Association for Information Systems
AIS Electronic Library (AISeL)

ICIS 2006 Proceedings

International Conference on Information Systems (ICIS)

December 2006

Management Perception of Unintentional Information Security Risks

Richard Taylor
University of Houston

MANAGEMENT PERCEPTION OF UNINTENTIONAL INFORMATION SECURITY RISKS

Security and Assurance

Richard G. Taylor
C.T. Bauer College of Business
University of Houston
rgtaylor@uh.edu

Abstract

This paper will examine the difference between management's perception of the information security risks and actual information security risks that occur within their organization, arguing that management's perceptions are based mostly on (1)technology solutions to protect organizational information and (2) their beliefs that employees follow established information security policies. Slovic's ***perception of risk theory*** *will be used as a theoretical foundation for this study. The paper will focus on the neglected human element of information security management, with the primary focus on employees' actions that unintentionally expose organizational information to security risks. These employee actions can threaten information contained within the organization's computer-based systems as well as information in the form of computer-based system output, such as printed reports, customer receipts, and backup tapes. There has been substantial literature exploring the human threat to organizational information; however past research has focused on intentional behavior, typically referred to as "computer abuse". Less research has investigated employees' actions that unintentionally expose an organization to information security risks. Based upon this premise, the purpose of this study is to draw attention to such human threats and in turn shed light on the relationship between unintentional threats caused by employees' behavior and information security risks. Using a case study conducted in a financial institution, this study investigates these unintentional threats and management's perception of potential information security risks that these employees' actions may cause. The research reveals that many of management's taken-for-granted assumptions about information security within their organization are inaccurate. It is suggested that by increasing management's awareness of these risks, they will take precautions to eliminate this behavior to ensure that the organization's information is better secured.*

Keywords: Information security, perception of risk, information security threats

Introduction

Within the last decade the availability and affordability of data storage have allowed organizations to systematically amass vast amounts of information contained within computer-based information systems. In fact, there have been more electronic information and digital assets amassed in the last two years than accumulated in the entire history of mankind (O'Rourke, 2005). This information, though undeniably valuable, has also created a new challenge for management — keeping the information secure. Every organization must provide assurances to customers that their information, such as credit card data, is secure. Organizational sales data and proprietary trade secrets are also vulnerable to theft (Frolick, 2003). Information is threatened by the actions of deviant individuals who intentionally try to gain unauthorized access to the information, and also by the actions of internal employees who unintentionally put organizational information at risk. The task of the organization is to protect the information from *intentional* and *unintentional* misuse.

In 2004, proceeds from information theft were estimated at $105 billion — greater than proceeds from illegal drug sales (Swartz, 2005). However, 2005 may prove to be even more costly. For example, in only 130 breaches of organizational information (out of many thousands), over 55 million Americans were exposed to ID theft. The

Internet has become one of the primary threats to organizational information (Swartz, 2005). In 1988, only six Internet incidents were reported; however for the year 2003 that number had increased to 137,527 (CERT, 2004). The Internet is not the only threat. Today, information security threats come from dishonest employees, discarded information, lost/stolen property, and other technical and non-technical means. Although legislation such as HIPPA, GLBA, and SOX has been introduced to force organizations to address information security issues, organizational information still remains at risk. According to a survey conducted by the Human Firewall Council (2002), less than 20% of organizations have fully instituted policies and procedures to ensure compliance to these established legislation requirements.

These statistics show that now more than ever organizational information is at risk. While organizational information takes many different forms, current definitions of information security seem to refer to information contained *within* an organization's computer-based systems (Mattia & Dhillon, 2003). Because of this, information security solutions are geared toward technology-based solutions to protect this electronic data. However, information security definitions need to be expanded to also consider data no longer contained within these computer-based systems — printed reports, diskettes, backup tapes, and any other documents that contain sensitive or confidential organizational information. In 2005 alone, 5.9 million people in the US had their personal information compromised because of a lost or stolen system backup tape (PRC, 2005). This technology-generated output is as crucial to protect as the information contained with the computer systems. Since the information is no longer contained within the computer systems, technology-based solutions are no longer sufficient to protect this valuable information. However, technology-based solutions still prevail as the primary countermeasures to security incidents, resulting in heavy spending on technology-based solutions that primarily attempt to keep unauthorized users from accessing their computer-based systems**.**

To properly protect information, organizations need to reconsider their existing approach to information security and expand their views to consider both technology threats and human threats. However the human aspect of information security is often overlooked, even though research suggests it is the violations of established organizational security safeguards by trusted insiders that often lead to information security incidents (Dhillon, 2001). These problematic situations in an organization's security strategies need to be addressed. Unfortunately, few IS researchers are investigating these human issues that lead to information security incidents.

To prevent information security incidents, organizations need to understand and identify the vulnerabilities that exist within their organization, and then take actions to correct or eliminate those vulnerabilities (Rosenthal, 2003). Knowing the cause of these information security risks is vital to developing an information security strategy (Whitman, 2003). Thus, the first part of creating an information security strategy is the identification of the dominant threats facing organizational information. This paper suggests that one of these threats involves the actions of employees that may unintentionally result in information security risks. In most cases, employees are unaware that their actions are putting the organization's information at risk.

Adding to the possible severity of these employee actions is management's perceptions of the frequency of these actions. Management often fails to consider the actual probabilities of these employee actions or to monitor the occurrences of these actions. Instead, management's perception is based largely on heuristics, which can negatively affect their decision process (Slovic et al., 1976). Therefore, the gap between management's perceptions of information security risks and actual information security risks can lead to serious threats to organizational information.

This paper, thus, seeks to shed light on human behavior, more specifically, on employee actions that may unintentionally expose the organization to information security risks and on management's perception of the frequency of these actions. This paper will explore the following research questions:

(1) What is management's overall perception of their organization's information security risks?

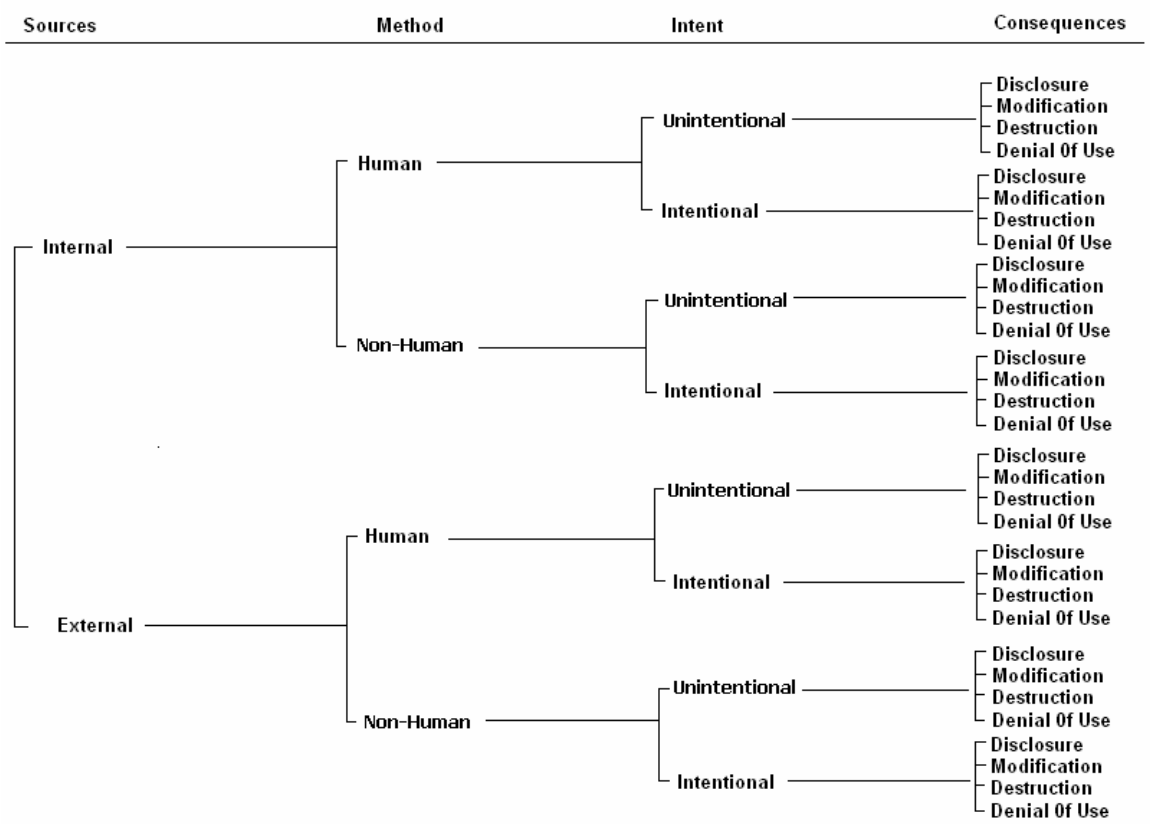
(2) What is management's perception of employees' actions that may unintentionally expose their organization to information security risks?

(3) How is management's perception of employees' actions that may unintentionally expose the organization to information security risks different from the actual actions of employees?

Based on a case study conducted in a financial institution, this research will attempt to answer these questions and, as a result, show the potential danger of management mis-perception of information security. This research can make a valuable contribution to the information security literature by providing research on topics that have received

little attention, such as unintentional information security risks and the threats posed by the output of computer-based systems. This paper can also contribute to practitioners by raising awareness of information security threats of which they were unaware.

Information Security Threats



adapted from The Four Dimensions of Information Systems Security (Loch et al. 1992)

Loch et al. (1992) identified threats to information systems as either internal or external. In both cases, the threats could be human or non-human, each of which could be the result of intentional or unintentional actions. Internal human threats include actions by employees and poor administrative procedures. External human threats consist of competitors or hackers attempting to access organizational information. Internal non-human threats involve mechanical and electrical problems as well as problems with the proper functioning of computer programs. Examples of external non-human threats are natural disasters and computer viruses.[1] Whether intentional or unintentional, human-based or non-human-based, internal or external, these threats can lead to the disclosure, modification, destruction, and denial of use of organizational information (Loch et al., 1992).

Although past research has been published addressing numerous external threats (Frolick, 2003; Rosenthal, 2003; Mitnik, 2003) this paper only focuses on internal human threats, therefore will only consider past literature related to this type of information security threat. A search of the literature found several references to internal human threats (Straub, 1990; Straub & Nance, 1990; Straub & Welke, 1998; Dhillon, 1999; Dhillon, 2001; Dhillon & Moores, 2001; Harrington, 1996); however all of these articles focused on intentional behavior most often referred to "*computer abuse*" (Straub & Welke, 1998; Straub, 1990). Computer abuse is defined as "the unauthorized and *deliberate* misuse of assets of the local organizational information system by individuals including violations against hardware, programs, data, and computer services" (Straub, 1990 p.257 emphasis added). Note that the definition

[1] Loch et al. (1992) refers to computer viruses as non-human threats; however since viruses must be created by humans it seems like Loch et al. misclassified this threat.

only refers to deliberate behavior and is focused on computer-based information, ignoring the informational output of the systems. The subjects of the previous research involve the prevention of these intentional actions by organizational insiders through the use of security countermeasures (Straub, 1990; Straub & Nance, 1990).

Although there is a group of individuals within an organization that *intentionally* cause information security risks, there is a larger group of employees within an organization whose behavior can *unintentionally* lead to information security risks[2]. "Most of the employees can be endowed with a strong enough set of beliefs and morals to act as effective controls over the way they conduct themselves within a company. It can be safe to assume that most employees will perform their duties according to the company credos, and will not try to subvert controls by engaging in illegal activities" (Dhillon & Moores, 2001 p.722). While it is obviously important for organizations to take all precautions possible to prevent intentional computer abuse, these intentional abusers are few compared to the number of employees whose actions may unintentionally cause information security risks. Most employees have no intentions of doing anything that would put their organizations' information at risk. However, unbeknownst to them, their daily actions could be creating significant information security risks. Unintentional threats could result from employees revealing information that would allow another person to gain access to the information within the computer-based systems. Examples of this behavior include revealing system passwords (Gordon et al., 2005), leaving passwords on 'post-it' notes at the user's desk (Zviran, 1999), and creating weak passwords (Spafford, 1991). Often overlooked, though, are the unintentional threats caused by neglecting the security of the computer-based system output. Employee behavior that unintentionally puts system output at risks includes throwing sensitive information in the trash (Jones, 2005) and leaving sensitive information where it can be easily accessed (even by the cleaning crew) (Buckner, 2005).

If information security policies are inadequate or no security awareness training is offered to address these issues, employees may not be aware of proper behavior for keeping information secure (Conger, et al., 1995). There is not an abundance of literature that focuses on these actions of employees that could *unintentionally* result in information security risks and of the threat posed by computer-based system output. It is important that these be understood by management to create an effective information security strategy for their organization.

Perception of Risks

Simon's (1957) theory of bounded rationality states that decision makers construct simplified models to deal with the world. Simon argues that the decision maker *"...behaves rationally with respect to this [simplified] model, and such behavior is not even approximately optimal with respect to the real world. To predict his behavior, we must understand the way in which this simplified model is constructed, and its construction will certainly be related to his psychological properties as a perceiving, thinking and learning animal"* (p. 198).

Cyert & March's (1963) behavioral theory of the firm shows that management decisions are limited by bounded rationality. They further indicate that managers make decisions without the availability of all necessary information. Starr (1969) and Slovic (1987) have utilized the theory of bounded rationality to research the effects of perceptions of risk. They have concluded that management is blind to the high risks posed by technology because of the perceived benefits of technology. Their results indicate that rational decision making is not always used "when judging probabilities, making predictions, or attempting to cope with probabilistic tasks" (Slovic, 1987, p. 281). Instead, people tend to use judgmental heuristics or simplification strategies. The heuristics may sometimes be valid in certain circumstances, but in others they can lead to biases that are "large, persistent and serious in their implications for decision making" (Slovic et al., 1976 p. 36).

The psychological dimensions of risk can be distilled into two primary factors: (1) the severity of the consequence, and (2) the probability of its occurrence (Slovic et al, 1976). Initial research on perceived risks focused on hazards such as earthquakes, nuclear power, food preservatives, etc. However other research has taken these theories and methods and applied them to more specific subjects such as the perception of risks toward using seat-belts (Slovic et al., 1978), adolescents' perceptions of risks from smoking (Slovic, 1998), and the risks of using a mobile phone

[2] Note that there is a difference in unintentional behavior that may cause information security risks and intentional behavior that may unintentionally cause information security risks. The focus of this paper is on the latter, arguing that the actions of employees may be *intentional*; however the potential results of those actions (information security risks) are *unintentional*.

while driving (White et al., 2004). This paper will use the perception of risk theory to investigate management's perceptions of information security threats. The two factors mentioned above can be applied to management's perception of employee behavior that unintentionally exposes the organization to information security risks. In consideration of the first factor, it is suggested that management is primarily concerned with the severity of the consequences from technology-based threats and will not be concerned with the unintentional threats posed by employee behavior. Management will also consider these employee actions to be rare occurrences, therefore posing little risk and needing no attention.

A long stream of research indicates that management's perceptions of risks have a direct impact on the decisions they make (Starr, 1969; Slovic, 1987; Slovic et al., 1974, 1976, 1979; Fischoff et al., 1978, 1979; Sjoberg, 1999; Siegrist et al., 2005) Applying this theory to information security management, the research indicates that management's perceptions of various information security risks leads to strategic decisions that often result in inadequate information security. This has been referred to as "executive blindness" (Slovic, 1987). Decision makers tend to misperceive events by ignoring probabilities and instead using heuristic-based mechanisms to measure uncertainty or avoid dealing with it. This leads to a reactive approach to information security threats (Slovic et al., 1974).

Misperception can lead to an "optimistic bias" (Helweg-Larsen and Shepperd, 2001) by management. The optimistic bias refers to the tendency for people to believe that they are more likely to experience positive events and less likely to experience negative events. This has been demonstrated in events such as auto accidents (McKenna, 1993), earthquakes (Helweg-Larsen, 1999), and crime (Preloff & Fetzer, 1986). The optimistic bias can be defined at both the individual level and group level, and results in people rating their own risks as lower than other similar people or groups (Helweg-Larsen and Shepperd, 2001). People perceive that they are better prepared to deal with negative events than are others. This leads to the first hypothesis:

H1: Management perceives the level of information security within their organization to be high.

The optimistic biases may also interfere with the institution of preventive measures to address risks (Helweg-Larsen and Shepperd, 2001), such as information security policies and security awareness training. Managers may feel overly optimistic regarding their employees' awareness of information security policies. This type of optimism can also be attributed to manager's perception that the organization's employees are part of a homogenous "in-group" whose behavior is based on a positive exemplar, which is often the manager herself (Judd & Park, 1988). Therefore, since they read and adhere to information security policies, they perceive that their employees will do the same. The leads to the second hypothesis:

H2: Management perceives that employees adhere to established information security policies.

When making decision, managers do not always have sufficient knowledge regarding threats to their organizational information. The manager will use all information and experiences that are readily available; however this often leads to a technology-based approach to addressing information security risks (Dhillon, 2001). Managers will turn to trusted advisors whose opinions they value (Siegrist & Cvetkovich, 2000). These advisors are often so-called experts who share the same values that the manager believes are important in a specific situation (Early & Cvetkovich, 1995). When information security advice is sought, management typically turns to the information security officer or the IT manager. This advice, though valuable in protecting organizational information, is often more technological in nature. If management relies solely on this advice, the human element of information security management may be entirely ignored. To make more informed decisions, managers must increase their awareness of their environment (Gigerenzer, 2001). This leads to the third hypothesis:

H3: Management is unaware of employees' actions that may unintentionally expose organizational information to security risks.

Research Method

A qualitative understanding of information security can be advantageous because of the ability to research the phenomenon within the scope of the organization (Dhillon & Backhouse, 2001). Yin (2003) states **"**the distinctive

need for case studies arises out of the desire to understand complex social phenomena" (p. 2). Therefore the case study is an ideal methodology for investigating the concerns of information security, allowing an in-depth investigation of a phenomenon in its original context (Benbasat et al., 1987).The case study methodology can be used both for the development of theory and for the testing of existing theory (Yin, 2003). Case studies may be exploratory, explanatory, or descriptive in nature and are especially effective when answering "how" and "what" questions that are exploratory in nature (Yin, 2003), which is the purpose of this study.

Construct validity was satisfied through data triangulation and having a draft of this research reviewed by a key informant (Yin, 2003). The multiple sources of data used in this case study are (1) interviews, (2) documents, and (3) direct observation. Because of the author's past experience within the industry and a positive rapport established with the CIO and CEO, full access to all employees, all documents, and office locations was granted. Twenty-four (24) employees were interviewed from all levels of the organization. Documents, including emails, policies, examination reports, and the employee handbook were made available. In addition, access was given to observe employee behavior during office hours, and to explore the offices after hours. After-hours access allowed the researcher to roam the organization to look for evidence of information security risks. Permission was also granted to "dumpster dive"[3] in an attempt to locate sensitive information that may have been thrown in the trash (instead of shredder bins).

To ensure reliability, the case study protocol proposed by Yin (2003) was followed. Employee interviews were conducted over a six month period. The interviews were focused, lasting about an hour each (Merton et al., 1990). The questions were semi-structured but allowed for open responses and discussion from the interviewees. The questions attempted to gain understanding from the employees regarding the following:

- Their understanding of information security
- Their perception of the information security level at their organization,
- Their understanding of information security risks and the behavior that cause information security risks,
- Their knowledge of consequences to the organization of information security risks,
- Their specific behavior or actions that have resulted in information security risks,
- The level of trust the employees have in their peers,
- The extent to which countermeasures are implemented within the organization to prevent information security risks.

To further add to the reliability a case study database was created, allowing the data to be analyzed by someone other than the researcher (Yin, 2003). The interviews were recorded on tape, and then transcribed indicating the date of each. (Miles & Huberman, 1994). The interview transcripts were combined with written documentation, and personal observations to form the entire case study database.

External validity involves the extent to which the results of this study can be generalized (Yin, 2003). The use of theory in a single-case study contributes to the external validity. The following case study is a theory-based interpretation of human behavior that may unintentionally lead to information security risks in a single organization. External validity could be improved with studies in other organizations to corroborate the findings of this study (Yin, 2003).

Case study research also requires a high degree of ethical consideration (Roth, 2005), especially when the research involves a subject such as information security. In any research, ethical considerations must remain on ongoing part of the research, well beyond the initial signing of a consent form (Malone, 2003). The CEO and CIO of the organization studied served as "gate-keepers" who allowed access to the organization and employees (Miller and Bell, 2002). It was important to keep these two individuals updated on a constant basis. Each staff interview was conducted with only the researcher and the employee present. Document review was conducted by the researcher alone after the documents were provided by the CIO. All other events, (dumpster diving and after-hours observations) were conducted with the CIO present. After each phase of the research, the CEO was briefed on the findings, and additional consent was sought (and granted) for the proceeding phase of the research.

[3] "Dumpster dive" refers to looking through the trash for discarded information.

The Organization and Analysis

First South Savings (FSS)[4] is a financial institution located in a major metropolitan area in the southern United States. There are seven FSS branches throughout the metropolitan area, consisting of approximately 200 full and part-time employees. Of the seven branches, one branch is located at the FSS 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, the author served as a technology 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. A continued involvement in the industry through speaking at various industry conferences and educational sessions, as well as publishing articles in the industry's journals, has established the author as an industry insider. Being considered an industry insider provided a high level of legitimacy with the FSS staff, resulting in employees' willingness to divulge information and greater access to organizational resources (Malone, 2003).

Second, FSS was chosen because it is in the financial services industry. Industry has been shown to be an important factor to be considered when conducting information security research because of the nature of the assets to be protected (Straub & Nance, 1990). The financial industry deals with a greater amount of sensitive and potentially damaging information than other industries. Specifically, banking institutions have a lot at stake when it comes to information security. Therefore employee behavior that unintentionally (or intentionally) leads to information security risks could have greater consequences. Employees in industries with high degrees of information security sensitivity should be more concerned about security (Goodhue and Straub, 1991). Because of the potential for information loss, the financial industry faces strict regulatory requirements regarding the protection of information. The Graham-Leach-Bliley Act (GLBA) was instituted in 1999 to protect financial information. GLBA requires all financial institutions to secure customer data from unauthorized access (SBC, 1999). Financial institutions also face regular federal examinations to ensure regulatory compliance. In the past few years, information security has been included in those examinations. Based on the requirements posed on FSS by GLBA and federal regulators, it was expected that FSS would consider information security a high priority. This lead to the first hypothesis to be tested:

H1: Management perceives the level of information security within their organization to be high.

During the initial interview with the CEO and subsequent interviews with other executives of FSS, it was confirmed that they perceived that information security was a top priority and that FSS had a significantly high level of information security. The first question asked of each executive staff member was "how secure is your organization's information"? According to the CEO:

> *On a scale of one to ten I would say we're an eight. 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; however that's more intuitive that data based.*

Time and time again, similar answers were echoed, such as the following made by 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.*

FSS invested in yearly security audits from an outside firm to ensure the organization was providing adequate security. These outside security audits seemed to give the organization a high level of confidence in their organizational security. According to the VP of Operations:

> *We have the outside audit firm come in and hack around and whatever they do, then come back and I sat in exit interviews where they say they found some places we need to improve on…some*

[4] This is not the organization's real name. I thank the management and employees of FSS for participating in this case study.

> *of it is non-critical and some is a little more critical. Based on what I've seen and from what people have come up and told us I feel pretty good.*

The CEO, as well as the other executives, perceived that the outside security audits and the federal examinations served more as a validation of their existing information security efforts than a service that improved organizational security.

> *I think what a third party does is either validate or invalidate your intuitive feelings about where you are. So I think that in the scope of how the world is sitting in this area I was pleased with what the 3rd party said. We also had an examination last year with regulators coming in. Again that was confirmation that compared to others in the industry we are in pretty good shape.*

Reliance on the results of the third party audit has led to a false sense of security by the executive staff. This reflects a typical technology-based approach to information security. The title of the written report from the outside auditors is ***Information Systems Security Review***. The objective listed in the audit report was as follows:

"We understand that the primary objectives of the project were to perform a comprehensive IS controls review of the automated controls within the existing computer environment and systems. In addition, we performed a firewall security review and internal and external intrusion testing. Our findings and recommendations will be useful in enhancing the systems and in providing cost-effective internal control improvements."

Clearly, from reading the objective, it can be determined that the security audit consisted of an assessment of the technological controls of information security. However, when the report was presented to the executive staff informing them that no security vulnerabilities were discovered, management was convinced that the organizational information was well protected from security threats.

Even without considering the results of the outside audit, managers felt the organization's information was secure based on their experience with the controls that existed on the system, again reflecting a technology-based view of information security.

> *I'm comfortable with the system being secure. You have to have a password to get into everything, so whether it be just the email or the system itself…you have a user name and a password in order to get into it, so I'm fairly comfortable with security.*

Even after discussions to distinguish "systems security" from "information security", management's opinion of the information security level of the organization was unchanged.

> *I think it's pretty high, especially when it comes to customer data, that level of awareness has been raised over the last year, year and a half. People are reminded of it on a regular basis. Is it 100 percent effective, no, nothing is 100 percent effective. But I think the general awareness of protecting customer information is fairly high.*

Management did not perceive information security to be a problem, whether the information is in the form of electronic data within the computer-based system or hard-copy data. Some managers referred to the results of the recent federal regulatory examination, which included ensuring the protection of customer information. After reviewing the examination report and speaking to the CIO it was discovered that the information security section of the examination consisted of a self-report questionnaire that was completed by the CIO. When questions regarding information security were asked, such as "has management established and documented an adequate information security policy to provide for the overall direction and implementation of information security", the CIO simply answered "yes". Because of a lack of expertise, the federal examiners who conducted the examination at FSS simply accepted the answers provided by the CIO. As a result, the examiners reported that information security at FSS was "satisfactory". This contributed to the overall perception of management that the organization was successfully providing adequate information security.

The consensus of the executive staff was that FSS considered information security a top priority and the organization has taken appropriate measure to ensure the protection of their information. The primary reason given for management's perception was the belief that FSS had sufficient policies in place to address information security issues. A review of FSS employee handbook found policies addressing physical control to the buildings and specific areas within the branches, password creation and protection, information securing, and the disposal of customer and organizational information. Management perceived that employees were reading and following these policies. If organizational information was put at risk, they perceived it would be the result of an outside attack or

an internal employee's deviant behavior. Employee behavior that would unintentionally put the organization's information at risk was perceived to happen on rare occasions; however not often enough to be concerned about. This leads to the second hypothesis:

H2: Management perceives that employees adhere to established information security policies.

Information security models have stressed the importance of the establishment and implementation of security policies (Segev et al.,1998). Information security policies at FSS were posted on the company intranet and updated throughout the year as needed. All employees had access to the intranet and were encouraged to read the policies. Once a year, employees were asked to sign a document verifying that they had read the policies. Management was asked about their perception of three areas of employee behavior which were addressed in their information security policies, which could unintentionally leads to information security risks: (1) revealing/sharing system passwords, (2) leaving sensitive information unsecured, and (3) throwing sensitive information in the trash. Management perceived that these were not problems for FSS because of existing policies that prohibit such actions. When asked if they thought employees would give out or share their system password, management unanimously proclaimed that employees would not. Managers felt that employees were well aware of existing password policies at FSS, and fully understood the importance of protecting 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.*

Regarding leaving sensitive information unsecured, managers again felt that this rarely occurred at FSS. Each office had a lock on the door and every desk and file cabinet had locks. All employees were given keys to the locks for their work areas. The securing of information, as required by GLBA, had been stressed to all employees.

> *Employees understand the importance of securing information. Even those who have locks on their doors know they have to put information away at night and lock it in their desks or file cabinets because the cleaning crew still comes in and empties the trash. The information we have here is just too sensitive to leave out in the open so we make it a top priority to see that it doesn't happen. Graham-Leach-Bliley really opened our eyes to protecting the privacy of our customer's information.*

Management also perceived that the FSS staff was quite effective at 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.*

Managers again pointed to the existence of a policy that stressed the importance of shredding sensitive information. They also pointed out that the number of shredder bins that were located throughout FSS made it very convenient for employees to use. To add to the convenience, each employee had an individual "shred can" at their desk in addition to their trash can. Employees were encouraged to keep the two receptacles separate to prevent accidentally throwing sensitive information into the trash can. A tour of the shredder bins located throughout the main branch was conducted. The shredder bins were large plastic garbage-can-like receptacles. Each bin had a large slit in the top approximately two feet long and five inches wide to allow employees to put large quantities of paper in at one time or to facilitate thicker green-bar reports. Each shredder bin was secured with a pad lock which required a key to unlock. The shredder bins did seem to be located in areas which made access easy for most employees. The "shred cans" at employees' desks were observed. These "shred cans" were clearly marked and kept very convenient for employee use.

> *I see them taking their shred each day over there [to the shred bins], but if they had something in the trashcan I don't go and check everybody's trashcan at night. Now on the teller line all of their shred is right there at their feet as they are working throughout the day and if they want to throw something in the trash it's back on the opposite side of the wall where they would actually have to get up out of their chair and I don't think they would get up to throw something in that trash can other than their trash.*

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. To verify the accuracy of management's perceptions, employees were interviewed. Because of their close proximity, 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 that those observed by management, because employees have opportunities to see diverse and disparate behaviors that management may not be aware of. In addition to interviews, employee behavior was observed to help test the final hypothesis:

H3: Management is unaware of employees' actions that may un*intentionally* expose organizational information to security risks.

System Passwords

The first attempt to validate or invalidate the perceptions of management was through the interview process. The interview process began with six employees of the IT department. These employees ranged in length of employment at FSS from two weeks to several years. After reviewing the results of the outside security audit, expectations were quite high that the IT department was making every attempt to keep the organization's information secure (from a technological point of view). Throughout the interviews, it was validated that the employees of the IT department seemed effective in providing technology-based solutions to keep information secure. Interview results showed that the employees of the IT department would not share their personal passwords with other employees. However, interviews revealed that employees of the IT department were sharing administrator passwords. Each of the IT employees had an individual network ID with administrator access; however when logging on to perform networking functions, employees would use the generic "Administrator" ID and password, which all IT employees had knowledge of. By doing this, there was no record of which IT employee was accessing the system, making it possible for information to be put at risk without the possibility of detecting which employee caused the risk.

Password sharing was also found throughout FSS, including all branches visited. Two staff employees and one branch manager admitted they would give out their passwords if asked by people they trusted, such as management or IT personnel. One actually admitted she has allowed another employee to user her ID and password. Another example of password sharing is said to be common at FSS.

> *We had a situation where our computers went down and all of our work had to be hand written, so when the computer system came back up everything had to be logged in and so by giving my password to the branch manager and assistant branch manager they were able to go in and help post my work and other tellers' so we were just up here until 9 o'clock instead of midnight. I can't remember if I changed my password the next day, but probably not, and I doubt that the other tellers did either.*

Access to these system passwords would allow someone to perform financial transactions using another tellers ID, preventing the detection of the act and identification of the abuser.

Even though most employees claimed that they would not reveal their system password, it was believed by the CIO (and from the author's past experiences in the industry) that employees were simply stating what they felt was the "appropriate answer". The CIO suggested that this should be verified by having his IT staff call employees and ask for their password. The IT staff contacted 60 employees randomly selected from the employee call list, being sure to select employees from every level of FSS, including executives. The employees were simply asked for their system password. Of the 60 calls made, 10 went directly to voice mail, therefore eliminating those employees from consideration. Of the 50 employees that were contacted, 50 passwords were surrender, with only one employee providing any objection before eventually surrendering his password[5].

In follow-ups, many employees said that even though they knew it was against FSS policy to give out their password, they thought it was okay because they believed that IT personnel could access their password anytime

[5] Employees who surrendered their passwords had their passwords automatically reset, forcing them to change it immediately.

through the system. Others claimed that they trusted the IT staff, believing that their password would not be used for any fraudulent activities. There was unanimous agreement among the employees who surrendered their passwords--there was no intention to put FSS's information at risk[6].

The other two employee actions investigated were (1) throwing sensitive information in the trash and (2) leaving sensitive information unsecured. Both of these actions involve the protection of information that is no longer only contained within the computer-based systems, but now also resides in the forms of printed reports, customer receipts, loan applications, etc. To verify these other two actions that could unintentionally put information at risk interviews were conducted and it was arranged to have access to the FSS headquarters and main branch after hours[7]. Intentions were to observe the existence of unsecured information and to perform "dumpster diving" to see if any sensitive information found its way into the trash. The CIO was ensured that this entire process would take no more than one hour.

Discarded Information

Employees were asked about throwing sensitive information in the trash. All employees interviewed proclaimed that this did not happen at FSS. They stated there were strict rules about using the shredder bins and they were adamant that those rules were strictly followed. An after-hours "dumpster diving" expedition contradicted the employee interviews. At the first stop, the marketing department, a discarded list containing the names and telephone numbers of the senior management and the Board of Directors of FSS was found. A stop in the office of the accounting manager resulted in finding documents containing FSS employee information, including employee name, FSS account number, and employee social security number. Also in the trash were copies of the accounting manager's personal checks, as well as confidential documents that had been manually torn, but were easily pieced together to identify names and account numbers. The next dumpster diving destination was the teller line, where several customer receipts, each containing customer name, account number, and account balance were found. The trash was also checked in a community printer room in the branch area. Inside this trash can were several completed loan applications and other documents that had been printed and discarded.

An interesting observation was also made regarding the "shred cans" that were at employees' desks. Many employees do not empty their "shred cans" into the shredder bins at the end of the day, instead choosing to wait until the "shred can" fills up. During the after-hours observation, the cleaning crew was observed emptying the "shred cans" into the trash, unbeknownst to employees or management.

Securing Sensitive Information

During interviews, employees were also asked if they left sensitive information unsecured. Many admitted that there were occasions when information was accidentally left on desks after hours, but according to them those occasions were rare. Each attributed this to the FSS policy that required employees to secure all sensitive information upon leaving every night. The results of after-hours observation found numerous violations which were potentially disastrous for FSS.

The marketing manager's office, loan manager's office, and the accounting manager's office were all unlocked. In the inbox on the marketing manager's desk were documents containing FSS employee information, including employee name, social security number, address, and salary for several employees. On the loan manager's desk were customer profiles and lending information containing customer names, address, telephone number, social security numbers, account numbers, etc. There was a large locked filing cabinet in the office; however the key was left in the lock. Upon unlocking the cabinet it was found that the cabinet contained all the information on every loan currently at FSS. Also, unsecured in the office was a notebook containing the credit scoring formula for FSS. There was a green-bar report on the accounting manager's desk which contained general ledger numbers and descriptions. Also on the desk were loan charge-off reports which contained all the necessary information to steal a customers'

---

[6] To prevent any negative effect on employee moral, an email was sent to all employees stating that the organization had failed to properly educate employees on password procedures, eliminating any blame on the employees.

[7] The CIO of FSS accompanied all after-hour observations.

identity. An open box containing confidential customer information was on a chair in the corner. Finally, a folder was observed in the inbox that contained the procedures for performing wire transfers at FSS.

The automated clearinghouse (ACH) room and the wire transfer rooms showed vulnerability. In the ACH room there was also a large locked file cabinet with the key still in the lock. Inside the file cabinet was all of the payroll information for every customer who currently had their payroll directly deposited at FSS. These records included customer name, address, telephone number, social security number, FSS account number, date of birth, place of employment, and salary. There were thousands of customer records left unsecured. The wire transfer provided completed copies of wire transfers containing customer information, sending and receiving financial institution routing and transit numbers, dollar amounts of transfers, and customer social security numbers. There were also binders containing many international wire transfers that been processed within the last week, showing all the pertinent information readily available. A binder containing the wire instructions was also found, with the id and password to the wire transfer system written inside the front cover.

The Individual Retirement Account (IRA) area and credit card area also had significant violations. In the IRA area a file cabinet containing all IRA's at FSS was unlocked. IRA information was also found on the employee's workstation. At this workstation all of the overhead compartments were unlocked except for one. The CIO informed that this compartment contained FSS company checks which must be kept secure because they are preprinted with FSS's corporate account number. However, even if accessed, these checks must be signed, which is done using an automatic "check signer" which requires a key to operate. Upon opening a drawer at the workstation a set of keys was found that unlocked the overhead compartment containing the corporate checks. The "check signer" was found in the same area with the key still in the lock.

The credit card department contained many overhead compartments which were all locked; however there were several boxes on the floor throughout the room. These boxes contained reports detailing the credit card information of FSS customers, including credit card number, expiration date, customer name and address, and available balance--everything needed to fraudulently use the credit cards.

The results of this one hour walk-around showed that information at FSS was not as secure as management perceived. This, along with the results of the employee password exercise, also indicates that management at FSS is "blind" to the information security risks that are occurring at FSS. There is a significant difference between management's perception of information security and the actual level of information security that exists at FSS.

Reaction of the CEO

Upon the completion of the interviews, documentation review, and observations, a final follow up meeting was scheduled with the CEO. He was shocked at the level of information security risks that were found at FSS.

> *It's surprising to the extent that we are open from the information side. I'm really amazed that you found it that easy. The stuff lying on the desk, there is some of that going on and…there is no punishment for that, but it's amazing that people are so fearless about giving away passwords and access.*

He was also amazed by the findings regarding unsecured information and information being thrown away.

> *We don't have someone supervising every area to make sure we are doing a good job…make sure we are not putting important information in the trash can. We don't have someone coming around making sure the desk is clear of paperwork that has important information.*

During the initial interview, the CEO ranked the FSS information security level an "8" on a scale of one to ten. However, after reporting the findings of this study, his opinion changed.

> *On the people side I guess it's more like a 3. That's where the exposure is.*

He also felt that the findings were so significant that immediate actions needed to be taken to correct the actions.

> *We need to get right on it. It's wide open. We are laying here wide open. It's not really an IT issue.*

In summing up his thoughts, the CEO seemed to finally understand the significance of the information security risks at FSS.

It's kind of like we are leaving the backdoor unlocked every night after night--nothing happens--eventually something does happen. From then on you are sure to lock you door.

Discussion

This case provides support for the three hypotheses presented in this study. Management at FSS perceived their information security level to high. The executives unanimously agreed that FSS had above average security and that they were doing everything possible to protect the organization's information. These perceptions were not based on the actual probabilities of information security threats, but rather on simplification strategies developed as a result the technology-based audits and federal examinations (Slovic, 1987). Without personal technological expertise, managers were forced to rely on the reports of these third parties (Siegrist & Cvetkovich, 2000). The CIO understood that the reports focused on the technology aspect of security, but that is all he was responsible for. Therefore he was pleased with the findings. Management failed to consider the human element of information 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). Strengthening their perceptions was the fact that FSS had not had any information security incidents (that they were aware of). If often takes a security incident to open management's eyes to threats within their organization (Dhillon & Moores, 2001). Therefore hypothesis 1 was supported.

Management did not perceive that employees were putting the organization's information at risk because of the established information security policies. Security policies have been identified by researchers as an effective deterrence to information security threats (Whitman, 2003). However, policies only deter risk-causing behavior if employees read the policies and adhere to them. FSS did have what was referred to as 'security policies', however most were focused on physical security and the threat from robbery. There was a systems usage policy that addressed the creation and changing of passwords, as well as the importance of keeping passwords confidential. Another general policy addressed the usage of the shredder bins and the securing of information after hours. These policies were on the FSS intranet which was available to all employees. However, there was no monitoring to ensure these policies were being read. Furthermore, there was no monitoring to ensure these policies were being followed. Because of an overly trusting environment existing within FSS, monitoring was felt to be unnecessary. Therefore management was unaware that information security policies were not being followed. This supports hypothesis 2.

People will respond only to the threats that they perceive (Slovic et al., 1980). Therefore management was unaware of the employee behavior that was occurring, and the frequency of occurrence, which unintentionally was putting their organization's information at risk. Because of these perceptions, management took an ethnocentric approach to information security management, focusing on the threats from untrusted outsiders and ignoring the potentially more dangerous threats from trusted insiders (Alport, 1954). Management perceived overall information security at FSS to be high. They were comfortable with the technology countermeasures that had been implemented to minimize information security incidents. They felt that the threats presented by employee behavior that could unintentionally put their information at risk were minimal. By perceiving that employee behavior was not a threat, the issue was not addressed by management. Management put too much trust in their employees, resulting in a lack of supervision (Dhillon & Moores, 2001). This study showed that management's perception of this type of employee behavior and the actual occurrence and frequency of this behavior was quite different. This supports hypothesis 3.

Some limitations of this research must be pointed out. Researchers have argued that research conducted by someone considered an "insider" may result in subjects' willingness to divulge information (Malone, 2003); however the role of an insider conducting research can also be very complex and situational (Sherif, 2001). An 'insider' familiarity with the industry can lead to a biased interpretation of the information collected. Avoiding biased interpretations of information was given a great deal of consideration. Interview transcripts and observation notes were reviewed by the CIO; however this is no guarantee that the researcher's line of questioning was not influenced by his knowledge of the industry.

This research was also limited by some other ethical considerations. For example, employees were questioned about their knowledge of social engineering[8] and (after explaining the definition) if they would be susceptible to such

[8] Social engineering is the art of deception to gain information.

tactics. Employees consistently believed that social engineering tactics would not work on them. Although the researcher and the CIO felt employees were naïve regarding social engineering, testing such beliefs was thought to be unethical since this would involve intentional attempts to deceive the employees.[9]

This brings up the question of whether this type of research should be duplicated. Although researcher must walk an ethical tightrope, there is a lot to gain from conducting security research in this manner. Organizations and employees may feel reluctant to admit to any security violations because of potential negative ramifications. Because of this, surveys and interviews alone may not provide the necessary data to properly understand the information security problems. Conducting case research can give a more in-depth understanding of the information security phenomena; however the researcher must walk a fine line between data gathering and the ethical considerations of research subjects. Researchers are encouraged to proceed with caution, always keeping key individuals informed and constantly gaining consent for every phase of research.

Conclusion

The study shows that organizational information is being put at risk by employee behavior. But unlike previous research, it focuses on employee behavior that unintentionally leads to information security risks. Although some of the employee actions may be intentional, the resulting information security risks are unintentional. The data from FSS revealed that a significant factor in the occurrence of this risk-causing behavior was management perception. Therefore to reduce these unintentional information security risks, management should not point their fingers at the employees. They should look towards the actions of the management staff. It is management's mis-perception of risk causing behavior within FSS and their technology-based approach that ignores the human factors that must be addressed. This blindness has led to insufficient countermeasures to protect organizational information from the unintentional risks caused by employee actions.

FSS and other organizations should be able to learn from this. This case study has pointed out the importance of addressing the human and organizational aspect of information security. Another important contribution to the practitioner community is to point out the fact that, even though there are individuals in an organizations who may intentionally attempt to defraud the organizations, there is as much potential information security risks from employee behavior that unintentionally causes information security risks. Employees at FSS consider their peers as family, and do not want to see any individual or the organization as a whole, harmed in any way. However, their lack of awareness may unknowingly result in unintentional harm. It is the responsibility of management to make all employees aware of the different behaviors that can result in information security risks. Management, as well as employees, must come to realize that they are in an industry where the gain from fraudulent activities based on exploiting sensitive information can potentially be significant. Because of the industry they are in, they must take extra measures to be certain that customer and organizational information are protected.

Organizations will continue to spend billions of dollars to protect their information. That spending will be in vain however if they neglect to consider the human aspect of information security. Organizations must also expand their definition of information security to include information both within their computer-based systems and information that is produced as output of those computer-based information systems. This study has attempted to investigate how employee behavior can unintentionally contribute to information security risks. As the paper has shown though, the fault does not lie entirely with the employees, but starts at the top of the organizational hierarchy with management's perception. This is a factor that can be controlled and have a direct impact on minimizing information security risks. As stated by the HR director of FSS:

> *People security lies with the managers who manage the people, and the managers who manage the managers.*

This research can prove to be valuable to the practitioner community by raising awareness of the existence of information security problems that exists in organizations today. By understanding these problems, management may seek better understanding of information security threats that they were unaware of, therefore ultimately resulting in action by management to improve information security. For the academic community, this research

[9] The researcher felt that this was different from the password gathering exercise, which was conducted by the IT department of FSS and did not involve deception.

investigates areas of information security management that have received little attention—unintentional human actions that put organizational information at risk and the risks created by system output. Hopefully, this research will lay the groundwork for more research to be conducted on this topic. Only one case study was conducted during this research; therefore additional case studies on this topic could increase the external validity of these findings. Subsequent empirical testing utilizing quantitative methodologies could also produce interesting findings. Additional studies could also investigate the factors that influence management's perception of information security risks. Finally, other information security studies utilizing Slovic's perception of risk theory could add to a greater understanding of management's perception of information security risks.

References

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

Benbasat, I., Gldstein, D, and M. Mead "The Case Research Strategy in Studies of Information Systems," *MIS Quarterly,* (11:3) 1987, pp 369-386.

Buckner, G. "Thwarting I.D. Theft, Part 2: What If You're a Victim?" in: *Fox News.com*, 2005.

CERT "2004 E-Crime Watch Survey," Carnegie Mellon University, Pittsburg, PA.

Conger, S., Loch, K.D., and Helft, B.L. "Ethics and Information Technology Use: A Factor Analysis of Attitudes to Computer Use," *Information Systems Journal* (5:3) 1995, pp 161-184.

Cyert, R.M., and March, J.G. *A behavioral theory of the firm* Prentice-Hall, Englewood Cliffs, NJ, 1963.

Dhillon, G. "Managing and controlling computer misuse," *Information Management & Computer Security* (7:5) 1999.

Dhillon, G. "Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns," *Computer & Security* (20:2) 2001, pp 165-172.

Dhillon, G., and Backhouse, J. "Current directions in IS security research: towards socio-organizational perspectives," *Information Systems Journal* (11) 2001, pp 127-153.

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

Earle, T.C., and Cvetkovich, G. *Social trust: Toward a cosmopolitan society* Praeger, Westport, CT, 1995.

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., and Combs, B. "How safe is safe enough? A psychometric study of attitudes toward technological risks and benefits," *Policy Science* (9) 1978, pp 127-152.

Fischhoff, B., Slovic, P., and Lichtenstein, S. "Weighing the risks: Which risks are acceptable?" *Environment* (21:4) 1979, pp 17-38.

Frolick, M. "A New Webmaster's Guide to Firewalls and Security," *Information Systems Management* (Winter) 2003, pp 29-34.

Gigerenzer, G. (2001). The Adaptive Toolbox. *Bounded Rationality*. G. Gigerenzer and R. Selten. Cambridge, Mass, MIT Press**:** 37-50.

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

Gordon, L.A., Loeb, M.P., Lucyshyn, W., and Richardson, R. "2005 CSI/FBI Computer Crime and Security Survey," Computer Security Institute.

Harrington, S.J. "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions," *MIS Quarterly* (20:3) 1996, pp 257-278.

Helweg-Larsen, M. (1999). "(The lack of) optimistic biases in response to the Northridge earthquake: The role of personal experience." *Basic and Applied Social Psychology* 29: 119-129.

Helweg-Larsen, M. and J. A. Sheppard (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.

HFC "Security Management Index, The Alarming State of Security Management Practices Among Organizations Worldwide," The Human Firewall Council, 2003.

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

Judd, C.M. and 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.

Lee, A. "A Scientific Methodology for MIS Case Studies," *MIS Quarterly* (13:1) 1989, pp 33-52.

Loch, K., Carr, H., and M. Warkentin "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly* (17:2) 1992, pp 173-186.

Malone, S. (2003). "Ethics at home: informed consent in your own backyard." *International Journal of Qualitative* Studies in Education 16: 797-815.
Mattia, A., and Dhillon, G. "Applying Double Loop Learning to Interpret Implications for Information Security Design," *IEEE*) 2003.
McKenna, F. P. (1993). "It won't happen to me: unrealistic optimism or illusion of control." *British Journal of Psychology* 84: 39-50.
Merton, R., Fiske, M., and Kendall, P. The focused interview: A manual of problems and procedures (2nd ed.) Free Press, New York, 1990.
Miles, M., and Huberman, A. *Qualitative data analysis: An expanded sourcebook* Sage, Thousand Oaks, CA, 1994.
Mitnik, K. "Are You the Weak Link?" *Harvard Business Review*), April 2003, pp 3.
Miller, T. and L. Bell (2002). Consenting to What? Issues of Access, Gate-Keeping and 'Informed' Consent. *Ethics in Qualitative Research*. M. Mauthner, M. Birch, J. Jessop and T. Miller. London, Sage Publications**:** 53-69.
Murphy, K.R., and Cleveland, J.N. *Performance appraisal* Allyn & Bacon, Needhan Heights, MA, 1991.
O'Rourke, M. "Data secured? Taking on cyber-thievery," *Risk Management* (Oct Issue) 2005.
Perloff, L. S. and B. K. Fetzer (1986). "Self-other judgments and perceived vulnerability to victimization." *Journal of Personality and Social Psychology* 50: 502-510.
PRC "A Chronology of Data Breaches Reported Since the ChoicePoint Incident," 2005.
Rosenthal, D.A. "Intrusion Detection Technology: Leveraging the Organization's Security Posture," *Information Systems Management* (Winter) 2003, pp 35-44.
Roth, W. (2005). "Ethics as a social practice: Introducing the debate on qualitative research and ethics." *Forum:* Qualitative Social Research 6(1).
SBC "Conference Report and Text of Graham-Leach-Bliley Bill," S.B. Committee (ed.), http://banking.senate.gov/con, 1999.
Segev, A., Porra, J., and Roldan, M. "Internet security and the case of Bank of America," *Communications of the ACM* (41:10) 1998, pp 81-87.
Sherif, B. (2001). "The ambiguity of boundaries in the fieldwork experience: Establishing rapport and negotiating insider/outsider status." *Qualitative Inquiry* 7: 436-447.
Siegrist, M., and Cvetkovich, G. "Perception of Hazards: The Role of Social Trust and Knowledge," *Risk Analysis* (20:5) 2000, pp 713-719.
Siegrist, M., Keller, C., and Kiers, H.A.L. "A New Look at the Psychometric Paradigm of Perception of Hazards," *Risk Analysis* (25:1) 2005, pp 211-222.
Simon, H. *Models of man* Wiley, New York, 1957.
Sjoberg, L. "Risk Perception by the Public and by Experts: A Dilemma in Risk Management," *Research in Human Ecology* (2:2) 1999, pp 1-9.
Slovic, P. "Perception of Risk," *Science* (236) 1987, pp 280-285.
Slovic, P. "Do Adolescent Smokers Know the Risks?" *Duke Law Review* (47:6) 1998, pp 1133-1141.
Slovic, P., Fischhoff, B., and Lichtenstein, S. "Cognitive Processes and Societal Risk Taking," in: *Cognition and Social Behavior,* J.S.C.J.W. Payen (ed.), Lawrence Erlbaum Associates, Potomac, MD, 1976, pp. 165-184.
Slovic, P., Fischhoff, B., and Lichtenstein, S. "Accident Probabilities and Seat Belt Usage: a Psychological Perspective," *Accident Analysis and Prevention* (10) 1978, pp 281-285.
Slovic, P., Fischhoff, B., and Lichtenstein, S. "Rating the risks," *Environment* (21:3) 1979, pp 14-39.
Slovic, P., Fischhoff, B., and Lichtenstein, S. "Facts and Fears: Understanding Perceived Risk," in: *Societal Risk Assessment: How Safe is Safe Enough?* R.C. Schwing and W.A.J. Albers (eds.), Plenum, New York, 1980.
Slovic, P., Kunreuther, H., and White, G.F. "Decision Processes, Rationality, and Adjustment to Natural Hazards," in: *Natural Hazards: Local, National, Global,* G.F. White (ed.), Oxford University Press, 1974.
Spafford, E. "OPUS: Preventing Weak Password Choices," CSD-TR 92-028, Purdue University.
Starr, C. "Social benefit versus technological risk," *Science* (165) 1969, pp 1232-1238.
Straub, D. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3) 1990, pp 255-276.
Straub, D., and Nance, W. "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS Quarterly* (14:2) 1990, pp 45-60.
Straub, D., and Welke, R. "Coping With Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4) 1998, pp 441-469.
Swartz, J. "2005 worst year for breaches of computer security," in: *USA Today*, 2005.
White, M.P., Eiser, J.P., and Harris, P.R. "Risk Perceptions of Mobile Phone Use While Driving," *Risk Analysis* (24:2) 2004, pp 323-334.

Whitman, M. "Enemy at the Gate: Threats to Information Security," *Communications of the ACM* (46:8) 2003, pp 91-95.

Yin, R.K. *Case Study Research, Design and Methods (3rd ed.)* Sage Publications, Beverly Hills, CA, 2003.

Zviran, M. "Password Security: An Empirical Study," *Journal of Management Information Systems* (15:4) 1999, pp 161-186.