homepage: http://www.tandfonline.com/loi/uiss19

Gaining Access with Social Engineering: An Empirical Study of the Threat

Michael Workman Ph.D.

To cite this article: Michael Workman Ph.D. (2007) Gaining Access with Social Engineering: An Empirical Study of the Threat, Information Systems Security, 16:6, 315-331, DOI: 10.1080/10658980701788165

To link to this article: http://dx.doi.org/10.1080/10658980701788165

Published online: 19 Dec 2007.

Information Systems Security, 16:315–331, 2007

ISSN: 1065-898X print/1934-869X online
DOI: 10.1080/10658980701788165

Taylor & Francis
Taylor & Francis Group

Gaining Access with Social Engineering: An Empirical Study of the Threat

Michael Workman
Security Policy Institute,
Florida Institute of Technology,
Melbourne, FL, USA

ABSTRACT Recently, research on information security has expanded from its purely technological orientation into striving to understand and explain the role of human behavior in security breaches. However, an area that has been lacking theory-grounded empirical study is in social engineering attacks. While there exists an extensive body of anecdotal literature, factors that account for attack success remains largely speculative. To better understand this increasing phenomenon, we developed a theoretical framework and conducted an empirical field study to investigate social engineering attacks, and from these results, we make recommendations for practice and further research.

Despite the general population becoming increasingly aware of the pervasive threats to information security, there continues to be information security violations that elude our ability to defend against. These breaches in security lead to billions of dollars annually in individual and corporate losses and even to crimes (Bresz, 2004; Calluzzo & Cante, 2004; Sasse, Brostoff, & Weirich, 2004; Shreve, 2004). Information security critics charge that extant systems have virtually ignored the creativity with which people find ways around any given security system, citing the ability of attackers to continually contravene available security defenses (Sherif, Ayers, & Dearmond, 2003).

Many security countermeasures can be automated through security technology by making them mandatory for users, but there are significant reasons why automation in-and-of-itself cannot alone solve the problem (Ong, Tan, Tan, & Ting, 1999; Ruighaver & Chang, 2007), and while information systems (IS) managers have attempted to automate security measures and implement mandatory access controls (MAC), there are situations where individuals must take on the personal responsibility of protecting their own systems (Sherif et al., 2003). One such example is in the case of social engineering. Social engineering consists of techniques used to manipulate people into performing actions or divulging confidential information (Mitnick & Simon, 2002) to be used for illicit financial gains from identity theft. For instance, there exists a black-market for selling bulk personal data such as driver licenses, credit card number, and social security numbers.

Address correspondence to Michael Workman, Ph.D., Associate Professor and Director, Security Policy Institute, Florida Institute of Technology, 150 West University Avenue, Melbourne, FL 32901.
E-mail: workmanm@fit.edu

Social engineers often attempt to persuade potential victims with appeals to people's emotions such as excitement or fear, while others utilize ways to establish interpersonal relationships or create a feeling of trust and commitment (Gao & Kim, 2007). For example, they may promise a valuable prize or financial interest on a transfer bank deposit if the victim complies with a request for bank account information. The emotional aspect of the interaction distracts people and serves to interfere with the potential victim's ability to carefully analyze the content of the message. The social engineer's illicitly gotten information may then be used to gain unauthorized access to computer systems to invade a person's privacy, commit fraud, industrial espionage, or to damage assets (Dodge, Carver, & Ferguson, 2007).

It is important to realize that not all successful social engineering episodes result from duplicity; some people willingly give up sensitive information in spite of their awareness of the pervasive threats (Calluzzo & Cante, 2004; Straub & Nance, 1990). For example, while people generally state they are concerned about information security and privacy—even claiming they are willing to pay a fee to protect their personal information—in many cases they are willing to trade-off privacy for convenience or even bargain the release of very personal information in exchange of relatively small rewards (Acquisti & Grossklags, 2005; Grossklags & Acquisti, 2007; Leyden, 2004).

Beyond the technological and procedural recommendations (i.e., conducting risk analyses) to address the problem, the research into the underlying behavioral causes of information insecurity has suggested interventions consisting primarily of raising security awareness (Calluzzo & Cante, 2004; Dodge et al., 2007), rewarding and punishing behaviors (Straub & Welke, 1998), providing instruction on situational ethics and responsible conduct (Harrington, 1996; Hsu & Kuo, 2003; Kurland, 1995), and using training on specific security techniques (Straub & Nance, 1990). To try to explain why people fail to take security precautions, a number of studies have investigated the relationships between processes and procedures and security-related behaviors (Debar & Viinikka, 2006, Leach, 2003, von Solms & von Solms, 2004). They have identified a number of situational impediments such as a lack of policy specificity and a shortage of time among security professionals to implement the recommended procedures (Albrechtsen, 2006). While these situational factors are important, they have not addressed the problem from a theoretical perspective, leaving unexplored factors such as personal and social characteristics that may explain why someone would or would not follow a well-specified security policy (Ruighaver & Chang, 2007).

In spite of all the behavioral recommendations to prevent security breaches, the studies have either not addressed the issue of social engineering directly or the investigations have not been grounded in theory to explain under which conditions social engineering intervention should work and why. Since theory explains phenomena so that managerial interventions can be instituted with a higher degree of efficacy confidence, we investigated the problem of social engineering security breach by reviewing the social psychology, management, and information security theory literature, which revealed no empirically tested theoretical framework in the study of social engineering security threats; although the extant literature does suggest a significant number of "ad hoc" countermeasures based on anecdotes (For an illustration, see, e.g., Denis, Trobec, Pavei, & Tasi, 2007). Therefore, we crafted an explanatory theory from the extant literature to lay down a framework for empirical study.

An important contribution of our research is the combination of subjective perceptions of behaviors that are triangulated with objective observations. Since there are characteristic differences between self-perceptions of behavior and actual behavior, social scientists prefer to observe behavior when possible because of this fact. However, since we cannot observe all possible behaviors in a category (e.g., social engineering security behavior), observation alone is also incomplete. By combining self-report perceptions with observational sampling in a triangulation, we are able to assess how congruent these are in a given study.

THEORY AND HYPOTHESES

Previous Research and Background

Our research investigates factors that may account for successful social engineering attacks. The perception of threat is defined as the anticipation of a

psychological (e.g., assault), physical (e.g., battery), or sociological (e.g., theft) violation or harm to oneself or others, which may be induced vicariously (Lazarus, 1991). Threats to information security include unauthorized interception of information; unauthorized modification of information; exposure of information to unauthorized individuals; and the destruction of hardware, software and/or information for which security measures exist to help protect the confidentiality, integrity, and availability of these information resources (SANS, 2005). Threat assessment research (e.g., Pyszczynski, Greenberg, & Solomon, 1997) indicates that when a threat is perceived, people adjust their behavior according to the amount of risk from the threat that they are willing to accept (sometimes known as risk homeostasis). This adjustment is based on the degree or severity and costs of damage they perceive to be associated with the threat (Grothmann & Reusswig, 2006). Thus, people tend to adjust their behavior in response to the extent of the damage the threat may cause (Pyszczynski et al., 1997). Since some people give up information for reasons other than duplicity (Acquisti & Grossklags, 2005; Grossklags & Acquisti, 2007), threat assessment is an important component of social engineering attack success.

Next, Aldoory and Van Dyke (2006) tied the situational theory of publics (Grunig, 1997) and the health-belief model (Rosenstock, 1974) to issues related to bioterrorism threats. The situational theory of publics asserts that a populace may be segmented based on the activeness or passiveness of communication behavior (Aldoory & Van Dyke, 2006). The factors purported by this theory are problem recognition, the level of active involvement, and constraint recognition (Grunig, 1997). Problem recognition reflects the extent to which an individual recognizes a problem as relevant to him or her; that is, how likely a threat is perceived to impact the person. The level of active involvement results from a perception of how emotionally the problem is felt, such as the perceived severity of damage to the person posed by the threat. Constraint recognition reflects the extent to which people perceive their behaviors as limited by factors beyond their own control.

According to Grunig (1997), if these three factors accurately depict external conditions then the environment must change before a person will respond, but if they are merely perceived (internal), they may be changed by persuasive communication, hence persuasion is a key element in whether and how people respond to messages about a threat. The elaboration likelihood model (Petty & Cacioppo, 1986) has been employed in marketing research to explain how people are persuaded into making purchases (Petty, Cacioppo, & Schumann, 1983) and in techniques used by telemarketers (Schumann, Hathcote, & West, 1991). While social engineering does not seek to sell a product or service, it does seek to persuade people to provide sensitive information in similar fashion (Mitnick & Simon, 2002). Thus, using threat assessment and the elaboration likelihood model (ELM) as a framework, we devised a field experiment to test its applicability in explaining the social engineering threats to determine whether the defenses generally suggested against succumbing to marketing ploys, or interventions suggested for other kinds of information security threats, might also be applied to social engineering countermeasures and interventions.

Working from these premises, we reviewed the social psychology, management, and information security literature to determine what had been studied relative to social engineering and information security. Four factors rose to the surface: perceptions of threat severity and personal vulnerability (Dorn & Brown, 2003), trust (Wang & Emurian, 2005), fear (Straub & Welke, 1998), and commitment (Theoharidou, Kokolakis, Karyda, & Kiountouzis, 2005). Also, Mitnick and Simon's (2002) seminal work on social engineering outlined attack architecture drawing from Petty & Cacioppo's (1986) elaboration likelihood model (ELM). From these, we synthesized theory from the literature to ground our investigation.

Threat Severity and Vulnerability

Perceived severity of threat will lead people to behave in a more cautious manner if their perception of the damage or danger increases. The reverse of this, however, is also true: when people perceive that a risk has diminished, they will behave in a less cautious manner. This reverse effect, which has been widely documented, has proven to be a complicating factor in a number of safety-related areas. More specifically, there is compelling evidence from traffic studies and the use of safety features such as car seat

belts, antilock braking systems, and bicycle helmets that demonstrate these effects. That is, people use seatbelts less when they are driving close to home (lower perceived danger) or at slower speeds (lower perceived damage) (Dorn & Brown, 2003).

In the threat assessment literature the perceived severity of threat and the associated acceptance of risk behavior are based on the premises that: (1) people place a certain intangible value on "life," "liberty," and "property"; (2) they have a threshold level of risk they will accept, tolerate, prefer, desire, or choose; (3) the "target level" of risk they will accept before putting up a defense depends on the perceived advantages or benefits versus the disadvantages or costs of safe and unsafe behavioral alternatives; and, finally, (4) this assessment determines the degree to which people will expose themselves to a threat or hazard before taking coping behaviors to mitigate the threat (Wilde, 2001). Thus, our first hypothesis is:

H1: People who perceive a lower severity of a social engineering threat will succumb to social engineering more frequently than those who perceive higher threat severity.

People operate day-to-day on the basis of assumptions and personal beliefs that allow them to set goals, plan activities, and order their behavior. This conceptual system is developed over time and provides them with expectations regarding their environment. While they operate on the basis of this conceptual system, they tend not to be aware of its central postulates. Among these generally shared postulates is the belief in personal invulnerability (Dorn & Brown, 2003; Hochhauser, 2004). For instance, people may recognize that crimes are common, but they believe at the same time that "it can't happen to them" (Roe-Berning & Straker, 1997). As an example, Lejunene and Alex (1973) found that mugging victims first defined the event with disbelief and in a nonthreatening way, such as a practical joke. Hence, people operate on the basis of an "illusion of invulnerability" to support their need to view the world as orderly, stable, and meaningful, thus underestimating the probability of their own misfortunes and overestimating the probability of misfortunes to others (Hochhauser, 2004; Roe-Berning & Straker, 1997).

Events such as criminal acts, accidents, disasters, and disease force people to recognize and make objective their basic assumptions about their environment and the world (Janoff-Bulman & Frieze, 1983). Those who have been subjected to a burglary, for example, tend to assess their chances of falling victim to future burglaries to be higher than those who have never been a victim (Lejeune & Alex, 1973). In general, the illusion of invulnerability is an immunizing stratagem from the fear, stress, and anxiety associated with the perceived threat of misfortune. Once victimized, however, it becomes easier to see oneself again in the role of victim (Janoff-Bulman & Frieze, 1983; Roe-Berning & Straker, 1997). Applying this line of thought to social engineering, we hypothesize that when people have been previous victims of social engineering, they are more likely to maintain higher vigilance and take precautions against such attacks (Dorn & Brown, 2003; Hochhauser, 2004). Therefore,

H2: People who perceive a lower vulnerability to social engineering threats will succumb to social engineering more frequently than those who perceive higher vulnerability.

Commitment Theory, Reciprocation, Consistency and Social Proof

The commitment concept has been used extensively in organizational research. Commitment is defined as an attitude that leads one to perseverant action, and is a fairly stable personal characteristic (McCaul, Hinsz, & McCaul, 1995; Mowday, Steers, & Porter, 1979; Sagie, 1998). Allen and Meyer (1990) delineated types of commitments based on the situation and the "target," such as a brand, person, or organization. Normative commitment comes from a reciprocal exchange with the target, where someone will expend effort and perform actions because it is customary or is obligatory (Beck & Wilson, 2000).

Social norms form around perceptions of a commitment. Consistency theories, such as Festinger and Carlsmith's (1959) cognitive dissonance theory, suggest that people are motivated to maintain congruence between attitudes, social norms, and behaviors in order to maintain a feeling of consonance. When a giver offers something valued by a receiver, there are varying degrees in which the receiver may experience cognitive dissonance until he or she provides

something to the giver that is likewise valued (Bergman, 2006; Gundlach, Achrol, & Mentzer, 1995). In this theory of social exchange, people decide fairness and develop a comparison against which they evaluate the "give-and-take." The extent of exchange varies according to the value or weighting they place on what is exchanged, and they consider whether the exchange is fair and reasonable (Kelley & Thibaut, 1978). In terms of ELM, people tend to honor a commitment to maintain this type of implied social contract even in some cases where there is imbalance (Theoharidou et al., 2005). For instance, if an incentive is given to someone in exchange for a promise, people who are highly committed tend to continue to live up to their end of the bargain even after the incentive is later withdrawn (Cacioppo et al., 1986; Cialdini, 2001).

In terms of information security, people sometimes will divulge sensitive or private information to those to whom they feel obligated (Bergman, 2006; Leyden, 2004; Theoharidou et al., 2005). In some forms of social engineering attacks, the perpetrator relies on this "reciprocal commitment norm" by offering something to the intended victim, and then requests or entices them to perform an action, for example, a perpetrator may offer a sum of money if the intended victim will allow the perpetrator the ability to "park funds" in the intended victim's bank account while performing an international money transfer, or the perpetrator may promise a valuable item in exchange for what appears to be a small financial transaction to cover shipping costs (Mitnick & Simon, 2002; Panko, 2004). Consistent with these theories, when social engineers utilize peripheral route persuasion geared toward reciprocation, people who are more normatively committed are more susceptible to social engineering scheme than those who are not. Stated more formally,

> *H3: People who are higher in normative commitment will succumb to social engineering more frequently than those who are lower in normative commitment.*

Consistency theories also suggest that when people commit to an action, they feel compelled to through to conclusion even in spite of disconfirming evidence of the efficacy of their commitment to retain a feeling of consonance. Thus, while normative commitment extends from a reciprocal exchange with a target, continuance commitment is the product of investment perceptions (time, effort, or money), where "commitment is viewed as a tendency to engage in consistent lines of activity based on the individual's recognition of the costs (or lost side-bets) associated with discontinuing an activity" (Allen & Meyer, 1990, pp. 2-3). With continuance commitment, people become psychologically vested in a decision they have made and maintain consistency in behaviors related to it (Petty, Briñol, & Tormala, 2002), such as in the case where people "pour good money after bad" in the economic concept of "loss aversion and sunk costs" by continuing to spend money on losing ventures despite new evidence suggesting that the decision might be wrong (Arkes & Blumer, 1985; Staw, 1981). According to Cialdini (2001), there is evidence that some people have a tendency to think that persistent effort will eventually "payoff." This type of commitment explains why "some people will pay escalating costs to try to win a cheap teddy bear at a carnival" (Brill & Molton, 2006, p. 33).

Some research (e.g. Milne, Sheeran, & Orbell, 2000) using protection motivation theory (Rogers, 1975) in heath-related threats have included psychological cost-benefit models, and extending from this line of reasoning to the information security and social engineering arena, people may be influenced in such a way as to continue investing in a risky proposition in order to gain something they value (Josephs, Larrick, Steele, & Nisbett, 1992; Pechmann et al., 1993). Relative to information security and social engineering, in most cases the threat is designed so that the level of effort the victim invests will be lower than the purported benefits, and thus the decision to disregard precautions toward the threat emerges from the reasoning that the costs or risks are outweighed by the perceived possible benefits (Charbaji & Jannoun, 2005; Pechmann, Zhao, Goldberg, & Reibling, 1993; Wilson, 2004). This cost-benefit assessment is a favorable or unfavorable affective and cognitive evaluation of a risk/reward that generally influences behavior, which may or may not lead to continuance commitment (Ajzen, 2002), where risk may be defined as a lack of predictability about an outcome or consequences of an action and reward as a monetary or nonmonetary item that has some intrinsic value to the recipient (Charbaji & Jannoun, 2005).

It is important to note that people maintain different cost-benefit assessments and hence continuance commitment attitudes independently of the perceived business value or sensitivity of the information assets, particularly when it comes to self-interests (International Federation of Accountants, 2006). For example, while people generally state that they are concerned about information security and privacy, and even claim that they are willing to pay a fee to protect their personal information, in many cases they are willing to trade-off privacy for convenience (Acquisti & Grossklags, 2005). This factor likely carries over to cost-benefit assessment and continuance commitment toward information security and whether people are willing to take precautions against social engineering threats or whether they continue to commit to their behavioral and psychological investments (Charbaji & Jannoun, 2005).

From the prospective of social engineering and information security, then, continuance commitment is the result of a positive cost-benefit association in reference to the advantages of perceived rewards that may yield compared to the cost of taking precautions or the opportunity costs associated with a social engineering threat (Thomas, 2004). On the other hand, if the cost of taking precautions is perceived as small relative to a threat, or if the value proposition from the threat delivers only a small incremental degree of perceived value, people may take precautions against the threat (Pechmann et al., 1993). When people perceive that benefits outweigh the cost of taking precautions, they exhibit continuance commitment where they are more likely to yield to social engineering threats to gain the perceived possible rewards and vice-versa (Hsu & Kuo, 2003). Stated formally, we hypothesize that:

H4: People who are higher in continuance commitment will succumb to social engineering more frequently than those who are lower in continuance commitment.

People form their self-concepts based in part on their relationships with or membership in certain social circles, which may be referred to as social identity (Tajfel & Turner, 1986), and this leads to affective commitment, which is a form of psychological attachment to others with whom they like and identify (Allen & Meyer, 1990). Affective commitment causes people to expend effort and perform actions in exchange for the satisfaction that is derived from the emotional ties with the target (a brand, person, group, or organization) (Beck & Wilson, 2000). For example, people model the behavior of valued peer-groups or important others to be associated with the restricted social group or "clique" (Asch, 1946). Many marketing campaigns take advantage of this tendency by persuading people to perform actions (i.e., make purchases) to maintain a relationship or an association with a certain fashionable group or famous individual (Cacioppo et al., 1986). In the context of this study, it is important to recognize that people vary in their degrees of social attachment and social identity (Asch, 1946; Beck & Wilson, 2000; Tajfel & Turner, 1986). That is to say, some people easily identify with others while others do not, and some people are more malleable than others in their affinity with people who they do not have personal association or contact, such as in the case of identification with a famous person (Fennis, Das, & Pruyn, 2006).

In terms of information security and social engineering, people sometimes will divulge sensitive or private information to those to whom they feel committed even if these others do not have "a need to know." People do this because they have an attachment to or emotional bond and believe that the relationship is paramount to the possible information security threat (Bergman, 2006; Theoharidou et al., 2005). Consistent with these theories, when social engineers utilize peripheral route persuasion geared toward social proof (those that involve an affinity or identification with a social entity or important other), people who are more affectively committed are more susceptible to social engineering schemes that utilize social proof than those who are not. Stated more formally,

H5: People who are higher in affective commitment will succumb to social engineering more frequently than those who are lower in affective commitment.

Likeability and Trust

The concept of "liking" from an ELM point of view draws from characteristics such as physical attractiveness, charisma, charm, or general popularity (Cialdini, 2001; Gass & Seiter, 1999). These features,

in the context of peripheral route persuasion, tends to lead people to comply with requests in order for be liked by those they like (Cacioppo et al., 1986; Horai et al., 1974). In most social engineering cases, the attacker avoids coming into physical contact with the intended victim and instead relies on email, postal letters, Websites, or telephone calls to perpetrate the attack, and thus it is difficult for the social engineer to telegraph characteristics such as charm or charisma (Dotterweich & Collins, 2006). Therefore, the social engineer tries to get the potential victim to *like* the perpetrator and gain his or her trust by establishing a friendly rapport (Gendall, 2005). They do this in what is sometimes referred to as a confidence scheme by preying on one's loneliness, or making appeals to one's need for friendship, or creating a sense of similarity with the potential victim, or feigning ties with or even pretending to be a likeable famous individual (Mitnick & Simon, 2002).

Asch (1946) and others (Casciaro & Lobo, 2005; Guadagno & Cialdini, 2002; Horai et al., 1974; Komito, 1994) have identified that people usually "trust those they like," and conversely they usually "like those they trust." Moreover, people trust those they perceive as credible such as having a special expertise or ability, even if the perceived ability or expertise is not related to the particular item the "expert" represents (Cacioppo et al., 1986; Gass & Seiter, 1999; Horai et al., 1974). For example, people may be persuaded by a professional basketball player or a famous actor they like to purchase batteries or a breakfast cereal (Giles & Wiemann, 1987). Hence, the basis for liking from an information security and social engineering perspective is trust (Charbaji & Jannoun, 2006; Guadagno & Cialdini, 2002; Wang & Emurian, 2005; Yakov, Shankar, Sultan, & Urban, 2005).

Some research (e.g., Walczuch & Lundgren, 2004) has defined various forms or types of trust; nevertheless, some people have a greater propensity to trust generally than others (Charbaji & Jannoun, 2006; Chen & Barnes, 2007; Krishnan & Martin, 2006; Stephenson, 2008). Under-trust in one setting may result in foregone beneficial opportunities, paranoia, and unnecessary tensions, but overtrust leads to ineffective monitoring, fraud, reduced efficiency, and incompetence (Stephenson, 2008). Overtrust may "limit the cognitive efforts of [people] when they consider their broader environment… and the cognitive comfort that trust brings about also limits variety of thought and action and attentiveness to detail" (Krishnan & Martin, 2006, pp. 894-895) making one more susceptible to peripheral route persuasion.

A substantial body of literature describes the nature of "online-trust" and its important role in conducting online business transactions, but also hints that a trusting nature can lead one into the potential of falling victim to social engineering ploys (Guadagno & Cialdini, 2002; Wakefield & Whitten, 2006; Yakov et al., 2005). Consider for example that online retailers often utilize techniques on their Websites that people associate with the familiar brick-and-mortar facilities, such as images of a building, trusted logos, or famous people (Walczuch & Lundgren, 2004). Social engineers regularly employ these same techniques in phony Websites or emails. They also utilize close-distance personal writing styles that attempt to establish a rapport with the potential victim in order to prey on his/her loneliness or need for friendship, and they strive to create a feeling of similarity with potential victims to gain their trust (Mitnick & Simon, 2002). Consequently we hypothesize that,

H6: People who are more trusting will succumb to social engineering more frequently than those who are less trusting.

Fear, Authority, and Scarcity

Telemarketers and debt collectors frequently utilize fear tactics and authoritative commands to gain a person's compliance (FTC, 2003). Borrowing from these techniques, social engineers have used authority and fear tactics to elicit information or actions from potential victims (Mitnick & Simon, 2002; Panko, 2004). A common phishing technique, for example, is to broadcast an email containing an urgent subject line to get the potential victim's attention. Samples of actual phishing email subject lines have included: "Alert From Chase Card Services," "Your eBay account will be Suspended!" "Please Update Your Bank of America Profile: Personal Information Error," and "Urgent! Invalid information added to your PayPal account." Contained within the emails are dire warnings along with official looking logos and formatting, followed by instructions to browse to a Web page and enter information or call

a particular phone number. A common pretext is to telephone members of an elderly association and impersonate a government official, then using pressure and fear tactics, instruct the potential victims to enroll in an unnecessary or even fraudulent insurance program (Rusch, 1999).

Milgram's (1983) landmark work on obedience to authority offered provocative evidence of the extent to which people will submit to commands of an authority figure. Obedience creates actions in deference to those who have perceived coercive power (Weatherly, Miller, & McDonald, 1999), such as in the case of one who can terminate a bank account or some valued privilege. Authority therefore can be used to engender fear, where people obey commands to avoid a negative consequence such as losing a privilege or something of value, punishment, humiliation, or condemnation (Milgram, 1983). Social engineers prey on the impulses of those who respond to fear from an authoritative command (Cacioppo et al., 1986; Cialdini, 2001; FTC, 2003; Miller, 2005; Mitnick & Simon, 2002).

However, people vary in their obedience and the degrees to which they will comply with commands (Helm & Morelli, 1985). Factors such as deference to authority play an important role in obedience and persuasion even when people are exposed to those who possess highly authoritarian characteristics (Blass, 2000). Moreover, when people feel threatened or coerced, they sometimes strive to repel the coercion by establishing a psychological defense mechanism of resistance (Donelson, 1973). This reactance may be triggered by events that impede a perceived freedom of choice, and by any perceived social influences that make an individual feel a force pushing him/her to act. It may at times motivate efforts to restore the lost freedom to prevent the loss of other freedoms (Brehm & Cole, 1966).

When fear appeals are made, people respond based on the magnitude of perceived severity of a depicted threat, the probability people perceive of that event's occurrence, and the efficacy of the recommended response (Rogers, 1975). If the portrayed threat is not believed, or if the event is thought not to be severe, or the recommended solution is not believed to be adequate to deal with the threat, people may resist (Severin & Tankard, 1997). Therefore, in some cases, people will readily comply with someone who "seems" authoritative while others remain skeptical and resist (Brehm, 1966; Donelson, 1973). When social engineers use authority to project fear or a threat, those who respond more readily and obediently to authority are more likely to comply with these requests than people who are more skeptical and remain defiant (Weatherly et al., 1999). Therefore, we hypothesize that:

> *H7: People who are more obedient to authority will succumb to social engineering more frequently than those who are less obedient to authority.*

Fear has an additional element that impacts how people may or may not respond to social engineering threats. Similar to how authority may trigger reactance, scarcity may engender a reactive hoarding impulse (Melamed, Szor, Barak, & Elizur, 1998; Plomin, DeFries, & McClearn, 2001) in which people may react quickly and at times illogically to perceived shortages (Brehm, 1966). Social engineers often try to gather information or elicit an action because of the premise that the potential victim will run out of time or the opportunity to capitalize on gaining some scarce item (Lynn, 1992; Rutte, Wilke, & Messick, 1987). Reactance theory (Brehm, 1966) posits that people may change their views and behavior when they think their ability to act might be curtailed by an external constraining force such as a shortage in the supply of a valued item. In essence, people react when an individual perceives that his freedom is restricted or threatened about an important matter on which he thinks himself capable to make a choice among different alternatives (Pennebaker & Sanders, 1976). Thus when some people feel their freedom to act and make choices is threatened they experience a dissonance that motivates a reactance to the perceived constraining threat (Rusch, 1999).

Yet people differ in their perceptions of perceived threats and whether they react or resist (Dowd & Seibel, 1990; Lindsey, 2005), particularly if the threat involves a perceived shortage rather than a direct personal threat (Dowd & Seibel, 1990). If social engineers use a technique that strives to gather information or elicit an action because of the premise that the potential victim may run out of time or the opportunity to capitalize on gaining some scarce item, then people who react more readily to the scarcity threat will become victims of this type of social engineering threat than those who tend to resist such threats

(Guadagno & Cialdini, 2002; Pennington & Hastie, 1986). We therefore hypothesize that:

H8: People who are more reactant will succumb to social engineering more frequently than those who are more resistant.

METHOD

We chose a field study employing two data-gathering techniques: a questionnaire containing antecedent factors, and an observation of behaviors related to the dependent variables (described below). Field studies, having strong ecological validity, are thought to be a good choice when the study is highly relevant to real-world events and the researchers wish to generalize to the world of practice. The organization in which we conducted the field study was a government-regulated entity that had had serious security breaches in the past. In the public interest, they encouraged us to study the problem and acceded to our requirement that participation would be anonymous and the data gathered held in strict confidence. Prior to engaging in the study, we received institutional human-subjects review approval, and received guidance from the company's attorneys and human resources department.

The company monitors data and communication as a standard practice and requires employees to sign an employment agreement that includes their consent to monitoring when they are hired. Laws in the United States and the European Union support the right of corporations to inspect and monitor work and workers, which arises from needs related to business emergencies and a corporation's rights to protect its interests (Keck, 2005; Losey, 1998; Borrull & Oppenheim, 2004). Companies can monitor employees, and while advisable to take overt action to notify its employees of the practice, it is not required by law (Scholz, 1997).

Sample and Data Collection

The data collection consisted of two parts, a questionnaire and objective observations. For the questionnaire, we drew from Allen and Meyer's (1990) items for commitments, Gendall (2005) for trust, and Lindsey (2005) and Weatherly, Miller, and McDonald's (1999) for obedience to authority and reactance/resistance. We also gathered self-report items for dependent variables to determine their correlation with the objective observations of subjective social engineering behaviors. Eight-hundred and fifty participants were randomly selected from the company directory and 612 responded; however, of those 612, 24 questionnaires were incomplete (perhaps the result of a loss of network connection as most contained duplicate message authentication codes with completed questionnaires) and were thus discarded, which yielded a 69% response rate at a ± 3.5% sampling confidence with a standard error of estimate of 0.05, which indicates a high level of sampling validity (Salant & Dillman, 1994).

Procedures

Corporate executive sponsors facilitated entrée once researchers had signed a nondisclosure and confidentiality agreement. Researchers were provided with a company directory of the population under study, including location and email addresses. The corporate sponsors sent each participant a message, with an acknowledgement flag set, in which they were informed with the cover story that researchers were interesting in studying employee perceptions about telemarketing, and asked for their cooperation. They were assured of the confidentiality of their responses in the message. The researchers then contacted participants via email and attachment with a cover letter once again using the cover story and ensuring confidentiality of the respondents, along with an announcement of the URL of the online data collection instrument. Also, each participant each received an authentication password. When participants took the questionnaire, the authentication password was used to produce a message digest to keep track of who had completed the questionnaire and to ensure that the questionnaire was taken only once by each participant.

The researchers collected phishing messages they had received over the course of many months as well those provided by an information security consultant who specialized in social engineering. Pretext scenarios were constructed with the assistance of an information security consultant, analysts from a market research firm, and members from the

company's security department who had collected successful and thwarted incidents at the company. The researchers, information security consultant, and the analysts from the market research firm reviewed the materials to ensure that the range of persuasive message characteristics was adequately covered. Student-actors were then enlisted from the university's college of visual arts and theatre to perpetrate the phishing and pretext ruses. Telemarketers from the market research firm rehearsed the student-actors on the delivery of persuasive messages, and the information security consultant coached them on specific pretexts. Phishing attacks were conducted using emails containing the various techniques to get participants to click on Web page URLs and enter personal or company confidential information, or open email attachments containing an executable program that created a network connection and reported back to the researchers that the file had been opened. Pretexts were done with telephone calls to participants where the actors pretended to be various officials, internal employees, employees of trading partners, customers, utility companies, and financial institutions, and solicited confidential information using the study range of persuasive techniques.

Measures

As indicated, the factors were collected as self-report items using an online questionnaire. To examine the construct validity of the self-report independent variables (IVs) on social engineering security behavior, we ran a Varimax rotated Principal Components Analysis on the relevant items. If items for the eight IVs discriminate the constructs as intended, they will load highly on the posited two outcome measures and not cross-load. The loadings did indeed cleanly discriminate between the measures (Table 1 shows item loadings and reliabilities). Whereas we tested the various factors via the direct effects of the eight IVs on behavioral social engineering responses, the analysis offers strong evidence that attempts to capture in-practice assessments of these threats at a macro level will likely find that the factors do account for the relationships with the social engineering outcomes.

Phishing emails and pretext attacks were carried out over a period of six months in which the coadjutors used social engineering to try to gain confidential information from each participant two times each week. An example was to send an email asking participants to click on a link to update personal and confidential information. The frequency of violations was collected and examined for each participant.

RESULTS

Before the hypotheses were tested, we needed to take a preliminary step to determine whether the objective measures of security behaviors (phishing and pretext) were relatively independent, or if they were indicators of an underlying security behavior construct. As a result, we looked at the frequency with which the person responded to pretexts and phishing attempts or opened "potentially" destructive email attachments. See the descriptive statistics in Table 2.

To determine whether these behaviors represented separate constructs or constituted a single variable (i.e., social engineering security behavior) we conducted an exploratory factor analysis. This analysis showed that the behaviors loaded on a single factor. Further, the reliability of the items in factor was high (β = .88), (Stevens, 1989). As a result, we standardized each of the observed items and then reverse coded the Z-score for the frequency that the person positively responded to an adverse social engineering behavior. We then created a single measure referred to as "observable social engineering security behavior." Thus, "objective" behavior represented samples of the objective measures of employee social engineering security behaviors, whereas the variable "subjective" represented the generalized perceptions employees had about their social engineering behavior. We retained both subjective and objective outcome measures in the analyses to triangulate the congruence of self-reported perceptions with samples of actual behavior.

Each of the hypotheses was then tested using both the self-reported social engineering behaviors and the objective social engineering behavior measures. This allowed for a more robust test of the hypotheses rather than relying upon subjective or objective measures alone. In the current study, the self-report and objective measures very highly correlated (r = .89). Even with this high degree of correlation, however, we cannot assume that the measures are

TABLE 1 **Scales, loadings, and reliabilities**

Threat Severity Items	Loading	Cross–Load	Composite reliability
I believe that protecting my confidential information is: Unimportant...important	0.907	0.130	0.95
Threats to the security of my confidential information are: Harmless...severe	0.877	0.144	
Having my confidential information obtained by someone without my authorization is: Harmless…severe	0.925	–0.231	
Threats from social engineering are: Harmless…severe	0.918	–0.140	
Vulnerability Items	**Loading**	**Cross–Load**	**Composite reliability**
The vulnerability of my confidential information to security violations is: Invulnerable…vulnerable	0.832	0.330	0.86
I believe that trying to protect my confidential information will reduce illegal access to it: Unlikely…likely	0.771	0.344	
The likelihood of someone getting my confidential information without my consent or knowledge is: Unlikely...likely	0.809	0.211	
The likelihood of a social engineering violation occurring to me is: Unlikely...likely	0.774	0.240	
Normative Commitment Items	**Loading**	**Cross–Load**	**Composite reliability**
When someone gives me something, I feel like I should return the favor	0.891	0.079	0.89
I was taught to keep my promises	0.868	0.154	
I believe in the keeping up my end of the bargain even when others don't	0.911	0.023	
When someone does something for me, I feel like I should do something for them	0.879	–0.040	
Continuance Commitment Items	**Loading**	**Cross–Load**	**Composite reliability**
I believe in finishing what I start	0.888	0.210	0.80
If I start on something, I cannot stop until it's done	0.756	0.368	
I will take risks if there is a chance I will be rewarded	0.722	0.322	
If I don't take a chance on things, I feel like I will lose out	0.811	0.176	
Affective Commitment Items	**Loading**	**Cross–Load**	**Composite reliability**
If I like someone, I will help them even when I probably shouldn't	0.921	0.049	0.87
I enjoy helping people I like	0.900	–0.178	
If my friends are doing something, I like to join in	0.877	0.252	
It's important to be part of the "in group"	0.724	0.324	
Trust Items	**Loading**	**Cross–Load**	**Composite reliability**
I have confidence in people who have made successes of their lives	0.844	0.073	0.82
Friendly people are usually trustworthy	0.893	0.093	
I think professional-looking advertising materials are more trustworthy than those shabbily put together	0.828	0.390	
I trust people who do advertising because they have special expertise	0.733	0.124	
Obedience Items	**Loading**	**Cross–Load**	**Composite reliability**
I believe it is important to follow the chain of command	0.901	–0.111	0.85
People who have confidence are good decision-makers	0.762	0.377	
I worry a lot when someone tells me I am about to lose my privileges	0.890	0.097	
I would rather comply with an order than to get into trouble	0.888	0.177	
Reactance Items	**Loading**	**Cross–Load**	**Composite reliability**
I think it is important to act quickly if time is running out	0.733	0.248	.74
I buy something if it's no longer going to be available and its value will increase	0.711	0.378	
When there is a limited time to act, I do act	0.812	0.152	
I don't like losing out on opportunities	0.861	0.224	

TABLE 1 **Scales, loadings, and reliabilities (continued)**

Subjective Measures Items	Loading	Cross–Load	Composite reliability
I update my information online when requested	0.862	0.333	.89
I provide confidential information when important people call to request it	0.888	0.277	
I open links in email to get important information	0.901	–0.038	
I don't give out sensitive information even if it would benefit me personally (reverse code)	0.899	0.190	

TABLE 2 **Descriptive statistics, scale reliabilities, and intercorrelations of study variables**

	M	S.D.	1	2	3	4	5	6	7	8	9	10	11	12	13
1. Threat severity	4.34	1.38	(.95)												
2. Vulnerability	3.74	0.99	.27	(.86)											
3. Normative commitment	4.34	1.38	.31	.21	(.89)										
4. Continuance commitment	3.74	0.99	.25	.38	.55	(.80)									
5. Affective commitment	3.96	1.19	.31	.21	.44	.25	(.87)								
6. Trust	3.95	1.23	.22	.20	.45	.37	.54	(.82)							
7. Obedience	3.80	0.92	.27	.31	.42	.35	.35	.26	(.85)						
8. Reactance	3.91	1.05	.55	.44	.51	.34	.61	.54	.29	(.74)					
9. Employee age	37.96	11.25	.15	.20	.35	.17	.17	.16	.26	.05	—				
10. Employee education	2.65	0.88	.31	.17	.31	.21	.13	.19	.18	.01	.09	—			
11. Employee gender	1.47	0.50	–.01	.03	.03	.01	.04	.05	.04	–.01	.01	–.09	—		
12. Subjective behaviors	4.19	1.25	.39	.37	.46	.48	.59	.38	.48	.32	.19	.09	–.09	(.89)	
13. Objective behaviors	.0000	3.39	.34	.43	.43	.46	.51	.33	.43	.27	.15	.13	–.06	.84	(.87)

Notes: N = 588. All correlations greater than r = .14 are significant at p < .001; correlations greater than .12 are significant at p < .01

completely interchangeable (Bommer et al., 1995). In fact, nearly 20% of the variance between these two measures remains unexplained. As a result, we left the objective and subjective measures separate so that the hypotheses could be tested against each criterion variable.

To test the hypotheses contained in this research, an ordinary least squares regression was conducted whereby the variables of interest and the controls were regressed on the self-report and objective measures of social engineering behavior. The intercorrelations, means, standard deviations, and scale reliabilities are reported in Table 2. The results of the regression models are reported in Table 3. To provide a more controlled assessment of the hypotheses of interest, we included a number of control variables to provide a better-controlled assessment. These control variables included the employee demographics of age, gender, and education.

The regression results provide a very consistent story across the two social engineering security behavior measures. The first hypothesis tested whether people who perceived greater severity of social engineering threat would fall victim less frequently. This hypothesis was supported for both self-report ($\beta = .13$, $p < .001$) and objective ($\beta = .12$, $p < .001$) social engineering security behaviors. Next, we tested whether those who felt more vulnerable to social engineering threats would fall victim less frequently. This hypothesis was

TABLE 3 **Ordinary least squares regression results for self-reported and objective observations of security**

	Behaviors	
Variable	Subjective Security Behaviors	Objective Security Behaviors
Threat severity	.13**	.12**
Vulnerability	.11**	.14**
Normative commitment	.13***	.11**
Continuance commitment	.17***	.20***
Affective commitment	.16***	.20***
Trust	.24***	.16**
Obedience	.10**	.11**
Reactance	.04	.06
Employee age	.13***	.10*
Employee gender	.01	.01
Employee education	.07*	.12**
Model adjusted R2	.47	.42

Notes: N = 588. All variables are standardized regression coefficients.

supported for both self-report (β = .11, $p < .001$) and objective (β = .14, $p < .001$) social engineering security behaviors. The next hypothesis stated that people who were higher in normative commitment would succumb to social engineering more frequently than those who are lower in normative commitment. This hypothesis was supported for both self-report (β = .13, $p < .001$) and objective (β = .11, $p < .01$) social engineering security behaviors. Likewise, we proposed that if people were higher in continuance commitment, they would succumb to social engineering more frequently than those who were lower in continuance commitment. Again this was supported for both self-report (β = .17, $p < .001$) and objectively observed (β = .20, $p < .001$) social engineering security behaviors. The next hypothesis stated that people who were higher in affective commitment would fall victim to social engineering more frequently than those who are lower in affective commitment. As hypothesized, this was supported for both self-report (β = .16, $p < .001$) and objective (β = .20, $p < .001$) social engineering security behaviors, and we proposed that people who were more trusting would succumb to social engineering more frequently than those who are less trusting. Again, as hypothesized, this was supported for both self-report (β = .24, $p < .001$) and objectively collected social engineering security behaviors (β = .16, $p < .01$).

Because there are indications that people comply with authority figures when requests are made, hypothesis five proposed that people who are more obedient to authority would succumb to social engineering more frequently than those who are less obedient to authority. This was supported for both self-report (β = .10, $p < .01$) and objectively collected (β = .11, $p < .01$) social engineering security behaviors. Our last hypothesis presented an interesting case. It proposed that people who were more reactant would yield to social engineering more frequently than those who are more resistant. Although the relationships were positive, they were not significant for either the self-report (β = .06, $p > .05$) or objective (β = .06, $p > .05$) measures.

DISCUSSION

In terms of information security defenses, most of the research has investigated either available security technologies or the management of security infrastructure such as conducting risk analyses for the application of technological defenses. But the defense problem has a behavioral grounding, and the significance of people's failure to take precautions against information security threats has been largely ignored, especially in regard to social engineering threats. Failing to take information security precautions is a significant issue. Carelessness with information and failure to take available precautions contribute to the loss of information and even to crimes such as corporate espionage and identity theft of which the U.S. Department of Justice (2004) estimates that one in three people will become victims at some point in their lifetime. Social engineering is a major avenue for information security breaches, yet other than anecdotal materials, there has been little to help managers address the problem because the relationships among personal factors and social engineering outcomes has not been thoroughly investigated nor explained.

Social engineering takes many different forms, although the techniques mainly rely on peripheral route persuasion. As such, the threat assessment theory and the ELM framework provide for understanding the ways in which social engineers gather sensitive information or get unwitting victims to comply with their requests for actions. Our investigation has attempted to bridge the theory that explains how people are persuaded through peripheral routes with the social engineering outcomes using an empirical field study in which we investigated whether the factors that account for how people are persuaded in marketing campaigns to make purchases may apply as well to social engineering to give up confidential information.

Specifically, we found that people who are high in normative commitment feel obligated to reciprocate social engineering gestures and favors such as receiving free software or gift certificates by giving up company email addresses, employee identification numbers, financial and insurance data, and other confidential and sensitive information. Likewise, people who are high in continuance commitment tend to provide information to escalating requests. We found that high continuance commitment people will even give up increasingly sensitive information as part of an online game just to try to win the game. High affective commitment was also

found to contribute to successful social engineering. These individuals tend to provide information because they want to be part of a socially desirable group or be accepted. Thus all three of Allen and Meyer's (1990) types of commitments were found salient in social engineering attacks.

Online trust has been studied in relation to whether people will conduct "e-business" and has provided some provocative indicators that this factor may as well lead to social engineering susceptibility. Social engineers often apply techniques that try to cultivate trust by a process of establishing a friendly rapport or by reference to likable famous individuals. Consistently, we found that people who were trusting were more likely to fall victim to social engineering more than those who are distrusting. This creates a double bind when juxtaposed with the need for online trust in e-business.

Whereas some people are more persuaded by trust and friendly rapport, others are more responsive to authority figures. We tested authoritative commands and fear tactics in relation to the levels of people's obedience to authority and reaction to scarcity. Higher degrees of obedience to authority were important factors in whether people responded to these types of social engineering attacks; however, we found no support for reactance to scarcity. In a marketing sense, perhaps people will strive to own something of dwindling supply, but it does not appear that reactance to scarcity such as using a "time is running out" technique accounts for whether people succumb to such social engineering ploys.

Based on these findings, we make several recommendations for managers. Since commitment is a fairly stable personal characteristic and is instrumental in effectively functioning organizations (McCaul, Hinsz, & McCaul, 1995; Mowday, Steers, & Porter, 1979; Sagie, 1998), managers need to be able to assist employees in recognizing and discriminating appropriate targets of their commitments; that is, commitment to company means withholding commitments from potential threats. Next a common security countermeasure is to compartmentalize roles and allocate information on a "need to know" basis so that sensitive information is not inadvertently leaked. But this technique runs counter to many organizational theories and interventions that strive for organic structuring and open communications. People need to be inculcated with sense of ethical conduct and responsibility and must be trustworthy. Trust, however, is a two-way street; trustworthy employees expect to be trusted. As such, training is seen as an important component in dealing with social engineering. It may be that people do not connect their general willingness to protect sensitive information with the duplicity that may occur, and training should mitigate first making employees aware and second in developing new coping behaviors. This is particularly important in relation to online trust. Technologies exist that are used as countermeasures such authentication and watermarking, and training can assist people knowing what to look for before trusting.

Finally, in dealing with the issue of obedience to authority, corporate security policies should be established that address the classification of information and the circumstances under which sensitive information can be divulged, and should also include the processes and accountability for reporting suspected incidents so that people who are obedient to authority have clear delineation of the lines of authority and the roles and responsibilities of the actors. Then regular, ongoing security awareness programs should be conducted to prevent complacency.

Beyond the obvious ones, there are some specific limitations that are worth noting. First, there is always some discrepancy between what people report about their behaviors and what they actually do, thus we utilized observational measures to address this limitation. The high correlation and the consistent results indicate that good congruence between our self-report subjective measures and those we observed. Outside of that issue, however, our participants were those who responded to the requests and filled out the questionnaire posted online. Even though our response rate and sampling confidence were good, clearly there is a complication as those who did not respond may have made important contributions to our investigation and to our findings. Next, to a large extent, the ways people cope with threats are socially influenced. Our study involved only people in the United States. It would be interesting to research an international population to determine if the framework could be generalized across social and cultural contexts. Also along these lines, additional research is needed in an organizational and group-work context.

REFERENCES

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making, *IEEE Security and Privacy,* 3: 26-33.

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior, *Journal of Applied Social Psychology,* 32: 665-683.

Albrechtsen, E. (2006). A qualitative study of users' view on information security, *Computers & Security,* 25: 6, 445-451.

Aldoory, L., & Van Dyke, M. A. (2006). The roles of perceived shared involvement and information overload in understanding how audiences make meaning of news about bioterrorism, *Journalism & Mass Communication Quarterly,* 83: 346-361.

Allen, N. J., & Meyer, J. P. (1990). The measurement and antecedents of affective, continuance and normative commitment to the organization, *Journal of Occupational Psychology,* 63: 1-18.

Arkes, H., & Blumer, C. (1985). The psychology of sunk cost, *Organizational Behavior and Human Decision Process,* 35: 124-140.

Asch, S. E. (1946). Forming impressions of personality, *Journal of Abnormal and Social Psychology,* 41: 258-290.

Beck, K., & Wilson, C. (2000). Development of affective organizational commitment: A cross-sectional examination of change with tenure, *Journal of Vocational Behavior,* 56: 114–136.

Bergman, M. E. (2006). The relationship between affective and normative commitment: Review and research agenda, *Journal of Organizational Behavior,* 27: 645-663.

Blass, T. (2000). Invited response to review of "Obedience to authority: Current perspectives on the Milgram paradigm," *British Journal of Educational Psychology*, 70: 624-625.

Bommer, W. H., Johnson, J. L., Rich, G. A., Podsakoff, P. M., & MacKenzie, S. B. (1995). On the interchangeability of objective and subjective measures of employee performance: A meta-analysis, *Personnel Psychology,* 48: 587-605.

Brehm, J. W. (1966). *A theory of psychological reactance.* New York: Academic Press.

Brehm, J. W., & Cole, N. H. (1966). Effects of a favor that reduces freedom, *Journal of Personality and Social Psychology,* 3: 420-426.

Bresz, F. P. (2004). People–often the weakest link in security, but one of the best places to start, *Journal of Health Care Compliance,* July-August: 57-60.

Brill D. W., & Molton, P. (2006). Escalation of economic costs, sunk costs, and opportunity costs: A psychological investment perspective, *International Journal of Human Decisioning,* 12: 29-38.

Cacioppo, J. T., Petty, R. E., Kao, C. F., & Rodriguez, R. (1986). Central and peripheral routes to persuasion: An individual difference perspective, *Journal of Personality and Social Psychology,* 51: 1032-1043.

Calluzzo, V. J., & Cante, C. J. (2004). Ethics in information technology and software use. *Journal of Business Ethics,* 51(3): 301-312.

Casciaro, T., & Lobo, M. S. (2005). Competent jerks, lovable fools, and the formation of social networks, *Harvard Business Review,* 83: 92-99.

Charbaji, A., & Jannoun, S. E. L. (2005). Individuality, willingness to take risk, and use of a personal e-card, *Journal of Managerial Psychology,* 20: 51-58.

Chen, Y-H, & Barnes, S. (2007). Initial trust and online buyer behavior, *Industrial Management and Data Systems,* 107: 21-36.

Cialdini, R. B. (2001). *Influence: Science and Practice*. Boston, MA: Allyn & Bacon.

Debar, H., & Viinikka, J. (2006). Security information management as an outsourced service, *Information Management & Computer Security,* 14:5: 417-435.

Denis, T., Trobec, R., Pavei, N., & Tasi, J. F. (2007). Information system security and human behavior, *Behavior & Information Technology,* 26: 113-118.

Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness, *Computers & Security,* 26: 73-80.

Donelson, E. (1973). *Personality: A Scientific Approach*. Pacific Palisades, CA: Goodyear Publishing.

Dotterweich, D. P., & Collins, K. S. (2006). The practically of super bowl advertising for new products and companies, *Journal of Promotion Management,* 11: 19-31.

Dowd, E. T., & Seibel, C. A. (1990). A cognitive theory of resistance and reactance: Implications for treatment, *Journal of Mental Health Counseling,* 12: 458-469.

Federal Trade Commission. (2003). Complying with the telemarketing sales rule. Accessed January 29, 2007, from http://www.ftc.gov/bcp/conline/pubs/buspubs/tsrcomp.htm

Fennis, B. M., Das, E., & Pruyn, A. Th. H. (2006). Interpersonal communication and compliance: The disrupt-then-reframe technique in dyadic influence settings, *Communication Research,* 33(2): 136-151.

Festinger, L., & Carlsmith, J. M. (1959). Cognitive consequences of forced compliance, *Journal of Abnormal and Social Psychology,* 58: 203-210.

Gao, W., & Kim, J. (2007). Robbing the cradle is like taking candy from a baby, Proceedings of the Annual Conference of the Security Policy Institute (GCSPI), October 4, Amsterdam, The Netherlands, *1*, 23-37.

Gass, R. H., & Seiter, J. S. (1999). *Persuasion, Social Influence, and Compliance Gaining*. Needham Heights, MA: Allyn-Bacon.

Gendall, P. (2005). Can you judge a questionnaire by its cover? The effect of questionnaire cover design on mail survey response, *International Journal of Public Opinion Research,* 17: 346-361.

Giles, H., & Wiemann, J. M. (1987). Language, social comparison and power. In C. R. Berger and S. H. Chaffee (Eds.), *The Handbook of Communication Science* (pp. 350-384). Newbury Park, CA: Sage.

Grossklags, J., & Acquisti, A. (2007). When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information, Sixth Workshop on the Economics of Information Security (WEIS 2007), June 6, Pittsburgh, PA, 7-18.

Grothmann, T., & Reusswig, F. (2006). People at risk of flooding: Why some residents take precautionary action while others do not, *Natural Hazards,* 38: 101–120.

Grunig, J. E. (1997). A situational theory of publics: Conceptual history, recent challenges and new research. In D. Moss, T. MacManus, & D. Vercic (Eds.), *Public Relations Research: An International Perspective* (pp. 3-48). London: International Thomson Business Press.

Guadagno, R. E., & Cialdini, R. B. (2002). On-line persuasion: An examination of differences in computer-mediated interpersonal influence, *Group Dynamics: Theory, Research and Practice,* 6: 38-51.

Gundlach, G. T., Achrol, R. S., & Mentzer, J. T. (1995). The structure of commitment in exchange, *Journal of Marketing,* 59: 78-92.

Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions, *MIS Quarterly,* 20(Sept.): 257-258.

Helm, C., & Morelli, M. (1985). Obedience to authority in a laboratory setting: Generalizability and context dependency, *Political Studies,* 14: 610–627.

Hochhauser, M. (2004). Smart executives, dumb decisions, *Journal of Risk Management,* 51: 64-73.

Horai, J., Naccari, N., & Fatoullah, E. (1974). The effects of expertise and physical attractiveness upon opinion agreement and liking, *Sociometry,* 37: 601-606.

Hsu, M-H., & Kuo, F-Y. (2003). An investigation of volitional control in information ethics, *Behavior and Information Technology*, 22: 53-62.

International Federation of Accountants. (2006). Intellectual assets and value creation: Implications for corporate reporting. Paris, France. Retrieved November 4, 2007, from: http://www.oecd.org/dataoecd/2/40/37811196.pdf

Janoff-Bulman, R., & Frieze, I. H. (1983). A theoretical perspective for understanding reactions to victimization, *Journal of Social Issues,* 39: 1-17.

Josephs, R. A., Larrick, R. P., Steele, M., & Nisbett, R. E. (1992). Protecting the self from the negative consequences of risky decisions, *Journal of Personality and Social Psychology,* 62: 26-37.

Keck, R. (2005). Disruptive technologies and the evolution of the law, *Legal Briefs,* 23(1): 22-49.

Kelley, H. H., & Thibaut, J. (1978). *Interpersonal Relations: A Theory of Interdependence*. New York: Wiley.
Komito, L. (1994). Communities of practice and communities of trust: Global culture and information technology, *Journal of Anthropology*, 4: 33-45.
Krishnan, R., & Martin, X. (2006). When does trust matter to alliance performance? *The Academy of Management Journal,* 49: 894-917.
Kurland, N. B. (1995). Ethical intentions and the theories of reasoned action and planned behavior. *Journal of Applied Social Psychology,* 25(4): 297-313.
Leach, J. (2003). Improving user security behavior, *Computers & Security*, 22: 685-691.
Lejeune, R., & Alex, N. (1973). On being mugged: The event and its aftermath, *Urban Life and Culture,* 2: 259-287.
Leyden, J. (2004). Clueless office workers help spread computer viruses, *The Register,* February 6: 17-21.
Lindsey, L. L. M. (2005). Anticipated guilt as behavioral motivation: An examination of appeals to help unknown others through bone marrow donation, *Human Communication Research,* 31: 453-481.
Losey, R. C. (1998). The electronic communications privacy act: United States Code. Orlando, FL: The Information Law Web. Accessed November 5, 2007, at http://floridalawfirm.com/privacy.html
Lynn, M. (1992). Scarcity's enhancement of desirability, *Basic and Applied Social Psychology,* 13: 67-78.
McCaul, H. S., Hinsz, V. B., & McCaul, K. D. (1995). Assessing organizational commitment: An employee's global attitude toward the organization, *Journal of Applied Behavioral Science,* 31: 80-90.
Melamed, Y., Szor, H., Barak, Y., & Elizur, A. (1998). Hoarding: What does it mean? *Comprehensive Psychiatry*, 39: 400-402.
Milgram, S. (1983). *Obedience to Authority: An Experimental View*. New York: Harper-Collins.
Miller, K. (2005). *Communication Theories: Perspectives, Processes, and Contexts*. New York: McGraw-Hill.
Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory, *Journal of Applied Social Psychology*, (30): 106-143.
Mitnick, K., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. New York: John Wiley & Sons.
Mowday, R. T., Steers, R. T., & Porter, L. W. (1979). The measurement of organizational commitment, *Journal of Vocational Behavior,* 14: 224-247.
Ong, T. H., Tan, C. P., Tan, Y. T., & Ting, C. (1999). SNMS – Shadow network management system, Symposium on Network Computing and Management, Singapore, May 21, 1-9.
Panko, R., DeFries, J. C., & McClearn, G. E. (1990). *Behavioral Genetics*. New York: W.H. Freeman.
Panko, R. R. (2004). *Corporate Computer and Network Security*. Upper Saddle River, NJ: Pearson/Prentice-Hall.
Pechmann, C., Zhao, G., Goldberg, M., & Reibling E. T. (2003). What to convey in antismoking advertisements of adolescents: The use of protection motivation theory to identify effective message themes, *Journal of Marketing*, 67(2): 1-18.
Pennebaker, J. W., & Sanders, D. Y. (1976). American graffiti: Effects of authority and reactance arousal, *Personality and Social Psychology Bulletin,* 2: 264-267.
Pennington, N., & Hastie, R. (1986). Evidence evaluation in complex decision making, *Journal of Personality and Social Psychology,* 51: 242-258.
Petty, R. E., Briñol, P., & Tormala, Z. L. (2002). Thought confidence as a determinant of persuasion: The self-validation hypothesis, *Journal of Personality and Social Psychology,* 82: 722-741.
Petty, R. E., & Cacioppo, J. T. (1986). *Communication and Persuasion: Central and Peripheral Routes to Attitude Change*. New York: Springer-Verlag.
Petty, R. E., Cacioppo, J. T., & Schumann, D. W. (1983). Central and peripheral routes to advertising effectiveness: The moderating role of involvement, *Journal of Consumer Research,* 10: 135-146.
Plomin, R., DeFries, J. C., McClearn, G. E., & McGuffin, P. (2001). *Behavioral Genetics* (4th ed.). New York: Worth Publishers.
Pyszczynski, T., Greenberg, J., & Solomon, S. (1997). Why do we need what we need? A terror management perspective on the roots of human social motivation," *Psychological Inquiry*, 8: 1–20.
Roe-Berning, S., & Straker, G. (1997). The association between illusions of invulnerability and exposure to trauma, *Journal of Traumatic Stress,* 10: 319-327.
Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change, *Journal of Psychology,* 91: 93-114.
Rosenstock, I. M. (1974). Historical origins of the health belief model, *Health Education Monograph*, 2: 328-335.
Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organizational security culture: Extending the end-user perspective, *Computers and Security*, 26(1): 56-62.
Rusch, J. J. (1999). *The social engineering of Internet fraud*. Report of the U.S. Department of Justice, INET'99 Conference. Retrieved February 6, 2007, from: http://www.isoc.org/inet99/proceedings/3g/3g_2.htm
Rutte, C. G., Wilke, H. A. M., & Messick, D. M. (1987). Scarcity or abundance caused by people or the environment as determinants of behavior in the resource dilemma, *Journal of Experimental Social Psychology,* 23: 208-216.
SANS. (2005). The SANS Security Policy Project. Bethesda, MD.
Sagie, A. (1998). Employee absenteeism, organizational commitment, and job satisfaction: Another look, *Journal of Vocational Behavior,* 52: 156-171.
Sasse, M. A., Brostoff, S., & Weirich, D. (2004). Transforming the weakest link–A human/computer interaction approach to usable and effective security, *BT Technology Journal,* 19(3): 122-131.
Scholz, J. T. (1997). Enforcement policy and corporate misconduct: The changing perspective of deterrence theory, *Law and Contemporary Problem,* (60): 153-268.
Schumann, D. W., Hathcote, J. M., & West, S. (1991). Corporate advertising in America: A review of published studies on use, measurement, and effectiveness, *Journal of Advertising* September*:* 35-55.
Severin, W. J., & Tankard, J. W. (1997). *Communication Theories: Origins, Methods, and Uses in the Mass Media.* New York: Addison-Wesley.
Sherif, J. S., Ayers, R., & Dearmond, T. G. (2003). Intrusion detection: The art and the practice, *Information Management and Computer Security*, 11(4): 175-186.
Shreve, M. (2004). The office now a major place for identity theft, *Crains,* (Sept.): 1-4.
Staw, B. M. (1981). The escalation of commitment to a course of action, *The Academy of Management Review,* 6: 577-587.
Stephenson, K. (2008). *The Quantum Theory of Trust: Power, Networks, and the Secret Life of Organizations*. New York: Prentice-Hall.
Stevens, J. (1989*). Intermediate Statistics: A Modern Approach*. Hillsdale, NJ: Lawrence-Erlbaum.
Straub, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study, *MIS Quarterly,* March 14: 45-62.
Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision-making, *MIS Quarterly,* 22: 441-469.
Tajfel, H., & Turner, J. C. (1986). The social identity theory of inter-group behavior. In S. Worchel & L. W. Austin (Eds.), *Psychology of Intergroup Relations*. Chicago, IL: Nelson-Hall.
Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799, *Computers and Security,* 24: 472-484.
Thomas, T. M. (2004). *Network Security First-Step*. Indianapolis, IN: Cisco Press.
U.S. Department of Justice. (2004). Violation of 18 USC. Gaining unauthorized access. *Information Security Report of the GAO*, 17: 188-219.
von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management, *Computers & Security*, 23: 371-376.
Wakefield, R. L., & Whitten, D. (2006). Examining user perceptions of third-party organization credibility and trust in an e-retailer, *Journal of Organizational and End User Computing,* 18: 1-19.

Walczuch, R., & Lundgren, H. (2004). Psychological antecedents of institution-based consumer trust in e-retailing, *Information & Management*, 42(1): 159-177.

Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications, *Journal of Computers in Human Behavior,* 21: 105-125.

Weatherly, J. N., Miller, K., & McDonald, T. W. (1999). Social influence as stimulus control, *Behavior and Social Issues,* 9: 25-46.

Wilson, R. (2004). Understanding the offender/environment dynamic for computer crimes: Assessing the feasibility of applying criminology theory to the IS security context, Proceedings from the 37th Hawaii International Conference on System Sciences (HICSS), January 5, Waikoloa, Hawaii, 1-10.

Workman, M., & Gathegi, J. (2005). Observance and contravention of information security measures, Proceedings of the World Conference on Security Management and Applied Computing, SAM01 June 16, Las Vegas, NV, 241-247.

Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: A comparative study of insider security contravention, *Journal of the American Society for Information Science and Technology,* 58: 212-222.

Yakov, B., Shankar, V., Sultan, F., & Urban G. L. (2005). Are the drivers and role of online trust the same for all web sites and consumers?: A large scale exploratory empirical study, *Journal of Marketing*, 69 (4): 133-152.

Yang, S., Hung, W., Sung, K., & Farn, C. (2006). Investigating initial trust toward e-tailers from the elaboration likelihood model perspective, *Psychology and Marketing,* 23: 429-445.