Journal of Systems and Information Technology

Perception deception: security risks created by optimistic perceptions

Richard G. Taylor Jeff Brice, Jr. Sammie L. Robinson

Perception deception: security risks created by optimistic perceptions

Richard G. Taylor, Jeff Brice, Jr and Sammie L. Robinson
Jesse H. Jones School of Business, Texas Southern University, Houston, Texas, USA

Received 14 July 2015
Revised 28 December 2015
Accepted 8 January 2016

Abstract

Purpose – The purpose of the paper is to determine whether management's optimistic perceptions of their organization's level of information security preparedness can ultimately result in increased information security risks.

Design/methodology/approach – A case study was conducted in a financial institution. In all, 24 employees were interviewed. These employees came from all functional areas and various positions, from tellers to executives. Interviews were conducted, internal policies and examiners' reports were made available and access was given to observe the employees during working hours and to observe the facilities after hours.

Findings – Executives were overly optimistic about the level of information security at their organization. These optimistic perceptions guided security priorities; however, the findings show that their perceptions were misguided leaving their organization open to increased security threats. More specifically, the results show that optimist perceptions by management can put an organization's information at risk.

Originality/value – The paper uses existing theory and evaluates it in a "real-world" setting. For security research, it can be difficult to get honest responses from questionnaires; however, the hands-on approach provided a deeper insight to the problem of optimistic perceptions in an organizational setting. For practitioners, the case can raise managements' awareness of perceptional inaccuracies, resulting in more informed information security decisions and ultimately improved security for their organization.

Keywords Optimism, Perception, Organizational behavior, Information security

Paper type Research paper

Introduction

Managers hold differing perceptions about the real value of information security. Without a major loss because of poor or nonexistent measures, it may be that information security concerns will generally be quite low. In fact, it may take a major loss to convince managers of information security risks. For example, the losses that Target and Neiman Marcus experienced during the 2013 Christmas season may serve as an eye opener for managers regarding their organizations' level of information security preparedness.

Current managerial views of information security remain technology oriented, resulting in heavy spending on technology-based solutions to protect organization information from outside breaches (Taylor, 2008). These technology-based preventative measures are an integral part of an organizations overall security infrastructure; however, these technologies alone do not provide an appropriate level of information security protection (Straub and Welke, 1998; Dhillon, 2001). These preventative

Journal of Systems and
Information Technology
Vol. 18 No. 1, 2016
pp. 2-17
© Emerald Group Publishing Limited
1328-7265
DOI 10.1108/JSIT-07-2015-0062

technology-based countermeasures can create a false sense of security for organizations resulting in management being overly optimistic about their level of information security protection (Frolick, 2003; Taylor and Brice, 2012).

When key managers ignore the likelihood that information security incidents may occur within their organizations, their optimism forms the basis for behavior that is reactionary when negative information security events occur, instead of taking overt action to prevent them from occurring at all (Slovic *et al.*, 1974). A security incident at their organization or one that they learn about becomes the sole basis for their decision to reevaluate their information security strategy. In essence, the information security strategy, which should be a major strategic consideration at all times, becomes a significant organizational priority only as an afterthought to adverse activity. Although the folly of this knee-jerk behavior may seem obvious, many organizations, however, continue to invest in technology-based security technologies following this reactive behavior pattern. They are compelled to "put out fires" to meet the latest threat rather than developing, managing and evolving comprehensive security management programs over time. As Whitman (2003, p. 46) explains:

> […] 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.

To better protect an organization's information, management must adopt security countermeasures that also address the human threats that can come from employees within their organization (Dhillon and Backhouse, 2001). Understanding information security as a social issue calls for an investigation of organizational behavior issues that may impact information security risks. Although several such issues may merit consideration, this paper will demonstrate the influence of perception and optimism on organizations' overall information security strategy and seek to determine if erroneous managerial perception is a primary contributor to the frequency of employee risk-causing activity.

Perception

Perception involves the process by which people organize and translate external cues into a rational and sense-based integrated idea about the world around them (Lindsay and Norman, 1977). Managers receive informational cues from the environment that exists outside of and within the firm's boundaries. Such information is filtered through their own perceptual lens (Mezias and Starbuck, 2003). Although these perceptions may be based on information that is incomplete or even unreliable, perception is commonly accepted as reality and directs general human behavior (Daniels, 2003).

Management decisions are limited by bounded rationality (Cyert and March, 1963). Managers attempt to be rational actors, but they have restrictions on their capacity to process information (Simon, 1956; Bromiley and Euske, 1986). In other words, managers make decisions based on the information and knowledge they have at hand, ignoring critical information that may be unknown to them. These business decisions reflect their information processing limitations because of bounded rationality and may lead to managerial misperceptions. Thus, managers draw conclusions based on inaccurate perceptions rather than on a critical review of all available environmental information (Starbuck and Mezias, 1996).

Organizational theorists suggest that decisions made in the fog of misleading perceptions tend to lead to flawed organizational strategy (Bourgeois, 1985; Boyd *et al.*, 1993) and can result in operational risks and industry threats (Barr *et al.*, 1992; Starbuck, 1992). Giddens (2002) supports this concept of misperception, writing that unless there is a real belief that a severe consequence can occur then little attention will be paid to it.

In decision-making involving uncertainty and risks, actions are either decided by rational and/or deliberate processes or, more often, formed by emotional perceptions which are optimistically biased (Kahneman, 2003; Bracha and Brown, 2012). When making these decisions, there is a tendency to accept supporting or confirming evidence and ignore conflicting evidence. This bias suggests that people will selectively adopt evidence that they believe is significant to their own optimistic perspective (Son and Rojas, 2011, Vasvari, 2015).

Optimism

Optimism is "an attributional style that explains positive events in terms of personal, permanent and pervasive causes, and negative events in terms of external, temporary and situation-specific ones" (Youssef and Luthans, 2007, p. 778). People have the tendency to believe that a negative event is less likely to happen to them than to their peers (Klein and Helweg-Larsen, 2002). Research in social perceptions and cognitions refers to this as an optimism bias (Weinstein, 1980). Optimism bias explores how people view themselves more positively than is objectively warranted (Fast *et al.*, 2012). Optimism bias may be present when people do not have the necessary information they need to make an accurate risk assessment.

The target used to form this optimism bias is typically the "average other". For example, in a 1981 study (Svenson, 1981), 82 per cent of people believed they were in the top 33 per cent of drivers, when it came to their driving abilities. Likewise, other research has shown that people believe they are less likely to be victims of auto accidents (McKenna, 1993), crime (Perloff and Fetzer, 1986) earthquakes (Burger and Palmer, 1992; Helweg-Larsen, 1999) and getting a serious illness (Perloff and Fetzer, 1986).

The causal factors for optimist bias may be event specific or vary from event to event (Atkinson and Feather, 1996). Therefore, it is possible that specific factors that evoke optimism bias for some events may not do the same for similarly related events (Chua and Job, 1999). If it has not happened in the past, then it is unlikely to happen in the future. This viewpoint has consistently been attributed as one of the strongest predictors of optimism bias (Weinstein, 1980; Chua and Job, 1999).

Optimism bias leads to overrating the likelihood of positive events and underestimating the likelihood of negative events (Zacharakis and Shepherd, 2001; Helweg-Larsen and Sheppard, 2001) over which there is no control (Koellinger *et al.*, 2007). People will compare themselves with inappropriate standards when events are perceived as controllable; however, if an event is considered uncontrollable, then there is less chance for optimism bias to be present (Weinstein, 1980).

Although optimism bias literature generally focuses on increased risks, it should be noted that the presence of optimism bias can actually cause the deflation of risk perceptions (Helweg-Larsen and Sheppard, 2001). Taylor and Shepperd (1998) suggest that when the severity of an event reaches high enough levels, then optimism may actually decrease. For example, if a threat occurs close to home or to someone known, then optimism decreases because the perceived probability of the event happening to that individual has increased.

In an organizational context, optimism bias can lead managers to credit themselves for positive outcomes, while blaming external factors, or plain bad luck, for negative outcomes (Baker *et al.*, 2006; Billett and Qian, 2008). They display what Langer and Roth (1975, p. 951) have dubbed a "heads I win, tails it's chance" attitude. It is not uncommon for managers to underestimate their risks of negative events when they compare the possibility of the same risk to members of their peer group (Chua and Job, 1999; Heine and Lehman, 1995; Job *et al.*, 1995).

Information system security risks are no different. Information security threats must be perceived as real or they will be ignored, exposing an organization to information security incidents (Taylor, 2016). These misperceptions can cause management to be overly optimistic about the information security preparedness.

Methodology

To investigate the relationship between optimist bias and information security risks, a case study was conducted. The case study methodology can be used both for the development of theory and for the testing of existing theory (Yin, 2003). 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) states that management information systems is a discipline appropriate for using 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 (Yin, 1993, p. 64). The growing interest in case studies as research tools serves a useful purpose for a phenomenon that is broad and complex, needs a holistic, in-depth investigation and cannot be adequately studied outside the context in which it occurs (Benbasat *et al.*, 1987; Bonoma, 1985; Feagin, 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, 1993, p. 14) 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. The case research strategy allows for flexibility and individual variation (Cavaye, 1996), thus making it an ideal methodology for investigating information security concerns.

Information security is a subject that is difficult to study outside the context in which it occurs (Benbasat *et al.*, 1987). Organizations may not feel comfortable being forthcoming with their responses regarding information security. The case study method allows the researcher to conduct probing interviews and engage in ethnographic observations of information security practices within the organizational context. For this case study, access was granted to a financial institution.

Data triangulation was used to satisfy construct validity. Multiple sources of data were used, including internal documents, interviews and direct observation. Documents included company policies, internal emails, employee handbook and reports from federal regulators. After-hour access was granted, allowing the primary research to look for the evidence of information security risks.

The organization

When developing an information systems security strategy, the type of industry in which an organization does business is an important consideration. The following information in this study was gathered at a financial institution: First South Savings (FSS). FSS is located in a large metropolitan city with numerous branches throughout the city and surrounding communities. All executives, as well as the IT department, were located at the central location.

Operations in the financial services industry, more so than other industries, involve processing a greater amount of sensitive and potentially damaging information. Therefore organizations, such as FSS, face a greater exposure to operational risks. The stakes are higher for financial institutions such as FSS, therefore requiring a higher degree of information security than that required by other industries. The financial services industry faces strict regulatory requirements regarding information protection because of the increased potential for information loss. The Graham-Leach-Bliley Act (GLBA) was enacted in 1999 to protect financial information. A major provision of GLBA is that all financial institutions secure customer data from unauthorized access (SBC, 1999). In addition, information security is now included in the regular federal examinations conducted for financial institutions to ensure regulatory compliance. Likewise, such institutions' records are subject to audits to verify compliance. FSS were subjected to yearly federal examinations and external audits.

Interviews were conducted with 24 employees from various functional areas of the organization. The interviews took place over a six-month period of time. Each interview consisted of semi-structured questions, allowing open responses and discussion from the interviewees. The questions addressed the employees the understanding of information security risks within FSS, their perception of the current state of their information security, their understanding of behaviors that could result in information security risks and their knowledge of countermeasures that existed within FSS that existed to minimize information security risks.

The chief executive officer (CEO) and chief information officer (CIO) of the organization served as "gate-keepers" who allowed access to the organization and its employees (Miller and Bell, 2002). Each staff interview was conducted with only the primary researcher and the subject employee present. Document review was conducted by the researchers after the documents were provided by the CIO. All other events, such as 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. A draft of the final research was review by the CEO and CIO.

The purpose of the research is to investigate the dangers of misperceptions, leading to optimism bias, in a real organizational environment. In the study, we analyze the perceptions of real-world managers at FSS who work in a real-world business which may face the real-world consequences of (in)activity based on their perceptions.

Analysis

Initial security perceptions

After interviewing the entire executive staff of FSS, it was evident that they had a great deal of confidence in the organization's level of information security. However, their confidence was based more on perception than on exact knowledge. When ask to rate their level of security, the CEO stated:

> 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.

Therefore, we see that the CEO's view of their information security strategy was based on intuition. In other words, the CEO perceived that FSS had effective information systems security countermeasures in place to protect the organization from security threats. After interviewing the other executives, the same theme became evident. They felt their information security was "solid", as the CFO put it. This optimism was not based on any direct fact, but was based on their perception. When questioned, the executives (other than the CIO) admitted that this perception was not based on their knowledge of IT, but on the fact that FSS had never experienced a security breach. They referenced their "strong IT department" as a factor in their perception.

IT department

Interviews of the IT employees were conducted to evaluate the information security capabilities and practices of IT department. The IT employees had strong backgrounds in their fields. The executives of FSS perceived that the IT department was doing their job to keep the organization security free from security incidents. Observation and interviews proved their perception to be false. Many security vulnerabilities were found within the IT department. One such example involved the use of dial-in modems. The IT employees believed the use of dial-in modems would add an additional level of security, as, unlike with the internet, they could control who accessed the system and when it could be accessed. However, observation revealed that dial-in modems were often left turned. The network manager also admitted that the dial-in passwords were never changed; therefore, anyone who knew the passwords and had the modem numbers, including ex-employees, could access the system at any time. The IT employees knew this created security risk; however, they found it easier for them to keep the modems connected rather than turn them on when their system vendor needed access, which at many times was after hours. The IT staff admitted that they were never informed by their vendors when employees quit or were terminated by the vendors; therefore, even ex-employees of the vendors could access their system.

It was also a common practice to use a generic ADMIN ID and password which all IT employees had access to as opposed to each employee having their own specific account with administrator access. They admitted that, because of this, they were unaware of which employee had accessed a specific system at a specific time.

The executives were not aware of these risks, or any other, that came from the IT department. Their misperception of the security behavior of the IT employees ultimately increased the overall security risk at FSS.

Auditors/examiners reports

Another key factor in the executives' perception involved the reports that came from outside auditors and bank examiners. According to the FSS executives, the auditors and examiners reconfirmed their perception that information security at FSS was good. The COO points out:

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

After reviewing the auditors' and examiners' reports, it was evident that the reports only considered the technology-related aspects of information security. The reports focused only on technology-based security. The information the auditors' and examiners' used to complete the reports came from a checklist that was given to the CIO to complete. Therefore, neither the auditors nor the examiners had direct knowledge of the FSS information systems. The reports failed to address any of the social aspects related to the human elements of information security. Bases on auditors' and examiners' reports, the executives perceived that their overall information security was adequate. They were unaware that the auditors or examiners never confirmed the checklist received from the CIO nor did they investigate security risks caused by employee behavior.

Policies

It is important for organizations to establish security policies for all of their information-sensitive areas. In fact, security policy development and enforcement is a key staple of any comprehensive organization security model (Segev *et al.*, 1998). Security policies serve to decrease employee risk-causing behavior and have been used as a leading deterrence technique to dissuade active security threats (Whitman, 2003). The weakness with security policies, however, is that they have no effect if employees do not read, or interpret, the policies as they are written. FSS security policies were posted on the company's intranet and were updated regularly. All employees were required to read the policies. Furthermore, employees were required to certify each year that they had reviewed and understood the policies. However, there was no mechanism to examine the employees for their competency or familiarity with any of the security policies. Clearly, the overriding managerial assumption was that all employees were dutifully applying the security protocols on a daily basis.

In regards to organizational policies, three areas of employee behavior were addressed: the likelihood that employees would:

(1) reveal or share system passwords;

(2) leave sensitive information unsecured; and

(3) discard sensitive information in the trash.

Management perceived that these were not problems for FSS because of existing policies that prohibited such actions.

Passwords

The executives were optimistic that employees would not share or reveal their password. The executives' perceptions were that password policies were in place and that employees were aware of the importance of protecting system passwords. According to the CFO:

> I wouldn't sit here and tell you that it would be 100 per cent, depending on who was asking […] some people would probably offer it up, but overall most would not.

This executive perception also proved to be wrong. After interviewing employees, time and time again, they freely admitted that they would often share their passwords. Many employees admitted that they kept their passwords clearly visible on their desks. This was verified through direct observation. To further test, the executives' perception; a social engineering method was used. An unnamed employee claiming to work for the IT department randomly called 60 FSS employees, including management and executives, and simply requested their personal passwords. Of the 60 calls that were made, 10 were forwarded directly to voice mail. Of the 50 employees who were contacted by the IT department, all of them revealed their password. This again shows the flaw in relying on perception to dictate their information security strategy.

Unsecured information

The perceptions of FSS executives were that employees did not leave sensitive information unsecured. Each office was equipped with a door lock and each desk and file cabinet had locks. All employees were issued keys to the locks for their work areas. As required by The Graham-Leach-Bliley Act, the importance of securing information had been stressed to all employees. A policy existed stating that sensitive information must be secured at all times. The COO shared his perception:

> 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.

Again, after observing the employees' behavior, sensitive documents such as credit reports, employee files and customer credit card information were found unattended throughout FSS. This exposed FSS to potential security incidents. Once again, the executive perceptions were wrong.

Shredding information

Management was optimistic that FSS employees were 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 per cent say there is nothing in there [the trash], but all in all the chances of it happening are very slim.

The executives again pointed to the existence of a policy that stressed the importance of shredding all documents that contained sensitive information. Large shredder bins were located throughout FSS offices, making it very convenient for employees to dispose of the sensitive information. To add to the convenience, all employees were given a "shred can" (blue) in addition to their trash can (black) that was placed at their desk. Employees kept the two receptacles separate as a precaution against unintentionally throwing sensitive information into the trash can. The executives were confident that all discarded sensitive information was shredded.

Examination of the shredder bins revealed that each was secured with a padlock. The shredder bins were located in areas that were easily accessible by employees. The "shred cans" at employees' desks were clearly marked and conveniently located for employee use. However, as expected, sensitive information was found in employee trash cans. Management trusted that employees would follow the policy, but there was no monitoring to ensure this. Executives, managers and supervisors did not want to dig through the employees' trash cans every day for verification. In addition to employees discarding sensitive information in trash cans, it was observed that the cleaning crew emptied all individual shred cans into the garbage. The employees thought their shred cans were emptied every night and taken to the larger shred cans, even though the policy stated that each employee was responsible for emptying their own shred cans nightly. The information security risk at FSS was greater than expected, contrary to the executives' perceptions.

Executive reaction

After the information gathering process, the CEO was informed of the findings. The level of security risk at FSS was quite surprising to him:

> 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 surprised the information security policies were not being followed:

> 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.

Initially, the CEO rated FSS's information security level as an eight out of ten. However, his perception was changed when he heard the results:

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

The findings convinced the CEO that immediate action needed to occur to minimize the information security risk that unknowingly existed:

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

The CEO admitted that he had been overly optimistic about 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 your door.

Discussion

Executives at FSS perceived the organization had above average information security protection. They believed they were providing the necessary countermeasures to protect the organization from information security threats. Their perceptions were based on simplified strategies that were developed using information from third parties instead of data collected about actual probabilities of operational security threats (Slovic, 1987). As they did not have personal technological expertise, managers relied on the conclusions of third-party reporters (Siegrist and Cvetkovich, 2000), including auditors, federal examiners and the IT staff.

Although FSS did have a systems usage protocol in place, most of the security policies addressed physical security and the more traditional procedures involving workplace violence, various emergencies and robberies. Other information system policies were related to the shredding of confidential documents, storing requirements and processes for secure entry into, and exit from, the building itself. As every employee at FSS had intranet access, there was no structural impediment to receipt of all stated policies, procedures and protocols concerning security. However, there was no monitoring system that ensured that each employee understood, or even read, the policies. Furthermore, there was no confirmation to make sure that, even if read and understood, the policies were being put into practice. As the corporate culture of FSS emphasized honor and trust, it was deemed redundant, and possibly insulting, to monitor employees for security policy compliance. It was because of this unquestioning nature that FSS executives were oblivious to the reality that security protocols were being wholly abandoned by their subordinates.

FSS executives' perceptions guided their managerial priorities. This study's results demonstrate that their erroneous managerial perception was a primary contributor to the frequency of employee risk-causing activity. Managers within FSS ignored the possibility that routine and unchecked employee behaviors could create additional operational security risks. It is this optimism in human reliability coupled with blind dependence on a technology-based approach that must be dealt with for FSS to restore confidence in its security preparedness. Now that the blinders are off, appropriate measures may be taken to shore up information security inadequacies.

Research informs us that individuals are only capable of responding to the threats that they recognize as apparent (Slovic *et al.*, 1980). Thus, it is not surprising to find that FSS managers were unaware that employees were repeatedly placing the organization's information assets in peril. While most managerial security efforts were directed to outside threats, they failed to perceive the potentially more significant threat emanating from irresponsible internal personnel. Management's perception of information security turned out to be a consequence of their misplaced trust in the efficacy of their workforce, which led to the lack of a control system to avoid information security breaches. There was no managerial insight that unmonitored employee behavior presented a significant and obvious security risk, yet they were keen to develop comprehensive procedures for external threats.

The usefulness of this study is that it highlights an instance where management's bounded rationality about employee behavior concerning information security was quite different from actual reality and therefore placed the organization's valued assets at risk. The data from FSS revealed that managerial perception was a significant factor in the occurrence of risk-causing behavior. It is the manager's (mis)perception of this risk-causing behavior within FSS that needs to be addressed. Management's optimistic-based blindness led to insufficient countermeasures to protect organizational information from the information security risks caused by employee actions.

There are several implications for firms in this predicament. First, the control mechanism that is used by management needs to be improved. Agency theory informs us that effective control of employees can be achieved when using some form of monitoring, as the problem of employee control is a matter of risk in itself

(Brice *et al.*, 2011). It implies that observability (employee monitoring) and outcome uncertainty (the probability of incorrect work) are the determinants of control, and that there is an element of risk in any control system. It is because of monitoring that management may be more knowledgeable about the work performed and, thus, misperceptions of risk can be decreased. The type of monitoring system that is indicated in this case is that of behavioral control. Behavior control assumes that the employees are paid to display appropriate work behaviors, which can be observed, to insure congruence with organizational standards and policies (Eisenhardt, 1988). To decrease the real risk of information security fallibility at FSS, management should scrutinize employee behavior by utilizing mechanisms to include routine security audits, video/audio recording, in-person observations and occasional security drills to emulate conditions of information security risk. In this way, management's perception of risk would be informed by the reality of workplace practices and not the fantasy of invulnerability brought about by wishful thinking.

A second implication exits in the methods by which employees learn to consistently apply appropriate security measures as outlined in company policies. FSS management assumed that employees were following company protocols simply because they were included in the company handbook. The lack of adherence to company policies can be explained, in part, by Social Learning Theory (Bandura, 1986). In Social Learning Theory, we discover that individuals learn what to do and how to behave by paying attention to environmental cues. The most important learning device is that of direct experience (Bandura, 1986). FSS managers should include, as a part of their management of the organization, strict adherence to company security policies as previously suggested. However, there are other learning cues that employees will follow. Another social learning device is that positive role modeling in the organization (Bandura, 1986). In essence, if managers expect for employees to follow suit and place a real importance to company security protocols, then management needs to be observed doing that. Employees follow the lead of organizational authority figures and will model their behavior to fit in to organizational culture. FSS management needs to set a clear example for others to follow. A last environmental influence is that of encouragement from important referents. Employees need to be occasionally reassured that they are performing well in the area of information security by those whom they respect and follow. This recognition is not necessarily that of financial incentives but rather verbal encouragement that displays confidence from important others in the organization that one is performing well. Therefore, employees learn to be diligent and consistent with information security because it is dictated, modeled and encouraged all throughout the working environment.

A last implication for FSS might be for a need to change organizational culture. It is apparent that the predominant logic (culture) in the organization is that of giving the illusion of a secure institution even if not sufficiently secured. Based on management and employee misperceptions of the level of security threat, the organizational culture should be modified to reflect the overt recognition of actual security achievement and a reverence for those who excel at keeping it that way. Organizational culture may be influenced, in part, through the manipulation of environmental artifacts (Buch and Wetzel, 2001). Artifacts such as signs, posters, mottos and anything that reinforce the idea of organizational security should be observable in the parking lot, on the grounds, by the entrances and everywhere internal employees, external constituents and managers are in the company (e.g. hallways, offices, meeting rooms and workspaces). These constant reminders send a message of the importance of security and bring individual values and assumptions in line with expected performance. With the implementation of appropriate employee controls, social learning tactics and organizational artifact manipulation, eventually the acceptance of information security as an important topic should infiltrate the psyche of employees to the point that the daily grapevine will be affected, which is the ultimate source or reflection of an organization's true culture (Buch and Wetzel, 2001).

The primary implication for academics is that this study highlights the inconsistency of managerial perceptions with organizational reality. Without the utilization of a study methodology where the researcher performed an independent investigation of the physical environment, it is apparent that the underlying truth of security vulnerability would have not been exposed. This is interesting because a traditional method for examining organizational phenomena centers around the use of scaled questionnaires. It is possible that this common use has mislead those in academia, as what managers report and what really occurs relating to a variety of study questions may be unintentionally deceptive. This may suggest that asking questions of research subjects may not be enough to accurately depict the realities of phenomena in question.

Conclusion

There are many information security threats that present diverse and complex challenges for organizations. Countermeasures such as policies, awareness training and education, deterrents, detection methods and technology are necessary to protect an organization's information from the vast number of security threats that exist. The extent to which these countermeasures are implemented is based on management's perception of their organizations current information security infrastructure. Sufficient resources need to be allocated to information security to meet the needs of the organization. As long as executives continue to misperceive their organizations' level of security preparedness, employees will continue to contribute to information security risks, because employee awareness will in turn be low, punishment will be inadequate or nonexistent, and prevention and detection methods will be ineffective.

Nystrom and Starbuck (1984) demonstrated that organizational behavior, specifically strategic and management decision-making, may sometimes have disastrous consequences when initiated by misguided perceptions. In this paper, we report our findings about the misguided perceptions of real-world managers who work in an actual firm. Their business is one which may face the serious real-world consequences of (in)activity based on those perceptions. Their perceptions were filtered through the lens of simplified cognitive heuristics which resulted in their drawing inaccurate conclusions about the true level of potential threats to information security. This finding is in agreement with Mezias and Starbuck (2003) who theorized that "managers may have inaccurate perceptions regarding information that is central to their jobs as well as about information they believe is someone else's responsibility." The study data reported here suggest that managerial optimism may have disastrous consequences as well. However, organizations can indemnify themselves against damaging outcomes if management seeks to uncover and correct, perceptual inaccuracies.

Being able to understand and identify information security vulnerabilities that exist within an organization is crucial for managements' attempts to prevent security breaches. Only then can management implement decisions that correct or eliminate those vulnerabilities (Rosenthal, 2003). Going a step further, management needs to know the actual causes of information security risks to develop an overall information security strategy (Whitman, 2003). To do this well, there needs to be a clear assessment and understanding of technology-based threats, employee (behavioral) threats and an accurate assessment of the organization's current state of information security preparedness. Therefore, for organizational value to be preserved (and possibly enhanced), managerial perceptions of information security risks need to be based in reality and not on flawed perceptions. By understanding the problem, managers may seek better understanding of the limits of their cognitive biases and devise policies and practices to widen their perceptional base. Ultimately, the goal is to improve overall information security by decreasing erroneous managerial perceptions.

As in all single-firm case studies, a primary limitation is that the study results are really only applicable to the subject organization. However, this firm is not so unique that it does not mimic the operations of other similar firms in the industry. Therefore, companies with moderate similarities, like other financial institutions with similar information security strategies, can learn from this study. To accomplish a wider application to all firms, further case study and testing are essential. For instance, to minimize the disparity in stipulations of the work setting and to begin to create lasting theory, comparison case studies of firms in other industries that must secure other varieties of information in this, and other countries, is required. The small number of subjects interviewed may also be viewed as a study limitation. However, in this case, we interviewed everyone whose perceptions maintained relevance to the research inquiry. It is our hope that future research projects will improve on these limitations.

References

Atkinson, J.W. and Feather, N.T. (1966), *A Theory of Achievement Motivation*, Wiley Press, New York, NY.

Baker, M., Ruback, R. and Wurgler, J. (2006), "Behavioral corporate finance: a survey", in Eckbo, B.E. (Ed.), *The Handbook of Corporate Finance: Empirical Corporate Finance*, Elsevier/North Holland, New York, NY.

Bandura, A. (1986), *Social Foundations of Thought and Action: A Social Cognitive Theory*, Prentice-Hall, Englewood Cliffs, NJ.

Barr, P., Stimpert, J.L. and Huff, A.S. (1992), "Cognitive change, strategic action and organizational renewal", *Strategic Management Journal*, Vol. 13, pp. 15-36.

Benbasat, I., Gldstein, D. and Mead, M. (1987), "The case research strategy in studies of information systems", *MIS Quarterly*, Vol. 11 No. 3, pp. 369-386.

Billett, M.T. and Qian, Y. (2008), "Are overconfident CEOs born or made? Evidence of self-attribution bias from frequent acquirers", *Management Science*, Vol. 54 No. 6, pp. 1037-1051.

Bonoma, T.V. (1985), "Case research in marketing: problems and opportunities and a process", *Journal of Marketing Research*, Vol. 22, pp. 199-208.

Bourgeois, L.J. (1985), "Strategic goals, perceived uncertainty, and economic performance in volatile environments", *Academy of Management Journal*, Vol. 28, pp. 548-573.

Boyd, B.H., Dess, G.G. and Rasheed, A.M. (1993), "Divergence between archival and perceptual measures of the environment: causes and consequences", *Academy of Management Review*, Vol. 18, pp. 204-226.

Bracha, A. and Brown, D.J. (2012), "Affective decision making: a theory of optimism bias", *Games and Economic Behavior*, Vol. 75, pp. 67-80.

Brice, J., Nelson, M. and Gunby, N. (2011), "The governance of telecommuters: an agency and transaction cost analysis", *Academy of Strategic Management Journal*, Vol. 10 No. 1, pp. 1-18.

Bromiley, P. and Euske, K.J. (1986), "The use of rational systems in bounded rationality organizations: a dilemma for financial managers", *Financial Accountability & Management*, Vol. 2 No. 4, pp. 311-320.

Buch, K. and Wetzel, D. (2001), "Analyzing and realigning organizational culture", *Leadership & Organization Development Journal*, Vol. 22 No. 1, pp. 40-44.

Burger, J.M. and Palmer, L. (1992), "Changes in and generalization of unrealistic optimism following experiences with stressful events: reactions to the 1989 California earthquake", *Personality and Social Psychology Bulletin*, Vol. 18, pp. 39-43.

Cavaye, A.L.M. (1996), "Case study research: a multifaceted approach for IS", *Information Systems Journal*, Vol. 6 No. 3, pp. 227-242.

Chua, F.J. and Job, R.F.S. (1999), "Event-specific versus unitary causal accounts of optimism bias", *Journal of Behavioral Medicine*, Vol. 22 No. 5, pp. 457-491.

Cyert, R.M. and March, J.G. (1963), *A Behavioral Theory of the Firm*, Prentice-Hall, Englewood Cliffs, NJ.

Daniels, K. (2003), "Asking a straightforward question: managers' perceptions and managers' emotions", *British Journal of Management*, Vol. 14 No. 1, pp. 19-22.

Dhillon, G. (2001), "Violation of safeguards by trusted personnel and understanding related information security concerns", *Computer & Security*, Vol. 20 No. 2, pp. 165-172.

Dhillon, G. and Backhouse, J. (2001), "Current directions in IS security research: towards socio-organizational perspectives", *Information Systems Journal*, Vol. 11 No. 2, pp. 127-153.

Eisenhardt, K. (1988), "Agency and institutional theory explanations: the case of retail sales compensation", *Academy of Management Journal*, Vol. 31 No. 1, pp. 488-511.

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

Feagin, J.R. (1991), "The continuing significance of race: anti-black discrimination in public places", *American Sociological Review*, Vol. 56 No. 1, pp. 101-116.

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

Giddens, A. (2002), "The consequences of modernity", in Calhoun, C., Gerteis, J., Moody, J., Pfaff, S. and Virk, I. (Eds), *Contemporary Sociological Theory*, p. 244.

Heine, S.J. and Lehman, D.R. (1995), "Cultural variation in unrealistic optimism: does the West feel more vulnerable than the East?", *Journal of Personality and Social Psychology*, Vol. 68, pp. 595-607.

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*, Vol. 21, pp. 119-129.

Helweg-Larsen, M. and Sheppard, J.A. (2001), "Do moderators of the optimistic bias affect personal or target risk estimates? A review of the literature", *Personality and Social Psychology Review*, Vol. 5 No. 1, pp. 74-95.

Job, R.F.S., Hamer, V. and Walker, M. (1995), "The effects of optimism bias and fear on protective behavior", in Kenny, D. and Job, R.F.S. (Eds), *Australia's Adolescents: A Health Psychology Perspective*, England University Press, Armidale, NSW, pp. 151-156.

Kahneman, D. (2003), "Maps of bounded rationality: psychology for behavioral economics", *American Economic Review*, Vol. 93 No. 5, pp. 1449-1475.

Klein, C.T.F. and Helweg-Larsen, M. (2002), "Perceived control and the optimistic bias: a meta-analytic review", *Psychology and Health*, Vol. 17 No. 4, pp. 437-446.

Koellinger, P., Minniti, M. and Schade, C. (2007), "'I think I can, I think I can': overconfidence and entrepreneurial behavior", *Journal of Economic Psychology*, Vol. 28, pp. 502-527.

Langer, E.J. and Roth, J. (1975), "Heads I win, tails it's chance: the illusion of control as a function of the sequence of outcomes in a purely chance task", *Journal of Personality and Social Psychology*, Vol. 32 No. 6, pp. 951-955.

Lindsay, P.H. and Norman, D.A. (1977), *Human Information Processing: An Introduction to Psychology*, Academic Press, New York, NY.

McKenna, F.P. (1993), "It won't happen to me: unrealistic optimism or illusions of control?", *British Journal of Psychology*, Vol. 84, pp. 39-50.

Mezias, J.M. and Starbuck, W.H. (2003), "Studying the accuracy of manager's perceptions: a research odyssey", *British Journal of Management*, Vol. 14, pp. 3-17.

Miller, T. and Bell, L. (2002), in Mauthner, M., Birch, M., Jessop, J. and Miller, T. (Eds), *Consenting to What? Issues of Access, Gate-Keeping and "Informed" Consent Ethics and Qualitative Research*, Sage Publications, London, pp. 53-69.

Nystrom, P.C. and Starbuck, W.H. (1984), "To avoid organizational crises, unlearn", *Organizational Dynamics*, Vol. 12 No. 4, pp. 53-65.

Perloff, L.S. and Fetzer, B.K. (1986), "Self-other judgments and perceived vulnerability to victimization", *Journal of Personality and Social Psychology*, Vol. 50, pp. 502-510.

Rosenthal, D.A. (2003), "Intrusion detection technology: leveraging the organization's security posture", *Information Systems Management*, pp. 35-44.

SBC (1999), "Conference report and text of Graham-Leach-Bliley Bill", SBC, available at: http://banking.senate.gov/con

Segev, A., Porra, J. and Roldan, M. (1998), "Internet security and the case of Bank of America", *Communications of the ACM*, Vol. 41 No. 10, pp. 81-87.

Siegrist, M. and Cvetkovich, G. (2000), "Perception of hazards: the role of social trust and knowledge", *Risk Analysis*, Vol. 20 No. 5, pp. 713-719.

Simon, H.A. (1956), "Rational choice and the structure of the environment", *Psychological Review*, Vol. 63, pp. 129-138.

Slovic, P. (1987), "Perception of Risk", *Science*, Vol. 236, pp. 280-285.

Slovic, P., Fischhoff, B. and Lichtenstein, S. (1980), "Facts and fears: understanding perceived risk", in Schwing, R.C. and Albers, W.A.J. (Eds), *Societal Risk Assessment: How Safe is Safe Enough?*, Plenum, New York, NY.

Slovic, P., Kunreuther, H. and White, G.F. (1974), "Decision processes, rationality, and adjustment to natural hazards", in White, G.F. (Ed.), *Natural Hazards: Local, National, Global*, Oxford University Press, Oxford.

Son, J.W. and Rojas, E.M. (2011), "Impact of optimism bias regarding organizational dynamics on project planning and control", *Journal of Construction Engineering and Management*, Vol. 137 No. 2, pp. 147-157.

Starbuck, W.H. (1992), "Strategizing in the real world", *International Journal of Technology Management*, Vol. 8 Nos 1/2, pp. 77-85.

Starbuck, W.H. and Mezias, J.M. (1996), "Opening pandora's box: studying the accuracy of managers' perceptions", *Journal of Organizational Behavior*, Vol. 17 No. 2, pp. 99-117.

Straub, D. and Welke, R. (1998), "Coping with systems risk: security planning models for management decision making", *MIS Quarterly*.

Svenson, O. (1981), "Are we all less risky and more skillful than our fellow drivers?", *Acta Psychologica*, Vol. 47, pp. 143-148.

Taylor, K.M. and Shepperd, J.A. (1998), "Bracing for the worst: severity, testing and feedback as moderators of the optimistic bias", *Personality and Social Psychology Bulletin*, Vol. 24, pp. 915-926.

Taylor, R. and Brice, J. (2012), "Fact or fiction? A study of managerial perceptions applied to an analysis of organizational security risk", *Journal of Organizational Culture, Communications, and Conflict*, Vol. 16 No. 1.

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

Taylor, R.G. (2016), "Potential problems with information security risk assessments", *Information Security Journal: A Global Perspective*, in Press.

Vasvari, T. (2015), "Risk, risk perception, risk management – a review of the literature", *Public Finance Quarterly*, Vol. 60 No. 1, pp. 29-48.

Weinstein, N.D. (1980), "Unrealistic optimism about future life events", *Journal of Personality and Social Psychology*, Vol. 39, pp. 806-820.

Whitman, M. (2003), "Enemy at the gate: threats to information security", *Communications of the ACM*, Vol. 46 No. 8, pp. 91-95.

Yin, R.K. (1993), *Applications of Case Study Research*, SAGE Publications, Thousand Oaks, CA.

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

Youssef, C.M. and Luthans, F. (2007), "Positive organizational behavior in the workplace: the impact of hope, optimism and resilience", *Journal of Management*, Vol. 33 No. 5, pp. 774-800.

Zacharakis, A. and Shepherd, D. (2001), "The nature of information and overconfidence on venture capitalist's decision making", *Journal of Business Venturing*, Vol. 16, pp. 311-332.

Further reading

Allport, G.W. (1954), *The Nature of Prejudice*, Addison-Wesley, Cambridge, MA.

Barr, P.S. and Huff, A.S. (1997), "Seeing isn't believing: understanding diversity in the timing of strategic response", *Journal of Management Studies*, Vol. 34 No. 3, pp. 337-370.

Dhillon, G. and Moores, S. (2001), "Computer crimes: theorizing about the enemy within", *Computers & Security*, Vol. 20 No. 8, pp. 715-723.

Taylor, R.G. (2006), "Management Perception of unintentional information security risks", *Twenty-Seventh International Conference on Information Systems, Milwaukee, WI*.

Corresponding author

Richard G. Taylor can be contacted at: taylorrg@tsu.edu