Using Situational Crime Prevention Theory to Explain the Effectiveness of Information Systems Security

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

Information is an intangible organizational asset of enormous value in the information age. Information systems (IS) security technologies play an important role in protecting that information from unauthorized disclosure, modification, and use. As such, the factors that influence the effectiveness of IS security strategies need to be understood. The existing theory base for studying IS security effectiveness is limited to three major perspectives since the mid-1980s: Straub's extension of general deterrence theory (1987, 1990); an argument for balanced technical, formal, and informal controls by Dhillon and colleagues (1999, 2001, 2004); and various hacker motivation taxonomies developed during the 1980's and 1990's. Our goal is to expand the range of the theoretical lens that can be used to understand IS security effectiveness. Towards this goal, we examine the appropriateness of extending situational crime prevention theory, a theory developed in the criminal justice domain to address physical crime, to the digital realm. Our conceptual analysis suggests that situational crime prevention theory may offer new insights into improving IS security effectiveness by reducing the criminal's anticipated rewards from the crime.

Keywords: *security, information security, electronic crime, computer crime, situational crime prevention theory*

I. Introduction

In today's hypercompetitive business environment, information is perhaps the most valuable asset that a business can possess (Hurd and Nyberg, 2004). The ability to store information in computers facilitates easy access and sharing by users, thus leveraging the value of the information. This stored information and, in some cases, stored knowledge (Nunamaker, et al., 2001), is susceptible to theft, alteration, and misuse. Organizations have to guard against these illegal or unethical activities, which may be perpetrated through electronic or other means. Our larger research goal is to develop a deeper theoretical understanding of electronic crime, i.e., crime committed through electronic and digital means. The current article focuses on one theoretical perspective—situational

crime prevention theory—to better understand what influences electronic crime targeting organizational information assets.

Electronic crime, whether perpetrated by an external hacker or an "insider" (trusted agent of the organization), is a significant threat to stored information, as evidenced by CSI/FBI Computer Crime and Security Survey results over the past decade. The average financial loss per incident has increased in 2005 with respect to both unauthorized access to information (588% increase since 2004; current average loss per incident of $303,234) and theft of proprietary information (211% increase since 2004; current average loss per incident of $355,552) (Gordon, et al., 2005). After computer viruses, unauthorized access to information and theft of proprietary information account for the highest percentages of all financial losses associated with computer crime and security incidents (combined 47.7% of all financial losses) (Gordon, et al., 2005). With each incident of computer crime targeting information valued at over $300K, it is vital that we better understand what affects the effectiveness of information systems (IS) security. Such an understanding will facilitate the conceptualization and design of improved strategies to protect organizational information resources.

Failures of IS security frequently involve criminal activity. Hence, the field of criminal justice, with its rich theoretical environment, is an appropriate reference discipline for the conduct of research in IS security. Historically, criminal justice has gone through three phases in developing theoretical perspectives about crime prevention. The first phase focused on the criminal, with the effort being on understanding the sociological and biological influences of criminal behavior. In the second phase, criminal justice theorists began to explore ways to remove the "suitable target" and/or increase "guardians" (Jeffery, 1971, Newman, 1972). Such purely environmental and protection oriented theories (i.e. opportunity theories), however, did not gain prominence. In the third phase, integrated theories emerged that combined criminal-centered, behavioral theories with crime-centered, situation focused theories. Situational crime prevention theory (Clarke, 1980, 1997) is one such integrated theory. The criminal focused component is consistent with rational choice theory and argues that a potential criminal's decision to commit a crime is a function of the perceived net benefits associated with the crime, moderated by the presence or absence of various behavioral rationalizations[1]. In situational crime prevention theory, situational factors constitute a direct barrier to the commission of the crime (i.e. reduce opportunity), but more importantly they influence the criminal's perception of costs and benefits, thereby influencing his/her behavior. In sum, situational crime prevention theory takes a holistic approach by using crime-centered, situational approaches to influence a criminal's rational choice and subsequent behavior.

Turning to IS security research, we see three explanations of computer crime that have emerged since the mid-1980s. The first is Straub's extension of general deterrence theory, wherein he found empirical support for the argument that potential offenders will be

[1] The idea of rationalizations as a moderator is based on Sykes and Matza's techniques of neutralization and drift theory (1957), which states that individuals can hold "subterranean values" that contradict cultural norms and provide the individual justification for committing a crime if certain conditions exist that apply to the deviant "subterranean values."

deterred by the certainty[2] and severity of punishment (Straub, 1987, 1990). Straub's theory suggests that IS security is influenced by the potential offender's perception of the net benefits associated with committing the crime. The next major explanation of computer crime offered explored the motivation of computer criminals. Several motivational taxonomies emerged that considered computer criminals' attitudes and intentions regarding electronic crime (Landreth, 1985, Hollinger, 1988, Chantler, 1996, Denning, 1998, Smith and Rupp, 2002). Finally, Dhillon and colleagues explained IS security effectiveness as a function of the balanced implementation of technical, formal, and informal controls (Dhillon, 1999, Dhillon and Moores, 2001, Dhillon, et al., 2004). Such controls serve to minimize opportunity and constrain a potential criminal's behavior via various technological and sociological influences. Straub's extension of deterrence theory, various hacker motivation taxonomies, and the informal controls portion of Dhillon's theory are all criminal-centered approaches. There are some references to the crime-centered perspective in the technical and formal controls portions of Dhillon's writings, but it would be fair to say that IS security research to date has been mostly criminal-focused.

The purpose of this paper is to extend[3] (Berthon, et al., 2002) Clarke's situational crime prevention theory to the IS domain to explain the effectiveness of IS security, as recommended by Willison (2000, 2005). Clarke's model (1997) argues that the incidence of crime is a function of the perceived costs, perceived benefits, and degree of rationalization. To increase perceived costs, one must: (1) increase the perceived effort associated with committing the crime, and (2) increase the perceived risk (probability) of being caught[4]. To reduce perceived benefits, one must decrease the criminal's anticipated, or expected rewards associated with committing the crime. Together, the perceived costs and benefits result in the criminal's perceived net benefit, which affects the likelihood of a criminal act. The relationship between net benefit and the likelihood of a criminal act is moderated by the perpetrator's ability to rationalize or neutralize the criminal behavior. The pivotal point of situational crime prevention theory is that the criminal's pseudo-rational[5] decision is a function of the perceived *net* benefits. If crime prevention measures do not adequately increase perceived costs *and* decreased perceived benefits, rational choice theory argues that the crime will still occur. We argue that the effectiveness of IS security is a function of such a balance between situational factors that increase the criminal's perceived cost and those that decrease the criminal's perceived benefit. Doing so, we argue, will adequately lower the criminal's perceived *net* benefit, thereby deterring them from committing the crime.

---

[2] Straub's operationalization of the punishment certainty construct regards it as the certainty of being caught, as opposed to the certainty of punishment once caught.

[3] We consider this a theoretical extension, as theory is being applied in a discipline different from the one in which it was developed. Additionally, the dependent variable changes slightly from the original theory.

[4] Interestingly, this is solely the perceived risk that the criminal will be caught. The theory argues that the certainty, severity, and celerity of punishment as defined by General Deterrence Theory is actually irrelevant in the mind of the criminal; such considerations do not significantly affect the criminal's perception of cost.

[5] Rational Choice Theory in a criminal justice context has been shown to be pseudo-rational in the sense that the decision is rational given the criminal's perception of reality, but that the decision may not be objectively rational (Akers, 1994).

This extension of situational crime prevention theory to the IS domain differs from Willison's previous extensions (2000, 2005). Situational crime prevention theory effectively integrates opportunity theory with rational choice theory. In doing so, Clarke found it useful to develop an opportunity structure—a model that serves as a framework to explain opportunity theory in the criminal context (Clarke, 1997). Willison's extension of situational crime prevention theory has predominantly focused on the reformulation of Clarke's opportunity structure in the IS security context. Our work differs from, yet complements Willison's work, by focusing instead on the rational choice portion of situational crime prevention theory. In doing so, it considers opportunity theory as supportive and influential to rational choice considerations.

The structure of the rest of the paper is as follows. We begin by providing a brief overview of criminological theory to help ground the reader's understanding of situational crime prevention theory. Next we explore the existing literature on theoretical explanations for IS security effectiveness. With the requisite background, we propose a theoretical model for explaining the variance in IS security effectiveness. Finally, we conclude with a discussion of the model's contribution to the IS domain, an anecdotal analysis of current IS security strategies relative to the proposed model, implementation recommendations, and limitations.

II. Literature Review

Criminological Theory

In studying crime and crime prevention, researchers can examine the crime itself, or alternatively, the criminal committing the crime. Criminologists have largely focused on the latter. It has only been in recent years that criminologists have begun to dedicate any appreciable resources to crime-focused research (Akers, 1994, Clarke, 1997).

Criminal Focused Research

Criminologists focusing on the criminal are primarily concerned with the sociological and biological factors that cause, or are correlated with a person becoming a criminal and engaging in criminal activity. There are several sociological theories that address why some individuals become criminals[6], while others don't: social learning theory (Burgess and Akers, 1966), social bonding theory (Hirschi, 1969), and rational choice theory. Social learning theory posits that crime increases when the would-be criminal socializes with and identifies with others engaged in criminal behavior. The theory suggests that the would-be criminal learns criminality from the criminal, because he/she wants to be like and/or imitate the criminal. The criminal tends to reinforce the would-be criminal's inclination to engage in criminal activity, which is further facilitated when the would-be criminal's attitudes and beliefs are consistent with deviant behavior. In other words, the

[6] Discussion of biological factors—why criminals may be "born criminals"—is beyond the scope of this paper.

would-be criminal learns crime facilitating morals and values while being raised, and then learns deviant behavior from the criminal(s) he/she associates with. In essence, a person becomes a criminal due to sociological influences wherein he/she learns to be a criminal.

In contrast, Hirschi's social bonding theory (1969) focuses on the influences that prevent an individual from engaging in criminal activities. The theory outlines four dimensions of an individual's bond with society that, if strong enough, will prevent him/her from committing crime, even in the face of need and/or opportunity. The four dimensions include: attachment, commitment, involvement, and beliefs. Attachment refers to ties of affection with others, wherein a person admires others and cares about what they think about them. Commitment occurs when an individual has a vested interest in conforming to a socially acceptable group. In other words, a person is motivated to behave conventionally, because to do otherwise would jeopardize their standing with the group (i.e. could get them ostracized, fired, etc.). Involvement refers to the degree to which a person is involved with conventional, socially acceptable activities. The person becomes preoccupied with those activities and is disinclined to do other, less socially acceptable things. Finally, one's beliefs with respect to the "rightness," or correctness of social norms and laws influences behavior. If one believes society is in fact right about what is good behavior vs. what is deviant behavior, he/she will be inclined to follow social norms and laws. Social bonding theory explains an individual's disinclination to commit crime based on their levels of attachment, commitment, and involvement, as well their beliefs.

Rational choice theory argues that people make a basic decision to commit a crime, or to not commit a crime, based on a simple cost-benefit analysis with respect to committing the crime. Simply put, if the perceived benefits from committing the crime outweigh the costs, both examined probabilistically, then one will decide to commit the crime. The interesting thing about rational choice theory, however, is that research has shown that while choices are rational with respect to the decision maker's perception of reality, they are seldom objectively rational (Akers, 1994). Criminals often overestimate the benefits and/or the probability of reaping the benefits and underestimate the costs and/or the probability of experiencing the costs (Akers, 1994).

Crime Focused Research

In the context of rational choice theory, it is reasonable to assume that some non-sociological factors influence the would-be criminal's perception of costs and benefits. For example, if a criminal is considering robbing a gas station attendant, his/her perception of the costs and benefits would change if there were noticeable surveillance cameras inside and outside the store, or if a sign was posted that stated the gas station attendant maintains less than $100 in cash in the register at any time. The presence of the surveillance cameras and cash-on-hand sign are non-sociological, situational factors that affect the person's rational decision making process. Rational choice theory states that these mechanisms have a deterrent value, because they reduce the overall perceived net benefit. In this example, the surveillance cameras increase the perceived risk of being caught, and the cash-on-hand sign reduces the perceived benefit from the theft (smaller

"take" in this case). In short, the criminal's perception of the situation has changed, because of situational, not sociological factors. This change in perception resulting from situational factors lowers the likelihood of the crime being committed. This rationale underlies the emergence of the situational crime prevention theory.

Situational crime prevention theory was introduced first by Ronald V. Clarke in 1980. It became popular in both European academic circles and in practice by the mid-1990's, but has gained prominence in the U.S. only recently. The impetus for a situational crime prevention theory perspective was the belief that a full understanding of and control over sociological factors is simply unattainable, i.e., a sociologically utopian view of crime prevention is unrealistic. Proponents of situational crime prevention theory argue that it is necessary to forestall the crime from occurring in the first place, as opposed to concerning themselves with detecting the crime or punishing the criminal after the crime has occurred. They argue that crime prevention is achieved by influencing the would-be criminal's decision making process via various environmental and protection measures, i.e. situational factors. It is important to distinguish between the implementation of environmental and protection measures intended to affect crime conduct ability, versus those intended to affect crime conduct motivation. Certainly, there is some duality involved here, but the intent of situational factor implementation, according to situational crime prevention theory, is to affect crime conduct motivation. In doing so, results in an integrated theory considering both the crime and the criminal.

Information Systems Security Effectiveness Theory

While criminological theory in the physical realm enjoys a rich history with diverse contributions and clear Kuhnian paradigm development and shifts, explanatory research with respect to electronic crime and information security success remains relatively undeveloped. Only a few theoretical explanations for IS security effectiveness have emerged in the last two decades: Straub's extension of general deterrence theory (Straub, 1987, 1990), Dhillon's theory of balanced control implementation (Dhillon, 1999, Dhillon and Moores, 2001, Dhillon, et al., 2004), and various motivational taxonomies for hackers and crackers.

General Deterrence Paradigm

In perhaps the earliest research on the effectiveness of information systems security, Straub adapts general deterrence theory and posits that severity of punishment, and to a lesser extent certainty of being caught, influence the incidence (frequency and severity) of electronic crime (Straub, 1987, 1990). In testing his computer abuse deterrence hypothesis, he also tests rival theories, including the impact of preventative, "target hardening" type measures, as well as various sociological factors, such as offender motivation and environmental factors. Straub concluded his empirical findings support the extension of general deterrence theory in explaining electronic crime.

Closer examination of Straub's study reveals his findings are most applicable to "insiders." His survey respondents were effectively IS professionals, and his primary

severity measure asked respondents what types of disciplinary actions are reflected in their company's acceptable use policy. As a result, the generalizability of his finding that punishment severity has a deterrent value is limited to employees engaged in electronic crime. Additionally, current standards for goodness of fit tests suggest that further research is warranted with respect to the general deterrence model for insiders[7].

Balanced Control Implementation Paradigm

Dhillon's balanced control implementation paradigm also focuses on the "insider." Dhillon and colleagues argue for the implementation of balanced technical, formal, and informal control strategies to curb computer crime and abuse by employees (Dhillon, 1999, Dhillon and Moores, 2001, Dhillon, et al., 2004). Although not presented as such, Dhillon's theory is a loose extension of criminological containment theory (Reckless, et al., 1956, Reckless, 1961, 1967). Containment theory adapts social bonding and control theory by suggesting that people are prevented from committing crimes because of various "outer containment" and "inner containment" conditions. Outer containment conditions include preventative measures and supervision, tantamount to a reduction in crime opportunity, or an increase in the degree of difficulty of committing the crime; strong group cohesion; and consistency of morality. Inner containment conditions include a strong sense of conscience and a good "self-concept."

Dhillon argues that the incidence of "insider" computer abuse is a function of the degree to which various technical, formal, and informal controls are in place. Technical controls reduce crime commission opportunities (e.g. firewalls, password protection, and encryption). 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 structure that defines roles and responsibilities, adequate supervision, and separation of responsibilities). These technical and formal controls then mirror outer containment conditions as described by containment theory. Finally, 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). Such informal controls correspond to containment theory's inner controls. Dhillon et al. (2004) empirically illustrate the negative effects that result from an imbalanced control strategy via a case study, and posit that organizations are most likely to prioritize control strategies in the following order: technical, formal, informal.

Hacker Motivation Taxonomies

In the intervening years between Straub and Dhillon's research regarding deterrence of the "insider" threat, researchers focused on motivational taxonomies for all computer criminals. Smith and Rupp have summarized offender motivation taxonomies as follows (Smith and Rupp, 2002). Landreth (1985) categorized hacker motivation based on the hacker's goal. The categories included: *novice* (inexperienced and seeking mischief),

[7] Fit statistics were GFI=0.68, AGFI=0.597 for the general deterrent model.

student (school-aged student who seeks to learn about computers via hacking, rather than learning school directed material), *tourist* (person seeking a conquest and/or merely enjoys the sense of adventure associated with hacking), *crasher* (person with a destructive intent), and *thief* (person seeking to steal money and/or information). Hollinger (1988) subsequently categorized hacker motivation on the basis of technical ability, along with the hacking goal. The categories included: *pirate* (least technical; seeking copyrighted material), *browsers* (moderately technical; seeking unauthorized access to others' files), and *crackers* (the most technical; seeking to do serious harm). Chantler (1996) then categorized hackers as: *elites* (highly knowledgeable; motivated by achievement, excitement, challenge, and self-discovery), *neophytes* (moderately knowledgeable; apprentices of *elites*), and *losers/lamers* (least knowledgeable, but with the most destructive goals—profit, vengeance, theft, and espionage). Finally, Denning (1998) introduced a more inclusive hacker taxonomy—one that includes categories for the infrequently caught and seldom interviewed hacker. Her taxonomy distinguished between insiders and outsiders and categorized them based on their motivation: *play* (motivated based on excitement, challenge, accomplishment, knowledge, recognition, power, and friendship), *crime* (motivated to commit fraud and/or steal intellectual property), *individual rights* (often referred to as "hactivists" and are driven by a sense of privacy and free speech rights), and *national security* (actions taken by adversaries of the state for the purpose of foreign intelligence operations, military operations, terrorism, and netwars). Each of these taxonomies incorporate two overlapping dimensions: the level of expertise of the hacker, and the motivation for committing crime, and thus inherently seek to explain computer crime based on individual dimensions. None of the discussions, however, theorize ways to influence such motivation, and thereby improving information security success.

III. Proposed Theoretical Model

The proposed model extends Clarke's situational crime prevention theory to the digital realm. In doing so, we replace the traditional dependent variable (general crime rates) with IS security effectiveness. We argue that situational crime prevention theory provides explanatory insight into the success and failure of IS security strategies.

Applicability of Situational Crime Prevention Theory to the Digital Realm

Clarke's situational crime prevention theory introduces sixteen "opportunity-reducing techniques," and then classifies them into four categories that have a direct impact on the would-be criminal's decision making process (Clarke, 1997). The first category includes a set of four techniques geared toward increasing the perceived level of effort to commit the crime—a cost element. The second category includes a set of four techniques designed to increase the perceived risk of being caught[8]—another cost element. The

[8] The reader is reminded that the perceived risk of being caught is completely independent of the expected punishment. Presumably there is *some* expected punishment, however empirical studies regarding deterrence theory have shown that the certainty, severity, and celerity of the punishment are rather inconsequential to the criminal's decision making process (Akers 1994).

third category is a set of four techniques that intends to reduce the criminal's anticipated rewards—a benefit element. Finally, the last category is a set of techniques designed to remove the would-be criminal's excuse (justification, rationalization) for committing the crime.

Clarke provides examples of measures that can be implemented in the physical realm corresponding to each technique (see Table 1 on next page). To test the extensibility of the theory to the digital realm, we derived an analogous list of measures that could be implemented in the digital realm for each technique (see Table 1). The list suggests that situational crime prevention theory has potential in the study of preventing electronic crime. We acknowledge that our list is not exhaustive. Further, we acknowledge that some of the examples provided could apply to more than one category (e.g. encryption could be considered both a benefit denying mechanism, as well as a target hardening mechanism). The list is simplified and presented only to show that the situational crime prevention theory can be applied to the study of electronic crime.

Proposed Model

Figure 1 shows a more detailed picture of the extension of situational crime prevention theory to the digital realm. As a theory, it was developed for the physical realm, in which domain the ultimate dependent variable is usually considered to be crime reduction or intention to commit a crime. In this case, the ultimate dependent variable is IS security effectiveness, a construct introduced by Straub in his seminal work on the subject (1990). IS security effectiveness and crime reduction do overlap conceptually to some degree.

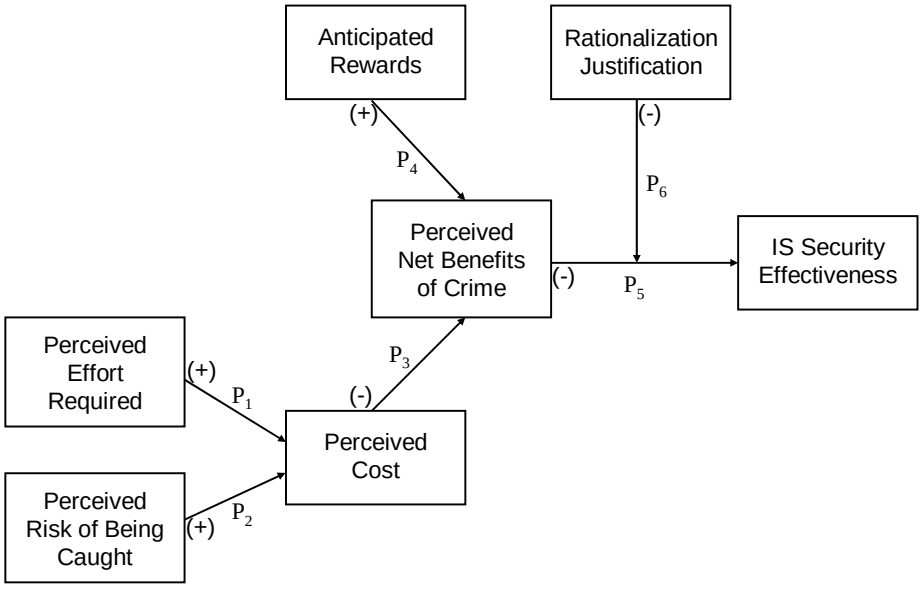

Figure 1.
Proposed Model

Table 1.
Clarke's (1997) Sixteen Opportunity-Reducing Techniques

	Opportunity-Reducing Technique	Physical Crime Analogy	Digital Crime Analogy
Increase Perceived Effort	1. Target hardening	Locks, safes, fences, barriers, armed guards	Firewalls, closed ports, vulnerability patches
	2. Access control	Gate codes, guard shack, receptionist, swipe cards	ID/authentication systems, digital certificates
	3. Deflecting offenders	Pedestrian/auto traffic redirection, no loitering	Honeypots/honeynets, information segregation
	4. Controlling facilitators	Gun control, limit ability to communicate	Masking IP addresses, leased lines, no broadcast
Increase Perceived Risk	5. Entry/exit screening	Metal detectors, screeners, merchandise tagging	Intrusion detection system, virus scanning
	6. Formal surveillance	CCTV, security guards, police patrols	Auditing & log reviews, anomaly detection
	7. Surveillance by employees	Responsibility and/or ability to monitor	Resource usage info, user training, reporting policies
	8. Natural surveillance	Lights, etc. so passers-by can see activity in building	Tamper-proof network cabling, visualization tools
Decrease Anticipated Reward	9. Target removal	Electronic donations vs. cash, cash diverted to safe	Information & hardware segregation, DMZs
	10. Identifying property	VIN etched in auto glass, write name in book	Information classification, watermarking
	11. Reducing temptation	Obscure valuables, gender neutral phone book	Minimize reconnaissance info, no port bannering
	12. Denying benefits	Security coded car radios, ink tags on clothing	Encryption, automatic data destruction mechanisms
Remove Excuses	13. Rule setting/clarification	Acceptable use policy, clear laws, licensing procedures	Acceptable use policy, user agreements, clear laws
	14. Stimulating conscience	"Shoplifting is stealing" signs, "current speed is…"	Multi-level warning banners, codes of ethics
	15. Controlling disinhibitors	Controlling drugs/alcohol, propaganda, violent TV	Cyber-ethics education, supervised computer use
	16. Facilitating compliance	"Graffiti boards," public urinals, shelters, barriers	"Hacker challenges," employment opportunities

The basic contention of the model is that IS security effectiveness is a function of the perceived *net* benefits as viewed by the would-be criminal, *and* that perceived net benefits can be influenced by resource owners and protectors via discrete environmental and managerial changes. The theory argues that such situational changes should strive to increase perceived costs, decrease anticipated rewards, and remove the would-be criminal's excuses and rationalizations. The theory emphasizes the need for balance

between increasing perceived costs and decreasing perceived benefits. An imbalance will either be positive or negative. A positive imbalance suggests benefits exceed costs, and rational choice theory then predicts crime will not be deterred. A negative imbalance will indeed deter crime, but increasing perceived costs beyond what is needed to counterbalance anticipated rewards is very likely a poor use of resources.

Extension of situational crime prevention theory to explain IS security effectiveness then leads to the following propositions:

Proposition 1. The perceived effort required to complete the criminal act is positively associated with the overall perceived cost of committing the act.

Proposition 2. The perceived risk of being caught when engaging in criminal activity is positively associated with the perceived cost of committing the act.

Proposition 3. The perceived cost of committing a criminal act is negatively associated with the perceived net benefit of the criminal act.

Proposition 4. The perceived anticipated rewards of successful crime commission is positively associated with the perceived net benefit of the act.

Proposition 5. The perceived net benefit of committing a crime is negatively associated with IS security effectiveness.

Proposition 6. The level of successful rationalization (AKA justification, neutralization) moderates the influence of perceived net benefit on IS security effectiveness.

Propositions 1 – 4 and 6 follow directly from situational crime prevention theory and, by extension, rational choice theory. Proposition 5 highlights the importance of striking a balance between decreasing anticipated rewards and increasing perceived cost.

IV. Discussion

Contribution to the Information Systems Domain

Previous theoretical explanations of IS security effectiveness have left gaps, many of which can be filled by extending situational crime prevention theory to the IS domain. The first and most obvious gap is generalizability. Both Straub's and Dhillon's theories focus on the insider, whereas situational crime prevention theory is applicable to both the insider and the external hacker. It is also generalizable to those motivated by criminal or national security interests, in accordance with Denning's taxonomy of hacker motivation.

The proposed model also solves several of the problems of the previously proposed theories. Straub's extension of general deterrence theory necessarily focused on affecting rational choice by using punishment as a deterrent. As previously stated, however, recent empirical findings in the criminal justice domain have largely invalidated punishment as an effective deterrent, suggesting that punishment does not appreciably increase perceived costs for criminal (Akers, 1994). As a result other deterrents must be explored. The proposed model suggests such alternative deterrents—increased perceived effort

required, increased perceived risk of being caught, and decreased anticipated rewards. Next, hacker motivation taxonomies leave a significant gap for IS professionals wondering what they can do to affect such motivations. Situational crime prevention theory is designed to influence offender motivation via discrete environmental and managerial, i.e., situational changes. Thus, IS professionals can apply the model and reduce the incidence of electronic crime targeting organizational information assets. Finally, Dhillon's balanced control implementation maps relatively well to the cost side of the perceived net benefits equation from rational choice theory, but pays insufficient attention to the benefits side of the equation. The proposed model addresses both influences of perceived net benefit.

We also argue that the proposed model can be applied and empirically tested at various levels of analysis, including the firm level, industry level, corporate level[9], and global level. A firm can evaluate electronic crime losses and/or attempts before and after the implementation of various cost increasing and benefit decreasing strategies, while carefully considering the balance between the two. Such evaluations can similarly be conducted at the industry level, corporate level, or global level. Studies conducted at the corporate or global level could also use longitudinal design to measure and aggregate individual perceptions of net benefit, and then correlate those perceptions to changes in overall electronic crime rates over time.

Anecdotal Analysis of Current IS Security Strategies Relative to the Model

Given the nascency of IS security in academic circles, researchers often find IS professionals outpacing them. A cursory examination of IS security strategies, however, shows that, like IS researchers, IS security professionals do not appear to see a need for balancing increased perceived costs against decreased perceived benefits. With the average financial loss per information targeted incident (unauthorized access to information or theft of proprietary information) exceeding $300K, it is evident that anticipated rewards are relatively high for such electronic crimes. Hackers are sufficiently motivated to dedicate extra resources and time to overcome increased perceived costs in order to reap anticipated benefits. If it is generally accepted that IS security effectiveness requires improvement, then the proposed model would argue that one or more of the following condition exists:

- Current IS security strategies insufficiently increase perceived costs;
- Current IS security strategies insufficiently decrease anticipated rewards; and/or
- The criminal's perceived moral intensity associated with the crime is low.

A qualitative review, conducted by the authors, of information security measures commonly implemented suggests a gross imbalance favoring strategies that increase the perceived cost and largely ignoring strategies that reduce anticipated reward[10]. Table 2 lists a wide array of technical and non-technical strategies commonly implemented by

[9] "Corporate level" in refers to all commercial organizations, all military organizations, all government, etc.
[10] While the occurrence of inter-rater disagreement is likely when mapping security strategies to SCP opportunity-reducing techniques, we argue that the overall SCP category imbalance far outweighs the probable level of disagreement on individual items.

organizations today to achieve higher levels information security. Each strategy is then mapped to the single situational crime prevention technique (recall Table 1) that captures the most common reason for implementation[11]. A simple count of the security strategies within each situational crime prevention category illustrates the imbalance:

- 58.1% of common IS security strategies increase the criminal's perceived effort;
- 20.9% increase perceived risk of being caught;
- 16.3% reduce anticipated rewards; and
- 4.7% remove the criminal's excuse for committing the crime.

This means that 79% of common information security strategies implemented today affect the perceived cost of the contemplated crime, and only 16.3% affect the perceived benefit. This has the net effect of increasing the perceived challenge of the crime, without appreciably reducing the anticipated rewards. Rational choice theory suggests the would-be criminal recognizes this imbalance, and thus, decides to commit the crime. Furthermore, it is arguable that criminals engaged in electronic crime targeting organizational information assets would be less deterred by an increased challenge, than would the average "street criminal." It then follows that decreasing anticipated rewards is even more important in an electronic crime context than a non-electronic crime one.

The cost-benefit imbalance becomes even more pronounced when one considers the frequency with which various technical and non-technical security strategies are implemented. Each security strategy (e.g. firewalls, access controls, etc.) was categorized by the authors, based on their experience, as "high frequency of use," "moderate frequency of use," or "low frequency of use" in Table 2. Table 3 then shows the recalculated percentages of cost increasing strategy implementation vs. benefit decreasing strategy implementation. The analysis reveals that 86.9% of those security strategies most frequently implemented are geared toward increasing perceived costs, while only 8.7% are geared toward decreasing anticipated rewards. Clearly, organizational information security strategies are currently directed toward increasing perceived cost, but very few are directed toward decreasing anticipated rewards. Again, increased perceived costs alone may not be sufficient to deter the criminal.

Situational crime prevention theory states that IS security strategies may be suboptimal when the balance is skewed in favor of perceived costs or anticipated rewards. The above analysis provides anecdotal evidence that such an imbalance exists in IS security programs today. It is our argument that better overall strategies can be formulated by paying equitably proportional attention to both perceived costs and perceived benefits of the criminal. Furthermore, consistent with Willison (2005), we argue that actions taken to influence the cyber criminal's perception of benefits must consider both tangible (e.g. money) and intangible (e.g. prestige/status) benefits.

[11] While multi-technique mapping is also a legitimate approach, single-technique mapping simplifies the analysis, and we argue that it generates conceptually equivalent results as multi-technique mapping.

Table 2.
Mapping of Current Information Security Strategies to SCP Opportunity-Reducing Techniques
(Note: Technique numbering references Table 1)

	Perceived Effort				Perceived Risk				Anticipated Reward				Remove Excuses			
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
Acceptable use policy‡‡													X			
Access control lists‡‡		X														
Anomaly detection‡						X										
Auditing‡‡						X										
Authentication systems‡‡		X														
Broadcast protection‡‡ [1]				X												
Digital forensics‡					X											
Employee background checks‡‡					X											
Encryption‡												X				
Firewalls‡‡	X															
Hardware design‡‡ [2]	X															
Hardware segregation‡‡ [3]			X													
Higher layer network devices‡‡ [4]	X															
Honeypots and Honeynets†			X													
Identification systems‡‡		X														
Information classification‡										X						
Information segregation‡									X							
Intrusion detection systems‡‡					X											
Intrusion prevention systems‡					X											
Layered protection (e.g. DMZ) ‡‡									X							
Leased communication lines‡				X												
Network address translation‡‡				X												
Network cable tamper proofing† [5]								X								
Network segmentation‡‡									X							
No-lone zones (phys./digital) †				X												
Physical security‡‡ [6]	X															
Port management (close, protect) ‡‡	X															
Proxy servers (for security) ‡		X														
Removable media control†				X												
"Sandboxes" (code execution) ‡‡					X											
Secure coding practices‡	X															
Security/privacy certifications‡	X															
Share protection‡‡ [7]				X												
Spam blockers‡‡	X															
TEMPEST protection†	X															
Third party digital certificates‡		X														
Tunneling & VPNs‡	X															
User digital rights management ‡‡		X														
User training‡‡				X			X						X			
Virus scanning‡‡					X	X										
Vulnerability patching‡‡	X															
Warning / log-on banners‡														X		
Watermarking†										X						
Wiping/cleansing mechanism† [8]									X							

‡‡ High frequency of implementation and use currently
‡ Moderate frequency of implementation and use currently
† Low frequency of implementation and use currently

[1] "Broadcast protection" refers to not broadcasting vital information such as wireless networking SSIDs, port/network service/protocol information (i.e. port 25 running SMTP via sendmail version 8.10), etc.
[2] "Hardware design" includes such things as "safe processors" (write disable bit to prevent buffer overflows), mitigation of covert channeling risk, etc.
[3] "Hardware segregation" refers to segregating major systems on different hardware platforms (i.e. DNS server on one hardware platform, email server on a different hardware platform, etc.)
[4] "Higher layer network devices" refers to using OSI layer 3 switches, rather than OSI layer 2 hubs, for example.
[5] "Network cable tamper proof." refers to tamper-proofing mechanisms for network cabling (Ethernet, fiber optics, etc.) that enable detection of tampering (e.g. pressurized network cable sheathing).
[6] "Physical protection" includes placing servers in locked server rooms, decreasing access to network cabling, etc.
[7] "Share protection" refers to minimizing and properly protecting network shares, file shares, etc.
[8] "Wiping/cleansing mechanisms" include data wiping utilities, degaussing tools, shredders, etc.

Table 3.
Relative Emphasis Placed on
SCP Opportunity-Reducing Techniques

	Increase Perceived Costs (Effort/Risk)	Decrease Anticipated Benefits (Reward)	Remove Excuses
HIGH FREQUENCY OF USE[1]	**86.9%**	**8.7%**	**4.3%**
MODERATE FREQUENCY OF USE	**69.3%**	**23.1%**	**7.7%**
LOW FREQUENCY OF USE	**71.4%**	**28.6%**	**0%**

[1] Security strategies included in each frequency category are identified in Table 2.

Decreasing Criminal Perception of Anticipated Benefits

A natural question then arises. If the IS domain is failing to balance decreased anticipated rewards against increased perceived costs, thereby failing to decrease perceived net benefits of electronic crime, then what do we do to decrease the perception of anticipated rewards on the part of the would-be criminal? We offer an initial framework through which such benefit decreasing strategies can be developed. There are three basic categories: *deception, assumption,* and *experience*. In the deception category, the criminal's perception of the anticipated rewards is artificially affected; that is to say that there is actually no change in anticipated rewards, but the criminal is deceived into thinking there is such a change. This deception can occur via placing deceptive claims about security strategy implementation on warning/notice banners, corporate websites, or news releases. Obviously there is some limit to such activities, due to the ethical implications of potentially misleading legitimate customers and investors. Other

deceptive techniques might include the use of decoy data/systems and the embedding of false data amongst legitimate data, allowing only legitimate users the means to distinguish between the two.

In the assumption category, the criminal assumes rewards have been reduced through various security strategies, but he/she does not actually know if rewards really have been reduced in a particular instance or not. Their assumption is based on an inference made by them in light of external information, such as wide-spread changes in the industry and security certifications. The target organization inherits assumed levels of security known to be typical among contemporaries. The organization may or may not actually be typical—this is not relevant to the criminal's perception. Fostering such assumptions can be achieved via corporate security certifications, news releases concerning industry-wide security guidelines, the development and wide-spread adoption of reward reducing technologies by industry leading security vendors, and general improvement over time in adoption levels of reward reducing security strategies. Each of these will likely influence a would-be criminal to assume their target employs certain security strategies that reduce anticipated benefits.

In the third category, experience, the criminal learns first hand that rewards have been diminished through various security measures. He/she gains unauthorized access and/or steals organizational information, but soon realizes it is of no value (i.e., it is encrypted and unbreakable for them). This category assumes the organization did, in fact, implement such reward reducing strategies. Such strategies include encryption, automatic data destruction mechanisms, separation (compartmentalization) of information, and data hiding. In this case, the criminal actually does steal the information, but finds he/she can do little with it. He/she learns "the hard way" that rewards have been reduced.

Domain of Proposed Model

The model is primarily applicable to those with criminal or national security motivations. It does not apply to individuals whose motivation is play or individual rights. This is not problematic, however, since the proposed theory is presented as an explanation for electronic crime targeting organizational information assets.

The model is applicable only to those criminals targeting the theft or alteration of data, as opposed to destruction. Many of the possible strategies designed to reduce anticipated benefits would likely diminish the criminal's usefulness of the targeted data and/or prevent his/her ability to alter it, but it is unlikely that the strategies will prevent the criminal from destroying data outright.

V. Conclusion

Information is an intangible organizational asset of enormous value to organizations. We argue that while IS security measures have vastly improved over the years, losses

exceeding $300K per incident of unauthorized access to information and theft of proprietary information are still too high. Current efforts need to be supplemented with new techniques based on fresh perspectives. We examined the usefulness of situation crime theory in gaining new insights into possible methods to fight electronic crime, as recently recommended by Willison (2005). Our analysis suggests that it may be useful to explore ways to reduce the criminal's anticipated rewards (perception of benefit) associated with the electronic crime. While the theoretical logic is reasonable, two challenges remain: What are the means to reduce perceived benefits? How do we test the effectiveness of any suggested measures to reduce the perception of high benefits? We offer our analysis as a first step in seeking innovative approaches to supplement the existing array of techniques to combat electronic crime.

References

Akers, R. L. (1994) Criminological Theories: Introduction and Evaluation, Roxbury Publishing Company: Los Angeles, 1-236.

Berthon, P., Pitt, L., Ewing, M. and Carr, C. L. (2002) Potential Research Space in MIS: A Framework for Envisioning and Evaluating Research Replication, Extension, and Generation, Information Systems Research, 13, 4, 416-427.

Burgess, R. L. and Akers, R. L. (1966) A Differential Association-Reinforcement Theory of Criminal Behavior, Social Problems, 14, 128-147.

Chantler, N. (1996) Profile of a Computer Hacker, www.infowar.com.

Clarke, R. V. (1980) Situational Crime Prevention: Theory and Practice, British Journal of Criminology, 20, 136-147.

Clarke, R. V. (1997) Situational Crime Prevention: Successful Case Studies, Harrow and Heston Publishers: Guilderland, 1-357.

Denning, D. (1998) Information Warfare & Security, Addison-Wesley: Reading, 1-522.

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

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

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

Gordon, L. A., Loeb, M. P., Lucyshyn, W. and Richardson, R. (2005) 2005 CSI/FBI Computer Crime and Security Survey, Computer Security Institute, 1-26.

Hirschi, T. (1969) Causes of Delinquency, University of California Press: Berkeley,

Hollinger, R. (1988) Computer Hackers Follow a Guttman-Like Progression, Social Sciences Review, 72, 199-200.

Hurd, M. and Nyberg, L. (2004) The Value Factor: How Global Leaders Use Information for Growth and Competitive Advantage, Bloomberg Press: Princeton, 1-130.

Jeffery, C. R. (1971) Crime Prevention Through Environmental Design, Sage: Beverly Hills,

Landreth, B. (1985) Out of the Inner Circle, Microsoft Books: Redmond, WA,

Newman, O. (1972) Defensible Space: Crime Prevention Through Urban Design, Macmillan: New York,

Nunamaker, J. F., Jr., Romano, N. C., Jr. and Briggs, R. O. (2001) A Framework for Collaboration and Knowledge Management, 34th Hawaii International Conference on System Sciences, Hawaii, 12.

Reckless, W. (1961) A New Theory of Delinquency and Crime, Federal Probation, 25, 42-46.

Reckless, W. (1967) The Crime Problem, Appleton-Century-Crofts: New York,

Reckless, W., Dinitz, S. and Murray, E. (1956) Self-Concept as an Insulator Against Delinquency, American Sociological Review, 21, 744-756.

Smith, A. D. and Rupp, W. T. (2002) Issues in Cybersecurity: Understanding the Potential Risks Associated with Hackers/Crackers, Information Management & Computer Security, 10, 4, 178-183.

Straub, D. W., Jr. (1987) Controlling Computer Abuse: An Empirical Study of Effective Security Countermeasures, Eighth Annual International Conference on Information Security, Pittsburgh, PA, 277-289.

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

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.

Willison, R. (2005) Understanding the Offender/Environment Dynamic for Computer Crimes, Working Paper No. 04-2005, Copenhagen Business School.