Communications of the Association for Information Systems

Volume 26 Article 17

3-2010

Improving Organizational Information Security Strategy via Meso-Level Application of Situational Crime Prevention to the Risk Management Process

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

V. Srinivasan Rao
The University of Texas at San Antonio

Recommended Citation
Beebe, Nicole L. and Rao, V. Srinivasan (2010) "Improving Organizational Information Security Strategy via Meso-Level Application of Situational Crime Prevention to the Risk Management Process," *Communications of the Association for Information Systems*: Vol. 26 , Article 17.
DOI: 10.17705/1CAIS.02617
Available at: https://aisel.aisnet.org/cais/vol26/iss1/17

Communications of the Association for Information Systems

CAIS

Improving Organizational Information Security Strategy via Meso-Level Application of Situational Crime Prevention to the Risk Management Process

Nicole Lang Beebe*

Information Systems and Technology Management, The University of Texas at San Antonio

Nicole.Beebe@utsa.edu

V. Srinivasan Rao

Information Systems and Technology Management, The University of Texas at San Antonio

*Author names are in alphabetical order. Both authors have contributed equally.

Abstract:

Existing approaches to formulating IS security strategy rely primarily on the risk management process and the application of baseline security standards (e.g., ISO 27002, previously ISO 17799). The use of existing approaches generally leads to measures that emphasize target hardening and incident detection. While such measures are appropriate and necessary, they do not capitalize on other measures, including those that surface when situational crime prevention (SCP) is applied to specific crimes. In particular, existing approaches do not typically surface measures designed to reduce criminal perceptions of the net benefits of the crime, or justification and provocation to commit the crime. However, the methods prescribed to-date for implementing SCP are cumbersome, requiring micro-level, individual analysis of crimes. In the current article, we propose that concepts derived from SCP can be strategically applied at an intermediate (meso) level of aggregation. We show that such meso-level application of SCP, when combined with the traditional risk management process, can reduce residual information security risk by identifying new strategies for combating computer crime. Using three illustrative cases, we demonstrate that the application of the proposed strategic approach does surface meaningful countermeasures not identified by the traditional risk management process alone.

Keywords: Situational Crime Prevention, SCP, strategic planning, IT strategy, security, risk

Volume 26, Article 17, pp. 329-358, March 2010

The manuscript was received 8/13/2008 and was with the authors 11 months for 2 revisions.

I. INTRODUCTION

Information assets in modern organizations are subject to an increasing range of threats and vulnerabilities. These threats and vulnerabilities are exacerbated by complexities that arise from system interdependencies, organizational interconnectivity, and ubiquitous digital data storage. Overall, organizations face daunting challenges in their efforts to safeguard their information assets. As such, organizations need to adopt an information security strategy to guide countermeasure identification and the optimal allocation of resources to minimize the risks from cyber threats. We define information security strategy as the pattern or plan that integrates the organization's major IS security goals, policies, and action sequences into a cohesive whole, based on Quinn et al.'s [1988] definition of strategy. We argue that a strategic approach to information security will help identify effective and cohesive countermeasures to threats and vulnerabilities, and facilitate efficient implementation of these measures. Further, the strategic approach will maximize information security, while minimizing costs. The focus of this article is to incorporate situational crime prevention (SCP) principles into the formulation of information security strategy.

Historically, *security strategy* has been used as an umbrella term to include security planning models [Straub and Welke, 1998], management of information security [Choobineh et al., 2007], and policy frameworks for information security [Rees et al., 2003]. The prevailing strategic approach to information security today is the risk management approach [Hoffman, 1989; Straub and Welke, 1998; Suh and Han, 2003; Alter and Sherer, 2004; Backhouse and Bener, 2004]. The generic risk management approach begins with the identification of assets, threats, and vulnerabilities, followed by risk assessment. Based on the risk assessment, countermeasures are considered and implemented, often with the assistance of baseline security standards (e.g., ISO 27002, FIPS, and COBIT). Recommendations for countermeasures usually include (1) target hardening via technical countermeasures, such as the use of passwords, antivirus software, firewalls, and encryption, (2) "insider" controls, such as policies and rules (e.g., Eloff and von Solms [2000]; Ma and Person [2005]), and (3) detection and investigative capabilities.

The current risk management approach artificially limits the range of countermeasures used to reduce computer crime. Traditional risk management and standards based security strategies focus on: (1) increasing the effort required by the criminal to commit a crime, and (2) increasing the risk of a criminal being identified and apprehended. Such measures are appropriate and very necessary. However, technical fortification of information assets is part of an ongoing and possibly never-ending cycle, in which criminals and information security professionals continually try to outdo the others' technologies. Furthermore, some criminals are simply not dissuaded by heavily fortified targets. Increasing risk to the criminal also has limitations, as hackers are often outside the jurisdictional reach of the appropriate authorities. In short, a need exists for information security measures beyond increasing requisite criminal effort and the likelihood of catching the criminal. We contend that organizations can bolster their information security posture by identifying additional countermeasures that influence offender decision making and proactively keep them from attempting the crime. In this article, we propose a new methodology to identify such countermeasures, based on the principles underlying Situational Crime Prevention (SCP).

SCP proceeds on the argument that criminals are rational and engage in crime to benefit themselves [Cornish and Clarke, 2006]. Based on research over several decades in the domain of non-digital crime, it has been shown that criminal motivation to engage in a specific crime is influenced by a criminal's perception of the following: (1) effort required to commit the crime, (2) risk of being caught, (3) benefit to the criminal, (4) moral justification of the crime, and (5) provocations to commit the crime. In the past decade, Willison et al. have proposed extending SCP to the information security domain [Willison, 2000; Willison, 2006b; Willison, 2006a; Willison and Backhouse, 2006; Willison and Siponen, 2009]. Because SCP is based on the rational choice perspective of the criminal, the belief is that using SCP will surface additional, new countermeasures to reduce computer crime by influencing cyber offender decision-making, rather than solely resurfacing standard countermeasures, such as fortifying targets and detecting breaches.

A major problem with extending SCP to the digital realm, from an organizational perspective, is that proponents of SCP emphasize that crime specificity is a key proposition, thereby requiring micro-level analysis [Cornish, 1994; Clarke, 1995; Wortley, 2003; Willison, 2006b; Willison and Backhouse, 2006; Willison and Siponen, 2009]. Micro-level analysis is argued, because macro-level analyses provide insufficient insight into the complexities of the offender-environment interaction needed to manipulate situational factors to prevent crime. Macro-level examination of offender-environment interaction yields high-level socio-economic structures that inform lifestyle theory, routine activities theory, and environmental criminology as explanations for criminal behavior [Clarke, 1995; Willison and

Backhouse, 2006]. On the other hand, micro-level examination of the offender-environment interaction often results in a solely procedural view of the crime. This helps illuminate very specific situational manipulations, but the approach is cumbersome. Micro-level analysis has other shortcomings, as well. First, the procedural view does not fully explain offender perception of opportunity. Second, it helps identify operational level countermeasures from the bottom-up, and does not necessarily benefit from an overarching, guiding strategy. Third, the approach is not necessarily predicated on a theoretically guided process for selecting good candidates for SCP application. As a result, organizations need a meso-level or intermediate level of analysis—a level that is not too high to manipulate situational factors effectively, nor so low that similarities between individual crimes are ignored.

In this article, we argue it is possible to relax the requirement of crime specificity and apply SCP at an intermediate (meso) level of aggregation, which makes SCP useful for formulating IS security strategy. The proposed meso-level application of SCP aggregates computer crimes according to offender characteristics and motivation. In short, understanding the criminal perspective by examining their characteristics and motivations permits an organization to select the appropriate balance of SCP's five categories: perceived effort, perceived risk, perceived benefit, perceived justification, and perceived provocation. This then facilitates the identification of new countermeasures not previously surfaced through traditional risk management and baseline security standards approaches. The meso-level application of SCP does not negate, nor prohibit the micro-level application (e.g., the script-theoretic approach), but it does provide the organization an opportunity to incorporate SCP at the strategic level of information security planning.

The rest of the article is structured as follows. In the next section, we review related research. Then, we present a framework to facilitate the use of SCP at an intermediate level of aggregation and describe the modified risk management approach to formulating IS security strategy. This is followed by three illustrative cases that implement the approach, show the expanded range of countermeasures, and demonstrate that the expansion does not add significantly to the complexity of the risk management process. Finally, we conclude with a discussion section which highlights the contributions and limitations of this research.

II. BACKGROUND AND RELATED RESEARCH

In this section, we review approaches currently used to formulate information security strategy. Again, we define information security strategy as the pattern or plan that integrates the organization's major IS security goals, policies, and action sequences into a cohesive whole (adapted from Quinn et al., 1988, definition of strategy). The strategy is the plan that results from a series of strategic, high-level decisions regarding which threats to counter and how to counter them. Strategy formulation is the process of developing the overall plan. There are two prevailing approaches to information security formulation: the risk management approach and the baseline security standards approach. We discuss both in this section. Then, we provide background on the situational crime prevention (SCP) approach to reducing crime, including a segment on its application to the area of computer crime.

Risk Management and Baseline Security Standards Approaches

There is no singularly accepted definition of the risk management (RM) approach, but in general it "is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organization's missions" [Stoneburner et al., 2002, p. 4]. The fundamental steps in the process of managing risk are shown in Table 1. Some may title the steps differently, represent them with varying degrees of granularity, or include additional steps, but the general scope and sequence remains.

The traditional risk management action sequence results in an RM-based information security strategy—a plan of action involving the implementation and periodic reevaluation of specific countermeasures designed to achieve information security goals from a risk management point of view. The organization does not presume absolute information security is attainable, nor does it consider it a desirable goal given the potentially prohibitive cost. Instead, an organization carefully considers its mission, assets, threats, and vulnerability and subsequently identifies, assesses (i.e., ranks), and mitigates risks accordingly. The decisions surrounding which risks to mitigate, to what extent, what types of countermeasures to employ, and at what cost, are strategic in nature. This collective set of decisions constitutes the strategy. The generic risk management approach does not guide the choice of specific operational level countermeasures. Professionals often turn to baseline security standards to help identify such countermeasures.

Table 1: Traditional Risk Management Process	
Steps	**Description**
1. Asset Identification and Classification	Determine what the organization needs to protect and to what extent.
2. Threat Identification and Classification	Determine who and what represent risks to those assets.
3. Vulnerability Identification and Classification	Determine the organization's weaknesses and how they relate to assets from Step 1 and threats from Step 2.
4. Risk Assessment	Quantitatively or qualitatively determine the risk of each vulnerability (considering asset value, threat probability, loss estimates, and vulnerability exposure).
5. Controls and Countermeasures Identification	Design preventative solutions (i.e. controls) to mitigate risks to the extent deemed desirable/ acceptable, considering cost (product costs, implementation costs, and maintenance costs) and operational impact.
6. Controls and Countermeasures Implementation	Put controls in place institutionally.
7. Re-evaluation	Continually examine the effectiveness of current controls and reconsider changes to mission, assets, threats, and vulnerabilities to identify appropriate changes.

Baseline security standards are generalized, codified sets of best practices, recommended controls, and practical guidelines used by organizations, from which they tailor organization specific, operational level information security policy. The standards may be advisory or compulsory, depending on the issuing and implementing agencies. The approaches underlying the major baseline standards, such as ISO 27002, FIPS, and COBIT, overlap with the RM-based approach to a large extent. Risk assessment is the first of twelve domains in ISO 27002. The U.S. Federal Information Security Management Act (FISMA) mandates federal systems comply with the Federal Information Processing Standards (FIPS), one of which is NIST SP 800-30, "Risk Management Guide for Information Technology Systems." "Assess and Manage IT Risks" is a major step in COBIT's first of four domains. Clearly, both the risk management approach and the standards based approach place strong emphasis on managing risk. However, the baseline security standards approach provides best practices and specific control/countermeasure recommendations, which the basic RM-based approach typically does not provide.

The controls recommended by baseline security standards yield security measures aimed at prevention and detection, primarily through technical, formal, and informal controls. Technical controls refer to the technical measures taken to prevent and detect unauthorized access. Formal controls refer to policies, procedures, and rules—managerial and organizational conditions—that limit employee activities. Informal controls refer to the development of ethical culture and to education to raise awareness of security-related issues. The historical emphasis has been on technical controls [Dhillon and Backhouse, 2001; Choobineh et al., 2007]. The prevailing goal of these controls, perhaps with the exception of informal controls, is to guard the information assets, rather than to influence offender decision making. Controls have seldom been designed and employed with the particular intention of influencing offender behavior—to dissuade offenders from making an event decision to commit a specific crime. Extending SCP to the digital realm is an attempt to do just that.

Situational Crime Prevention

Background

Situational crime prevention (SCP) involves "the management, design or manipulation of the immediate environment in as systematic and permanent a way as possible" [Clarke, 1997, p. 4] to reduce opportunities to commit a crime. Opportunity reduction is accomplished by making "the crime more difficult and risky, or less rewarding and excusable as judged by a wide range of offenders" [Clarke, 1997, p. 4]. Opportunity is further lessened by reducing provocations to crime commission [Wortley, 2001; Cornish and Clarke, 2003]. In short, the situational manipulations are designed to influence the offender's perception of the opportunity. When the perceived costs outweigh the perceived benefits, the situation is not perceived as an opportunity. When the offender does not perceive the crime as sufficiently excusable, or justifiable, the situation is not perceived as an opportunity. Clarke [1997] compiled a list of case studies in the physical domain (i.e., non-computer technology related crimes) that lend support to the situational crime prevention approach.

The theoretical basis of SCP is the rational choice perspective [Clarke, 1997], which is presented in its full or summarized form in many different publications, including Cornish and Clarke [2006]. The rational choice perspective assumes that offenders are rational, within the limitations of bounded rationality, and that they act in self-interest. The basic argument is that offenders, consciously or subconsciously, weigh costs (effort and risk) and benefits to determine the perceived net benefit associated with committing a crime. Further, offender event decision making is moderated by criminal perception of justification to commit crime [Clarke and Homel, 1997] and provocations [Wortley, 2001]. SCP suggests that it is possible to manipulate the environment associated with a specific crime to influence the criminal's (bounded) rational evaluation of the opportunity. Environmental manipulations alter the criminal's perception of the effort involved in committing the crimes, the risk of being caught, benefits from the crime, the moral inhibition to commit a crime, and/or provocation to commit the crime. (The five factors will henceforth be referred to as effort, risk, benefit, justification and provocation respectively, in the interest of brevity.) The current model of SCP classifies twenty-five opportunity reducing techniques along the five factors just listed [Cornish and Clarke, 2003].

SCP literature emphasizes the notion of crime specificity when implementing its twenty-five opportunity reducing techniques. Crime specificity is defined by the procedural set of actions and pre/post-conditions necessary for a unique crime event. Thwarting necessary steps, and/or altering necessary conditions is argued to thwart the crime. Thus, crime specificity requires that situational manipulations be tailored to specific crimes (e.g., a rash of breaking into cars parked in poorly lit areas to steal music systems), rather than to broad categories of crime (e.g., burglary) [Clarke and Homel, 1997; Willison, 2006b].

SCP in the Digital Realm

Researchers have suggested two formal, micro-level methods of implementing SCP in the digital realm: (1) using the crime-specific opportunity structure [Willison and Backhouse, 2006], and (2) the script-theoretic approach via universal scripts [Willison, 2006b; Willison and Siponen, 2009]. The crime-specific opportunity structure [Willison and Backhouse, 2006] is based on Clarke's [1995] model of the opportunity structure of crime. In his model, Clarke integrated several related theories, such as environmental criminology, routine activities theory, lifestyle theory, and SCP. The integration shows that even though each has a different origin and was developed for a somewhat unique purpose, the theories are still related and mutually reinforcing. Willison and Backhouse [2006] argued that this general model can be made more specific by considering a particular crime. They referred to this as the crime-specific opportunity structure, extended it to the digital realm, and conducted a post-hoc analysis of a case in which a local government employee committed computer input fraud. In the analysis, they mapped the steps taken by the offender to the concepts of the crime-specific opportunity model and argued that a prospective analysis could have identified steps that needed to be implemented to prevent such a crime.

The other approach to implementing SCP introduced in past literature is the script-theoretic approach. Cornish [1994] put forth the idea of using crime scripts to analyze how a specific crime can be prevented. Crime scripts refer to the sequence of steps that an offender must go through to commit a crime. The use of crime scripts to thwart a crime relies on thwarting one or more steps required to commit the crime successfully. Ideally, offender input, or actual crime accounts are used in generating scripts. However, such information is seldom available, so Cornish [1994] recommends the use of universal scripts. Universal scripts comprise a set of generalized scenes that can be used to model the steps involved in the commission of a specific crime (e.g., preparation, entry, pre-condition, doing, post-condition, and exit) [Cornish, 1994]. Again, Willison et al. [2006b; Willison and Siponen, 2009] perform a post-hoc analysis of a computer input fraud case to demonstrate how the method could have helped identify countermeasures to fight that specific instance of computer input fraud. Using their approach, the development of the script assists the practitioner in operationally identifying the appropriate countermeasures (selecting among SCP's 25 opportunity reducing techniques) to implement to prevent a specific crime.

There are two concerns with the crime-specific opportunity structure approach, as well as the script-theoretic approach. First, both require micro-level analyses and strict interpretation of the crime specificity assumption of SCP. The micro-level analysis requires a focus on implementation at the operational level rather than the strategic level, which makes it very cumbersome to implement the techniques across the broad spectrum of digital crimes. From an organizational resource perspective, it would be helpful to identify good cyber crime candidates for SCP before engaging in micro-level analyses of any or all cyber crimes. Further, the crime specificity assumption requires scripts to be developed. It is questionable whether such scripts can be reliably developed for all instances of crime to which SCP may be amenable, particularly those that have not yet occurred in an organization. In the case of computer crimes, even for crimes that have already occurred, organizations do not always gain a full step-by-step understanding into how a breach occurred.

The second concern is that both the crime-specific opportunity structure and script-theoretic approaches are focused on the procedural and environmental aspects of opportunity, rather than on perceptual opportunity (i.e., whether a crime is "worth it" in the mind of an offender). Neither approach focuses on understanding offenders, their motivation, and their perception of an opportunity from a rational choice perspective. This understanding is paramount in determining the utility of applying SCP to specific cyber crimes. The remainder of this article demonstrates how SCP can be incorporated into the traditional risk management process to identify organization specific risk classes that are amenable SCP crime reducing techniques, using an offender classification framework.

III. MESO-LEVEL APPLICATION OF SCP TO THE RISK MANAGEMENT PROCESS

In this section we present a modified risk management process that integrates SCP at a meso-level to surface additional, new information security countermeasures designed to influence offender decision making and proactively deter crime events. We begin by providing and discussing a framework for such classification. Then, we introduce the modified risk management process, showing exactly where SCP fits into the process and how the process changes in a reasonable and manageable manner. In the next section, we use three, real-world illustrative cases to show how the approach is integrated into the risk management process to surface new countermeasures.

The Offender's Perspective

SCP views criminal acts from the offender's perspective, i.e., the offender's perception of the current crime opportunity. Returning to the roots of SCP, there are five theoretical dimensions of the offender's perception of a criminal opportunity—perceived effort, perceived risk, anticipated rewards, rationalization/justification, and provocations. Much empirical research over the past two decades has demonstrated the sufficiency of these dimensions in explaining offenders' crime event decisions. The dimensions are not strictly orthogonal to each other, but the overlap is limited. Five techniques have been enumerated within each of the five theoretical dimensions, resulting in the well-known twenty-five cell table of opportunity reducing SCP techniques (see Table 2). However, only the columns have dimensional labels. The rows have no common theme or dimensional consistency. So, from the perspective of theoretical rigor, when applying SCP to crimes, one should consider offender perception in relation to the theoretically substantiated dimensions (the columns in Table 2), not all twenty-five cells. Once the influence(s) of criminal perception are identified, then specific situational manipulations (i.e., countermeasures) can be considered for each of the rows under the applicable columns for that crime.

The key issue is, how does an organization use SCP principles to reduce overall cyber crime risk? Past research [Willison, 2006b; Willison and Backhouse, 2006; Willison and Siponen, 2009] has taken a procedural view of the crime to select opportunity reducing techniques from the classic 25-cell SCP table. We contend that while this approach is a useful decision aid in identifying operational level countermeasures, it is not a theoretically guided approach for making strategic level decisions to reduce cyber crime risks in an organization. Further, its procedural bias largely ignores the role offender motivation and individual characteristics play in influencing offender perception of a criminal opportunity. We argue that the information security strategy should be based on the SCP dimensions most useful in reducing offender propensity to commit a crime. Assessing offender propensity requires an understanding of the offender perspective of the crime. Toward this end, we begin by proposing an offender framework, based on offender characteristics.

Proposed Offender Classification Framework

Our literature review of hacker taxonomies [Landreth, 1985; Hollinger, 1988; Chantler, 1996; Denning, 1998; Parker, 1998; Power, 1998; Rogers, 2006] surfaced four key offender characteristics that are largely independent of each other, that should influence offenders' perception of "opportunity." These offender characteristics are: offender motivation, offender skill level, offender-victim relationship, and offender involvement. They are shown in Table 3, along with their sub-categories. Each dimension is introduced more thoroughly in the following sections. In particular, we provide arguments to show that the dimension will influence the offender perception of the crime opportunity.

Table 2: Twenty-Five Opportunity Reducing Techniques of SCP [Cornish and Clarke, 2003]				
Increase Effort	**Increase Risks**	**Reduce Rewards**	**Reduce Provocation**	**Remove Excuses**
1. Target harden	6. Extend guardianship	11. Conceal targets	16. Reduce frustration and stress	21. Set rules
2. Control access	7. Assist natural surveillance	12. Remove targets	17. Avoid disputes	22. Post instructions
3. Screen exits	8. Reduce anonymity	13. Identify property	18. Reduce emotional arousal	23. Alert conscience
4. Deflect offenders	9. Utilize place managers	14. Disrupt markets	19. Neutralize peer pressure	24. Assist compliance
5. Control tools and weapons	10. Strengthen formal surveillance	15. Deny benefits	20. Discourage imitation	25. Control drugs and alcohol

Table 3: Proposed Offender Classification Framework	
Dimension	**Categories**
Offender Mtivation	Play, Crime, Hacktivism, National Security
Offender Skill	High, Medium, Low
Offender-Victim Relationship	Insider, Outsider
Offender Involvement	Anti-social Predator, Mundane, Provoked

Offender Motivation

Most hacker taxonomies use offender motivation as a primary taxonomical dimension. Some researchers create a more expansive list of hacker categories based on nuanced differences in motivation, while others create hacker categories that encompass many different motivations. A review of hacker motivation taxonomies suggests that they can be collapsed into a parsimonious set of four motivations: play, crime, hacktivism, and national security. This categorization is a slightly modified version of Denning's taxonomy (1998). The "play" domain consists of unauthorized computer activities engaged in for fun and/or intellectual challenge, without malicious intent. The goal of those operating in the "crime" domain is to commit a specific crime that happens to involve a computer or network during the commission of that crime. Those operating in the "hacktivism" domain are using technology merely as a transport mechanism for their activist message. Finally, those operating in the "national security" domain have transnational goals, i.e. foreign intelligence, war, terrorism, and espionage.

It can be readily seen that offender motivation identified in previous research [Landreth, 1985; Hollinger, 1988; Chantler, 1996; Denning, 1998; Parker, 1998; Power, 1998; Rogers, 2006] maps to the parsimonious set proposed (see Table 4). Other classifications of hacker motivations have been published [Mulhall, 1997; Calkins, 2000; Embar-Seddon, 2002], but the categories suggested by these are subsumed by the categories in Table 4.

Criminal motivation has significant influence on the effectiveness of the five SCP countermeasure categories. For example, highly skilled hackers motivated by "play" are often seeking a challenge. As such, increasing perceived effort required would not dissuade them from committing a specific crime. In fact, it might even incentivize him. On the other hand, the external, financial fraud criminal, seeking credit card numbers and personal data in a target-rich environment may very well be influenced to target a different organization (or no organization at all) if the perceived effort required to hack an organization is high. For her, time is money, and the end goal is money, not an intellectual challenge. If offender motivation is crime, then increasing effort by installing firewalls and strong passwords is an option to consider. Other options, such as reducing justification or reducing provocation may be more useful for the "play" attacker, but would be less useful when offender motivation is crime. Similar comparative examples exist for the other countermeasure categories.

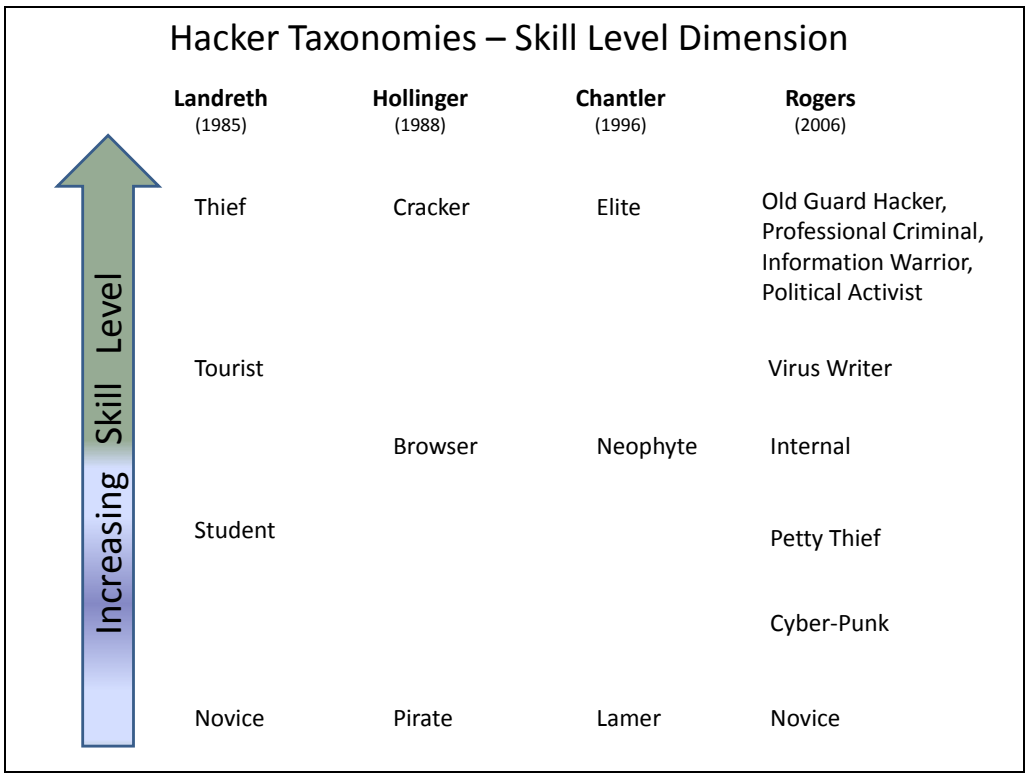
Table 4: Classifications of Offender Motivation

	Play	Crime	Hacktivism	National Security
Denning [1998]	Fun; play; intellectual challenge	Illegal financial gain	Ideological gain; individual rights	Patriotism
Landreth [1985]	Fun; play; intellectual challenge—learning; intellectual challenge—conquest notoriety; peer esteem	Criminal theft	Notoriety	
Hollinger [1988]		Copyright violation; unauthorized access to data/information; damage to data/information systems	Unauthorized access to data/information; damage to data/information systems	Unauthorized access to data/information; damage to data/information systems
Chantler [1996]	Peer esteem; achievement; self-discovery; excitement; challenge	Profit; theft	Vengeance	Espionage
Power [1998]	Sports intruders	Vandalism; personal interests; corporate interests		National interests
Parker* [1998]	Fun; intellectual challenge	Harm to data/information systems; criminal livelihood	Social justice; terrorism	Terrorism
Rogers [2006]	Excitement; peer esteem; media attention; Intellectual challenge; curiosity	Financial gain	Revenge	Patriotism

* Parker [1998] has two classifications called "personal problem solvers" and "malcontents/ addicts/irrational/incompetent people" that do not fit well with any of Denning's categories.

Offender Skill Level

While some hacker taxonomies differentiate hackers solely along the "motivation" dimension, others use skill level, or a combination of both, to categorize hackers [Landreth, 1985; Hollinger, 1988; Chantler, 1996; Rogers, 2006]. Skill level is typically described as a composite function of: (1) programming skill (i.e., ability to create or modify exploits and hacker tools), (2) system and network administration skill (i.e., ability to gain unauthorized access, escalate privileges, navigate systems, reconfigure systems, and alter evidence of their presence), and (3) cryptographic skill (i.e., ability to crack cryptographic algorithms). Figure 1 summarizes four hacker taxonomies that use skill level to differentiate hackers.



Note: The vertical distances between taxonomy categories is ordinal only, and each taxonomy should be considered independent from the others (i.e., Hollinger's [1988] "Browser" may or may not exhibit a skill level identical to Chantler's [1996] "Neophyte").

Figure 1: Hacker Taxonomies – Skill Level.

Offender skill level is an important dimension to consider when examining the applicability of the five SCP theoretical dimensions, because the offender's skill level influences their perception of countermeasures designed to increase effort and risk. Highly skilled individuals may not be slowed by techniques that call for greater effort, whereas a less skilled criminal probably will be. In the case of the highly skilled attacker, techniques that reduce the perceived benefits of the crime become increasingly important, so as to make the crime unattractive.

Offender-Victim Relationship

The offender's relationship to the organizational target ("insider" vs. "outsider") is an oft-cited attribute differentiating computer criminals. This difference often affects the anatomy of the attack, the targeted or opportunistic nature of the attack, and the offender's fear of being caught. Each of these affects the decision making process.

The anatomy of the attack is different for insiders and external hackers. Insiders have unique access, both electronic and physical, to information systems. The external hackers' need to gain initial access, cover their tracks, and implement back doors often diverge from those of insiders—insiders already have some level of access, and their actions may be seen technologically as authorized given their role in the organization. Insiders also possess advanced organizational knowledge not readily privy to an external hacker. The outsider or external hacker, must often engage in additional steps related to target acquisition, such as footprinting, scanning, and enumeration [Bento and Bento, 2004]. Such extra steps will affect the offender's perspective of the crime opportunity.

An external hacker may attack an opportunistic target or a specific, pre-determined target. An opportunistic attack is likely to seek easy targets, and hence is more likely when the target is perceived to be vulnerable. Since an opportunist is not targeting a specific victim, the offender-environment interaction becomes paramount. In a targeted attack, however, the target is selected for some reason, which may extend beyond environmental variables. For example, the identity thief targets a specific organization, due to the plethora of personal identifying information the organization stores digitally; the recreational hacker targets a government agency, because of the conquest it represents; and so on. In a targeted attack, the offender's perception of opportunity, in particular the choice of a target, is not fully explained by the procedural view of the crime—offender motivation and individual characteristics play a role.

Communications of the Association for Information Systems

Insiders, by definition, attack their employing organization, and are, therefore, engaging in targeted attacks, although the timing may be opportunistic. Frequently, insiders are disgruntled employees, motivated by specific employment-related grievances [Wilson et al., 1992; Dhillon and Moores, 2001; Rogers, 2006]. Such grievances tend to rationalize, or justify computer crimes in the mind of the insider. This is keenly important to the "remove excuses" and "reduce provocations" dimensions of SCP. The external attacker is less likely provoked, and more likely motivated by play or crime, which is important to the cost and benefit dimensions of SCP, more so than the excuses and provocation dimensions. Of course, there are other SCP dimension combinations possible. For example, the external hacktivist would be influenced by the excuses and provocation dimensions.

The "risk of being caught" dimension is also important considering the offender-victim relationship. This dimension has two elements: (1) incident detection and organizational recovery, and (2) offender apprehension and punishment. The risk of being caught relative to incident detection and organization recovery is a function of the fact that detection and recovery diminishes the utility of the attack. Often the attacker seeks long-term access to some resource (e.g., warez site[1] or pass-through victim), or information (e.g., identities or financial accounts). Detection and recovery often disrupts such long-term access. The risk of being caught relative to apprehension and punishment is a function of classic General Deterrence Theory. This second element is particularly important with respect to the offender-victim relationship dimension. Insiders are more susceptible to general deterrence measures, and are, therefore, more influenced by situational manipulations that increase the risk of being caught [Straub, 1990]. External hackers, on the other hand, are more difficult to detect and apprehend and are often under the purview of other jurisdictional authorities, making apprehension and prosecution difficult, if not impossible. Thus, different approaches may be necessary to reduce crime by insiders versus outsiders.

Offender Involvement

Offender involvement (or criminal involvement) refers to the centrality of criminal behavior (or criminality) to the criminal's life—his/her time and his/her livelihood. Cornish and Clarke [2003] argue that criminal behavior is central to the predator's life, marginal to the mundane criminal's life, and atypical of the provoked offender's life. Although not expressed formally as a taxonomical dimension, prevailing hacker taxonomies imply varied levels of criminal involvement. For example, Landreth's (1985) *novice, student,* and *tourist* categories suggest lesser commitment to criminality as a way of life, than does his *crasher* category, which in turn suggests lesser commitment than his *thief* category. This commitment continuum is also evident in Hollinger's (1988) *pirate* → *browser* → *cracker* taxonomy, in Parker's (1998) *career criminal* → *malicious hackers* → *pranksters* (among others) taxonomy, and in Rogers' [2006] *professional criminals* → *petty thieves* → *cyber-punks* (among others) taxonomy. Other taxonomies [Calkins, 2000; Embar-Seddon, 2002] reflect similar criminal involvement categories as the Cornish and Clarke [2003] classification. Thus, the Cornish and Clarke [2003] categorization (predator, mundane criminal, and provoked offender) provides a good basis to differentiate levels of criminal involvement.

Offender involvement helps explain why different offenders perceive opportunity differently [Cornish and Clarke, 2003]. Anti-social predators are those offenders whose criminal "readiness" is presumed. Mundane offenders are normally receptive to criminal activity, but not necessarily ready at all times. Provoked offenders are normally not ready, nor receptive to criminal activity, but are readied by provocative situational factors. The significance of this offender attribute can be seen in the use of the approach to reduce provocation. The provoked offender is likely to respond to reductions in provocation, but the anti-social predator, whose criminal involvement is not a response to provocation, is less likely to respond to changes in provocation. A similar reaction would be expected with respect to the criminal's perception of justification—excuses to commit the crime. The anti-social predator need not rationalize the crime, whereas the mundane and provoked offenders may need to, thus perceptions of "excuses" should influence offender behavior along this dimension.

Criminal involvement also influences offender perception of, and reaction to, situational changes. For example, the predatory criminal is already motivationally ready and has already made an involvement decision respecting crime commission. Thus, he/she is more committed to crime commission and may be less perceptive to, and/or less influenced by increased target hardening measures than the "mundane offender," whose criminal readiness is not constant and cannot be presumed.

In summary, our proposed offender classification framework consists of four primary dimensions: offender motivation, offender skill level, offender-victim relationship, and offender involvement. Motivation sub-dimensions include: play, crime, hacktivism, and national security. Offender skill level sub-dimensions include: high, medium, and low. Offender-victim relationship sub-dimensions include: insider and outsider. Offender involvement sub-

[1] Warez sites are computers used to store cyber offender files and software, particularly those containing illegal, copyrighted, or contraband content.

dimensions include: anti-social predator, mundane offender, and provoked offender. Organizational information security risks are classified according to this framework. This, of course, is limited to risks that are a function of intentionally malicious acts, perpetrated by cyber offenders. Risks to information assets that stem from natural disasters and human errors are not applicable to SCP opportunity reducing techniques.

The Proposed Modified Risk Management Process

In our approach, the overall risk management process is retained (i.e., identify assets, threats, vulnerability, risks, and countermeasures, implement countermeasures, and evaluate). SCP is incorporated into this sequence by modifying the threat and countermeasure identification steps (see Table 5). Step 2 of the Risk Management process, "Threat Identification and Classification," is modified by aggregating the identified risks and classifying them according to the proposed offender classification framework. Step 5, "Controls and Countermeasures Identification" is modified with the addition of two new sub-steps. First, SCP is applied at the meso-level by determining which of the five SCP dimensions would influence perceptual opportunity and motivation of the offenders in each aggregated threat class. Second, countermeasures are enumerated within each applicable SCP dimension. The operational-level identification of countermeasures is not part of the strategy formulation process, but is part of the overall risk management process and is, therefore, included. The modified risk management process is shown in Table 5. Modifications are made as sub-steps—the major risk management process steps remain the same.

IV. ILLUSTRATIVE CASES

To provide support for the proposed methodology, we present three illustrative cases, based on interviews with senior executives of three real-world organizations. These cases show how the methodology is implemented and demonstrate that the incorporation of SCP into the risk management process is relatively straight-forward, not particularly resource intensive, and nets an expanded range of countermeasures to achieve organizational information security objectives.

Data Gathering

We conducted one-on-one interviews (approximately forty-five minutes in duration) with the Chief Information Security Officer (CISO) (or equivalent) of each of three real-world organizations (names changed to protect anonymity). The organizations included: (1) a small Internet service and information technology service provider (ITforYou, Inc.), (2) a large financial services company (MoneyCo.), and (3) a moderately sized independent, public school district (EduISD). We obtained and documented information concerning each organization's information assets, threats, risks, and countermeasures. We also obtained their subjective evaluation of their organization's current information security effectiveness. We then applied our proposed methodology to each organization's situation and presented each with a written analysis that: (1) classified their high-risk human threats according to our proposed framework, (2) determined the applicability of SCP countermeasure categories (the five SCP dimensions) to mitigate residual risk of the organization's high-risk human threats, and (3) recommended specific countermeasures designed to influence their high risk human threats to *not* attack the organization. It took us an average of three hours to prepare each report, including time for analysis and writing. After giving the CISOs several days to evaluate the proposal, we asked them for feedback regarding the proposal. Essentially, we asked if they thought such a strategy would improve their information security effectiveness (i.e., "would it dissuade the target offenders?"), and whether the recommended countermeasures could reasonably be expected to be implemented in their organization.

During each interview, we obtained a basic understanding of the organization, its mission, and their past risk management activities. Respondents identified their key information assets, highest risk threats, general countermeasures in place, and their prior experience with both successful and unsuccessful attempts involving those threats. Responses are summarized in Table 6.

All three companies agreed with our conclusions that (a) their current strategy focuses on preventing and/or detecting cyber crimes, and, (b) they do not specifically design countermeasures to influence offender decision making and proactively deter them from attempting specific crimes against their organization. Each organization rated their current information security effectiveness highly, but each indicated residual risk existed in key human threat classes for which additional prevention and detection countermeasures are either not available, or have been deemed nonviable solutions (e.g., too costly, impedes business operations, low residual risk).

After we completed each interview, we analyzed the information and made recommendations for security countermeasures based on the proposed SCP-based risk management process. A full explanation of the application of the modified risk management process to each organization is contained in Appendices 1 through 3. The following sub-section provides a condensed analysis for the ITforYour, Inc. case to illustrate how the modified risk management process is implemented. Following that, all three illustrative cases are comparatively summarized.

Table 5: Modified Risk Management Process

Major Steps Remain Unchanged	Traditional Sub-Steps	Additional Sub-Steps
1. Asset Identification and Classification	a. Determine what the organization needs to protect and to what extent.	(none)
2. Threat Identification and Classification	a. Determine who and what represent risks to those assets.	b. Classify and group human threats according to the proposed offender classification framework.
3. Vulnerability Identification and Classification	a. Determine the organization's weaknesses and how they relate to assets from Step 1 and threats from Step 2.	(none)
4. Risk Assessment	a. Quantitatively or qualitatively determine the risk of each vulnerability (considering asset value, threat probability, loss estimates, and vulnerability exposure).	(none)
5. Controls and Countermeasures Identification	a. Design preventative solutions (i.e. controls) to mitigate risks to the extent deemed desirable/ acceptable, considering cost (product costs, implementation costs, and maintenance costs) and operational impact.	b. Determine the applicability of SCP's five countermeasure categories for each human threat class identified in Step 2b and selected for risk mitigation in Step 4. c. Identify countermeasures that proactively influence offender decision making in accordance with the SCP countermeasure categories deemed applicable in Step 5b.
6. Controls and Countermeasures Implementation	a. Put controls in place institutionally.	(none)
7. Re-evaluation	a. Continually examine the effectiveness of current controls and reconsider changes to mission, assets, threats, and vulnerabilities to identify appropriate changes to the risk management strategy.	(none)

Table 6: Illustrative Cases—Situational Summary			
	ITforYou, Inc.	**MoneyCo.**	**EduISD**
Organization Type	Internet and IT services co.	Financial services co.	Public school district
Organization Size	Very small (2 people)	Large (5,800 people)	Large (3,000 staff and students) (moderately sized for a school district)
Organization Location	U.S. (Midwest)	U.S. (Southwest)	U.S. (Southwest)
Brief Description	Web hosting, programming, data center services	Payment services, check manufacturing, financial marketing services	Kindergarten–12th grade education
Key Assets	Hosted websites Computing resources	Personally identifying info Business financial data Personal financial data	Personally identifying info Student grades Social program enrollment
Primary Threats	1. External, target of opportunity seekers 2. Anti-spam hacktivists who believe ITforYou is permitting spam (but e-mails are not spam)	1. Cyber criminal seeking personal and financial data 2. External, recreational hackers	1. Student users (insiders) who are failing courses and seek grade changes 2. Student users (insiders) motivated by "play"
Main Counter-measures	Tight technical controls, maintains "low profile"	Formal, technical, informal controls (in priority order)	Technical, formal, informal controls (in priority order)
History of Attacks	One successful target of opportunity hack from external source. Several unsuccessful attacks by anti-spam hacktivists who mistakenly believe ITforYou is permitting its customers to send unsolicited e-mail promotions to them.	Fallen victim to a wide variety of attacks over the years, but with low frequency. Predominant attack in the **past** was mischievous, target of opportunity. Predominant attack **currently** is targeted attack related to financial fraud and identity theft.	Several successful attacks and many more unsuccessful attacks over the years by both types of threats identified above. Frequency of successful attacks has decreased, as technical controls have improved, but continue to occur nonetheless.

Case Discussion: ITforYou, Inc.

Recall, the modified risk management process introduces three new sub-steps:

- Step 2b: Classify and group human threats according to the proposed offender classification framework.
- Step 5b: Determine the applicability of SCP's five countermeasure categories for each human threat class.
- Step 5c: Identify countermeasures that proactively influence offender decision making.

Our discussion focuses on the modifications to the risk management process.

ITforYou, Inc. identified two high-risk human threat classes: target of opportunity hackers and anti-spam hacktivists, who believe ITforYou, Inc. is knowingly facilitating spam. In accordance with Step 2b of the modified risk management process, we classified these threat classes according to the proposed offender classification framework. Our classification is summarized in Table 7. A full explanation of this classification can be found in Appendix 1. It is important to note that this classification is organization specific. For example, the classification is not meant to suggest that all opportunists are medium to highly skilled, rather that ITforYou does not perceive poorly skilled opportunists to be a threat, given their current security posture.

The goal of Step 5b is to determine the applicability of SCP's five countermeasure categories for each human threat class identified in Step 2b and selected for risk mitigation in Step 4. Different SCP dimensions will be applicable in different threat classes, both within and between organizations.

Table 7: ITforYou Application of Offender Classification Framework (Step 2b of the Modified Risk Management Process)

Framework Dimension:	Threat Class*:	
	Opportunists	**Anti-Spammers**
Offender Motivation	Play, Crime, National Sec.**	Hacktivism
Offender Skill	Med-High	Med-High
Offender-Victim Relationship	Outsider	Outsider
Offender Involvement	Predator; Mundane	Provoked

* See Table 6 for further descriptive information of threat classes and organizations.
** Victim is a used as a "pass-through" in the case of 'national security' motivation.

The opportunist with whom ITforYou is concerned is moderately to highly skilled and is likely able to overcome situational manipulations that increase perceived effort. However, because he is usually seeking a victim that he can exploit quickly and easily, increasing perceived effort in committing the offense may be sufficient to thwart this category of offender. In contrast, increasing the perceived effort will likely prove inconsequential for the anti-spam hacktivist, because his skill level is probably relatively high and his target is specifically related to his motivation.

Increasing the perceived risk of detection may be beneficial in the case of the opportunist, but primarily from the standpoint that detection may impede the utility of the hack (e.g., long-term use of the resource or information). The hacktivist, on the other hand, *wishes* to be detected. Without detection, his point is not made. Detection risk from the standpoint of apprehension and punishment is probably inconsequential to both offenders. Neither believes their acts will likely be attributed to them, given the relative impunity with which cyber offenders are often able to operate.

Decreasing anticipated benefits is a difficult proposition to use in defending against both classes of offenders. Opportunistic hackers have no prior knowledge of the value of information in the computer system, nor the value of the system as a computing resource. Hence, it is difficult to formulate mechanisms to alter their perception of the value of information assets in the system, or of the utility of the system as a computing resource. The primary benefit that the hacktivist is seeking is the cessation of the alleged spam. Self-gratification from retribution might be a secondary anticipated benefit. For this SCP category to be useful in influencing offender decision making, the organization must make the hacktivist believe that attacking them will *not* result in the cessation of the alleged spam, nor will it bring them satisfaction from retribution. Given the offender's probable skill level, it is unlikely that the organization can effectively convince him of either reduced benefit.

The fourth SCP dimension influencing the offender's perception of opportunity is rationalization/justification. SCP argues that if the offender can mentally excuse their criminal behavior, they will be more inclined to make an event decision to commit a crime. The opportunist may internally justify their crimes as harmless if their motivation is *play.* The opportunist does not seek justification if their motivation is *crime* or *national security*; they know their crime is illegal. Regardless of their motivation, however, a target of opportunity does not likely have a means for reducing the opportunist's perception of rationalization and justification. On the other hand, this dimension is important to the anti-spam hacktivist. He rationalizes that "hacking back" is justified, because ITforYou, Inc. is culpable in the situation. Accordingly, countermeasures that remove the hacktivist's excuse will likely influence their decision making and proactively influence them to *not* attack ITforYou, Inc.

The last SCP dimension is provocation. The opportunist is not provoked, particularly as it pertains to an event decision involving a specific target. They have made an involvement decision to engage in crime, but their specific event decision is not provoked. The anti-spam hacktivist, on the other hand, is provoked upon receiving what he believes is spam. Accordingly, countermeasures that lessen the hacktivist's provocation, will likely influence their decision making and proactively influence them to *not* attack ITforYou, Inc.

This analysis concludes Step 5b of the modified RM process. Our conclusions are summarized in Table 8.

Table 8: Applicability of SCP Dimensions to ITforYou (Step 5b of the Modified Risk Management Process)

SCP Dimension	Threat Class*	
	Opportunists	Anti-Spammers
Increase Perceived Effort	✓	
Increase Perceived Risk	✓	
Decrease Anticipated Benefit		
Remove Excuses		✓
Reduce Provocations		✓

* See Table 6 for further descriptive information of threat classes.
Key: A check mark indicates the respective SCP dimension has definite potential for yielding new, additional countermeasures for the threat class.

While the operational, micro-level analysis that identifies specific countermeasures (Step 5c of the modified risk management process) is not part of the information security strategy formulation, we continue the discussion for the ITforYou, Inc. case by identifying some influential countermeasures to help the reader conceptualize the entire approach, and to demonstrate that useful countermeasures do surface. Using the script-theoretic approach, countermeasure identification is facilitated by considering the crime sequence, or script actions. In our approach, countermeasure identification is facilitated by identifying the applicable SCP dimensions for threats classified according to the proposed offender classification framework.

ITforYou, Inc. identified two possibly useful SCP dimensions for the opportunist threat class: increased perceived effort and increased perceived risk of being caught. While increasing required offender effort through stronger technical defenses will likely deflect opportunist, this is a preventive measure. If ITforYou, Inc. could proactively notify would-be offenders of the increased defenses, then they would influence their offenders and dissuade them. However, since the opportunist likely initiates automated scans of large IP address ranges for potential targets, ITforYou, Inc. questions whether they could proactively communicate such increased defenses to would-be offenders. Similar rationale holds true for the "increase perceived risk of detection" category. In short, ITforYou, Inc. decides that while possible, influencing offender decision making is not an effective means for reducing the residual risk of the target of opportunity threat class. They decide *not* to identify and implement additional countermeasures designed to increase the opportunistic hacker's perception of the effort required and risk of being detected.

On the other hand, ITforYou, Inc. sees significant potential in the notion that they can reduce the provocations that incite anti-spam hacktivists, and that they can decrease anti-spam hacktivists' ability to rationalize and justify their hacktivist behavior. One possible approach might be to post a message on ITforYou, Inc.'s company website. The message would explain the source of and reason for the e-mails, i.e., that the e-mails are being sent by ITForYou, Inc., on behalf of vendors, who market via e-mail using e-mail addresses directly supplied by the recipients and/or legally obtained through the purchase of mailing/marketing lists. This, as well as reminding offenders that hacking is illegal, may serve to remove excuses (rationalization/justification) from offenders. Finally, the promotional messages, which are being viewed as spam, should provide a mechanism for disgruntled recipients to opt out of receiving such messages, complain to ITforYou, and/or complain to the sender. In short, ITforYou, Inc. provides an alternative solution for the would-be attacker, reduces the attacker's frustration (i.e., provocation), and/or convinces the hacktivist that retaliation is not warranted. Depending on the prominence of the website message, it is reasonable to presume that the hacktivist will see the message, because viewing the target's website is a very standard reconnaissance step for hackers [Bento and Bento, 2004].

Table 9 summarizes the above analysis—Step 5c, countermeasure identification, for the ITforYou, Inc. case. For opportunists, two SCP dimensions were identified to reduce offender propensity to commit crime: (1) increase perceived effort, and (2) increase perceived risk. However, the analysis did not surface any additional, new countermeasures over those already in place. For the anti-spammers, the SCP dimensions with potential to influence offender decision making are: (1) remove excuses, and (2) reduce provocations. Several countermeasures are identified, such as do not send unwanted e-mails, explain source of and reason for e-mail, and so on. In effect, the analysis nets new and unique countermeasures other approaches would not typically net, since other approaches are biased toward prevention and detection, as well as procedural interruption, rather than offender dissuasion (or deterrence) via the rational choice perspective.

Table 9: Countermeasure Identification for ITforYou (Step 5c of the Modified Risk Management Process)

SCP Dimension:	Threat Class*:	
	Opportunists	**Anti-Spammers**
Increase Perceived Effort	No New Countermeasures	Not Applicable
Increase Perceived Risk	No New Countermeasures	Not Applicable
Decrease Anticipated Benefit	Not Applicable	Not Applicable
Remove Excuses	Not Applicable	Explain source and reason for e-mails. Do not send unwanted e-mails. Remind that hacking is a crime.
Reduce Provocations	Not Applicable	Provide instructions for opt-out process. Explain source of and reason for e-mails.

* See Table 6 for further descriptive information of threat classes.

This concludes the specific discussion of the ITforYou, Inc. case, which highlights the implementation of the modified risk management process. Further detail is provided in the supporting appendices. The following section provides a short, comparative analysis of all three illustrative cases. The goal is to demonstrate that different SCP dimensions are influential across cyber offender threat classes, which vary across organizations.

Comparative Analysis Across All Three Cases

After each interview, we classified aggregated human threats according to the proposed offender classification framework, in accordance with Step 2b of the modified risk management process. Our classification is summarized in Table 10. The practitioners involved in the three illustrative cases were in general agreement with our application of the framework. However, in practice, the framework should be applied by individuals very familiar with the organization's security issues.

Steps 3, 4, and 5a of the risk management process remain as they were before, so next we applied SCP at a meso-level, in accordance with Step 5b of the modified risk management process. The application determined the applicability of the five SCP countermeasure categories (theoretical dimensions) for each human threat class identified in Step 2b and selected for risk mitigation. Table 11 provides a summary of the results of SCP application to each category of identified offenders for the different organizations.

At this point, the process of strategy formulation is complete, i.e., the SCP dimensions which will guide countermeasure selection have been identified. The identification of the specific countermeasures is an operational step. The goal of the article was to propose an approach to strategy formulation. Nonetheless, we continued on to identify the operational measures to demonstrate that the process yields meaningful countermeasures not previously considered by the CISOs of the organizations studied.

Table 10: Illustrative Cases—Application of Offender Classification Framework (Step 2b of the Modified Risk Management Process)

	ITforYou, Inc.		MoneyCo.		EduISD	
Threat Class*:	**1 Opportunists**	**2 Anti-Spammers**	**1 Financial Fraudsters**	**2 Recreational Hackers**	**1 Grade Changers**	**2 Script-Kiddies**
Offender Motivation	Play, Crime, National Sec.**	Hacktivism	Crime	Play	Crime	Play
Offender Skill	Med-High	Med-High	High	Med-High	Low-High	Low-Med
Off.-victim Relationship	Outsider	Outsider	Outsider	Outsider	Insider (student)	Insider (student)
Offender Involvement	Predator; Mundane	Provoked	Predator	Mundane	Provoked	Mundane

* See Table 6 for further descriptive information of each threat classes and organizations.
** Victim is a used as a "pass-through" in the case of 'national security' motivation.

Table 11: Applicability of SCP Dimensions to Illustrative Cases (Step 5b of the Modified Risk Management Process)

	ITforYou, Inc.		MoneyCo.		EduISD	
Threat Class*	**1 Opportunists**	**2 Anti-Spammers**	**1 Financial Fraudsters**	**2 Recreational Hackers**	**1 Grade Changers**	**2 Script-Kiddies**
Increase Perceived Effort	✓		✓		✓	✓
Increase Perceived Risk	✓		✓		✓	
Decrease Anticipated Benefit			✓		✓	
Remove Excuses		✓		✓		✓
Reduce Provocations		✓				

* See Table 6 for further descriptive information of threat classes and organizations.
Key: A check mark indicates the SCP dimension has definite potential for yielding new, additional countermeasures for the threat class.

Once an organization applies the offender classification framework and intellectually considers the utility of each SCP dimension, specific countermeasure identification exercises follow, in accordance with Step 5c of the modified risk management process. These countermeasures are summarized in Table 12. Note, this table reflects only additional, new countermeasures identified by the application of SCP. The application will likely net some countermeasures that current approaches already identify, which is an added benefit, but we focus our results and discussion only on what is new.

The operational countermeasure identification process is facilitated by the meso-level application of SCP, in that the classic SCP 25-cell table of opportunity reducing techniques is reduced to the subset of columns deemed applicable during Step 5b of the modified risk management process. Once the appropriate SCP dimensions are identified, the rows within the table are considered. This approach reduces the complexity of operational countermeasure decision making process.

Table 12: Sample New Countermeasures (Step 5c of the Modified Risk Management Process)

	ITforYou, Inc.		MoneyCo.		EduISD	
Threat Class*:	**1 Opportunists**	**2 Anti-Spammers**	**1 Financial Fraudsters**	**2 Recreational Hackers**	**1 Grade Changers**	**2 Script-Kiddies**
Increase Perceived Effort	No new measures identified	N/A	Compartmentalize information	N/A	Double entry requirements	No new measures identified
Increase Perceived Risk	No new measures identified	N/A	IDS/IPS; file access audits; customer alert processes	N/A	File access audits	N/A
Decrease Anticipated Benefit	N/A	N/A	Very Strong Encryption	N/A	Change notifications	N/A
Remove Excuses	N/A	Website notices	N/A	No new measures identified	N/A	No new measures identified
Reduce Provocations	N/A	Opt-out process	N/A	N/A	N/A	N/A

* See Table 6 for further descriptive information.

To recap, we provided each organization with a written proposal that: (1) classified their aggregated high-risk human threats according to our proposed framework, (2) identified the appropriate balance of SCP countermeasure categories to mitigate residual risk of the organization's high-risk human threats, and (3) recommended specific countermeasures designed to influence their high risk human threats to *not* attack the organization. After giving them several days to evaluate the proposal, we asked each organization (the same respondent originally interviewed) for feedback regarding the proposal. In each case, the response was very positive. All three CISOs expressed interest in the approach, said it was something they had not previously considered, thought it showed promise for reducing their residual risk, and thought the recommended countermeasures were feasible. We acknowledge the possibility of demand bias in their responses. The effectiveness of operational countermeasures suggested by us will need to be demonstrated in field sites to fully validate the usefulness of the proposed method.

V. CONCLUSION

Contributions

This research makes five significant contributions to the area of information security strategy formulation. First, our approach yields an expanded range of information security countermeasures, specifically those that proactively influence offender decision making by altering their perception of effort, risk, benefit, rationalization, and provocation. This is an approach to crime-reduction that is not typically considered by organizations when formulating information security strategy, whose focus tends to net preventive and detective countermeasures. Our approach extends SCP to the digital realm with an emphasis on offenders' rational decision making. SCP is a robust and well-established theory in the area of criminal justice that has benefitted from several decades of intellectual debates. It is theoretically complete, i.e., it includes all factors that offenders take into consideration, consciously or subconsciously, in their decision to engage in a crime.

Second, we provide a methodology for netting the expanded range of information security countermeasures discussed above. The method adapts the most widely used strategy formulation approach currently used—the risk management process. It introduces no new major steps and adds only a few new sub-steps. The methodology is relatively simple and quick to employ. We proposed an offender classification framework, based on past literature and by integrating several widely accepted cyber offender taxonomies. The framework enables organizations to group similar human threats into classes, which then facilitates the meso-level application of SCP. The meso-level application of SCP then provides a framework by which organizations can identify appropriate countermeasure categories (effort, risk, benefit, justification, and provocation) for each human threat class. This ultimately facilitates the countermeasure identification process.

The third contribution of this article is our demonstration that meso-level application of SCP is both possible and useful for strategy formulation. Previous proponents of SCP have argued that a micro-level analysis of the steps necessary to execute a crime is necessary to effectively implement security measures based on SCP. While we agree that a crime specific, procedurally oriented view can identify unique countermeasures, we have demonstrated the utility of the meso-level application of SCP and the rational choice perspective. In particular, SCP can help identify categories of countermeasures to be considered based on the framework that we have proposed.

Fourth, our approach emphasizes the influence of perceptual opportunity on offender decision making, whereas past extensions of SCP to the digital realm [Willison, 2006b; Willison and Backhouse, 2006; Willison and Siponen, 2009] have focused on the procedural aspects of crime commission. While past extensions have netted new countermeasures beyond those produced by traditional approaches, they are still largely preventive and detective in nature. Our approach focuses on influencing offender decision making—proactively dissuading them from wanting to attempt a crime. The procedural view, specifically through the use of crime scripts, provides "… a clearer understanding of which safeguards to implement" [Willison and Siponen, 2009, p. 135]. Still, as with traditional approaches, the emphasis is on safeguards, i.e. *controls*. Our focus is on perception of costs, benefits, excuses, and provocations, rather than on safeguards that digitally prevent or detect cyber offenses.

The fifth contribution is empirical. The proposed method was used to analyze the security strategy of three real life companies. The analysis surfaced two points worthy of note. One, the method surfaced additional categories of countermeasures not typically surfaced by current approaches—specifically, countermeasures that change offender perception of benefit, justification, and provocation. These additional categories can yield simple and inexpensive solutions, as evidenced by the cases analyzed in the current article. Two, the method surfaced new countermeasures in categories typically surfaced by current approaches—specifically, countermeasures that change offender perception of effort and risk.

Limitations and Future Research

There are two limitations that suggest the need for additional research to put our proposal on a stronger foundation. First, this research assumes that cyber offenders will be influenced by SCP technique categories (effort, risk, benefit, justification, and provocation), as has been shown to be the case in the physical realm. The effectiveness of the SCP categories has been empirically validated for the physical realm. The effectiveness of SCP categories that increase effort and increase risk in the cyber realm has been empirically validated to some extent, although research has not separated the impacts of such countermeasures with respect to controls-based prevention versus detection versus decision making influence. Further validation of the effectiveness of increasing perceived effort and increasing perceived risk is necessary, as is the validation of the effectiveness of reducing perceptions of benefits, justification and provocation in the cyber realm. Empirical research is needed to determine to what extent cyber offenders' rational decision making process mirrors that of non-cyber offenders, what differences exist, and why differences exist (if they do). Preliminary evidence can be gathered using laboratory experiments, but will have to be corroborated with field data.

Also, this research assumes that successfully manipulating the SCP techniques will raise the security effectiveness of the organization. The question remains, however, do countermeasures based on SCP technique categories actually result in greater information security effectiveness for the organization? The empirical demonstration of the effectiveness of the new categories of countermeasures (benefit, justification, and provocation), as well as the new view of existing categories (effort and risk) requires organizations to implement and evaluate solutions. To the best of our knowledge, no organization has implemented such techniques.

Concluding Remarks

Currently, risk management and standards-based approaches guide the development of security strategies in organizations. However, such approaches typically surface only countermeasures designed to prevent and detect cyber offenses. They do not typically surface countermeasures designed to influence cyber offender decision making, i.e., is it beneficial to the criminal to target a specific organization, at a specific time, for a specific reason, in a specific manner? We have proposed the use of SCP and the rational choice perspective to fill this gap. We integrated it into a modified risk management approach and provided a supporting cyber offender classification framework, based on past literature and cyber offender taxonomies. The framework enables us to apply the SCP concepts at a meso-level, which is useful in strategy formulation. We gathered qualitative data about security strategies currently employed by three organizations, and then provided theoretically logical arguments to demonstrate that SCP may facilitate in the identification of additional countermeasure categories (benefit, justification, and rationalization) and new countermeasures in existing categories (effort and risk).

The war against computer crime is seemingly endless. Stronger, more complex, more expensive technical defenses soon reach a point of diminishing returns. Also, apprehension and prosecution of criminals has limited potential for computer crime committed from afar. Hence, the two commonly used approaches to fight computer crime (risk management and baseline security standards approaches), which focus on prevention and detection, may not be sufficient in all cases. We argue that it is necessary to continue to search for other methods to reduce the incidence of computer crimes. Toward this end, we have proposed the incorporation of SCP into the risk management process for formulating information security strategy. Doing so results in an innovative approach to IS security strategy development—one that surfaces an expanded range of measures to reduce computer crime.

ACKNOWLEDGEMENTS

Srinivasan Rao's participation in this research was supported in part by a grant from the College of Business at UTSA.

We wish to express our utmost gratitude to the two anonymous reviewers and associate editor for their invaluable comments and suggestions regarding this article. We engaged in two major revisions as a result of their feedback and whole-heartedly agree that the article is much better for their suggestions. We also wish to thank Dr. Ilze Zigurs, CAIS Editor-in-Chief, for her patience as she guided us through the last revision. The article has benefited greatly from her suggestions.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the paper on the Web, can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Alter, S., and S.A. Sherer (2004) "A General, But Readily Adaptable Model of Information System Risk", *Communications of the Association for Information Systems* (14)1, p. 28.

Backhouse, J., and A. Bener (2004) "Risk Management in Cyberspace", http://www.foresight.gov.uk/.

Bento, A., and R. Bento (2004) "Empirical Test of a Hacking Model: An Exploratory Study", *Communications of the Association for Information Systems* (14), pp. 678–690.

Calkins, M.M. (2000) "They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models", *Georgetown Law Journal* (89)1, pp. 171–224.

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

Choobineh, J., et al. (2007) "Management of Information Security: Challenges and Research Directions", *Communications of the Association for Information Systems* (20), pp. 958–971.

Clarke, R.V. (1995) "Situational Crime Prevention" in Tonry, M., and D. Farrington (eds.) *Building a Safer Society. Strategic Approaches to Crime Prevention. Crime and Justice: A Review of Research*, Chicago, IL: University of Chicago Press, pp. 91–150.

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

Clarke, R.V., and R. Homel (1997) "A Revised Classification of Situational Crime Prevention Techniques" in Lab, S.P., *Crime Prevention at a Crossroads*, Cincinnati, OH: Anderson, pp. 21–35.

Cornish, D.B. (1994) "The Procedural Analysis of Offending and Its Relevance for Situational Prevention" in Clarke, R.V. (ed.) *Crime Prevention Studies,* Monsey, NY: Criminal Justice Press, pp. 151–196.

Cornish, D.B., and R.V. Clarke (2003) "Opportunities, Precipitators and Criminal Decisions: A Reply to Wortley's Critique of Situational Crime Prevention" in Smith, M.J., and D.B. Cornish (eds.) *Theory for Practice in Situational Crime Prevention*, Monsey, NY: Criminal Justice Press, pp. 41–96.

Cornish, D.B., and R.V. Clarke (2006) "The Rational Choice Perspective" in Lanier, M.M., and S. Henry (eds.) *The Essential Criminology Reader*, Boulder, CO: Westview Press, pp. 18–30.

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

Dhillon, G., and J. Backhouse (2001) "Current Directions in IS Security Research: Towards Socio-Organizational Perspectives", *Information Systems Journal* (11), pp. 127–153.

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

Eloff, M.M., and S.H. von Solms (2000) "Information Security Management: A Hierarchical Framework for Various Approaches", *Computers & Security* (19)3, pp. 243–256.

Embar-Seddon, A. (2002) "Cyberterrorism", *The American Behavioral Scientist* (45)6, pp. 1033–1043.

Goles, T., et al. (2006) "Moral Intensity and Ethical Decision-Making: A Contextual Extension", *The DATA BASE for Advances in Information Systems* (37)2–3, pp. 86–95.

Hoffman, L.J. (1989) "Risk Analysis and Computer Security: Toward a Theory at Last", *Computers & Security* (8)23–24.

Hollinger, R.C. (1988) "Computer Hackers Follow a Guttman-Like Progression", *Sociology & Social Research* (72)3, pp. 199–200.

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

Ma, Q., and J.M. Person (2005) "ISO 17799: 'Best Practices' in Information Security Management?" *Communications of the Association for Information Systems* (15), pp. 577–591.

Mulhall, T. (1997) "Where Have All the Hackers Gone? Part 3—Motivation and Deterrence", *Computers & Security* (16)4, pp. 291–297.

Parker, D. (1998) *Fighting Computer Crime: A New Framework for Protecting Information,* New York: John Wiley & Sons, Inc.

Power, R. (1998) *Current and Future Danger*, Computer Security Institute.

Quinn, J.B., H. Mintzberg, and R.M. James (1988) *The Strategy Process: Concepts, Contexts, and Cases,* London: Financial Times Management.

Rees, J., S. Bandyopadhyay, and E.H. Spafford (2003) "PFIRES: A Policy Framework for Information Security", *Communications of the ACM* (46)7, pp. 101–106.

Rogers, M.K. (2006) "A Two-Dimensional Circumplex Approach to the Development of a Hacker Taxonomy", *Journal of Digital Investigation* (3)2, pp. 97–102.

Stoneburner, G., A. Goguen, and A. Feringa (2002) "Risk Management Guide for Information Technology Systems—Recommendations of the National Institute of Standards and Technology", NIST, Technology Administration, U.S. Department of Commerce, I.T. Laboratory, pp. 1–55.

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

Straub, D.W., and R.J. Welke (1998) "Coping with Systems Risk: Security Planning Models for Management Decision Making", *MIS Quarterly* (December), pp. 441–469.

Suh, B., and I. Han (2003) "The IS Risk Analysis Based on a Business Model", *Information & Management* (41)2, pp. 149–158.

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

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

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

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

Willison, R., and M. Siponen (2009) "Overcoming the Insider: Reducing Employee Computer Crime Through Situational Crime Prevention", *Communications of the ACM* (52)9, pp. 133–137.

Wilson, J.L., E. Turban, and M. Zviran (1992) "Information Systems Security: A Managerial Perspective", *International Journal of Information Management* (12), pp. 105–119.

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

Wortley, R. (2003) "Situational Crime Prevention and Prison Control: Lessons for Each Other" in Smith, M.J., and D.B. Cornish (eds.) *Theory for Practice in Situational Crime Prevention*, St. Louis, MO: Willow Tree, pp. 97–117.

APPENDIX 1—CASE 1 ANALYSIS

CASE OVERVIEW

Organization: "ITforYou, Inc."

Organization Type: Small Internet Service Provider (ISP)

Brief Overview of Organization: "ITforYou, Inc." is a very small business that provides Internet and information technology services (e.g. web hosting, programming, and data center services) in support of customers' business operations. They have been in business for approximately fifteen years. It is essentially a one-person company, with the exception of occasional part-time support over the years. The company's owner/manager does not have formal education, training, or certifications in information security, but has self-taught himself information security and takes it very seriously.

Prior Attacks: To the best of the owner/manager's knowledge, ITforYou, Inc. has been successfully hacked only once since the company's inception. His internal investigation disclosed that he was a target of opportunity for the hacker—the hacker scanned a wide range of systems for a specific vulnerability and hacked ITforYou, Inc. upon realizing the company site was vulnerable. The owner/manager is aware of frequent, targeted attempts to hack into the company's system by individuals who receive e-mail that they perceive to be spam, but which is actually legitimate e-mail from legitimate companies, who are customers of ITforYou, Inc.

Perceived Threats (Step 2a): ITforYou, Inc. perceives two primary threats—the opportunist seeking a target of opportunity and the anti-spam hacktivist receiving what they believe is spam from ITforYou, Inc.

Opportunist: The opportunist typically seeks systems that are vulnerable to specific exploits possessed by the attacker. The attacker is seldom seeking specific information. Rather, the attacker is seeking a storage location for their "warez," a pass-through point to facilitate other crimes, or computers that they can control (i.e., "zombies") in the furtherance of other goals (e.g., establishing communication networks and launching distributed attacks).

Anti-Spam Hacktivist: The anti-spam hacktivists attack systems for one of two reasons, usually. First, the system, or the attack of the system, may provide a "stage" from which the hacktivists can communicate their "message." Second, the hacktivists might target specific systems they believe are facilitating the dissemination of spam. The latter is the case here. In this case, the hacktivist(s) is(are) trying to send a message to the victim company, ITforYou, Inc.—"stop sending and facilitating spam." The hacktivists incorrectly believe ITforYou, Inc. is permitting and facilitating its clients to spam the hacktivists and others.

Security Measures Implemented: The primary approach to information security at ITforYou, Inc. is to "lock everything down" as much as possible and stay "below the radar" of would-be attackers. Locking down refers to

ensuring that unnecessary ports and services are unavailable, maximally restrictive firewall policies are in force, patches against vulnerabilities are diligently implemented, and an effective antivirus solution is employed. The owner/security officer asserts these actions protect company assets from external script-kiddies seeking a target of opportunity. He consciously maintains a "low profile" to minimize the risk that the company will be targeted for attacks for specific resources and/or information. The company seldom employs support staff, and those who are employed are personally known to the owner, are given limited permissions, and are not perceived to be a potential insider threat.

CASE ANALYSIS

Other Threats to Consider: None. Based on the general information provided to us, we assessed whether additional threats exist. In the case of this company, we do not see any additional threats of significance.

Application of the Offender Classification Framework (Step 2b)

Opportunists: Opportunist attackers motivated by play may victimize a vulnerable organization for any of the reasons listed above (store warez, control zombies, and/or obtain pass-through points). Those motivated by crime either seek pass-through points, or are targeting certain *types* of information and are indiscriminate about the source of the information (e.g., anyone's personal identifying information, not a specific person's identifying information). Those motivated by anti-national pursuits are most likely seeking a pass-through point. The single motivation absent is hacktivism. Hacktivists typically seek targets to send a message to the world, or to obtain information of value pertaining to the hacktivist cause. Targets of opportunity are inconsistent with the notion of obtaining specific information. They may seek targets of opportunity to send a message, but for the hacktivists' message to have a high impact, the hacked site must be prominent and have high a traffic level. ITforYou, Inc. does not have a sufficiently high profile for hacktivists with a general message to the world at large. So, we argue that the motivation of the opportunist in the case of ITforYou, Inc. is not likely to be one of hacktivism.

Opportunists can exhibit a wide variety of skill levels. Because ITforYou, Inc. believes they are well protected through vigilant security, they do not perceive low-skilled opportunists to be much of a threat. However, more highly skilled opportunists may pose a greater threat to their organization. The opportunist here is external to the organization, and such activity is not atypical of his/her day-to-day life. The criminal activity is either marginal to their daily lives, or central to it. In other words, it is more systemic than occurring solely due to provocation.

Based on this reasoning, we characterize this threat according to the framework as follows:

Offender motivation: Play, Crime, National Security (victim is a "pass-through" mechanism)
Offender skill: Medium to High
Offender–victim relationship: Outsider
Offender Involvement: Anti-social predator, Mundane

Anti-Spam Hacktivists: In this case, the hacktivist is trying to send a message specifically to the victim company, ITforYou, Inc. The company is being incorrectly perceived as facilitating spam from its clients to the hacktivist and others. We argue that the hacktivist is likely to possess medium to high levels of technical skills. Individuals with lower levels of skills are more likely to just ignore the spam, tighten their spam controls, or just complain either to ITforYou, Inc. or the client company. The offender is external to the organization and is provoked upon receiving what he/she perceives is spam.

Based on this reasoning, we characterize this threat according to the framework as follows:

Offender motivation: Hacktivism
Offender skill: Medium to High
Offender–victim relationship: Outsider
Offender Involvement: Provoked

Meso-Level Application of SCP (Step 5b): We assessed each of the five factors from SCP for their potential to help reduce the likelihood of crime by each of the two categories of identified offenders.

Opportunists

Increasing Perceived Effort: Increasing the offender's perceived effort to commit the crime will deflect hackers who are looking for a target of opportunity, because they are looking for relatively quick and/or easy targets.

Increase Perceived Risk: Risk of being caught has two elements: (1) offender apprehension and punishment, and (2) incident detection and organizational recovery. Increasing perceived risk of apprehension and punishment will probably not be very successful for a number of reasons. First, external hackers are often under the purview of other jurisdictional authorities, making apprehension and prosecution difficult, if not impossible. Second, it is a common and relatively successful tactic for attackers to "hop through" multiple compromised systems, thereby successfully disguising their original point of origin. Third, the number of cyber attack cases successfully prosecuted relative to the number of incidents is relatively low, and the severity of punishment in those cases is also low. In all, cyber offenders operate with relative impunity. Thus, increasing the perceived risk of being caught with respect to apprehension and punishment is not a particularly worthwhile approach.

However, increasing perceived risk with respect to incident detection and organizational recovery will likely deflect hackers. In many cases, opportunists desire long-term availability and access concerning the victimized system. If the attack is detected, the organization will contain, eradicate, and recover from the attack. As a result, the offender's access to the system and availability of the system's resources ends. Thus, increasing perceived risk of the incident being detected is a worthwhile approach.

Decrease Anticipated Benefits: Opportunistic hackers have no prior knowledge of the value of information in the computer system, nor the value of the system as a computing resource. Hence, it is difficult to formulate mechanisms to alter their perception of the value of information assets in the system, or of the utility of the system as a computing resource.

Reducing Justification: Hackers who are motivated by the crime or anti-national activity do not engage in rationalization, because the criminal activity is central to their life as predatory offenders. In the case of hackers who are motivated by play, justification would be relevant to consider. However, we contend that changing this perception will be difficult, and influencing their perception of the effort required and/or risk of incident detection will be much easier. Thus, while this SCP category is potentially applicable, it is not recommended.

Reducing Provocation: The hackers in this category are not being provoked. So, the issue of reducing provocation does not arise.

Anti-Spam Hacktivists

Increasing Perceived Effort: In this case, hacktivists are not likely to be dissuaded by increasing perceived effort. They are skillful and have a message to deliver specifically to ITforYou, Inc. So, the hackers are likely to be persistent. Given that they are skillful, risk from this source will continue despite strong technical defenses.

Increasing Perceived Risk: Again, risk of being caught has two elements: (1) offender apprehension and punishment, and (2) incident detection and organizational recovery. Since the hacktivist desires to send a message to ITforYou, Inc., the hacktivist *wants* to be detected. Thus, increasing perceived risk of incident detection is not applicable in this case. Theoretically, increasing perceived risk of offender apprehension and punishment is applicable, but for the same reasons as for the opportunist, the offender is unlikely to believe that apprehension is likely, and will be even less likely to fear probable punishment(s).

Decreasing Anticipated Benefits: The primary benefit that the hacker is seeking is the cessation of the alleged spam. Self-gratification from retribution might be a secondary anticipated benefit. For this SCP category to be useful in influencing offender decision making, the organization must make the hacktivist believe that attacking them will *not* result in the cessation of the alleged spam, nor will it bring them satisfaction from retribution. Given the offender's probable skill level, we do not believe the organization can effectively convince him of either reduced benefit.

Decreasing Justification: The hacker justifies their behavior by rationalizing that he/she needs to send a message to the company that engages in the unethical practice of spam. If situational manipulations could remove (or lessen) the hacktivist's ability to rationalize and justify their actions, they would likely be dissuaded from attacking. This might be accomplished by website notices that: (1) explain ITforYou's zero-tolerance policy for spamming, (2) explain that e-mails from specific clients are not spam and are sent out as part of legitimate marketing campaigns using e-mail addresses legally obtained (e.g., supplied by the recipient or contained in legally purchased marketing/mailing lists).

Decreasing Provocation: The alleged spam is the provocation. Removing, lessening, or reversing the provocation will dissuade the offender from attacking. In this case, this can be accomplished if the hacker is able to understand why the e-mail is not spam, but a message of potential use, or, if the e-mails are stopped. This can be accomplished by (a) providing means for the individual to be taken off the mailing list, and/or (b) affording the individual a mechanism to inquire why the message is being sent to him/her. These actions will either cause the e-mails to no

longer be seen as spam, or to cease. In either case, the provocation will cease to exist, and consequently there will be no more hacking.

In summary**,** our analysis suggests that increasing the effort, and increasing the risk, of detection are approaches to influence the opportunists' perception of the crime opportunity, and, reducing justification and reducing provocation are two approaches to influence the hacktivists' perception of the crime opportunity.

Countermeasure Identification (Step 5c): This discussion does not include countermeasure identification, because the focus of our research is information security strategy development, not operational level countermeasure identification.

APPENDIX 2—CASE 2 ANALYSIS

CASE OVERVIEW

Organization: "MoneyCo."

Organization Type: Large Financial Services Company

Brief overview of Organization: "MoneyCo." is a large business that provides financial services (e.g., payment services, check manufacturing, and financial marketing services) to customers—both individuals and companies. Because of the nature of their business, they possess important personally identifying information (PII) and confidential financial data that can be criminally exploited (e.g., for identity theft and financial fraud). MoneyCo. has a well-qualified Chief Information Security Officer (CISO) and a highly skilled information security team.

Prior Attacks: MoneyCo. states they have fallen victim to a wide variety of attacks and attackers over the years, but indicates the frequency of incidents is low. They did not provide additional information regarding the attacks, but instead focused on characterizing the attackers involved in the attacks.

Perceived Threats (Step 2a): MoneyCo. perceives two primary threats—the financial fraudster and the recreational hacker. It could be argued that the opportunist is a threat to *any* organization, however, MoneyCo.'s risk assessment did not identify that threat as a significant risk, due to its highly vigilant and strong security posture.

Financial Fraudster: This offender is part of the growing criminal industry of identity theft and online financial fraud. To facilitate their crimes, this offender seeks PII and access to financial information and systems. This offender is a threat to organizations, because PII theft is subject to regulatory oversight, and can lead to financial liability, loss of customer confidence, bad publicity, and lost revenue. This is currently MoneyCo.'s highest risk threat.

Recreational Hacker: The recreational hacker is motivated by "play." The offender targets MoneyCo. out of pure mischief, curiosity, and challenge. Here the value to the hacker is the thrill and possible accolades of successfully hacking a large, well-known company. This used to be their highest risk human threat, but is currently considered to be a relatively low-risk threat relative to the financial fraudster threat.

Security Measures Implemented: MoneyCo. has formally dedicated manpower and monetary resources toward the identification and assessment of risks to its information security. They have a multifaceted security program, which includes technical, formal, and informal controls. Their program also incorporates a wide range of security assessments and audits, including internal vulnerability assessments, patch compliance reviews, strict configuration management controls, external audits, and reviews of policies, processes, and procedures. MoneyCo. consciously attempts to stay "below the radar" of would-be attackers, so as to not call attention to themselves, their information, and their resources.

CASE ANALYSIS

Other Threats to Consider: None. Based on the general information provided to us, we assessed whether additional threats exist. In the case of this company, we do not see any additional threats of significance.

Application of the Offender Classification Framework (Step 2b)

Financial Fraudster: Because the financial fraudsters' goal is criminal—identity theft and/or financial fraud—their motivation is clearly "crime." They could be internal or external to the organization, but MoneyCo. is particularly

concerned about the external threat. The financial fraudsters, who have chosen cyber space as the environment for their criminal activity, are probably technically skilled, else they would have chosen to operate in the non-cyber environment. Externally situated financial fraudsters are likely engaging in such activity as a way of making a living. Based on this reasoning, we characterize this threat according to the framework as follows:

Offender motivation: Crime
Offender skill: Moderate to High
Offender–victim relationship: Outsider
Crime Involvement: Anti-social predator

Recreational Hacker: Because the recreational hackers' end-goal is not criminal, and because they target organizations out of curiosity or for a challenge, their motivation is clearly "play." Recreational hackers can exhibit a wide variety of skill levels, but because MoneyCo. believes they are well protected through vigilant security, they do not perceive low-skilled hackers to be much of a threat. The recreational hackers here are external to the organization, as internal employees engaging in recreational hacking would not likely target their own organization for fear of detection and punishment. Hacking is not central to the day-to-day life of the recreational hackers, nor does it require provocation. Based on this reasoning, we characterize this threat according to the framework as follows:

Offender motivation: Play
Offender skill: Medium to High
Offender-victim relationship: Outsider
Crime Involvement: Mundane

Meso-Level Application of SCP (Step 5b): We assessed each of the five factors from SCP for their potential to help reduce the likelihood of crime by each of the two categories of identified offenders.

Financial Fraudsters

Increasing Perceived Effort: On the one hand, moderately to highly skilled offenders will not be deterred by increases in the perceived effort required, because they believe they can overcome things that alter this perception (i.e., target hardening mechanisms). On the other hand, MoneyCo. is concerned with the financial fraudster who seeks PII and financial data in general, not that of someone in particular. So, in a sense, the offender seeks targets of opportunity within a certain class of targets—those storing PII and financial data. Accordingly, increasing the offender's perceived effort to commit the crime will deflect financial fraudsters, because they are looking for relatively quick and/or easy targets.

Increased Perceived Risk: Risk of being caught has two elements: (1) offender apprehension and punishment, and (2) incident detection and organizational recovery. Increasing perceived risk of apprehension and punishment will probably not be very successful for a number of reasons. First, external hackers are often under the purview of other jurisdictional authorities, making apprehension and prosecution difficult, if not impossible. Second, it is a common and relatively successful tactic for attackers to "hop through" multiple compromised systems, thereby successfully disguising their original point of origin. Third, the number of cyber attack cases successfully prosecuted relative to the number of incidents is relatively low, and the severity of punishment in those cases is also low. In all, cyber offenders operate with relative impunity. Thus, increasing the perceived risk of being caught with respect to apprehension and punishment is not a particularly worthwhile approach.

However, increasing perceived risk with respect to incident detection and organizational recovery will likely deflect financial fraudsters. In the case of identity theft, offenders often wish to "use" the identity for some period of time to obtain maximum benefit from the false ID. With respect to financial fraud, offenders may seek only short-term access to financial data (e.g., credit card information), so as to minimize the risk of being apprehended (i.e., repeated use increases the chances of being caught). Other times, they may seek long-term access, so as to gain maximum benefit from the access and/or data (e.g., embezzle small amounts of money over a long period of time to minimize suspicion, but maximize benefit). In any case, if the organization can detect and respond to such compromised data quickly, continued utility of the data might be lessened. For instance, if a credit card is stolen and the theft is known, the credit card number can be deactivated. Similarly, one benefit of a social security number lies in its use in acquiring additional credit cards. Thus, if a social security number is stolen, then steps can be taken to register with credit agencies to monitor if unauthorized requests for credit cards are being made. These mechanisms lessen the utility of the information upon incident detection. Thus, increasing the perception of the risk of incident detection is a worthwhile approach.

Reducing Anticipated Benefit: The anticipated benefits of the financial fraudster include: (1) utility of stolen information in furtherance of identity theft and financial fraud schemes, and/or (2) access to key financial systems to divert funds for their personal use. For this SCP category to be useful in influencing offender decision making, the organization must make the offender believe that the utility of the information and/or system access is limited. To do this, the organization might encrypt all PII with very strong encryption (via algorithms the likely offenders are not able to break) and "advertise" such policies. In sum, decreasing anticipated benefit is a worthwhile approach.

Reducing Justification: Generally, financial fraudsters are seasoned criminals (or criminal organizations), who do not seek to rationalize their behavior. Their behavior is predatory, and thus does not require internal moral justification, per se. So, measures to reduce justification are not meaningful.

Reducing Provocation: There is no provocation. MoneyCo.'s strategy is to stay below the radar, and hence this is not an issue. Financial fraudsters are not being provoked. So, the issue of reducing provocation does not arise.

Recreational Hacker

Increasing Perceived Effort: Increasing perceived effort required to successfully hack MoneyCo. will increase the intellectual challenge to the recreational hacker. The increased challenge will motivate many recreational hackers to continue hacking, rather than dissuade them. Thus, attempts to increase the perceived effort of the "play" hacker will most likely be counterproductive.

Increasing Perceived Risk: For reasons already stated, the recreational hacker is not likely to perceive the threat of apprehension and punishment as high, regardless of situational manipulations. The perceived risk of being caught with respect to incident detection is also inconsequential, because the recreational hacker is not after long-term information and/or system use. Thus, efforts to increased perceived risk are not applicable in this instance.

Reducing Anticipated Benefit: The primary benefits to the recreational hacker are ego gratification (i.e., to have bragging rights) and increased knowledge and skill. For this SCP category to be useful in influencing offender decision making, the organization must make the offender believe that attacking them will not gratify their ego, nor will it "teach" them anything. We contend that changing this perception will be difficult, thus reducing anticipated benefits is not a particularly worthwhile approach in this instance.

Reducing Justification: Since play hackers do not plan to misuse any information that they may gain access to, they often rationalize their behavior as being harmless. Past research has suggested that people often perceive a lesser ethical problem with activities in cyber space, due to moral distancing issues and a decreased perception of situational moral intensity in cyber space [Goles et al., 2006]. Thus, situational manipulations that reduce an offender's ability to rationalize the crime as being harmless might prove worthwhile.

Reducing Provocation: The hackers in this category are not being provoked. So, the issue of reducing provocation does not arise.

In summary, our analysis suggests that increasing the effort, increasing risk, and decreasing anticipated benefit are approaches to influence the financial fraudsters' perception of the crime opportunity, and, reducing justification and reducing provocation are two approaches to influence the recreational hackers' perception of the crime opportunity.

Countermeasure Identification (Step 5c): This discussion does not include countermeasure identification, because the focus of our research is information security strategy development, not operational level countermeasure identification.

APPENDIX 3—CASE 3 ANALYSIS

CASE OVERVIEW

Organization: "EduISD"

Organization Type: Moderately-sized, K–12, Independent School District (ISD)

Brief overview of Organization: "EduISD" is a moderately sized independent school district. It serves a combined user community consisting of 3,000 students (kindergarten through high school), faculty, and staff. In the past, their only information security concern was system/resource availability. In recent years, their conceptualization of information security and capability to achieve it has matured to include concerns about access control, information confidentiality, and data integrity. In particular, they must protect PII, student grades (both from a privacy and integrity point of view), and student enrollment in social service programs. The Assistant Technology Director (#2 IT position for the ISD) is responsible for information security and feels that the ISD administration, all the way up to the Superintendent, places a very high importance on information security. This is contrasted, however, with an unsupportive user base—the staff, faculty, and students simply do not understand the need for information security and express concerns that it interferes with their job productivity.

Prior Attacks: To the best of EduISD's knowledge, they have not fallen victim to any external attacks by individuals unconnected with the school. In contrast, they fall victim to insider attacks by students quite frequently. (We define *insider* as users with authorization to access all or part of the information technology resources. Students are allowed access to academic computing, and, hence, can be considered users with authorization to part of the IT services of the organization.) The attacks have involved changing academic grades, as well as less serious "play" attacks by curious and mischievous students.

Perceived Threats (Step 2a): EduISD perceives two primary threats—grade changers and internal script-kiddies.

Grade Changers: Of the greatest concern to the ISD are high school students who are receiving failing course grades. They have a high number of incidents, in which students gain unauthorized access to electronic grade books and change their course grades. Incidents are facilitated largely by lackadaisical faculty and staff members who leave their computing resources unprotected (i.e., logged in, physically absent, with grade-book applications open). Such incidents are also accomplished by technically savvy, moderately skilled students who are able to gain unauthorized access in the more traditional sense (i.e., hacking).

Script-Kiddies: Another insider threat faced by EduISD is the student "script-kiddie." These students are motivated by "play," are relatively unskilled, and are mundane offenders. They are not provoked to attack and are not necessarily predisposed to continuous criminal activity, but rather seize opportunities to "see if they can do it" and see if the school will notice. They are motivated by a sense of curiosity and general mischief.

Security Measures: EduISD's approach to information security is informal, unstructured, and consists primarily of technical controls, such as host-based intrusion detection, host-based firewalls, antivirus solutions, and content filtering. Formal controls are limited to rule-based access controls and acceptable use policies. Informal controls are limited to brief education and awareness presentations during annual teacher in-service training. They are further protected by the nature of the state's network architecture and infrastructure. The state provides network connectivity to ISDs through their regional service centers, which are apparently well protected via formal, mature, and multi-faceted information security programs. In other words, external access to ISD resources is protected not only by ISD-level information security measures, but also (and first) by regional education service center information security measures.

CASE ANALYSIS

Other Threats to Consider: It should be recognized that grade changing may be done by a skillful surrogate, i.e., most likely, a skillful student who is paid to change the grade of a not-so-skillful student.

Application of the Offender Classification Framework (Step 2b)

Grade Changer: This offender seeks unauthorized access to ISD information systems for the purpose of compromising the integrity of academic grade information. The student changing his own grade may very well have a low skill level, whereas the surrogate grade changer might be moderately to highly skilled. In either case, the

offender is internal to the organization and is provoked by the environmental stress of an impending failing grade (and monetary incentive in the case of a surrogate grade changer). Based on this reasoning, we characterize this threat according to the framework as follows:

Offender motivation: Crime
Offender skill: Low to High
Offender-victim relationship: Insider (student)
Crime Involvement: Provoked

Script-kiddie: The script-kiddie is the student seeking unauthorized access to ISD information systems out of curiosity and mischief. EduISD has not found such threats to be particularly highly skilled. Their behavior is neither provoked, nor central to their daily life. Instead, it is something fun and interesting to do. Based on this reasoning, we characterize this threat according to the framework as follows:

Offender motivation: Play
Offender skill: Low to Moderate
Offender-victim relationship: Insider (student)
Crime Involvement: Mundane

Meso-Level Application of SCP (Step 5b): We assessed each of the five factors from SCP for their potential to help reduce the likelihood of crime by each of the two categories of identified offenders.

Grade Changers

Increasing Perceived Effort: Minimally skilled offenders will likely be dissuaded from the attack, because they will determine either that success is unlikely or that it is not worth the effort. Some students are failing because of laziness on their part, thus if grade changing is a difficult task, they will likely not perceive it as an opportunity. It is currently perceived as an opportunity, because it is so easy to do when faculty are not security-minded and leave their electronic grade books open and unattended. While it will likely dissuade highly skilled, surrogate grade-changers less, increasing perceived effort required will have some impact. If it appears to require more effort, the price commanded for the grade-change activity will increase—potentially to the point of deterring the attack.

Increasing Perceived Risk: Risk of being caught has two elements: (1) offender apprehension and punishment, and (2) incident detection and organizational recovery. Increasing perceived risk of apprehension and punishment will probably not be very successful in this case, because EduISD has a long history of poorly enforcing rules and very minimal punishments. Furthermore, the student was failing before the attack anyway, so other punishments (e.g., suspension or expulsion) are not likely to be highly influential to this offender. They may be to the surrogate grade changer, but again punishment is neither certain, nor severe in EduISD.

The risk of incident detection is of much greater consequence in this instance. The presumption is, like in the case of MoneyCo., that detection limits attack utility. In this case, if the grade change is detected, then a reversal is possible, thus denying the offender the benefit of the grade change. This is the case with both the grade changer and his surrogate, thus increasing the perception of the risk of incident detection is a worthwhile approach in this instance.

Reducing Anticipated Benefit: The benefit accruing to the “failing student” (the changed grade) is the primary benefit of the crime. For this SCP category to be useful in influencing offender decision making, the organization must make the offender believe that the changed grade will not stand. Once detected, if proper records are available, it is relatively easy to correct the grades and undo the benefit. One approach is to institute procedures to regularly verify if the grades have been changed without authorization. Given the importance of the anticipated benefit to the offender’s motivation, mechanisms that reduce anticipated benefit should be considered in this instance.

Reducing Justification: EduISD does not believe students who gain unauthorized access to change their grades rationalize their behavior, at least not in the sense of making it psychologically acceptable behavior. They rationalize that it’s better than failing a course, but they do not rationalize that somehow their behavior is excusable. As such, EduISD does not believe that situational manipulations aimed at removing excuses is called for in this situation.

Reducing Provocation: Normally, reducing provocations would be a very applicable SCP technique to deterring provoked offenders from committing crimes. However, in this case, the provocation is an environmental stress (a failing course grade) caused by the student’s academic performance. While replacing an earned failing grade with a passing grade would indeed reduce the offender’s sense of provocation, thereby deterring the offense, it is not an acceptable solution. Thus, reducing provocation is not applicable in this instance.

Script-Kiddies

Increasing Perceived Effort: The low-skilled 'play' offender, does not have sufficient technical skills to get past higher levels of defenses. They are motivated more by mischief, than curiosity, or challenge. Thus, increasing the perceived effort required will dissuade them from attacking.

Increasing Perceived Risk: For reasons already stated, the script-kiddie is not likely to perceive the threat of apprehension and punishment as high, regardless of situational manipulations. The perceived risk of being caught with respect to incident detection is also inconsequential, because the script-kiddie is not after long-term information and/or system use. Thus, efforts to increased perceived risk are not applicable in this instance.

Decreasing Anticipated Benefit: The benefit to the script-kiddie is the thrill of breaking in. For this SCP category to be useful in influencing offender decision making, the organization must make the offender believe that successfully attacking them will not net such a feeling. We contend that changing this perception will be difficult, thus reducing anticipated benefits is not a particularly worthwhile approach in this instance.

Reducing Justification: Since play hackers do not plan to misuse any information to which they may gain access, they often rationalize their behavior as being harmless. Past research has suggested that people often perceive a lesser ethical problem with activities in cyber space, due to moral distancing issues and a decreased perception of situational moral intensity in cyber space [Goles et al., 2006]. Thus, situational manipulations that reduce an offender's ability to rationalize the crime as being harmless might prove worthwhile.

Reducing Provocation: The hackers in this category are not being provoked. So, the issue of reducing provocation does not arise.

In summary, our analysis suggests that increasing the effort, increasing risk, and decreasing anticipated benefit are approaches to influence the grade changers' perception of the crime opportunity, and, increasing effort and reducing justification are two approaches to influence the script kiddie's perception of the crime opportunity.

Countermeasure Identification (Step 5c): This discussion does not include countermeasure identification , because the focus of our research is information security strategy development, not operational level countermeasure identification.

ABOUT THE AUTHORS

Nicole Lang Beebe (nicole.beebe@utsa.edu) is an Assistant Professor in the Department of Information Systems & Technology Management, at the University of Texas at San Antonio (UTSA). UTSA a National Center of Academic Excellence in Information Assurance for both education (CAEIAE) and research (CAE-R). Dr. Beebe received her Ph.D. in Information Technology from UTSA. She has over ten years experience in information security and digital forensics, from both the commercial and government sectors. She has been a Certified Information Systems Security Professional (CISSP) since 2001. She has published several journal articles related to information security in digital forensics in *The DATABASE for Advances in Information Systems, Digital Investigation,* and *Journal of Information System Security (JISSEC).* Her research interests include digital forensics, information security, and data mining.

V. Srinivasan (Chino) Rao (chino.rao@utsa.edu) is an Associate Professor in Information Systems at the University of Texas at San Antonio. He obtained his Ph.D. from the University of Texas at Austin. His areas of research interest include electronic commerce and behavioral issues in computer security. He has published in leading academic journals, such as *MIS Quarterly, Management Science,* and *Group Decision and Negotiation.*

Communications of the Association for Information Systems

ISSN: 1529-3181