2014

THE ROLES OF POSITIVE AND NEGATIVE EXEMPLARS IN INFORMATION SECURITY STRATEGY

Richard Taylor, *Texas Southern University*

THE ROLES OF POSITIVE AND NEGATIVE EXEMPLARS IN INFORMATION SECURITY STRATEGY

Richard G. Taylor
Texas Southern University
taylorrg@tsu.edu

Sammie L. Robinson
Texas Southern University
robinsonsl@tsu.edu

THE ROLES OF POSITIVE AND NEGATIVE EXEMPLARS IN INFORMATION SECURITY STRATEGY

Richard G. Taylor
Texas Southern University

Sammie L. Robinson
Texas Southern University

ABSTRACT

The strategic approach used to manage organizational security is strongly influenced by management's perception of risk. These perceptions often lead executives to focus on the use of technology based solutions. Such solutions, aimed primarily at keeping data safe from outsiders, overlook the potential that more severe security breaches may be perpetrated by trusted insiders. Behavioral concepts such as ethnocentrism, group membership and intergroup bias, form the basis of an investigation that is aimed at developing our understanding of information security as a social issue. This paper considers the influence of in-group trust and out-group distrust, and the potential impact that positive and negative exemplars have on information security strategies.

Keywords
Information security, ethnocentrism, intergroup bias, exemplars

INTRODUCTION

On September 11, 2001 two planes crashed into the World Trade Center in New York City. Most of us can recall where we were on that morning. For many of us, hearing the date, or remembering 9/11 evokes strong emotions, causing us to automatically feel fear, sadness, hate…or an overwhelming sense of patriotism. However, by contrast, another date, August 2, 1988 probably doesn't have the same effect.

What thoughts come to mind when you think of the name Barack Obama? Again, does the name evoke strong emotions, both positive and negative, depending on your political views? For many African-Americans his name evokes a sense of accomplishment and a belief that anything is possible.

Each of these can be considered exemplary; a representative example of what typifies a person, group, event or instance (Zhou, 2008). Exemplary people and events have such an impact that when encountered, they trigger or activate an automatic affective response. This paper will examine how such exemplars, both positive and negative, play a role in an important organizational context: information security strategy.

Evidence gathered since the 1980s suggests that organizations continue to be victims of serious incidents that put their information at risk (Hoffer & Straub 1989; Taylor, 2006; Taylor & Brice, 2012). Occurrences of information security breaches continue to be an issue even though there are continually highly publicized events that amplify the risk potential to organizations (Kasperson et al., 1988). These breaches should serve as wake-up calls for managers.

Security breaches by some specific individuals (i.e. Edward Snowden) are well-known by company executives, and understandably, cause them to reflect on the level of information security of within their organizations. These executives become concerned that their organization could be vulnerable to the same type of attacks.

However, many of security breaches are perpetrated by individuals who still remain unknown, such as the 2013 event that exposed Target customer information Even though the names of the perpetrators are not known; the representative nature of such events, as exemplars (Zhou, 2008) leads executives to question their vulnerability.

These recent high profile incidents support the contention that information security is currently not being adequately addressed, leaving many organizations critically exposed. Clearly, security remains a top concern for IS managers, who acknowledge escalating risks to organizational information resulting in financial losses for their organizations.

To address the issue of vulnerability to information security threats, organizations must change their current perspective on information security and adopt a new view. The current view of information security is very technology oriented (Taylor, 2008). As a result organizations spend heavily on technology-based solutions to protect organizational information. These technology solutions include firewalls for perimeter security, anti-virus software to prevent viruses and worms, and intrusion detection systems to discover potential abusers (Cavusoglu, et al., 2005). Properly installed and maintained these hardware and software solutions do create a solid foundation for effective information security.

However, these technology-based solutions are primarily intended to prevent outsiders from gaining access to organizational information and are thus inadequate to prevent all security

breaches. This can ultimately create a false sense of security for an organization (Frolick 2003, Taylor 2006, Taylor & Brice, 2010). The authors' position is that along with these technology-based solutions, organizations must also adopt a human-based approach to address the information security risks introduced by the social and cultural aspects of the human element (Frolick 2003, Taylor, 2008).

Understanding information security as a social issue calls for an investigation of organizational behavior issues that may affect information security. While several such issues may merit consideration this paper will consider the influence exemplars, both negative and positive, associated with group membership.

CLASSIC ETHNOCENTRISM & GROUP MEMBERSHIP

Ethnocentrism is part of a "family of constructs" (Raden 2003, p.803) in the general area of prejudice. Classic ethnocentrism is a special and distinctive form of bias. According to Hewston, Rubin, and Willis, (2002), intergroup bias refers to the tendency to evaluate members of one's own group (designated the in-group) more favorably than non-members (designated the out-group). This group-serving tendency involves favoring the in-group--"us" and/or derogating "them"-- the out-group. The term "bias" implies that this favoring and/or derogation involves an interpretive judgment that may be unfair and unjustifiable (Brewer & Brown 1998).

Throughout history societies have formed group relationships for the purpose of survival, thus creating in-groups. Those not associated with one's in-group were considered the out-group. Sumner (1906) coined the term 'ethnocentrism' to refer to positive sentiments toward one's in-group—pride, loyalty, and perceived superiority.

Being attached to an in-group does not necessarily mean there is hostility toward the out-group (Allport, 1954); it may simply represent a preference for one's in-group. Raden (2003, p.805) characterizes this absence of hostility as forms of ethnocentrism involving "simple in-group bias" and "mere in-group preference".

However, hostility toward the out-group is not uncommon. If out-group members are perceived as posing a threat, strong intergroup bias will exist (Stephen & Stephen 2000). Threats can involve the in-group's social identity, values, or goals, and may or may not be realistic (Esses, Jackson, & Armstrong 1998). Derogation of an out-group is often associated with fear of the out-group members (Stephan & Stephan 2000).

In its classic formulation, (Sumner, 1906) the connection of favorable evaluations of one's own group with negative evaluations of other groups as when an in-group rates itself favorably and an out-group unfavorably on the ***same*** traits is central, even essential. According to Raden (2003, p.803-804), "the distinguishing feature of the ethnocentrism construct continues to be that it jointly involves ***attitudes*** (emphasis added) of the in-group toward both the in-group and the out-group".

Research in the area of intergroup bias has also established the concepts of in-group trust and out-group distrust (Allport 1954; Brewer 1979; Brewer 1999). Favoring takes the form of trust in and among in-group members; derogation occurs because there is distrust of out-group members.

The psychological expectations of in-group members result in a high level of interpersonal trust in and among "us" in-group members.

> *"… in-groups can be defined as bounded communities of mutual trust and obligation that delimit mutual interdependence and cooperation. An important aspect of this mutual trust is that it is depersonalized, extended to any member of the in-group whether personally related or not. Psychologically, expectations of cooperation and security promote positive attraction toward other in-group members and motivate adherence to in-group norms of appearance and behavior that assure that one will be recognized as a good or legitimate in-group member"* (Brewer 1999, p. 431).

In-group-trust and out-group-distrust can also be attributed to the "homogenous effect" (Judd & Park 1988). Members of an in-group are seen as homogeneous with behavioral expectations based on positive exemplars, while members of the out-group are also seen as homogeneous, however behavioral expectations are highly influenced by negative exemplars.

EXEMPLARS & EXEMPLIFICATION OF GROUP MEMBERSHIP

The concept of exemplars has been used extensively in psychology, communications studies, organizational behavior, and strategic management research (Brauer, 2000; Thomas, Schermerhorn and Dienhart, 2004; Lockwood, et.al., 2005; and Zhou, 2008). An exemplar is a representative example of a type of object or thing; a model that is typical of a person, group, event or instance. An exemplar can be an individual, that person's situation, or an event happening to and/or around the individual if it models shared group attributes (Zhou, 2008). Exemplars offer concrete information about typical individuals and representative experiences that raise issues in a given setting (Zhou, 2008). Exemplars are activated during attitude assessment (Sia et al., 1997), and they offer heuristics to simplify and expedite information intake and utilization (Brosius, 2003). This process is especially pertinent in organizational contexts where evaluation and judgments are often made and responsive behavior and actions are the result.

Conceptually, exemplars represent an idea or mental image that allows for items that share common properties to be grouped together or categorized as either person or event based. Exemplar representation "may be constructed on the basis of actually perceiving the stimulus object, imagining it, being told about it second-hand, etc." (Smith, 1998, p. 411). As Reisberg (2006) notes, the more frequently an item is encountered, the more stored representations of it will be held in memory.

Research on the characteristics of exemplars often focuses on their vividness and salient nature to explain effects (Zillman & Brosius, 2000). Vividness can come from the power of the language used to describe the exemplar, the imagery it evokes or the emotional value attached to the instance when it occurs. Salience refers to those aspects of the exemplar that draw more attention since they stand out because of their unusual character. The use of emotion-evoking imagery has been found to create perceptions and dispositions that actually gain strength over time. The presence of exemplars automatically activates affective responses. This exemplar activation is unintentional (Macrae, et.al, 1998).

POSITIVE EXEMPLARS

A positive exemplar, as an individual, is one whose conduct should be emulated. A positive exemplar can also be an instance or event that is worthy of being repeated. As the representation of an ideal, an exemplar is worthy of imitation, serves as a pattern or archetype and deserves to copied (Merriam-Webster, 2014). An example of a positive exemplar is Dale Beatty, a 2013 CNN Hero of the Year, who founded an organization that built or modified homes for disabled veterans.

A single exposure to a positive exemplary act is a sufficient condition for the influence process to occur; a series of such events can help build mindful behavior in areas such as ethics (Thomas, Schermerhorn & Dienhart, 2004), workplace safety (Gyekey & Salminen, 2005) or any area of strategic emphasis (Zillman, 1999). Thomas, Schermerhorn & Dienhart (2004, p. 57) showed that leaders who are viewed as positive exemplars can influence a substantial majority of an organization's membership. However, it should be noted that individuals may consider *themselves* to be the positive exemplar. In such instances, therefore, that individual's judgments about fellow in-group members are based on their own self-perceived positive behavior (Brauer, 2000; Judd & Park, 1998; Park & Rothbart, 1982).

NEGATIVE EXEMPLARS

In contrast, negative exemplars represent behavior or situations that are undesirable (Reisberg, 2006). In the case of a negative exemplar, recipients can give disproportional attention to an errant actor or a concrete, often vividly displayed event that engages the emotions. Negative exemplars can motivate others to avoid a specific behavior or an event that may result in an unpleasant fate (Lockwood et al., 2005). For example, the recent death of actor Paul Walker, who died in a car accident attributed to excessive speed, may motivate others to avoid fast driving, especially when he (Paul Walker), or the actual event, is recalled. Lockwood et al. (2005: p. 1) describe an advertising campaign featuring an overweight teen named Eddy, who "has a passion for burgers, butts and his sofa", that is aimed at encouraging teens to eat healthy. The purpose was to depict Eddy as a negative exemplar whose behavior, if emulated, would result in becoming overweight.

The strategic use of exemplification in addressing issues is effectively the starting point in that the world of exemplars, examples, or representations influences perceptions of and judgments about phenomena and issues encountered in the organizational context. Their vividness, salience and affective characteristics explain how groups of people will blindly trust members of their in-group, while out-group members are shrouded by suspicion, distrust, and hate, even when little is known about the actual members of the out-group (Insko, Schopler, Hoyle, Dardis & Graetz, 1990).

Exemplars, both positive and negative, and exemplification theory form the basis of this investigation of the influence of group membership on managers' perceptions of information security risks in their organizations. The discussion in the next section raises and addresses the connections between managers' biased perceptions and information security behavior.

GROUP MEMBERSHIP AND INFORMATION SECURITY RISK

Past research on intergroup bias was primarily focused on societal level biases; however, these same principles can be applied to business organizations and the philosophies they use to create their information security strategies. We expand the concept of ethnocentrism to include not only beliefs or attitudes, but expectations about practices, actions and behaviors that members of a group are likely to perform.

This research investigates what happens when biases based on group membership leads to in-group trust (favoritism) and out-group distrust (derogation). In the information security context on which this paper is based, the in-group is composed of persons who are employed by the organization while the out-group members consist of everyone else.

Members of an in-group are expected to act one way, generally in compliance with security measures and accepted industry standards of practice. Members of the out-group, however, are subject to suspicion based on the perception that they are likely to engage in behaviors that are detrimental to the maintenance of information security. Such suspicion is grounded in the forms of bias (e.g. in-group trust and out-group derogation or distrust) that are described in the preceding paragraph.

Perceived threats from outsiders seem to be the driving factor for an organization's information security strategy (Taylor, 2008). Hence, out-group distrust is evident in most aspects of an organization's security strategy.

Management utilizes physical security measures to keep the organization protected from outsiders through the use of door locks, electronic entry systems, video cameras, and security guards. Information security management is approached in the same manner. Technological solutions such as firewalls and intrusion detection systems are put in place for the primary purpose of keeping an organization's information protected from outsiders—the out-group.

Internal Information security measures directed toward in-group members are generally less stringent. Managers may require employees (members of the in-group) to change passwords, attend security awareness training, and review policies and procedures on an annual basis. These practices reflect managers' overall beliefs about the willing compliant behavior of subordinates, who represent in-group members.

Both in-group and out-group members can be the source of information security threats. However, group membership influences management's perception of both the source and severity of the threat posed to information security.

Perceptions about the existence or severity of threats which underlie organizational information security management are based largely on group membership. According to Park and Rothbart (1982) in-group judgment can be group level or based on a particular member of the group, including *the self*. This notion can be applied to perceptions about security behavior of in-group members. Positive security behavior can be influenced by positive exemplars**.** Often the manager(s) who are ultimately responsible for security management (*the self*) represent positive exemplars. Managers trust that employees are reading information security policies and adhering to established norms to protect the organization's information. These expectations exist because the manager him/herself follows policies and norms and therefore blindly trusts that other employees (in-group members) will do the same. In organizations, as well as society, such in-group trust (as well as out-group distrust) can also be attributed to the "homogenous effect"

(Judd & Park 1988). Members of an organizational in-group (the employees) are seen as homogeneous whose behavioral expectations are "similar to" and based on a positive exemplar (e.g. the manager).

In-group trust is a significant contributor to information security risks. For example, research (Dhillon 2001. Taylor, 2006; Taylor & Brice 2012) confirms that in-group trust is grossly overlooked as a factor in information security management. Ingroup-trust can result in fewer information security countermeasures and lower levels of employee monitoring (Dhillon 2001), both of which have been identified as factors in increased information security risks (Straub & Welke 1998). In this research, IT Managers are considered positive exemplars and in-group members are expected to follow their behavior example (e.g. security practices). As a result, managers perceive fewer risks associated with information security breaches by in-group members.

We posit that such trust increases the potential for internal threats due to the gap between the expectations held by a positive exemplar and employees' actual behaviors and actions. Managers whose trust in employees' information security behavior is based on their confidence in fellow in-group members are the focus of our first hypothesis.

H1: Management perceptions of themselves as positive exemplars increase Information Security risks.

As with in-group members, members of the out-group are also viewed as being homogeneous, that is sharing common within-group attributes and attitudes. Perceptions about security breaches by out-group members are influenced by the presence of negative exemplars**.** Although security breaches are carried out by individuals, for the most part it's the threat of external security events that represents the negative exemplar, as these are what guide management's information security decisions. Accounts of high-profile security breaches, such as those mentioned earlier in this paper, identify events as the outside factors that can be characterized as negative exemplars. In other words, perceptions of threats posed by out-group members are based largely on the characteristics of the events with which these outsiders become identified, *after* those events take place. The perceived likelihood is that negative exemplars (events) will be perpetrated by outsiders. Therefore, managerial expectations regarding behaviors for out-group members are highly influenced by persons such as Snowden or the anonymous hackers in the Target Stores case whose actions trigger major events. This is supported by Linville et al. (1987), whose research showed that information about an individual member of an out-group or a specific event associated with an out-group is stored in memory and subsequent group judgment can be made when these memories are recalled. It can be expected that when managers recall Snowden (the actual individual) or the Target Store incident (the event) they will likely consider the potential risk to their operation and thus evaluate their organization's information security protection against the specifically triggered event. The second hypothesis addresses the impact of management's assessment of negative exemplars and perceptions of the associated risks.

H2: Management perceptions of negative exemplars decrease Information Security risks.

METHODOLOGY

As a research tool, the case study method is both appropriate and effective for investigating a complex subject such as information security, especially when the study offers a unique opportunity to observe what is becoming an increasingly important focus of organizational and management studies. Yin (1993) presents the domain of management information systems as an application for employing the case study method as a research strategy. He reports that management scholars have successfully extended the use of case studies beyond their traditional use as teaching tools (1993, p 64). The growing interest in case studies as research tools serves a useful purpose for a phenomenon that (a) is broad and complex, (b) needs a holistic, in-depth investigation, and (c) cannot be adequately studied outside the context in which it occurs (Benbasat et at. 1987; Bonoma 1985; Feagin et al. 1991; Yin 2003).

The case study makes it possible to "retain the holistic and meaningful characteristics of real-life events such as [the] organizational and managerial processes..."(Yin, 1984 p14) that accompany the continued expansion of management information systems. A holistic, in-depth investigation which follows a naturalistic approach to generating a qualitative understanding of information security concerns, certainly offers advantages. Lincoln & Guba (1985) outline a method that takes into account time, context and human social interaction, factors that foster a holistic view of the problem domain, especially within the scope of the networked organizational forms, instead of the simplistic, one-dimensional, explanation, more suitable for hierarchically structured organizations (Dhillon & Backhouse 2001). The case research strategy allows for a great deal of flexibility and individual variation (Cavaye 1996). This makes the case study an ideal methodology for investigating the concerns of information security.

Management information systems security is difficult to study outside the context in which it occurs (Benbasat, Goldstein, and Mead 1987). It may be difficult to get honest answers to questions regarding information security. Therefore the case study method allows the researcher to conduct probing interviews as well as engage in ethnographic observations of information security practices within the organizational context. For this case study, access was granted to a financial institution.

THE ORGANIZATION

Financial One (not the organization's real name) is a financial institution located in a major metropolitan area in the southern United States. There are seven Financial One branches throughout the metropolitan area, consisting of approximately 200 full and part-time employees. Of the seven branches, one branch is housed at the Financial One headquarters. At this location are the executive offices, the information technology (IT) department, accounting, credit card services, wire transfers, and other back-office and support services. This organization was chosen for several important reasons.

First, financial institutions are at greater risk because of the potential gain for perpetrators who steal or corrupt organizations' information assets (Yeh & Chang, 2007). For example, information systems in the financial services industry can provide access to customer credit card and account information.

Second, the presence of both federal and state information security regulations put pressure on affected organizations to ensure proper security measures are being taken. For these reasons financial institutions would be more likely to emphasize information security than organizations in other industries (e.g., a restaurant chain). Finally, one of the authors served as an executive in this industry for over 10 years before entering the academic community, therefore providing additional insight into the organizational environment and the issues facing the industry. Being considered an industry insider provided a high level of legitimacy with the Financial One staff, resulting in employees' willingness to divulge information and permit greater access to organizational resources (Malone, 2003).

Case study research requires a high degree of ethical consideration (Roth, 2005), especially when the research involves a sensitive subject such as information security. The CEO and CIO of the Financial One served as "gate-keepers" who allowed access to the organization and its employees (Miller and Bell, 2002). It was important to keep these two individuals updated on a constant basis. Each staff interview was conducted where only the primary researcher and the subject employee were present. Document review was conducted by the researcher alone after the documents were provided by the CIO. All other events were conducted with the CIO present.

After each phase of the investigation, the CEO was briefed on the findings, and additional consent was sought (and granted) before moving ahead to the next phase of the research. Schwandt (1997) defines such briefings as member or respondent validation. These member checks were initially made to establish the current level of information security. Their baseline perception formed a risk assessment of information security systems that were in place. As the investigation progressed, these briefings were used to share and corroborate findings.

These research activities establish what Lincoln and Guba (1985) refer to as the credibility of the process and help ensure the trustworthiness of findings. These authors developed four criteria that serve as case study research equivalents for internal and external validity, reliability and objectivity (Schwandt, 1997). Careful steps were taken to assure that interviewee observations that are used to support results match the respondents' views of the organization. Finally, the results reported herein are linked directly to the interview data in order to establish that findings are not simply products of the researchers' imaginations.

In accordance with the suggestion of Yin (2003) the authors concluded that conducting the case study within Financial One would be an effective method to obtain in-depth data and generate rich analysis needed to apply existing theory to a phenomenon in a different context, which is what we are doing. We seek support for hypotheses that address the influence of positive and negative exemplars as the source of intergroup bias as applied to information security risks within organizations.

RESULTS

Positive Exemplar Analysis						
Employee	Will Give Out Password (exemplars/managers)	Others Will Give Passwords	Would Fall For Social Engineering (exemplars/managers)	Others Would Fall For Social Engineering	Reviews IS Policies (exemplars/managers)	Others Review IS Policies
Exec 1	NO	NO	NO	NO	YES	YES
Exec 2	NO	NO	NO	NO	YES	YES
Exec 3	NO	NO	NO	YES	YES	YES
Exec 4	NO	NO	NO	NO	YES	YES
Exec 5	NO	NO	NO	YES	YES	YES
Exec 6	NO	NO	NO	NO	YES	YES
Exec 7	NO	NO	NO	NO	YES	YES
Exec 8	NO	NO	NO	NO	YES	YES

Table 1. Managers as Positive Exemplars

H1 Management perceptions of themselves as positive exemplars increase Information Security risks.

Executives at Financial One were in unanimous agreement that their organization operated with a high level of information security. This belief was expressed in their personal observations, documented in reports from outside audit firms, and even based on "intuition". According to the CFO:

> *"I believe our information security is solid. My opinion is not based on our IT department, but based on what the so-called experts have told me. That's where my decision is coming. Not that I have any concerns with our IT department, but if I hear it from an expert what else am I to believe?"*

The executives at Financial One considered themselves positive exemplars (Table 1). Because they believe that "our employees are well trained" in information security issues (CEO of Financial One), these executives believed their information security behavior was emulated by the other employees, who are considered members of the in-group. They expressed confidence that their employees read Information security policies, would not share their password with anyone, and were not vulnerable to social engineering involving the gathering of confidential information through lying or other types of deception.

Evidence in support of this hypothesis comes from the application of exemplar theory to in-group and out-group trust in Financial One. The positive exemplar analysis of eight executives in this setting demonstrates that these managers (1) acted in accordance with (1) their beliefs in their strength as positive exemplars and (2) an illusion of control that produced an optimistic bias that employees, as in-group members, would act accordingly.

To verify the accuracy of management's perceptions, employees throughout the organization were interviewed. Employees have been shown to be the best source for understanding the behavior and actions of other peers (Murphy & Cleveland, 1991). Behavior that is observed by employees is different than that observed by management, because

employees have opportunities to see a wider range of behaviors of which managers may not be aware.

Policies

Organization security models have stressed the importance of the establishment and implementation of security policies (Segev et al.,1998). Security policies at Financial One were posted on the company's intranet and updated continually as needed. All employees were encouraged to read the security policies. Every year employees were required to sign a document verifying that they had done so. Because of the existence of policies that had been established to protect organizational information, management perceived that these policies were being followed by the staff. It was also perceived that department supervisors were effective in the enforcement of these policies.

The executives who were interviewed were aware of organizational information security policies and procedures. As positive exemplars, they believed that others would be also. Furthermore, these executives regularly reviewed and followed information system policies and assumed that the employee in-group members did so also.

Statements made by employees, didn't, however, confirm the executives' belief regarding reading policies. One employee admitted receiving the handbook, and was aware that it was online, but stated:

> *"I haven't read the handbook to be honest with you. I guess I might have pulled it up to find the answers to thing that I have questions to…but it's going to be on something that interest me like wage compensation, raises…merit raises…stuff like that…but not security stuff."*

This sentiment was confirmed by other employees within the organization. When one was asked about reading security policies she replied:

> *"For someone that has been here for five or six years then they know it…they know what they are supposed to do."*

Yet, when the same employee was asked if she was aware that it was against company policy to give out her password, she replied, "…*our company has a policy like that?....no [I was not aware of it]".*

Interviews with other employees at Financial One provided additional support for the hypothesis. Interview data also supports previous findings that managers may feel overly optimistic regarding their employees' awareness of organization security policies (Taylor & Brice, 2012).

When interviewed, the executives also pointed to the existence of a policy that stressed the importance of shredding sensitive information.

> *"Anything dealing with customers' accounts goes to that shred bin and it's kept locked up in a back room with the door shut and the cleaning people don't go into. We are pretty good about putting things in shredder bins. Could I 100% say*

there is nothing in there [the trash], but all in all the chances of it happening are very slim."

To emphasize the importance of this policy, each employee workstation was equipped with a trash can (black) and a shred can (blue). According to the security policy, each employee was responsible for emptying their blue shred can each night into a larger shred bin that was located in a secured area. However, after personal observation by the first author of this paper, who was allowed to remain on the premises afterhours while the CIO was present elsewhere in the building, it was noted that employees did not empty their shred cans into the dedicated shred bin. It was also further noted that the evening cleaning crew stopped at each desk, where both the black trash can and the blue shred can were emptied into a single trash receptacle. Contents of that receptacle were then bagged and thrown into the outside dumpster. Employees expressed surprise when asked about this the next day. They assumed that their blue shred cans were being picked up each night and taken to the dedicated shred receptacle.

Passwords

Notably, there is another security policy at Financial One that requires employees not to share or reveal their system passwords to anyone. When asked if they thought employees would give out or share their system password, management unanimously declared that employees would not. Managers felt that employees were well aware of existing policies and that they fully understood the importance of protecting their system passwords.

"I wouldn't sit here and tell you that it would be 100%, depending on who was asking, some people would probably offer it up, but overall most would not."

Based upon interviews with Financial One employees it was noted that although most employees were aware of the policy, it was not an uncommon practice to share passwords if deemed necessary. An employee confirmed that she would give her password to anyone in the IT department, to the VP of Branch Operations, and to her Branch Manager. She stated that she had shared her password on several occasions. Employees of the IT department also admitted to sharing passwords among themselves when it was necessary for one of them to access a system they did not generally have access to.

To further test whether employees would give out their password, the IT department was asked to call 60 employees (in-group members) from all levels of the organization, and simply ask them for their password. Of the 60 calls that were made they obtained 10 voicemails and 50 passwords. Employees who surrendered their passwords had their passwords automatically reset, forcing them to change it immediately.

Two of the passwords were received from executives who stated they would not give out their password (as shown in Table 1). When informed of this, the CEO expressed both surprise and concern:

"It's like IT was saying here's a lollipop give me your password…but they weren't even giving them a lollipop….they just asked for it."

Social Engineering

Infamous hacker, Kevin Mitnik stated that he rarely relied on hacking to access a company's computer system because technology controls were getting better to prevent outside access, and even though he could still get through most of the controls it took a lot of effort. However, with social engineering, he said it was like taking candy away from a baby (Mitnik & Simon, 2002).

Executives at Financial One were asked if they would fall for social engineering attacks. They each gave assurances that they would not. Again, relying on themselves as positive exemplars, they believed their employees were also too well trained and would not fall for the deceptive tactics. Notable exceptions were the two executives mentioned in the preceding section, who didn't have the same level of confidence in their employees, presumably because they had violated the password policy (Table 1).

Financial One employees were told about a scenario used by infamous hacker Kevin Mitnik in which he would randomly place CD-ROMs throughout an organization in areas, such as restrooms, where he was allowed and that employees would typically go. The CDs would be labeled "Employee Salaries". Any employee, who was tempted to look at this CD, would have keystroke capture software installed on that. The results were then emailed to Kevin, which would automatically give him access to the organizations computer system. In response to hearing the scenario, one employee offered this observation,*"I think you have people that would be nosey enough to stick it in their CD ROM and try to look at it."*

A second social engineering scenario was presented to the employees: Someone claiming to be an employee of their primary information system vendor called and described a fictitious problem that required the employee's password to correct. The vendor thus tricked the employee to revealing their password to them. In response, a different Financial One employee observed, *"Wow…that's pretty good…I bet at least half of the people would fall for that."*

When given the two social engineering scenarios, most of the employees admitted that that would fall for one or both of them, again providing support for the hypothesis.

Further additional support for this hypothesis comes from the fact that researchers consistently found evidence of blind trust for the in-group employees. The fact that these executives were dealing with employees who were known to them personally as individuals compounded the risks of insider threats to information security.

> *"Most of the guys have been here for almost as long as I have or a lot longer…so I would tend to trust them more than someone brand new walking in the door."*

The CEO believed that the ingroup members were displaying good security behavior based on his perception that employees followed his own exemplary behavior:

> *"We have a lot of in house expertise and I think we have devoted a lot of resources trying to provide good security. I think that we have had pretty good performance down the line. It's more intuitive than data based".*

As seen in the previous quote, the CEO's expressed optimism that employees were performing well when it came to information security was based totally based on his intuition.

This lack of concern about security risks was rooted in the confident optimistic perception that employees would follow his exemplary security behavior example. These findings demonstrate that management was clearly unconcerned with negative employee behavior insofar as information security.

Due both to the executives perceptions of their influence as exemplars, and their beliefs that their employees' (in-group members) behavior was not a threat, the issue of information security was not adequately addressed. Management put too much trust in their employees, resulting in a lack of monitoring and supervision which ultimately increased information security risks within their organization, thus providing support for Hypothesis 1.

H2 Management perception of negative exemplars decreases Information Security risks

In this case the negative exemplars are actually events that trigger the affective response. Findings in this study indicate that negative exemplars affect managers' perceptions of threats to information security posed by out-group members. Thus, threats posed by out-group members increased awareness of the probability of their occurrence which ultimately leads to increased security measures.

Consider these observations by both the CEO and COO of Financial One:

> *"When you're working out front, seeing people come in with long coats and ski-masks on is typically a bad sign. With online stuff, you can't distinguish who will try to get into your system. Could be some kid, an ex-employee, or some professional hacker. There's no way to know."*

The impact of the media can also have "lasting effects on impressions, beliefs, and associated disposition" (Zillman, 1996, p. 70) which heighten the executives' awareness of security threats.

> *"I hear stories on the news or read about them in the paper…they really concern me. I remember one night on the news where people's cancelled checks showed up in gift baskets. They were shredded….but they could easily be put back together."*

When information security incidents occur in a manner that the executive is more closely associated with, a personal connection is made which further strengthens the impact of the negative exemplar (Aust & Zillmann, 1996). In this instance, the CEO has an increased affective reaction because the incident occurs in the same industry, and even more so because it is in close proximity to him.

> *"We always think it won't happen to us, but it still hits home when I read in the newspaper or see on TV that a bank has had a security incident…especially if it's local. If it can happen to them it can surely happen to us."*

In each of these instances, the negative exemplar was an event (e.g. shredded cancelled checks showing up in gift baskets, security incidents). Only after a security breach occurs (Snowden) or when an event compromises or threatens information security (Target Department stores), identifying the perpetrator and characteristics of the individual and outgroup becomes an important consideration as part of the effort to minimize the potential for a similar incident to occur at their organization.

The possibility of such negative exemplars affects management's perceptions of the threats and influences their decisions related to avoiding breaches and maintaining information security. When managers' perceptions and expectations of the likelihood and severity of negative exemplars increase so does distrust of persons associated with such events.

The lack of information in decision making is a psychological reality and can weigh heavily on the decisions that have to be made by the Financial One executives (Gigerenzer, 2001). When making decision, the executives will use information and experiences that are readily available. According to Selten (2001, p.212),

> *"It is useful to distinguish between familiar and unfamiliar problems of this kind. A problem is familiar if the decision maker knows the optimal way to attack it, i.e., knows what to do through prior training or mathematical investigation, or perhaps the problem is so simple that a suitable method immediately suggests itself. In the case of an unfamiliar problem, the decision maker must devise a method for finding the alternative to be chosen before it can be applied.*
> *…risky decisions are rarely based on explicit probability judgments."*

Managers are required to make nonprogrammed decisions under suboptimal conditions of environmental uncertainty such as lack of information (Simon, 1957). When making these information security decisions, the Financial One executives did not always have sufficient knowledge regarding threats to their organizational information. Managers will use all information and experiences that are readily available and will often turn to trusted advisors whose opinions they value (Siegrist & Cvetkovich, 2000). For example, when information security advice is sought, Financial One management typically turns to the Information Security Officer (ISO) or the Information Technology (IT) manager. According to the CEO of Financial One, when he becomes aware of a negative exemplars he seeks out someone more qualified to assess the organization's risk**.**

> *"I usually call [CIO] just to make sure we are protected from something like that happening to us" (CEO).*

Applied in this context, the social amplification of risk (Kasperson et al., 1988) suggests that high profile security breaches (negative exemplars such as the security information leaks that were traced to NSA contractor Edward Snowden and the theft of Target Stores' customer credit information that is believed to have been perpetrated by hackers) serve as a wake-up call, the result of which is an information security risk analysis of the threats posed by out-group members which ultimately decreases the information security risks for that organization, thus supporting hypothesis 2.

DISCUSSION

This case provides support for the two hypotheses presented in this study. Financial One executives were in agreement that their level of information security was "solid" and "above average". They relied on several different perceived factors to reach their conclusion: they had a strong information technology department with experienced IT employees, outside firms provided confirmation to them regarding their level of security, they had never experienced an information security breach, and they trusted their employees to "do the right thing".

In most cases, people want to do the right thing (Pelletier and Vallerand, 1996). Policies have been shown to be an effective in getting this result. Security policies have been identified by researchers as an effective deterrence to security threats (Whitman, 2003; Siponen and Iivari, 2006). However policies must be followed for them to be effective. Financial One had policies regarding password security, and research has shown that the existence of password policies do decrease security risks (Zvirian, 1999; Ives et al., 2004). Financial One also had a policy regarding shredding confidential information; however even though policies exist against throwing confidential in the trash, it still happens on a regular basis (Jones, 2005).

The existence of formal security policies did not appear to be associated with security-related behavior because the policies were often unread therefore employees were unaware of their expected behavior (Frank et al., 1991). Even though the information security policies were readily available to all employees on Financial One's intranet, there was no method in place to ensure that employees were actually reading the policies, even though employees were required to sign a document claiming that they had indeed read the policies and agreed to abide by them. Effective monitoring to ensure policies are being followed is an important part of an organization's information security strategy (Straub & Welke, 1998). Financial One did not have effective monitoring in place.

If often takes a security incident to open management's eyes to threats within their organization (Dhillon & Moores, 2001). People only respond to threats they perceive (Slovic et al., 1980). Therefore Financial One executives had no reason to take additional information security precautions against insider threats since they believed their employees were following their positive exemplar behavior. They perceived that employees were acting in a manner that would not put the organization at risk. In all the instances observed in this study, employees were not intending to put the organization at risk; however their behavior was unintentionally putting the organization at risk (Taylor, 2006).

Information security is about risk assessment, so focus is placed where the threat is perceived to be the greatest (Slovic et al., 1980). The amount of resources an organization invests in information security is a factor of the risk they are willing to accept and the management's perceived probability of their exposure to security threats (Gordon & Loeb, 2002). Resources are limited and must be allocated in a manner that sufficiently addresses information security within a limited budget (Farahmand, et al., 2005); therefore Financial One executives believed they should focus their information security strategy on protecting their information from untrusted outsiders. This ethnocentric approach to their information security strategy was not based on the probabilities of information security threats at Financial One. Their strategy was developed as a result of the federal examinations and technology-based third party audits. Because of their lack of personal security experience, the executives relied on the

knowledge of more trusted individuals (Siegrist & Cvetkovich, 2000), such as the auditors, examiners, and the CIO, to make security recommendations or to validate their existing information security risks. The recommendations of these individuals resulted in technology-based approach to keep out-group members from accessing their information systems.

Because of this approach, the executives failed to consider the human-based behavioral element of organization security; "…we often overlook the human solution and instead opt for technology solutions, when in fact the human factor must be addressed first, with technology assisting in the enforcement of desired human behaviors" (Whitman, 2003, p.92). The executives trusted their employees, the in-group members, would follow their exemplary behavior. However their in-group trust lead to their own security blindness resulting in increased risks to the organization's information. Therefore, Hypothesis 1 was supported.

The executives at Financial One were familiar with some negative security events (i.e. shredded checks showing up in gift baskets), primarily those reported in the media. These events served as negative exemplars that made them question the adequacy of their information security (Aust & Zillmann, 1996). The concerns were amplified when the exemplar were local or in their industry. Their concerns led them to reevaluate their current security countermeasures that were in place to prevent such attack from happening to them. This provides support for Hypothesis 2.

CONCLUSION AND IMPLICATIONS FOR FUTURE RESEARCH

Present day managers face increasingly complex, dynamic and changing conditions. The landscape has expanded from the traditional view of MIS as a company subfunction to a newer conceptualization of systems with the potential to restructure an entire organization. The broader scope, accompanied by increased complexity, explains our call for a new view of information security that considers both behavioral and technical factors.

This paper focuses on understanding how the managerial actions undertaken by organizational actors are influenced by their perceptions of risk. Specifically, we address how assessments of the threat to information security are based on attitudes about group membership. Several important areas of organization and management theory are necessary to understand and to generate conclusions about the roles of positive and negative exemplars. Managers' perceptions about threats and group membership as a factor in decisions about how to address information security needs must be considered.

Organizational behavior (group characteristics) and interpersonal processes form the backdrop for this examination of interpersonal factors that influence information security decisions within a specific context. As management information systems continue to expand, theoretical underpinnings of this investigation include models of decision-making, organizational change processes, and organizational design considerations.

This paper takes a new look at information security risks, by applying theoretical perspectives that have, in the past, been reserved for sociological studies of bias and discrimination. We have made the case that these theories can provide a new lens through which to view the level of trust that develops among members of an organizational in-group and how that relationship affects management decisions about information security.

For the academic community, this research introduces another method to study questions about managerial perceptions regarding their information security strategies. In this case,

management's perceptions were filtered through a lens of simplified cognitive heuristics which resulted in inaccurate conclusions about the actual level of potential threats to organizational security. These perceptions came from an optimistic view of themselves as positive exemplars. Yeh and Chang (2007) found that a gap existed between management's perception of their information security threats and the perception of the proper countermeasures they have in place to prevents threats. Their findings show that management tends to be overoptimistic about their information security risks. Our results support their findings.

This research can be valuable to the practitioner community by increasing awareness of the inaccuracies of managerial perceptions. Ultimately, the goal of this study is to point out to management that there are factors that affect their perception of their organization's information security risks. By understanding the problem, managers may seek better understanding of the limits of their cognitive biases and devise methods and controls to prevent the projection of their own behaviors onto their employees. Managers should continue to be positive security exemplars but they must also enforce ways to monitor their employees' behaviors to ensure they are following the managers' exemplary behavior. When employees perceive that security is a concern to management, they tend to increase the awareness of their security related behavior to be in line with that of the managers (Hoffman & Morgenson, 1999).

This research can also help organizations better understand attitudinal and behavioral issues that contribute to information security risks. The results of this investigation offer strong support for our hypotheses and make a case for a human-based approach to information security, viewing it as a social issue. As long as managers continue to focus primarily on the outside threats, organizations will remain vulnerable to threats from insiders.

Organizations should realize that technology-based actions such as monitoring of employee behavior and the implementing security countermeasures are not necessarily signs of distrust (Dhillon & Backhouse, 2000). It is the fiduciary responsibility of organizations to insure that their information is adequately protected. They surely have to take adequate measures to protect their information from out-group members who may attempt to gain unauthorized access. But they cannot stop there. They must also insure that members of their in-group are not abusing the trust relation within the organization, thus putting the organization's information at risk. This research is not suggesting that trust within organizations be decreased, because research has shown that organizations that create trusting environments are able to accomplish more than a comparable group without that trust (Coleman 2002). However, organizations can benefit from understanding how these high levels of trust can also have negative ramifications.

Das (2003) complained that managerial perception research occurs without "even a modicum of appreciation of the real-world managerial environment." This study analyzed the perceptions of real-world managers who work in a real-world organizations, which may face the real-world consequences of (in)activity based on those perceptions.

Future research should continue to investigate the effect of optimism bias on exemplars. Early research has shown that managers are overly optimistic about their adequacy of their information security (Goodhue & Straub, 1991); however even though this has been understood for a long time, the problem still exists. Because of this optimism bias, knowledge about negative exemplars may not always result in reduced information security risk, especially if an optimism bias is present. For example, the recent hacking attacks on the Target Stores should have served as an eye-opener for other organizations, especially since shortly thereafter both Nordstrom's

and Neiman Marcus stores were the victims of similar attacks. Where Nordstrom's and Neiman Marcus management overly optimistic about their security countermeasures that were in place to prevent the same type of attack? Gal & Chose (2005) found that there is value for everyone when security information regarding threats, systems vulnerabilities, and fixes for such system vulnerabilities are shared. Overly optimistic managers may not feel the necessity to acknowledge or act on the shared information.

Developing an information security strategy is filled with uncertainty for managers making it difficult for them to fully understand the risks involved, including their level of exposure to specific threats, and the consequences that a security breach could have on their organization (Vonsolms, et al., 1994; March and. Shapira, 1987). This study, supported by statistics and other research (Dhillon 2001; Taylor & Brice 2012), confirms that in-group trust and out-group distrust are significant factors in information security management that should not be overlooked. Executives' perceptions of both positive and negative exemplars play a role in their information security strategy. Negative exemplars increase their awareness of potential threats, therefore resulting in precautionary actions to protect the organization's information. By seeing themselves as positive exemplars, executives develop unwarranted faith that employees will mimic their exemplary behavior. Such blind trust of insiders can potentially pose the greatest risks to the organization. By understanding these issues, organizations can learn to counteract behaviors that increase information security risks.

REFERENCES

Allport, G.W. (1954). *The nature of prejudice*. Cambridge, MA: Addison-Wesley.

Aust, C.F., & D. Zillmann (1996). Effects of victim exemplification in television news on viewer perception of social issues. *Journalism & Mass Communication Quarterly*, 73, 787-803.

Benbasat, I., D. Goldstein, & M. Mead (1987). The case research strategy in studies of information systems. *MIS Quarterly*, 11(3), 369-386.

Bonoma, T.V. (1985). Case research in Marketing: problems and opportunities and a process. *Journal of Marketing Research,* XXII, 199-208.

Brauer, M. (2001). Intergroup perception in the social context: the effects of social status and group membership on perceived out-group homogeneity and ethnocentrism. *Journal of Experimental Social Psychology,* 37, 15-31.

Brewer, M.B. (1979). In-group bias in the minimal intergroup situation: A cognitive motivational analysis. *Psychological Bulletin*, 86, 307-324.

Brewer, M.B. (1999). The psychology of prejudice: In-group love or out-group hate?. *Journal of Social Issues*, 55(3), 429-444.

Brewer, M.B. & R.J. Brown (1998). Intergroup relations. In D.T. Gilbert, S. T. Fiske, & G. Lindzey, (Eds.), *The Handbook of Social Psychology*, Vol. 2. Boston: McGraw-Hill. 4th ed.

Brosius, H. (2003). Exemplars in the news: A theory of the effects of political communication. In J. Bryant, D. Roskos-Ewoldsen & J. Cantor (Eds.), *Communication and emotion: Essays in honor of Dolf Zillmann*. Mahwah, NJ: Erlbaum.

Castelli, L., C. Zogmaister, E.R. Smith, & L. Arcuri (2004). On the automatic evaluation of social exemplars. *Journal of Personality and Social Psychology*, 86(3), 373–387.

Cavaye, A.L.M. (1996). Case study research: A multifaceted approach for IS. *Information Systems Journal* 6(3), 227-242.

Cavusoglu, H., B. Mishra, & S. Raghunathan (2005). The Value of intrusion detection Systems in information technology security architecture. *Information Systems Research*, 16(1), 28-46.

Coleman, J. S. (2002). Social capital in the creation of human capital. In Calhoun, Gerteis, Moody, Pfaff, &Virk (Eds.), *Contemporary Sociological Theory*, (pp.110).

Das, T.K. (2003). Managerial perceptions and the essence of the managerial world: What is an interloper business executive to make of the academic-researcher perceptions of managers? *British Journal of Management*, 14, 23-32.

Deutsch, M. (1973). *The resolution of conflict: Constructive and destructive processes*. New Haven, CN: Yale University Press.

Deutsch, M. (1962). Cooperation and trust: Some theoretical notes. *Nebraska Symposium on Motivation* Lincoln: Nebraska University Press, 275-320.

Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computer & Security*, 20(2), 165-172.

Dhillon G. & J. Backhouse (2000). Information system security management in the new millennium, *Communications of the Academy of Computer Machinery*, 43(7), 19-41.

Dhillon, G., & S. Moores (2001). Computer crimes: theorizing about the enemy within. *Computers & Security,* 20(8), 715-723.

Esses, V.M., L.M. Jackson, & T.L. Armstrong (1998). Intergroup competition and attitudes toward immigrants and immigration: An instrumental model of group conflict. *Journal of Social Issues,* 54, 699-724.

Farahmand, F., S. B. Navathe, G.P. Sharp, & P.H. Enslow (2005). A management perspective on risk of security threats of information systems. *Information Technology and Management,* 6, 203-225.

Fast, N.J., N. Sivanathan, N.D. Mayer, & A.D. Galinsky (2012). Power and overconfident decision making. *Organizational Behavior and Human Decision Processes*, 117, 249-260.

Feagin , J. R. (1991). The continuing significance of race: Anti-black discrimination in public places. *American Sociological Review,* 56(1), 101-116.

Frank, J., B. Shamir, & W. Briggs, (1991). "Security - related behaviour of PC users in Organisations. *Information & Management* 21, 127 - 135.

Frolick, M. (2003) . A new webmaster's guide to firewalls and security. *Information Systems Management*, Winter, 29-34.

Gal-Or, E. & A. Ghose (2005). The economic incentives for sharing security information. *Information Systems Research*, 16(2), 186-208.

Gambetta, D. (1988). *Trust: Making and breaking cooperative relations*. New York: Basil Blackwell.

Gattiker, U. & H. Kelley (1999). Morality and computers: Attitudes and differences in moral judgments. *Information Systems Research,* 10(3), 233-255.

Gigerenzer, G. (2001). The adaptive toolbox. In *Bounded Rationality*. G. Gigerenzer & R. Selten (Eds.), Cambridge, MA: MIT Press (pp. 37-50).

Goodhue, D. & D. Straub (1991). Security concerns of system users. A study of perceptions of the adequacy of security. *Information & Management*, 20, 13-27.

Gordon, L. A. & M. P. Loeb (2002). The Economics of Information Security Investment. *Academy of Computer Machinery Transactions on Information Systems Security,* 5(6), 438-457.

Gyekye, S. A. & S. Salminen (2005). Are "good soldiers" safety conscious? An examination of the relationship between organizational citizenship behaviors and perception of workplace safety. *Social Behavior and Personality*, 33(8), 805-820.

Helweg-Larsen, M. & J.A. Shepperd (2001). Do moderators of the optimistic bias affect personal or target risk estimates? A review of the literature. *Personality and Social Psychology Review*, 5(1), 74-95.

Hewstone, M., M. Rubin, & H. Willis (2002). Intergroup bias. *Annual Review of Psychology*, 53, 575-604.

Hoffer, J.A. & D.W. Straub (1989). The 9 to 5 underground: Are you policing computer crimes? *Sloan Management Review*, Summer, 35-43.

Hoffman, D. A. & F. P. Morgenson (1999). Safety-related behavior as a social exchange: The role of perceived organizational support and leader-member exchange. *Journal of Applied Psychology,* 84(2), 286-296.

Hogan, R., & J. Hogan (1994). The mask of integrity. In T. Sarbin, R. Carney, & C. Eoyang (Eds.), *Citizen espionage: Studies in trust and betrayal* (pp. 107-125). Westport, CT: Praeger.

Johnson, J.L. (1989). Privacy and the judgment of others. *Journal of Value Inquiry,* 23, 157-168Insko, C.A, J. Schopler, R. Hoyle, G. Dardis, & K. Graetz (1990). Individual-group discontinuity as a function of fear and greed. *Journal of Personal Social Psychology*, 58, 68-79.

Ives, B., K. R. Walsh, & H. Schneider (2004). The Domino Effect of Password Reuse. *Communications of the Academy of Computer Machinery,* 47(4), 75-78.

Jones, A. (2005). How much information do organizations throw away? *Computer Fraud & Security* , 3, 4-9.

Judd, C.M. & B. Park (1988). Out-group homogeneity: Judgments of variability at the individual and group levels. *Journal of Personality and Social Psychology*, 54(5), 778-788.

Kasperson, R.E., O. Renn, P. Slovic, H.S. Brown, J. Emel, R. Goble, J.X. Kasperson, & S. Ratick (1988). The social amplification of risk: A conceptual framework. *Risk Analysis* 8(2), 177-187.

Klein, C. & M. Helweg-Larsen (2002). Perceived control and the optimistic bias: A meta-analytic review. *Psychology and Health*, 17(4), 437-446.

Lincoln, Y.S. & E.G. Guba (1985). *Naturalistic Inquiry*. Beverly Hills, CA: Sage

Linville, P. W., G. W. Fischer, & P. Salvoes (1987). *The PDIST model of in-group/out-group perceptions.* Paper presented at the Society of Experimental Social Psychology, Charlottesville, VA

Lockwood, P., C. Wong, K. McShane, & D. Dolderman (2005). The impact of positive and negative fitness exemplars on motivation. *Basic and Applied Social Psychology,* 27(1), 1–13.

Malone, S. (2003). Ethics at home: informed consent in your own backyard. *International Journal of Qualitative Studies in Education,* 16, 797-815.

March, J. G. & Z. Shapira (1987). Managerial Perspectives on Risk and Risk Taking. *Management Science*, 33(11), 1401-1418.

Mayer, R., J. Davis, & F.D. Schoormann (1995). An integrative model of organizational trust. *Academy of Management Review*, 20, 709-734.

McKenna, F.P. (1993). It won't happen to me: Unrealistic optimism or illusion of control. *British Journal of Psychology,* 84, 39-50.

Merriam-Webster.com Merriam-Webster, n.d. Wed 21 Feb. 2014 from http://www.merriam-webster.com/dictionary/exemplar

Miller, T. & L. Bell (2002). Consenting to what? Issues of access, gate-keeping and 'informed' consent. In M. Mauthner, M. Birch, J. Jessop & T. Miller (Eds.) *Ethics and Qualitative Research* (pp. 53-69). London: Sage Publications.

Mitnick, K.D. & W.L. Simon (2002). *The art of deception: Controlling the human element of security.* Indianapolis, IN: Wiley Publishing.

Murphy, K.R. & J.N. Cleveland (1991). *Performance Appraisal.* Needham Heights, MA: Allyn & Bacon.

Park, B., & M. Rothbart (1982). Perception of out-group homogeneity and levels of social categorization: Memory for the subordinate attributes of in-group and out-group members. *Journal of Personality and Social Psychology,* 42, 1051-1068.

Pelletier, L. G. & R. J. Vallerand (1996). Supervisor's beliefs and subordinates' intrinsic motivation: A behavioral confirmation analysis. *Journal of Personality and Social Psychology*, 71(2), 331-340.

Raden, D. (2003). In-group bias, classic ethnocentrism, and non-ethnocentrism among American whites. *Political Psychology*, 24(4), 803-828.

Reisberg, D. (2006). Memory for emotional episodes: The strength & limits of arousal based accounts. In B. Uhl, N. Ohta, & A. Segenthaler (Eds.) *Memory and emotion inter-disciplinary perspectives* (pp. 15-36). NY: Blackwell.

Robinson, S. & R. Bennett (1995). A typology of deviant workplace behaviors: A multi-dimensional scaling study. *Academy of Management Journal*, 38, 555-572.

Roth, W. (2005). Ethics as a social practice: Introducing the debate on qualitative research and ethics. *Forum: Qualitative Social Research,* 6(1).

Schwandt, T.A. (1997). *Qualitative Inquiry: A dictionary of terms.* Thousand Oaks, CA: SAGE Publications.

Security Management Index (2003). *The Alarming State of Security Management Practices Among Organizations Worldwide*, The Human Firewall Council.

Segev, A., J. Porra, & M. Roldan (1998). Internet Security and the case of Bank of America. *Communications of the Academy of Computer Machinery,* 41(10), 81-87.

Selten, R. (2001). What is bounded rationality? In G. Gigerenzer & R. Selten (Eds.), *Bounded Rationality*, Cambridge, MA: MIT Press.

Sia, T.L., C.G. Lord, K. Blessum, C.D. Ratcliff, & M.R. Lepper (2001). Activation of exemplars in the process of accessing social category attitudes. *Journal of Personality & Social Psychology,* 76(4), 517-532.

Siegrist, M. & G. Cvetkovich (2000). Perception of hazards: The role of social trust and knowledge. *Risk Analysis* 20(5), 713-719.

Simon, H.A. (l956). Rational choice and the structure of the environment. *Psychological Review*, 63, 129-138.

Siponen, M. & J. Iivari (2006). Six design theories for IS security policies and guidelines. *Journal of the Association for Information Systems,* 7(7), 445-472.

Sitkin, S., & N. Roth (1993). Explaining the limited effectiveness of legalistic "remedies" for trust/distrust. *Organization Science*, 4, 367-392.

Smith, E. R. (1998). Mental representation and memory. In D. T. Gilbert, S. T. Fiske, & G. Lindzey (Eds.), *Handbook of Social Psychology (Fourth Edition)* 1, 391-445. New York: McGraw-Hill

Stephan, W. G., & C. W. Stephan (2000). An integrated threat theory of prejudice, In S. Oskamp (Ed.), *Reducing Prejudice and discrimination* (pp. 23-45). Mahwah, NJ: Lawrence Erlbaum.

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

Sumner, W.G. (1906) . *Folkways*. New York: Ginn.

Taylor, R. G. (2006). Management perception of unintentional information security risks. *Proceedings of the twenty-seventh International Conference on Information Systems*, Milwaukee, WI.

Taylor, R.G. (2008). The social side of security. In I. Chen & T. Kidd (Eds.), *Social Information Technology: Connecting Society and Cultural Issues*, Hershey, PA: Idea Group Inc.

Taylor, R. & J. Brice (2012). Fact or fiction? A study of managerial perceptions applied to an analysis of organizational security risk. Forthcoming : *Journal of Organizational Culture, Communications, and Conflict.*

Thomas, T., J.R. Schermerhorn, & J.W. Dienhart (2004). Strategic leadership of ethical behavior in business. *Academy of Management Executive,* 18(2), 56-65.

Thompson, R. C., T.F. Hilton, & L.A. Witt (1998). Where the safety rubber meets the shop floor; A confirmatory model of management influence on workplace safety. *Journal of Safety Research*, 29, 15-24.

Tuttle, B.A., A. Harrell, & P. Harrison (1997). Moral Hazard, ethical considerations, and the decision to implement an information system. *Journal of Management Information Systems,* 13(4), 7-28.

Vonsolms, R., & H. Vandehaar (1994). A framework for information security evaluation. *Information & Management,* 26(3), 143-153.

Weinstein, N.D. (1980. Unrealistic optimism about future life events. *Journal of Personality & Social Psychology,* 39, 806-820.

Whitman, M. (2003). Enemy at the gate: Threats to information security. *Communications of the Academy of Computer Machinery,* 46(8), 91-95.

Yeh, Q.J. & A.J.T. Chang (2007). Threats and countermeasures for information system security: A cross-industry study. *Information & Management,* 44(5), 480-491.

Yin, R.K. (1984). *Case study research: design and methods*. Beverly Hills, CA: SAGE Publications, Inc.

Yin, R.K. (1993). *Applications of case study research (Second edition).* Thousand Oaks, CA: SAGE Publications, Inc.

Yin, R.K. (2003) *Case Study Research, Design and Methods* (*Third edition*). Beverly Hills, CA: Sage Publications, Inc.

Zhou, S. (2008). Effects of exemplars, affinity and affect on reactions to presidential election stories. *The Open Communication Journal*, 2, 29-33.

Zillmann, D. (1999) Exemplification theory: Judging the whole by some of its parts. *Media Psychology*. I, 69-94.

Zillmann, D., & H. Brosius (2000). *Exemplification in communication*. Mahwah, NJ: Erlbaum.

Zviran, M. (1999). Password security: An empirical study. *Journal of Management Information Systems*, 15(4), 161-186.