Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2009 Proceedings

Americas Conference on Information Systems (AMCIS)

2009

Examination of Organizational Information Security Strategy: A Pilot Study

Nicole Lang Beebe
University of Texas at San Antonio, nicole.beebe@utsa.edu

V. Srinivasan Rao
University of Texas at San Antonio, chino.rao@utsa.edu

Examination of Organizational Information Security Strategy: A Pilot Study

Nicole Lang Beebe
The University of Texas at San Antonio
nicole.beebe@utsa.edu

V. Srinivasan Rao
The University of Texas at San Antonio
chino.rao@utsa.edu

ABSTRACT

The prevailing approach to cyber security continues to be the implementation of controls—technical, formal, and informal. We have seen little departure from a fundamentally preventive strategy. The criminal justice field has called for an increased emphasis on deterrence strategies, specifically Situational Crime Prevention (SCP). This paper presents the results of an exploratory (pilot) study based on interviews of CISOs (or approximate equivalents). We found that while the balance of controls does appear to be improving, technical controls are still the priority—particularly in small organizations. We found that IS security strategies are still predominantly preventive; organizations do not view offender deterrence as a strategy. The respondents definitely see room for strategic improvement. By and large, the information security professionals interviewed believe that cyber offenders are rational decision makers, that reducing anticipated benefit would be the most lucrative influence, followed by perceived effort required and perceived risk of being caught, in that order.

Keywords

Security, strategy, situational crime prevention, SCP

INTRODUCTION

Computer and information security is a critical issue. Despite its unequivocal importance, however, organizations are still struggling to identify and implement effective computer and information security strategies. Annual computer crime surveys, such as the CSI/FBI Computer Crime and Security Survey, continue to show alarmingly upward trends in attack frequency, attack novelty, and the average financial loss per incident (Richardson, 2007). Against the backdrop of a rapidly changing technological landscape, organizational information security tactics have improved, but evolution of information security strategies has lagged behind. Prevention via technical controls (e.g. via firewalls, password protection, and encryption) continues to be the primary information security strategy employed by organizations (Choobineh, Dhillon, Grimaila and Rees, 2007; Dhillon and Backhouse, 2001). The effectiveness of a preventive strategy based primarily on target hardening measures appears finite—there appears to be a point of diminishing returns. This results in a call for additional, new strategic approaches to securing information and corresponding information systems.

In recent years, Willison et al. (2000, 2005, 2006a, b; Willison and Backhouse, 2006) extended Situational Crime Prevention (SCP) (Clarke, 1980) from the criminal justice realm to the information systems arena. They offered SCP as a new way to identify and implement specific crime countermeasures. We believe SCP represents an opportunity for a fundamental, paradigmatic shift in IS security strategy (not intended to replace current strategies, but rather augment them). Whereas previous strategy shifts (e.g. implementation of formal and informal controls) continue to focus on prevention, SCP shifts the focus to deterrence—influencing potential offenders' decision making process, such that the offender is dissuaded from launching a specific attack against a specific target.

For clarity, this research adopts the following definitions for prevention and deterrence:

> *"Preventive measures are attempts to ward off criminal behavior through controls. These measures constitute the line of defense when potential abusers choose to ignore deterrent measures. Preventive measures can impede criminal activities…" (Kankanhalli et al., 2003: 142).*
>
> *"Deterrent measures are attempts to dissuade people from criminal behavior by influencing their rational decision making process" (adapted from Kankanhalli et al., 2003: 141).*

Overall, there are few (if any) empirical studies that examine organizational security strategies. In the current study, we report the results of an exploratory (pilot) study based on interviews of nine senior level information security professionals (CISOs or approximate equivalents). The aim of the study is to explore what strategies are currently in use and why. Additionally, we have gathered information on the current thinking of CISOs on the usefulness of information security strategies based on reducing offender motivation.

LITERATURE REVIEW

Information systems (IS) security effectiveness refers to the degree to which information security strategies and countermeasures control computer security incidents, and thereby limit associated losses for organizations. Generally speaking, computer security incidents include:

- Organizational members violating technical, formal, and informal security controls (Choobineh et al., 2007) without malicious intent (e.g. user error or negligence);
- Intentionally disruptive actions intended to interrupt, intercept, modify, and/or fabricate data, information, and communications (Jung, Han and Lee, 2001) from internal and external human sources; and
- Natural disasters and other non-human related influences (Jung et al., 2001)

An important research stream within IS security has focused on strategies to improve IS security effectiveness, particularly with respect to controlling computer security incidents stemming from human sources. Early studies extended General Deterrence Theory (GDT) from the criminal justice domain to explain variations in IS security effectiveness (Straub, 1987, 1990). While significant variation was explained via his studies, Straub's construct operationalization limits the generalizability of the findings to "insiders." Straub also tested rival theories, including the impact of preventative and "target hardening" measures, as well as various sociological factors (e.g., offender motivation) and found little empirical support for them. This lack of support is intriguing, given the prevailing strategic approach to organizational information security has been, and continues to be, preventative in nature.

Since Straub's seminal works, additional theory for explaining IS security effectiveness has been proposed, arguing that general deterrence is insufficient for achieving IS security effectiveness. This theoretical redirection is consistent with criminological theory and practice, which have reconsidered the general deterrence model and its assumptions (Kennedy, 1997, 1998; Kennedy and Braga, 1998). Accordingly, researchers have proffered additional theory to explain IS security effectiveness. They have posited that deterrence through the fear of severe and likely punishment is insufficient, as is a defensive strategy based solely on target fortification. In a series of articles, Dhillon and colleagues argue for a balanced information security strategy consisting of technical, formal, and informal controls (Dhillon, 1999; Dhillon and Backhouse, 2001; Dhillon and Moores, 2001; Dhillon, Silva and Backhouse, 2004).

Later studies extended socio-behavioral theories, such as Social Bonding Theory, Social Learning Theory, and Theory of Planned Behavior to explain IS security effectiveness (Lee and Lee, 2002; Lee, Lee and Yoo, 2004). Such theory helps explain why certain individuals are inhibited from committing crime (social bonding theory), why others are motivated and encouraged to commit crime (social learning theory), and why offenders generally decide to commit or not commit crime based on their attitudes, existent social norms, and perceived behavioral control (theory of planned behavior).

The latest theory suggested to explain IS security effectiveness is Clarke's (1980) Situational Crime Prevention (SCP) theory. SCP is a model that integrates both crime-focused and criminal-focused perspectives to explain why specific crimes are committed by specific individuals at a specific place and time. It argues that situational manipulations can influence an offender's rational decision-making process. It presumes offenders are rational decision makers, balancing costs vs. benefits, moderated by rationalizations/justifications and provocations to committing a specific crime. In a series of publications, Willison et al. (2000, 2005, 2006a, b; Willison and Backhouse, 2006) extend SCP to the digital realm. To date, support for the extension has been limited to conceptual/theoretical arguments and two post-hoc analytical case studies (Willison, 2000, 2006a, b; Willison and Backhouse, 2006).

Research Gap

Relatively speaking, information security research is nascent. Given criticisms that information security methods, tools, and management have overemphasized technical controls (Choobineh et al., 2007; Dhillon and Backhouse, 2001) and have "…suffered because of a lack of theoretical conceptualizations" (Choobineh et al, 2007: 963), research has focused on theory development. Little research has empirically tested assumptions regarding the nature of prevailing organizational IS security strategies. Researchers have not empirically answered the following research questions:

- Do organizational IS security strategies balance technical, formal, and informal control? If not, why not?
- Does this balance or imbalance vary across organizations (e.g. respecting industry, organizational size, etc.)?
- Are organizational IS security strategies preventive and/or deterrent in nature? To what extent, in both cases?
- If strategies are primarily preventive, is there room for an increased emphasis on deterrent strategies?
- If there is room for an increased emphasis on deterrent strategies, what influences cyber offender decision making?

The current research seeks answers to these questions.

THEORETICAL BACKGROUND

Because this research answers questions involving current strategic approaches to IS security, a brief overview of those approaches is warranted, to ensure commonality of understanding regarding the research questions and subsequent answers. This section provides a brief overview of controls-based approaches, GDT, and SCP.

Control-Based Approaches

Technical controls reduce crime commission opportunities by technically preventing the successful commission of the crime (e.g. via firewalls, password protection, and encryption). Dhillon and Moores (2001:719) describe controls in general as "…basic safeguards that organizations can put in place thereby minimizing chances of a computer crime taking place... [they] deal with restricting access…"

Formal controls are organizational and managerial measures that clearly outline acceptable behavior (e.g. policies, procedures, and standards) and introduce a system of checks and balances (e.g. organizational structures that define roles and responsibilities, adequate supervision, and separation of responsibilities). Formal controls "…deal with establishing rules and ensuring compliance …[through]…organizational structures and processes" (Dhillon and Moores, 2001: 720).

Informal controls are those measures that serve to inculcate employees into a culture of ethics, accountability, and proper conduct (e.g. education and training programs, widespread prioritization placed on ethical behavior and accountability, and facilitating an ethos of self-control/restraint) (Dhillon and Moores, 2001). Informal controls make it clear what behavior and attitudes are appropriate for an organization, and they make it clear that organization members will be held accountable for inappropriate behaviors and attitudes.

General Deterrence Theory (GDT)

General Deterrence Theory relies on rational decision making. It argues that the certainty, celerity, and severity of punishment will influence offenders, convincing them that the cost of the crime outweighs its benefits. It presumes offenders believe punishment is certain, swift, and severe. Its utility has been questioned over the years, however, due to inconsistent effectiveness indicators. Most have pointed to the notion of bounded rationality when explaining GDT failures—offenders simply do not accurately perceive a crime's punishment to be certain, swift, and/or severe. In short, the punishment is incorrectly perceived, or is too conceptually distant from the commission of the crime.

Situational Crime Prevention (SCP)

SCP is also grounded in the rational choice perspective, which suggests that offenders are relatively rational in their decision to be involved in criminal activity in general (i.e., "the involvement decision"), as well as their decision to commit a specific criminal act (i.e., "the event decision"). SCP was designed to address highly specific forms of crime by systematically manipulating or managing the immediate environment in as permanent way possible, with the purpose of reducing opportunities for crime as perceived by a wide range of offenders (Clarke, 1983). More recently, researchers have recognized that environments and situations not only create opportunities for crimes, but at times provide the motivation, via provocations, which elicit criminal responses (Wortley, 2001). Therefore, SCP techniques have focused on effectively altering opportunity structures and/or motivations of a particular crime by: 1) increasing the perceived effort, 2) increasing the perceived risk, 3) reducing the anticipated reward, 4) reducing provocations, and 5) removing excuses (Cornish and Clarke, 2003) (see Table 1). On its face, SCP changes the "event decision" by altering the offender's perceptions of a specific criminal opportunity. However, an offender's experience during a criminal event directly affects his or her continual "involvement decision" over time.

Therefore, addressing the opportunity structures for crime not only prevents an impending criminal event, but also appears to influence an offender's desistance decision.

Increase the Effort	Increase the Risks	Reduce the Rewards	Reduce Provocations	Remove Excuses
Target harden	Extend guardianship	Conceal targets	Reduce frustrations and stress	Set rules
Control access to facilities	Assist natural surveillance	Remove targets	Avoid disputes	Post instructions
Screen exits	Reduce anonymity	Identify property	Reduce emotional arousal	Alert conscience
Deflect offenders	Utilize place managers	Disrupt markets	Neutralize peer pressure	Assist compliance
Control tools/ weapons	Strengthen formal surveillance	Deny benefits	Discourage imitation	Control drugs and alcohol

Table 1. SCP Opportunity Reducing Techniques (Cornish and Clarke, 2003)

Theoretical Relationships

In one sense, SCP subsumes GDT and controls-based approaches. At the same time, important distinctions should be noted. Security strategies that focus on GDT clearly identify significant punishments for specific wrong-doing, consistently and swiftly enact those punishments, and actively 'advertise' those situations to deter future offenses the offender and others. So, GDT-based security measures should theoretically serve to increase perceived risk of being caught. However, there is a subtle, but important difference between GDT and risk-increasing SCP techniques. SCP techniques seek to increase the perception of the *risk in being caught*—GDT seeks to increase the perception of the *risk of punishment once caught*. If the offenders do not perceive punishment is certain, severe, or swift, the punishment fails to deter. In the cyber realm, offenders arguably act with relative impunity, so punishment-based deterrence is arguably ineffective. Further, one could argue that the risk of being caught is particularly influential in the cyber realm, because should an attack be detected (i.e. caught), the benefits of the attack might be diminished (i.e. the system is patched, data becomes unusable, etc.). Detecting the occurrence of physical crimes does not tend to diminish the utility of the 'fruits of the crime' as much as it does in the cyber realm.

Respecting the relationship between controls-based approaches and SCP, again there is some overlap. Perceived technical and formal controls will result in an increased perception of effort required. Formal and informal controls will result in a decreased perception of crime rationalization and justification. Again, there is a subtle, but important distinction. The strategic intent of traditional controls-based approaches is *prevention*. The strategic intent of SCP-based approaches is *deterrence*. The former case is not concerned with dissuading the offender from attempting a crime, just preventing success. The latter case is more concerned with manipulating situational factors such that the offender does not attempt a crime.

METHODOLOGY

Research Design

This study is exploratory in nature, intended to obtain insight into organizational information security strategies--their nature, prevailing trends, and organizational motivation in implementing them (i.e. desired outcomes). We also seek feedback from information security professionals regarding the general theory being proposed. We believe a qualitative method is best suited to obtain such information, because of the study's exploratory nature. The underlying philosophical perspective is positivist, but formal hypotheses and propositions were not developed a priori. The survey method was employed. The primary data source for this qualitative study was a series of one-on-one interviews with key, senior-level, information security personnel at organizations of varying size in a variety of industries. An open-ended, semi-structured survey (see Appendix A) was used to guide the interview and ensure consistency between interviews. Interviews were conducted face-to-face when possible. All interviews were recorded, but personal and organizationally identifiable information was not recorded. Respondent participation was invited and voluntary. Invitations were extended to individuals possessing direct knowledge of their organization's information security strategy(ies). Recorded interviews were analyzed using content analysis and discourse analysis.

Scope

As previously stated, computer security incidents can include human and non-human (e.g. natural) events, intentional and unintentional human actions, malicious and benign behavior, etc. Organizational IS security strategies should cover all such incidents. The scope of this research, however, is limited to examining IS security strategies intended to address intentional, malicious cyber offenses. The scope is inclusive of:

- human threats internal and external to the organization,
- all offender motivations—play, crime, individual rights, national security (Denning, 1998),
- all offender skill levels, from novice to elite,
- all criminal involvement classifications—anti-social predator, mundane offender, provoked (Cornish and Clarke, 2003),
- all attack goals—interruption, interception, modification, and fabrication (Jung et al., 2001), and
- attacks that attempt to victimize an organization and/or exploit data/information.

Sample

This paper discusses the pilot study sample only. The pilot study consisted of nine face-to-face interviews comprising ten organizations and their respective information security strategies. (One respondent's knowledge and experience was deemed adequate to obtain responses relative to two organizations.) All interviews were approximately 45-60 minutes in duration.

Sample Demographics

All respondents were senior-level personnel in key information security positions. Example titles include: general manager, vice president, assistant director, director, senior manager, etc. Respondents were managers/directors of IS security for their organization, respecting large organizations. Respondents were general managers, vice presidents, etc., respecting small organizations (those that do not have dedicated IS security personnel). The average information security experience was 12.4 years. The average age was 40.7 years. All were college graduates; five had advanced collegiate degrees (masters or Ph.D. degrees). Two-thirds held professional certifications in information security.

ID	Industry Type	Organization Size
1	Government – Federal (Military)	Very Large (>30,000)
2	Services – Info Technology	Small (6)
3	Services – Info Technology	Small (2)
4	Education – Collegiate	Very Large (>30,000)
5	Financial & Manufacturing	Large (5,800)
6	Government – Federal (Military)	Small (80)
7	Government – Federal (Military)	Large (7,000)
8	Education – K-12	Large (3,000)
9	Healthcare	Medium (300)
10	Government– State (Dept of Revenue)	Large (4,000)

Table 2. Sample – Organization Demographics

DISCUSSION

Results

Employment of Preventive Strategies

All four government organizations, representing both state and federal levels of government, reported a balanced implementation regarding technical, formal, and informal controls (IDs: 1,6,7,10). The two smallest organizations (less than ten employees), show a continued, sole reliance on technical controls (IDs: 2,3). The remaining organizations (IDs: 4,5,8,9) indicate they implement some degree of all three types of controls, but they vary with regard to their emphasis and balance. The university (ID: 4) prioritized technical controls over formal controls and formal controls over informal controls. The other educational organization (a K-12 independent school district) (ID: 8) also prioritized technical controls over formal and informal controls, but reported a balanced, low emphasis on formal and informal controls. The financial & manufacturing firm (ID: 5) prioritized formal controls over technical controls, and technical controls over informal controls. Lastly, the healthcare organization (ID: 9) prioritized informal controls over formal controls and formal controls over technical controls.

The prevailing trend across all organizations was *prevention.* This is possibly related to another prevailing trend across all organizations—a generally reactive approach to countermeasure identification and implementation. All organizations indicated a desire to be more proactive, but stated they have historically been and continue to be reactive. They reported that their resources are fully employed with identifying and implementing appropriate safeguards to the latest threats. The underlying purpose of controls is important to examine, because it cannot necessarily be presumed. The same control may hold a preventative and/or deterrent purpose, strategically speaking.

Employment of Deterrent Strategies

According to respondents, all of the organizations represented definitely prioritize controls-based strategies over General Deterrence based strategies. Organizations with IDs 1, 2, 3, 5, and 8 report absolutely no strategic focus on General Deterrence Theory and no security countermeasures that would possibly have a GDT-based deterrent effect on potential offenders. Organizations with IDs 4 and 10 report a limited, but thus far unsuccessful strategic focus on GDT-based security countermeasures. In other words, they have a stated intent of deterring cyber offenses through GDT-based countermeasures, but the respondents do not feel such countermeasures have had any appreciable deterrent effect to date. When asked why, both respondents felt it was due to the lack of formality and lack of intensity with which GDT-based countermeasures are communicated to would-be offenders. In other words, for a potential offender to be deterred by the threat (severity, certainty, and celerity) of punishment, they must be made aware of potential consequences and believe they are likely to occur. Both respondents felt their organization did not do enough to communicate the potential consequences. Finally, organizations with IDs 6, 7, and 9 appear to have successfully implemented a GDT-based strategy, but the role it plays in their overarching IS security strategy is very small. They expect relatively little benefit from such countermeasures, but have realized such benefit to date.

An interesting observation is that the organizations with a reportedly disgruntled user-base respecting computer security countermeasures (IDs 1, 7, 8, and 9) did not mirror the organizations who viewed deterrence as an important strategy. Organization with IDs 1 and 8 did not include deterrence in their strategy at all, and organizations with IDs 7 and 9 did, but to a very small degree. This is interesting, because GDT-based computer security countermeasures have historically been implemented specifically with 'insiders' in mind—the organization's own employees who represent an intentional computer security threat to the organization (Straub, 1987; Straub and Nance, 1990). While that threat can certainly manifest itself in the form of crimes such as financial fraud, economic espionage, etc., it often manifests itself in the form of countermeasure circumvention. Employees who fail to understand the importance of computer security and who see countermeasures as an impediment to their operational productivity will often circumvent those countermeasures. Given that, one might expect those organizations with a disgruntled user-base to view the insider as a greater threat, and therefore view GDT-based security countermeasures with greater strategic importance than is apparently the case in these organizations. One possible explanation of this contradiction is the past research that shows limited success of GDT (Kennedy, 1997, 1998; Kennedy and Braga, 1998). In other words, perhaps respondent organizations wish to deter potential offenders, insiders in particular, but perhaps they do not believe GDT is the best way, due to its lack of success. (This is merely a postulated explanation; it was not examined during the interviews.)

IS Security Effectiveness – Self-Evaluation

Respondents were asked to qualify their perception regarding the effectiveness of strategies implemented in their organization. They were asked how effective they believe their organization is in *preventing* and *deterring* cyber offenses. Five out of nine respondents, reflecting six out of ten organizations, perceived their preventive strategies as being very good. Three said they were very effective across the board, while three said they were very good with preventing successful attacks against critical targets. In other words, they viewed their strategy as highly effective from a risk management point of view. Three of the remaining four organizations evaluated their preventive strategies as being "pretty effective." They said there was room for improvement, but that their prevention strategy was generally working. Only one organization (ID #9) reported their organization's preventive effectiveness negatively, and this was reported by an individual who was recently hired specifically to "fix" the organization's poor information security posture.

When asked to qualify their perception regarding the effectiveness of their deterrent strategies (in those cases where such strategy was reported), three out of five said they were very ineffective. The remaining two out of five said they were relatively ineffective. What is interesting to note, is the two who reported relative ineffectiveness (IDs #4 and 10), were the two organizations who reported an as of yet ineffective strategy. This contrasts with the other three organizations who reported their deterrent strategy was very ineffective, yet reported their deterrent strategy was a small focus of their overall strategy, but relatively successful at what little it was expected to deter.

Cyber Offender Decision Making Influences

Respondents were asked what they thought factored into cyber offenders' event decisions – the specific decision to commit a specific crime, in a certain way, against a single target, at a given time. This research does not purport that information security professionals' perceptions can be used as a proxy for cyber offender decision making, but given the exploratory nature of this research, respondents were asked their professional opinion about what influences a cyber criminal to offend in a specific instance. Overwhelmingly, "anticipated benefit" was the primary decision influence, followed by "perceived amount of effort required." The amount of "perceived risk of being caught" was the third greatest influence. Recalling the five classes of opportunity reducing SCP techniques, this leaves "rationalization and justification, AKA removing excuses" and "provocations." Clearly the first three (effort, risk, and benefit) are the core of SCP's underlying rational choice perspective—that offenders weigh the pro's and con's and choose to commit the offense if the benefits outweigh the amount of effort required and risk of being caught. The remaining two classes of techniques (rationalization/justification and provocation) were not deemed influential to offender event decision making at all by three of the respondents. In five of the remaining organizations, respondents viewed the offender's ability to rationalize/justify their crime to be more influential than being provoked. In the final two organizations, respondents viewed the offender's sense of provocation to be more influential than their ability rationalize/justify their crime. Respondents reported very little was being done, if anything at all, in their organization to affect potential offenders' perception of the costs, benefit, and justification, as well as their sense of being provoked. Some respondents reported their informal controls reduce excuses for insiders.

Contributions

Though largely descriptive in nature, this study provides insight into what is *actually* happening in real-world organizations with respect to IS security strategy. While this paper itself only presents the results of a small number of organizations (10), we took care to ensure we got a mix of industry representation and variation in organizational size. We know of no theory, nor did we observe any indications, which would suggest that the interviews with more companies will result in drastically different observations. We believe the results of this pilot study yield knowledge and answers to the research questions posed.

This paper's contribution is not entirely descriptive. There is an important exploratory component to the interviews. Before engaging in decidedly difficult research efforts to empirically test the effectiveness of SCP-based cyber security strategies, we feel it is important to see if organizations even see room for improvement at the strategic level. We also want to gain confidence in the value of the theoretical extension by asking information security professionals what they think would influence cyber offender decision-making. Such insight will help us test rival theories and may help explain the resultant observations.

Limitations

The primary limitation of the current study is the small sample size, which limits generalizability. With only ten responses, the results represent a good starting point. Further research with a larger number of responses is needed to generate more robust results. A second concern may be that there is only a single respondent from each organization. We do not view this as a serious limitation. The respondent from each organization was in a key position, with full knowledge of all aspects of security-related decisions in the organization, including its information security strategy(ies).

A third limitation of this study is the assumption that offenders are rational decision makers, since SCP is based on the rational choice perspective. The many successful implementations of SCP in the physical realm suggest offenders are indeed rational decision makers. Certainly, their rationality is bounded, but as long as offenders are relatively homogeneous in their bounded perceptions of the costs and benefits in a given type of situation, manipulations can be engineered accordingly. It is reasonable to expect that cyber criminals will exhibit similar behavioral characteristics, but that remains to be demonstrated. If offenders are not rational decision makers, SCP will be an inappropriate basis for analyzing cyber crime.

CONCLUSION

This pilot study suggests that while the balance of technical, formal, and informal controls does appear to be improving, technical controls are still the priority—particularly in small organizations. The study suggests that IS security strategies are still predominantly preventive in nature; organizations do not view deterrence as a strategy, per se. The respondents interviewed definitely see room for improvement regarding their IS security strategies. By and large, the information security professionals interviewed believe that cyber offenders are rational decision makers, that reducing anticipated benefit would be the most lucrative influence, followed by perceived effort required and perceived risk of being caught, in that order.

REFERENCES

1. Choobineh, J., Dhillon, G., Grimaila, M. R. and Rees, J. (2007) Management of Information Security: Challenges and Research Directions, *Communications of the Association for Information Systems*, 20, 2007, 958-971.

2. Clarke, R. V. (1980) 'Situational' Crime Prevention: Theory and Practice, *British Journal of Criminology*, 20, 2, 135-147.

3. Denning, D. (1998) Information Warfare & Security, Addison-Wesley, Reading.

4. Dhillon, G. (1999) Managing and Controlling Computer Misuse, *Information Management & Computer Security*, 7, 4, 171.

5. Dhillon, G. and Backhouse, J. (2001) Current Directions in IS Security Research: Towards Socio-Organizational Perspectives, *Information Systems Journal*, 11,

6. Dhillon, G. and Moores, S. (2001) Computer Crimes: Theorizing About the Enemy Within, *Computers & Security*, 20, 8, 715-723.

7. Dhillon, G., Silva, L. and Backhouse, J. (2004) Computer Crime at CEFORMA: A Case Study, *International Journal of Information Management*, 24, 2004, 551-561.

8. Jung, B., Han, I. and Lee, S. (2001) Security Threats to Internet: A Korean Multi-Industry Investigation, *Information & Management*, 38, 8, 487-498.

9. Kankanhalli, A., Teo, H.-H., Tan, B. C. Y. and Wei, K.-K. (2003) An Integrative Study of Information Systems Security Effectiveness, *International Journal of Information Management*, 23, 2, 139-154.

10. Kennedy, D. M. (1997) Pulling Levers: Chronic Offenders, High-Crime Settings, and a Theory of Prevention, *Valparaiso University Law Review*, 31, 449-484.

11. Kennedy, D. M. and Braga, A. A. (1998) Homicide in Minneapolis, *Homicide Studies*, 2, 3, 263-290.

12. Lee, J. and Lee, Y. (2002) A Holistic Model of Computer Abuse within Organizations, *Information Management & Computer Security*, 10, 2/3, 7.

13. Lee, S. M., Lee, S.-G. and Yoo, S. (2004) An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories, *Information & Management*, 41, 12.

14. Straub, D. W., Jr. (Year) Controlling Computer Abuse: An Empirical Study of Effective Security Countermeasures, in (Eds.), *Eighth Annual International Conference on Information Security*, Pittsburgh, PA, 277-289.

15. Straub, D. W., Jr. (1990) Effective IS Security: An Empirical Study, *Information Systems Research*, 1, 3, 255-276.

16. Straub, D. W. and Nance, W. D. (1990) Discovering and Disciplining Computer Abuse in Organizations--A Field Study, *MIS Quarterly*, 1990, March, 45-60.

17. Willison, R. (2000) Understanding and Addressing Criminal Opportunity: The Application of Situational Crime Prevention to IS Security, *Journal of Financial Crime*, 7, 3, 201-210.

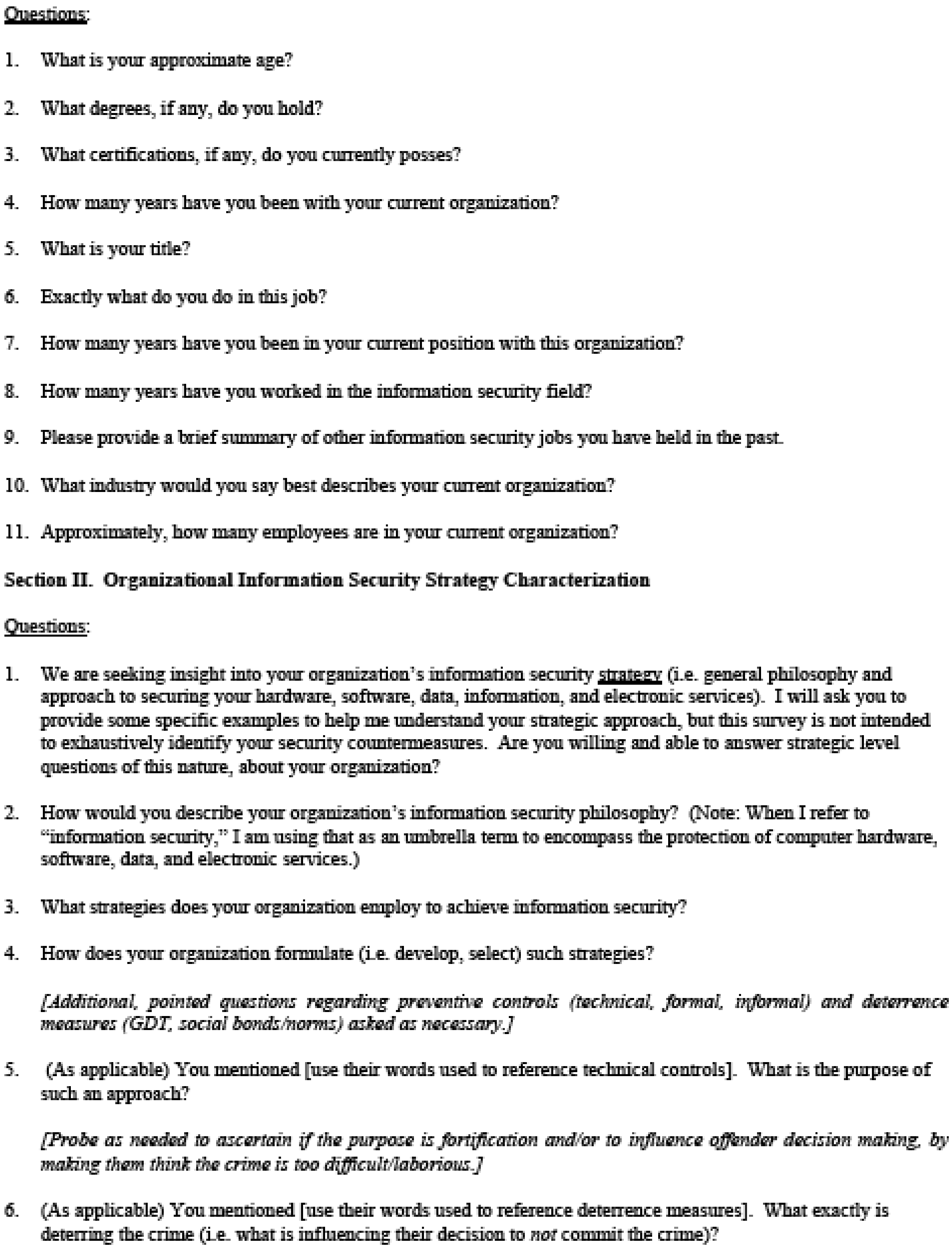
18. Willison, R. (2006a) Understanding the Offender/Context Dynamic for Computer Crimes, *Information Technology and People*, 19, 2, 170-186.

19. Willison, R. (2006b) Understanding the Perpetuation of Employee Computer Crime in the Organizational Context, *Information and Organization*, 16, 4, 304-324.

20. Willison, R. and Backhouse, J. (2006) Opportunities for Computer Crime: Considering Systems Risk from a Criminological Perspective, *European Journal of Information Systems*, 15, 4, 403-414.

21. Wortley, R. (2001) A Classification of Techniques for Controlling Situational Precipitators of Crime, *Security Journal*, 14, 63-82.

APPENDIX A – SEMI-STRUCTURED, OPEN-ENDED SURVEY INSTRUMENT



<u>Questions</u>:

1. What is your approximate age?
2. What degrees, if any, do you hold?
3. What certifications, if any, do you currently posses?
4. How many years have you been with your current organization?
5. What is your title?
6. Exactly what do you do in this job?
7. How many years have you been in your current position with this organization?
8. How many years have you worked in the information security field?
9. Please provide a brief summary of other information security jobs you have held in the past.
10. What industry would you say best describes your current organization?
11. Approximately, how many employees are in your current organization?

Section II. Organizational Information Security Strategy Characterization

<u>Questions</u>:

1. We are seeking insight into your organization's information security <u>strategy</u> (i.e. general philosophy and approach to securing your hardware, software, data, information, and electronic services). I will ask you to provide some specific examples to help me understand your strategic approach, but this survey is not intended to exhaustively identify your security countermeasures. Are you willing and able to answer strategic level questions of this nature, about your organization?

2. How would you describe your organization's information security philosophy? (Note: When I refer to "information security," I am using that as an umbrella term to encompass the protection of computer hardware, software, data, and electronic services.)

3. What strategies does your organization employ to achieve information security?

4. How does your organization formulate (i.e. develop, select) such strategies?

   [Additional, pointed questions regarding preventive controls (technical, formal, informal) and deterrence measures (GDT, social bonds/norms) asked as necessary.]

5. (As applicable) You mentioned [use their words used to reference technical controls]. What is the purpose of such an approach?

   [Probe as needed to ascertain if the purpose is fortification and/or to influence offender decision making, by making them think the crime is too difficult/laborious.]

6. (As applicable) You mentioned [use their words used to reference deterrence measures]. What exactly is deterring the crime (i.e. what is influencing their decision to *not* commit the crime)?

7. (As applicable) What type of person/people do you believe this is meant to deter (i.e. influence their decision to *not* commit the crime)?

   [Probe further as needed, asking respondent if they think such measures are directed toward any/all individuals varying along the following dimensions: offender motivation, offender skill level, insider/outsider, commitment to criminality, attack goal, target type.]

8. To summarize, please correct me if I have erred, your organization employs the following strategic approaches to secure information assets: [list strategic approaches identified by respondent]. Can you help me understand how these approaches are prioritized? Are they all of equal importance, or are some considered more important than others? Please explain.

Section III. Perception of Organization's Information Security Effectiveness

Questions:

1. How effective is your organization's information security strategy in deterring offenders (dissuading them from committing the crime)?

2. How effective is your organization's information security strategy in preventing computer crimes (keeping offenders from being able to successfully commit the crime)?

Section IV. Suggestions for Strategic Improvements

Question:

1. What strategic changes would you suggest and/or make to your organization's information security strategy to improve your organization's ability to protect hardware, software, data, and/or computer services?

Section V. Feedback Regarding Extension of SCP to Computer Crime Realm

Questions:

1. How do you believe computer criminals arrive at a decision to commit a specific crime (i.e. specific target, specific action, specific time)? What do you believe influences that decision?

2. To what extent do you believe computer criminals consider the ***amount of effort required*** to commit a specific crime?

3. To what extent do you believe their perception influences their decision whether or not to commit a specific crime?

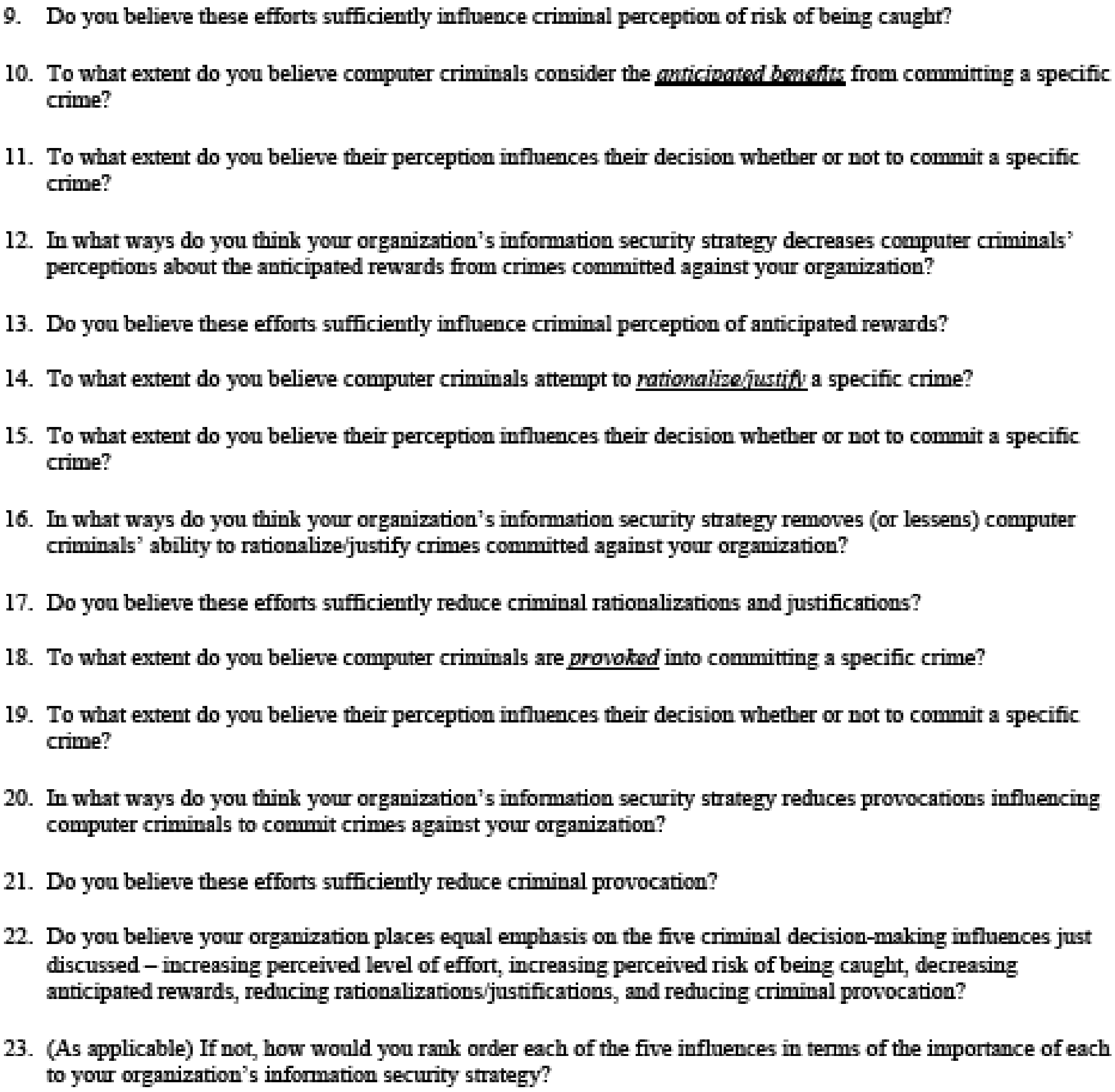
4. In what ways do you think your organization's information security strategy increases computer criminals' perceptions about the amount of effort required to commit crimes against your organization?

5. Do you believe these efforts sufficiently influence criminal perception of level of effort required?

6. To what extent do you believe computer criminals consider the *risk of being caught* committing a specific crime?

7. To what extent do you believe their perception influences their decision whether or not to commit a specific crime?

8. In what ways do you think your organization's information security strategy increases computer criminals' perceptions about the risk of being caught when committing crimes against your organization?



9. Do you believe these efforts sufficiently influence criminal perception of risk of being caught?

10. To what extent do you believe computer criminals consider the *anticipated benefits* from committing a specific crime?

11. To what extent do you believe their perception influences their decision whether or not to commit a specific crime?

12. In what ways do you think your organization's information security strategy decreases computer criminals' perceptions about the anticipated rewards from crimes committed against your organization?

13. Do you believe these efforts sufficiently influence criminal perception of anticipated rewards?

14. To what extent do you believe computer criminals attempt to *rationalize/justify* a specific crime?

15. To what extent do you believe their perception influences their decision whether or not to commit a specific crime?

16. In what ways do you think your organization's information security strategy removes (or lessens) computer criminals' ability to rationalize/justify crimes committed against your organization?

17. Do you believe these efforts sufficiently reduce criminal rationalizations and justifications?

18. To what extent do you believe computer criminals are *provoked* into committing a specific crime?

19. To what extent do you believe their perception influences their decision whether or not to commit a specific crime?

20. In what ways do you think your organization's information security strategy reduces provocations influencing computer criminals to commit crimes against your organization?

21. Do you believe these efforts sufficiently reduce criminal provocation?

22. Do you believe your organization places equal emphasis on the five criminal decision-making influences just discussed – increasing perceived level of effort, increasing perceived risk of being caught, decreasing anticipated rewards, reducing rationalizations/justifications, and reducing criminal provocation?

23. (As applicable) If not, how would you rank order each of the five influences in terms of the importance of each to your organization's information security strategy?