Information Systems Research
Vol. 20, No. 1, March 2009, pp. 121–139
ISSN 1047-7047 | EISSN 1526-5536 | 09 | 2001 | 0121

DOI 10.1287/isre.1080.0174

Choice and Chance: A Conceptual Model of Paths to Information Security Compromise

Sam Ransbotham
Carroll School of Management, Boston College, Chestnut Hill, Massachusetts 02467,
sam.ransbotham@bc.edu

Sabyasachi Mitra
College of Management, Georgia Institute of Technology, Atlanta, Georgia 30308,
saby.mitra@mgt.gatech.edu

No longer the exclusive domain of technology experts, information security is now a management issue. Through a grounded approach using interviews, observations, and secondary data, we advance a model of the information security compromise process from the perspective of the attacked organization. We distinguish between deliberate and opportunistic paths of compromise through the Internet, labeled *choice* and *chance*, and include the role of countermeasures, the Internet presence of the firm, and the attractiveness of the firm for information security compromise. Further, using one year of alert data from intrusion detection devices, we find empirical support for the key contributions of the model. We discuss the implications of the model for the emerging research stream on information security in the information systems literature.

Key words: information security management; computer crime; information systems risk management
History: Ritu Agarwal, Senior Editor; Anandhi Bharadwaj, Associate Editor. This paper was received on May 10, 2006, and was with the authors 9 months for 2 revisions. Published online in *Articles in Advance* June 20, 2008.

1. Introduction

With the growing importance of information security in the current environment, there has been increased interest in the topic in the academic literature. The vast technical literature, especially in the computer science area, has focused on the development of technologies to secure computer systems, such as secure networking protocols (DiPietro and Mancini 2003), intrusion detection techniques (Ning et al. 2004), database security methods (Sarathy and Muralidhar 2002), and access control technologies (Sandhu and Samarati 1996). Sociologists have studied the computer hacker community, investigating issues such as hacker motivation (Voiskounsky and Smyslova 2003), hacker actions (Embar-Seddon 2002), and typical hacker profiles (Halbert 1997). From an economics perspective, researchers have examined the cost-benefits of information security (Gordon and Loeb 2002), optimal models for vulnerability disclosure (Arora et al. 2004, Kannan and Telang 2005), and the impact of security breaches on the market value of the firm (Cavusoglu et al. 2004).

At the same time, the trade literature emphasizes that information security is not merely a task for technical professionals sequestered behind computer screens. A common theme is that "security . . . starts at the top, not with firewalls, shielded cables, or biometrics" (Dutta and McCrohan 2002, p. 67). Similarly, there is a growing trend of senior executive involvement in computer security (Lohmeyer et al. 2002). Recognizing its importance, recent regulations such as Sarbanes-Oxley (Schultz 2004) and the Health Insurance Portability and Accountability Act[1] (Speers et al. 2004) provide penalties for failing to address security considerations. Clearly, information security has moved closer to the top of the management agenda.

Consequently, a new perspective on information security, that we term the organizational perspective, is emerging in the information systems (IS) literature. The organizational perspective focuses on

[1] Both Sarbanes-Oxley and HIPAA specify that management is ultimately responsible for the security, accuracy, and privacy of information relating to corporate financial records and individual health records, respectively.

the managerial processes that control the effective deployment of technical solutions, tools, resources, and personnel to create a secure computing environment in an organization. The perspective is that of business managers charged with securing the information technology (IT) assets of the enterprise. In this perspective, technical solutions are important, but the focus is on managerial actions that promote a secure information environment.

Early work on information security in the IS area identified the managerial challenges in implementing security (Boockholdt 1989), the effectiveness of security countermeasures (Straub 1990), discovering and disciplining IS abuse (Straub and Nance 1990), the unique threats that exist in a networked environment (Loch et al. 1992), and security methods in systems development (Baskerville 1993). More recent research has focused on employee attitudes toward computer ethics (Banerjee et al. 1998, Harrington 1996), the characteristics of workers involved in IS abuse (Gattiker and Kelley 1999), and security planning models (Straub and Welke 1998). Dhillon and Backhouse (2001) provide a synthesis of this research stream.

Even though information security has been consistently identified at the top of the IS agenda (Brancheau et al. 1996), research on the organizational perspective is limited but emerging. Consequently, we focus this paper on the organizational perspective of information security. Our purpose is to develop a conceptual model of the information security compromise process (ISCP) from the perspective of the target organization, and to validate empirically some of the key elements of the model. We conduct the research in two phases. First, we use a grounded approach (Glaser and Strauss 1967) that utilizes interviews, observations, web searches, and document reviews to identify the constructs relevant to the ISCP, and propose a conceptual model that links the constructs into paths to information security compromise. Second, we utilize a large data set of information security alerts to validate some of the key concepts of our grounded model. The alert data is generated by placing sensors within the corporate networks of several hundred clients of a managed security service provider (MSSP).

Our model and empirical findings articulate three important and related concepts. First, attacks are part of a process rather than a single event because they build on each other. Second, the ISCP has two distinct paths (deliberate and opportunistic) that have different antecedents and characteristics, but merge with the opportunistic path leading to the deliberate path. Finally, organizational countermeasures play a moderating rather than a direct role to deter the progression of attacks in each path. Specifically, we argue that some countermeasure practices (e.g., vulnerability patching) are most effective in the early stages of the ISCP, while other practices (e.g., traffic filtering) are more effective during the later stages.

There are two broad contributions of this research to the emerging literature on the organizational perspective of information security. First, at this early stage of empirical research in this area, a conceptual model that identifies the main constructs and their interrelationships is central to the development of a research stream that can ultimately influence practice (Whetten 1989). Such a model builds a cumulative tradition of knowledge and integrates empirical research into a cogent and comprehensive whole, rather than a piecemeal effort (Weber 2002, Zmud 1998). Moreover, the process perspective underlying our conceptual model allows us to categorize attacks in a manner that highlights their progression to information security compromise. This provides for a finer-grained analysis of the role of countermeasures at various stages of the process, and clarifies the role of antecedents. Empirical research on the efficacy of countermeasures and the impact of antecedents is a crucial missing element in the literature on information security (Dhillon and Backhouse 2001, Siponen 2005). A conceptual model provides guidance in developing empirical constructs and evaluating their nomological validity.

Second, our analysis of alert data provides insights to IS researchers that can lead to a more detailed analysis of this important data source. Similar data sets have been used in the computer science literature to analyze attack characteristics from a technical perspective (Kemmerer and Vigna 2002). However, the primary goals have been to develop methods for efficient handling of alert data through aggregation (Julisch 2003, Ning et al. 2004), and to develop automated data mining tools for identifying attacks in progress (Dickersen et al. 2001). We are unaware of research using alert data to validate a conceptual

Table 1 Criminology Perspectives and the ISCP

Theoretical perspective	Summary and references	Relevance for the ISCP context	Limitations for the ISCP context
Rational choice and related theories	Criminals are rational individuals who weigh the cost-benefits of criminal activity. Crime decreases with "target hardening" or with increasing negative consequences. Cohen and Felson's routine activities theory views motivated offenders, suitable targets, and the absence of capable guardians as prerequisites of crime. Cohen and Felson (1979), Ehrlich (1996)	Organizational countermeasures "harden" targets and reduce information security attacks.	Anonymity, proliferation of tools, and difficulty of enforcement reduces the cost of crime in the Internet context, reducing the applicability of a cost-benefit approach.
Social learning, subculture, and labeling theories	Criminal behavior is learned through association and social interaction with others, as in Sutherland's theory of differential association, Aker's theory of social learning, or Cohen's subculture of delinquency theory. Labeling of individuals as deviants reinforces behavior. Sutherland (1947), Akers et al. (1979), Cohen (1955)	The "hacker" subculture provides tools and motivation, defines target attractiveness, and impacts attacker behavior.	The disparate groups involved in information security attacks make it difficult to identify them, understand their methods, or identify a single subculture.
Social control theories	Social control theories focus on strategies that reinforce compliance with the rules of society and thereby reduce crime, such as Gottfredson and Hirschi's low self-control theory and Braithwaite's reintegrative shaming theory Gottfredson and Hirschi (1990), Braithwaite (1989)	Control the external environment through formal and informal regimes such as laws, sharing information, and public relations.	Attacker anonymity and lack of enforcement in the ISCP context limit the applicability of social control theories.
Victim theories	Many authors, especially in the racial, sexual, and child abuse contexts where repeat victimization is common, have implicitly or explicitly argued that victimization should be conceptualized as a process rather than a single event. Bowling (1993), McShane and Williams (1997)	The view of crime as a process rather than a single event fits with the ISCP.	The process of victimization in the contexts studied is distinct from the process of information security compromise.
Organizational crime theories	White-collar crime encompasses a wide range of illegal or unethical practices by individuals with high social status on behalf of a firm or against an organization. Theories focus on the coincidence of motivation and opportunity for criminal behavior. Coleman (1987), Sutherland (1947)	Similarities in motivation, e.g., financial gain, identity with subcultures, and conforming with perceived norms.	Primary focus on occupational crime committed by persons connected with the firm in the course of their normal occupation.

model of the attack process developed from the perspective of a target organization.

The rest of this paper is organized as follows. Section 2 briefly describes the research methodology. Section 3 discusses the results of interviews, observations, and document reviews, and presents our conceptual model. Section 4 describes the analysis of alert data to validate empirically the key concepts in our model. Section 5 concludes the paper and outlines its implications for future research.

2. Research Methodology and Conceptual Model

Theoretical Perspectives

A vast literature in sociology, criminology, and economics provides various theories and perspectives on crime and its consequences. A comprehensive review of this literature clearly is beyond the scope of this research; instead, we focus on the relevance and limitations of the traditional theories in the context of the ISCP (Table 1).

Theories that are related to rational choice view crime as an economic phenomenon with rational criminals who weigh the cost-benefits of criminal activity (Ehrlich 1973, 1996). The distinguishing feature of this literature is the attempt to study criminal behavior through the familiar tools of equilibrium analysis (Ehrlich 1996). In a similar vein, routine activities theory (Cohen and Felson 1979) identifies three prerequisites for criminal activity—motivated offenders, suitable targets, and the absence of capable guardians to protect targets. These theories emphasize countermeasures in reducing the incidence of crime by hardening targets or raising negative consequences.

However, anonymity, proliferation of tools, and the difficulties in enforcement have reduced the cost of crime significantly in the Internet context.

A large class of theories in criminology, such as the theory of differential association (Sutherland 1947), the theory of social learning (Akers et al. 1979), and subculture theories (Cohen 1955) proposes that criminal behavior is learned through association with others. Such learning occurs within intimate personal groups and involves learning both the detailed techniques of committing the crime as well as a general attitude that views the crime favorably. In the context of the ISCP, these theories emphasize the importance of the hacker subculture in influencing attacker behavior and providing motivation and tools, but the disparate groups involved in attacks makes it difficult to identify and understand these subgroups.

Social control theories focus on strategies to reinforce compliance with the rules of society (Braithwaite 1989, Gottfredson and Hirschi 1990). These theories often focus on laws and other formal control systems, but also emphasize informal bonds that tie individuals to societal norms. The applicability of these theories is limited in the ISCP context because of the difficulties in the enforcement of laws, the anonymity of the criminal, and the diversity of possible attackers.

To aid in understanding its dynamics and temporal evolution, theories that focus on the victim rather than the criminal often advocate that victimization should be conceptualized as a process rather than a single event (Bowling 1993, McShane and Williams 1997). The contexts that are studied include racial, sexual, and child abuse where repeat victimization is the norm. However, while these theories emphasize the process of victimization, because the process is dependent on the context, the identified processes cannot be readily applied in the ISCP context.

Theories of organizational crime typically focus on white-collar crime (Sutherland 1947) committed by individuals of high social status on behalf of or against an organization. Theories of white-collar crime focus on the coincidence of motivation and opportunity as an explanation for criminal behavior (Coleman 1987). There are similarities in motivation with the ISCP context such as personal enrichment, conforming to the norms of a subculture, and rationalization of criminal behavior by deviating blame (Coleman 1987). However, white-collar crime theories focus on occupational crime that is committed by persons connected with the firm in the course of their normal occupation, limiting its relevance to the anonymous environment of the ISCP.

Unique Characteristics of the Information Security Environment

Three specific differences between the ISCP and the general crime context highlight the need for a conceptual model that draws from previous literature, but also takes into account the unique characteristics of the ISCP environment (Whetten 1989). The first difference lies in the difficulty with enforcement of laws in the ISCP context. The anonymity provided by the Internet, the physical remoteness of the attacker, and the subsequent challenges of multijurisdictional coordination of enforcement alter relationships borrowed from traditional criminology such as the impact of punishment in classical criminology (Ehrlich 1996), or shame in Braithwaite's reintegrative shaming theory (Braithwaite 1989). The second difference is that the reach of the Internet has led to the wide distribution of automated tools for attacking information resources and to a wide variety of people involved in the attack process. Consequently, target firms face a constant barrage of incidents where the attacker is merely relying on chance to find and exploit vulnerability (Willison 2002). The factors that drive such random incidents are different from those that drive the more deliberate incidents that have been the focus of traditional criminology. The third difference lies in the perspective, which in the case of the ISCP is that of the target organization. While the criminology literature has extensively examined the victimization process in contexts such as racial, sexual, and child abuse where repeat victimization is common (McShane and Williams 1997), the ISCP is obviously distinctive in terms of the stages and progression of attacks, leading to a distinct set of constructs and processes.

Grounded Research Method

We develop the conceptual model of the ISCP through the iterative investigation of four primary sources of information: (1) observations of MSSP operations,

Table 2 Combining Data Sources Through the Grounded-Theory Approach

Data source	Observations	Interviews	Document reviews	Discussion groups
Details	Observation of activities at an MSSP data center	Interviews with 30 IS security experts from 8 target firms	Review of security guidelines from multiple organizations	Review of over 150 postings on hacker motivation/operations
Theoretical sampling—Choosing data sources based on the needs of the emerging theory				
Rationale for use of data source	An MSSP faces a wide range of security alerts due to a diverse client base	Security experts can provide details of the attack process from the target viewpoint	Guidelines represent best practices in organizational countermeasures	Efficient and nonintrusive way to reach persons who attack computer systems
Comparative method—Comparing new data with emerging theory and assessing fit				
Open coding Identifying constructs	Compared MSSP reactions to security alerts to classify security incidents	Analyzed expert responses to identify constructs that affect security compromise		
Axial coding Identifying associations	Observations and interviews provided the relationships between high-level constructs (Internet presence, 2×2 attack typology. Countermeasures, attractiveness)			
Selective coding Identifying construct dimensions			Compared security guidelines to identify the dimensions of organizational countermeasures	Compared postings to identify the dimensions of attractiveness and presence
Outcome of the grounded process				
Resulting model elements	Four types of attacks—attack scans, info scans, targeted probes, and targeted attacks. The other major constructs—countermeasures, Internet presence, and attractiveness		The complete conceptual model in Figure 2 with the dimensions of each construct.	

(2) interviews with information security experts, (3) reviews of postings in Internet discussion groups to understand attacker motivation and modus operandi, and (4) reviews of IS security-related guidelines and best practices from industry organizations. Table 2 describes the grounded process we followed in developing the conceptual model (Corbin and Strauss 1990, Glaser and Strauss 1967). The table shows the data sources and the rationale for their use (theoretical sampling), the method followed in identifying the constructs (open coding), their relationships (axial coding), and their dimensions (selective coding), as well as the resulting model elements.

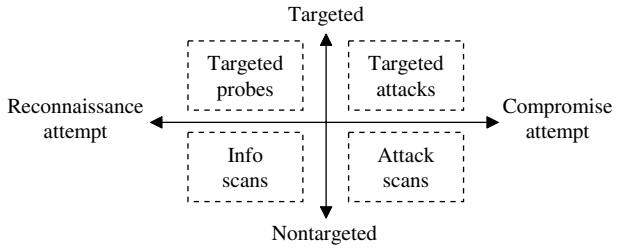
3. A Conceptual Model of the ISCP

A Typology of Security Incidents

The computer science literature provides methods for classifying attacks based on the specific technical vulnerabilities that the attack seeks to exploit. In a comprehensive taxonomy, Chakrabarti and Manimaran (2002) identify four basic categories: domain name system (DNS) hacking, route table poisoning, packet mistreatment, and denial of service attacks. Howard (1998) provides a results-oriented classification scheme that also identifies four basic categories: corruption of information, disclosure of information, theft of service, and denial of service. Other similar classifications appear in DeLooze (2004) and Kemmerer and Vigna (2002).

To generate a parsimonious conceptual model, we employed a pragmatic reduction (Bailey 1994) of the attack categories in the literature by abstracting to two dimensions that were of relevance from the perspective of the target organization, either in terms of actions they take in response, or the antecedents that drive these attacks. First, alerts exhibited a range of immediacy of attack. Some alerts represented definitive attempts at compromise in progress that resulted in immediate action by the security operators at the target organization. At the other end of the range, some alerts represented reconnaissance attempts that could not be filtered without seriously hampering

Figure 1 A Typology of Information Security Alerts



legitimate activity. Thus, this first dimension captured the dichotomy in the actions typically taken by the target organization in response to the attack. Second, we identify an additional dimension that is important for our analysis—target specificity. This dimension represented whether the activity targeted a specific firm, or whether it was indiscriminate. As we demonstrate later, this dimension allows us to separate out two paths of attack that have distinct antecedents in the conceptual model.

Using these two dimensions, we developed a typology (Figure 1 and Table 3) with the four possible permutations. First, nontargeted low-severity attacks, labeled *information scans*, gather information about systems and services, such as a simple check to see if any machine responds at a particular IP address. Second, targeted low-severity attacks, labeled *targeted probes*, test a specific set of potential victims for vulnerabilities. Third, nontargeted high-severity attacks, labeled *attack scans*, are widespread, indiscriminate attempts to damage systems, such as a self-replicating worm. Fourth, targeted high-severity attacks, labeled *targeted attacks*, represent a severe attempt to compromise a specific system.

The Primary Constructs in the Conceptual Model

We conducted unstructured interviews with a 30 IS security staff from nine organizations of four different types (three North American financial institutions, two managed security providers, two large Western European based nongovernmental organizations, and two universities). We explained to the participants that the fundamental question of our study was, "Why are some organizations attacked more than others?" We asked them to base their responses on their professional expertise without revealing any firm-specific information.

Table 3 Attack Categories and Examples

Constructed type	Empirical example from alert signatures
Information scan	Using TCP/IP ping to see if an IP address has a computer
Attack scan	Blaster worm which exploits a remote procedure call vulnerability
Targeted probe	Port scanning a specific computer to see what services are running
Targeted attack	Using SQL injection to create an unauthorized database account

As we progressed through the interviews, we found that three constructs affect the incidence of the four attack categories described in the previous section: the size of the firm's Internet presence (*Internet presence*), the efficacy of the countermeasures put in place (*organizational countermeasures*), and its overall attractiveness to attackers as a target based on firm-specific factors (*perceived attractiveness*). Further, in describing these constructs, interviewees identified two fundamental attack paths that differed in terms of their antecedents. The first represents deliberate attacks on a selected victim, labeled *choice*. The second follows an opportunistic path, labeled *chance*. We describe these two paths and their antecedents in the next few sections.

The Path of Choice: Deliberate Compromise

Target attractiveness plays an important role in the deliberate path to compromise. Interviewees consistently identified both the utility-maximizing aspect of rational criminals, as well as a changing focus from status-based utility to financial motivation. As one interviewee from a financial institution described, "Formerly there was defacement, looking for high splash value. So, identifiable brands were targeted. Now attacks follow money." An interviewee from a financial organization offered the summary that "Crooks do cost-benefit analysis too."

Persons who attack systems are an obviously difficult group to reach. To obtain a better understanding of the target attractiveness construct, we reviewed postings in Usenet groups[2] with keywords such as "hacker or attacker" and "motivation." We reviewed more than 150 such postings to reach theoretical saturation (Glaser and Strauss 1967), noted the major

[2] Groups include alt.2600.hackerz, alt.hacker, alt.hackers.malicious, comp.security.misc, fa.firewall, among others.

Table 4 Coding the ATTRACTIVENESS Construct and Its Three Dimensions

Dimension	Tangible value	Iconic value	Reprisal value
Definition Potential of a compromise to...	...provide valuable information and resources	...provide recognition within the attacker's peer group due to the target's stature	...provide satisfaction as an act of reprisal against an individual or entity
Explanation	Some attackers are motivated by access to information and resources that can be sold to others	Motivation comes from recognition within peer groups for attacking large, prominent, and impenetrable targets	Incidents may be motivated as acts of reprisal. There is also a sense of vigilantism among attackers.
Sample quotes from discussion groups	"The real crackers tend to be searching for sites that have data worth getting..."	"If the corporation has top-level documents, such as... NASA, it is cool to acquire them."	"I just hacked into the hardest system on the Web... that was being run by child rapists."
	"...there are hackers who take over a machine to sell it to spammers."	"A real hacker will be tempted by the most impenetrable sites"	"Most people cannot cancel the phone service of those who upset them... to a proficient hacker this is not a difficult problem."
	"Machines... can be collected to form large collections with malware."	"...whoever's the first one to break in [will] be recognized by his peers as the 'Top Dog' in hackerdom."	

reasons behind attacking systems, and derived from them the factors that make a target attractive. Sample quotes from the discussion groups bring out three broad dimensions of target attractiveness (tangible, iconic, and reprisal value) that drive deliberate attacks.

Table 4 provides the definitions and details of these three dimensions, as well as quotes from the discussion groups that point to them as antecedents in the deliberate path to compromise.

The economic literature on criminal behavior also supports the relevance of tangible value in the deliberate path to compromise. Clearly, the effort required to compromise a system must be commensurate with the perceived tangible benefits for the attacker (Becker 1968, Schechter and Smith 2003). Further, iconic and reprisal value of a client influences the hacker subculture and is an antecedent in the deliberate path in the Social learning, subculture, and labeling theories of crime in Table 1 (Sutherland 1947, Akers et al. 1979, Cohen and Felson 1979). Thus, interviews, discussion group postings, and criminology literature support the following proposition.

Proposition 1 (P1). *Higher perceived attractiveness of the target firm* (*tangible, iconic, and reprisal value*) *is associated with a larger number of targeted probes.*

The Path of Chance: Opportunistic Compromise

However, as the Internet has evolved, attacks are no longer the exclusive domain of the expert. While expertise is needed initially to find vulnerabilities and devise techniques to use them, they are disseminated quickly as packaged tools, making the expertise widely available. Then, these tools are used to find vulnerable systems, frequently by iterating through IP addresses. In these probes, the target is not preselected; rather, the attacker finds victims who are vulnerable to a specific type of attack. In this opportunistic path of compromise, the degree of Internet presence influences the number of attacks. Internet presence does not only refer to the number of visible IP addresses, but also to the number of servers, open ports, products offered over the Internet, visitors to the website, and the volume of online advertising. Demonstrating the idea that mere Internet presence leads to a certain level of attack, many interviewees commented, "there is definitely an element of randomness in attacks," and that "most automated attacks are all out attacks with no scaling—there is no reason not to try all at once."

To identify the dimensions of Internet presence, we analyzed the typical tools used by attackers and their methods of operation. We conducted a search on the Usenet discussion groups with a combination of keywords such as "hacker," "how to," "tools," and

"method." Often, discussion group postings pointed to websites where a variety of tools are reviewed or made available. We identified five categories of tools shown in Table 5. While reviewing these tools, we identified the factors that would make a target more vulnerable to compromise. Through this process, we identified two dimensions (Table 5) of Internet presence—passive and active.

Passive presence is the number and functionality of the Internet connections of a target firm. A larger passive presence on the Internet leads to more attacks through the opportunistic path using the foot printing and vulnerability exploitation tools described in Table 5. Foot-printing tools enumerate reachable IP addresses, open ports, and services running. Thus, a larger passive presence leads to a greater number of information scans generated through the foot-printing tools. Vulnerability-exploitation tools provide the ability to exploit known vulnerabilities. A larger passive presence leads to more attack scans through such tools that often indiscriminately blanket the Internet to find and exploit vulnerabilities opportunistically. In the criminology literature, situational factors (such as living in a specific neighborhood or near a public area) are recognized as determinants of victimization (Miethe and Meier 1994), and are analogous to passive presence in the Internet environment. With low search costs, economic theory also predicts that attackers search extensively to identify easy targets (Cohen and Felson 1979, Ehrlich 1996). Consequently, interviews, analysis of tools, and existing criminology literature support the following proposition.

Table 5 Coding the INTERNET PRESENCE Construct and Its Two Dimensions

Dimension	Passive presence	Active presence
Definition	The number and functionality of connections to the Internet	The volume and richness of Internet activities
Details	Passive presence is the size of the organization's Internet footprint. A larger footprint results in a larger number of nontargeted attacks that spread indiscriminately across the Internet.	Active presence is affected by the Internet activities of an organization. Richer and more frequent Internet activity reveals more information about the firm that can be used in automated and targeted attacks.
Examples	The number of IP addresses, ports, users, dial-in lines, and hosts	E-mail marketing campaigns and online ads, participation in discussion groups and chat rooms, electronic commerce activity with partners
Tools	Foot-printing tools provide information about reachable IP addresses, open ports, and services running. A larger passive presence leads to more connections to the Internet that can be exploited.	Code-breaking tools decipher encrypted transmission and passwords. Larger active presence leads to more transmission that can be deciphered.
	Vulnerability-exploitation tools provide the ability to exploit known vulnerabilities. A larger passive presence leads to more attacks through such tools that often indiscriminately blanket the Internet.	Data-sniffing tools enable the attacker to examine transmission content. Larger active presence leads to more traffic that can be intercepted.
		System-control tools enable the attacker to control sessions and hosts. Larger active presence leads to more systems that can be exploited.

Proposition 2 (P2). *Larger passive Internet presence of the target firm is associated with a larger number of attack* (*A*) *and info* (*B*) *scans*.

Active presence, on the other hand, refers to the volume and types of Internet activities performed by the firm and its stakeholders. Richer and more frequent activity on the Internet reveals more information about the firm that can be used in targeted attacks. As more data about the firm traverses the Internet, it provides more information that attackers can exploit through data-sniffing and code-breaking tools. It further identifies more systems and sessions that the system-control tools described in Table 5 can potentially manipulate. This was also noted by several interviewees who said, "Increased market presence leads to more attacks," and "The number and types of products offered [over the Internet] leads to more open ports, more servers, and more attacks." Further, even in the traditional crime environment, variables associated with routine activities performed by a target affect the chances of victimization (Miethe and Meier 1994). Thus, people are more likely to be assaulted if they routinely go out at night or to dangerous places. Thus, interviews, analysis of tools, and the criminology literature support the next proposition.

Proposition 3 (P3). *Larger active Internet presence of the target firm is associated with a larger number of targeted probes*.

Choice and Chance: Convergence of the Two Paths

Both widespread and directed attacks may be used in conjunction. Attackers can use widespread, shotgun attacks to find companies with vulnerabilities, and then from a list of vulnerable companies, select specific companies for more directed attacks. Interviewees from an MSSP with experience in analyzing a wide range of attacks indicated that "results of reconnaissance scans can be used in two ways, both directly and as a signal showing [a company is] likely to leave things open." Thus, from scans, an attacker develops a list of vulnerable targets, and, with this list, the attack may turn from opportunistic to deliberate. While the convergence of the opportunistic and deliberate paths of attack is a unique characteristic of the Internet environment, there is also some support in the criminology literature. The rational choice and related theories of crime (Cohen and Felson 1979, Ehrlich 1996) posit that criminals are rational individuals who pursue easy targets. The foot-printing and vulnerability-exploitation tools in Table 5 lower the cost of search and enable the identification of such targets through the opportunistic path. Once identified, the attack turns from opportunistic to deliberate. Thus, the next proposition links the opportunistic and deliberate paths of attack in the ISCP.

Proposition 4 (P4). *A larger number of info scans at a target firm is associated with a larger number of targeted probes*.

Choice and Chance: Progression of Attacks

An overriding theme on how attacks are linked was summarized simply by an interviewee at a financial institution as "attacks are a process," and by another at an MSSP as "attacks often start small, then graduate." Thus, many interviewees described a progression of an incident, starting with initial exploratory attempts, and then using the knowledge gained from these attempts to compromise systems. Indeed, the foot-printing tools in Table 5 enable targeted information gathering that may appear innocuous and is difficult to prevent without hampering legitimate activity; this reconnaissance facilitates later targeted attacks. In the criminology literature, especially in the racial, sexual, and child abuse contexts where repeat victimization is common, many authors have implicitly or explicitly argued that victimization should be conceptualized as a process rather than a single event (Bowling 1993, McShane and Williams 1997). Although the context is different from the ISCP, this literature also describes a progression of incidents with relatively minor to major impact. Thus, information gathering progresses to compromise attempts.

Proposition 5 (P5). *A larger number of targeted probes at a target firm is associated with a larger number of targeted attacks*.

Further, due to the evolving nature of information security attacks, protection is necessarily imperfect and residual risk remains (Siponen 2005, Straub and Welke 1998) for three reasons. First, security technology is often error-prone, generating many false positives and false negatives (Cavusoglu et al. 2005). Second, as new vulnerabilities are discovered and exploited, there is often a time lag in developing remedial countermeasures (Arora et al. 2004). Third, target firms may also be slow in adopting available countermeasures (Siponen 2005, Straub and Welke 1998). Thus, as new attacks emerge, some will find their way to information security compromise. We add the following proposition to capture this residual risk.

Proposition 6 (P6). *Larger numbers of* (*A*) *targeted attacks and* (*B*) *attack scans at a target firm are associated with a larger number of IS security compromises*.

Organizational Countermeasures: Managing Threats

Information security practices seek to reduce risk by analyzing vulnerabilities and instituting policies, procedures, and technology to reduce the threat from cyber attacks. Firms employ multiple countermeasures, as summarized by an interviewee from a university: "Defense in depth is key—multiple layers including patch management, firewalls, intrusion detection systems, and user training." To understand the multiple countermeasures used in practice and their role in the ISCP, we reviewed security guidelines and best practices from multiple sources. Our primary data source were the IS security guidelines published

by the Department of Defense—Defense Information Systems Agency (DISA). We reviewed detailed security checklists (Defense Information Systems Agency website, www.disa.mil) related to application security, network security, desktop security, database security, and server security. We also reviewed the ISO 17799 specifications (Code of Practice for Information Security Management from the International Standards Organization), and security guidelines from the National Institute of Standards and Technology (Bowen et al. 2005).

We categorized the guidelines into five dimensions (Table 6) and then further decompose the dimensions into three main categories based on the stage of the ISCP where they are likely to have the most impact. Traffic control and access control measures rely on their ability to identify improper activity and restrict usage, such as through attack signatures and access restriction policies. Their efficacy in restricting scans and probes is limited because, by definition, such activities can be legitimate (albeit suspicious) and the target organization cannot stop them without hindering other critical applications. Thus, traffic control and access control measures are most effective in reducing the progression of attack scans and targeted attacks to information security compromise. On the other hand, vulnerability control and feature control reduce the number of weaknesses found through informational scans and targeted probes, reducing the progression of these reconnaissance activities. Another category of countermeasures, audit control, does not have a direct effect on the ISCP, but improves the other countermeasures over time through monitoring and learning. The following propositions reflect the moderating role of deterrence. Figure 2 summarizes the conceptual model.

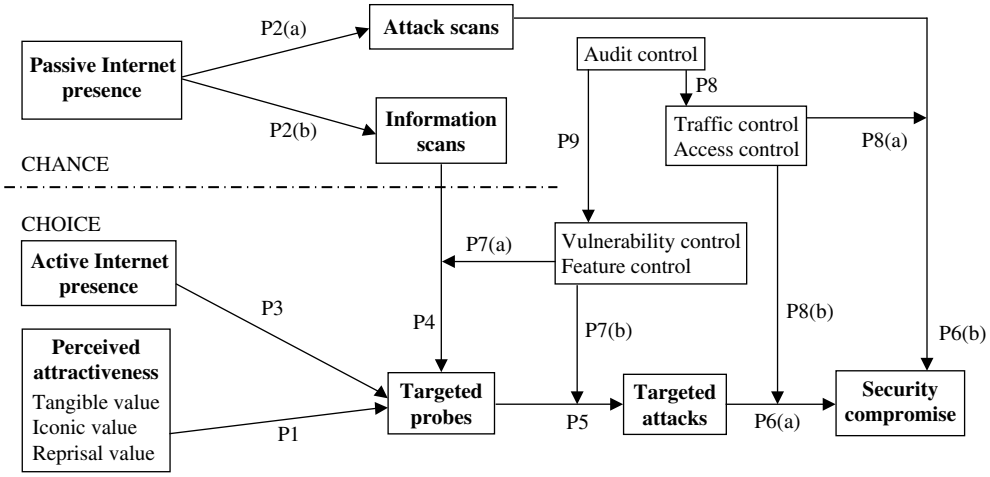
Proposition 7 (P7). *Vulnerability and feature control measures moderate the relationship between info scans and targeted probes* (*A*) *and between targeted probes and targeted attacks* (*B*). *Firms with less-effective controls have a stronger relationship between info scans and targeted probes* (*A*) *and between targeted probes and targeted attacks* (*B*).

Proposition 8 (P8). *Access and traffic-control measures moderate the relationship between targeted attacks and security compromise* (*A*) *and between attack scans and security compromise* (*B*). *Firms with less-effective controls have a stronger relationship between targeted attacks and security compromise* (*A*) *and between attack scans and security compromise* (*B*).

Table 6 Coding the COUNTERMEASURES Construct and Its Five Dimensions

Dimension	Access control	Vulnerability control	Feature control	Traffic control	Audit control
Definition	Restricting access by people and software based on need	Removing known errors in hardware/software that can be exploited for inappropriate use	Setting parameters in devices and software to reduce inappropriate use	Monitoring and blocking traffic based on identification of inappropriate activity	Documentation of systems and activity that can be used for audits and actions
Example of topics	Identification User and server authentication Access restrictions Removal of inactive user-id Restricted access to devices, data, data centers, wireless networks, system management, root accounts Role-based privileges Restricted application access through defined interfaces Policies on collocation of programs and data Control of trusted systems Approved software/device list	Commercial software Up-to-date patching Software development No unused code in libraries Appropriate error handling Removing memory objects Validation of user input Clear logout features Vulnerability practices Approved virus protection Compliance verification for client programs Periodic discovery of vulnerability Verification of remedies	Software settings Policies for browser settings Session limits and timeouts Lowest possible range for wireless devices Appropriate router, DNS and DHCP settings Enablement/disablement Disabling certain ports Enabling security features Preventing file downloads from routers Session encryption Disabling unused devices Disabling insecure protocols	Packet filtering by sensors Blocking specific packet types Review of packet source addresses Up-to-date signatures Activity filtering by servers and applications	Documentation Documentation and inventory of software/devices Automatic discovery of devices and software Logging Logging and management of activity records

Figure 2 Conceptual Model of the ISCP



Information scans	Nontargeted attempts to gather information about systems that can be used later for security compromise
Attack scans	Nontargeted attempts to compromise systems
Targeted probes	Targeted attempts to gather information about a specific system that can be used later for security compromise
Targeted attacks	Targeted attempts to compromise systems
Security compromise	Successful attempt to compromise the information security of a firm

Notes. Definitions for passive and active Internet presence, perceived attractiveness, and organizational countermeasures appear in Tables 4–6.

Proposition 9 (P9). *Audit-control measures do not directly affect the ISCP, but improve the other organizational countermeasures over time.*

4. Empirical Examination Using Alert Data

The Data Set

We had partial access to a database of alert data provided to us by an Atlanta-based MSSP, SecureWorks, Inc. There were approximately 847 million security alerts for the one-year period from January 2006 until December 2006. The data set is generated in real time by sensors (network monitors) that are installed by the MSSP at the Internet entry points of the networks of their clients. The purpose of network monitors is to identify potential attacks and suspicious activity. Identification is done through *signatures*, which are data-traffic patterns that indicate a possible problem. As new threats and vulnerabilities are uncovered, they are distilled into signatures and distributed to the network monitors to improve their ability to identify threats.

For consistency of analysis, we restricted our analysis to the 364 million alerts from the 821 clients who had only a single sensor located between their internal and external network. Within the subset, 3,444 distinct signatures triggered at least one alert during the year. Signatures ranged from appearing in one to 54,365,983 alerts with an average of 105,758 alerts per signature. Of the 821 possible clients, the number of clients affected per signature ranged from one to 782 with an average of 39. Further, 102 of the signatures appeared every day of the year. Alert volume per day varied dramatically and ranged from 199,689 to 3,514,819 alerts. The particularly high-volume alert days were due primarily to widespread nontargeted viruses and worms.

Purpose of the Empirical Analysis

Although the data set is rich and unique, it has three key limitations with respect to our conceptual model in Figure 2. First, we have no measure of the three dimensions of target attractiveness to construct a reliable measure of the construct. For security and privacy reasons that are common with this type of data,

we did not have access to the client or client information beyond the alert data. Second, we also had no measure of the level, type, and sophistication of countermeasures instituted by the firm. In fact, because they were protected by the same MSSP, it is likely that they had similar countermeasures in place, with little variation across clients. Third, the signature-based identification scheme is not perfect, introducing considerable randomness in the data. However, the data also has several advantages, the primary being the large number of records and the panel nature of the data, that allow us to evaluate firm and time fixed-effect models to control for unobserved heterogeneity both across firms and across time. It is an important data source of actual attacks that has not been adequately exploited in the IS literature.

Thus, while the alert data does not enable us to evaluate some of the propositions in our conceptual model related to target attractiveness and organizational countermeasures, it does allow for detailed examination of the key contributions of our model through three fundamental research questions. The following questions also summarize the key differences between the ISCP and the general crime contexts studied in earlier research.

- Are there distinct opportunistic and deliberate paths to information security compromise?
- Do these distinct paths converge with the opportunistic path leading to the deliberate path?
- Does the targeted path progress from information gathering (probes) to targeted attacks?

Opportunistic and Deliberate Paths

Experts from the MSSP independently classified the signatures into targeted and nontargeted subgroups based on the description and detailed technical specifics. This classification existed in the database independent of our research. Because of the signature volume, experts classified only the 2,914 that represented the current, frequently occurring signatures. The expert assessments of targeting were "never," "sometimes," "usually," "always," and "unknown;" for our analysis, we used dichotomous groupings of targeted (including "usually" and "always") and nontargeted ("never") and removed the ambiguous remaining signatures from the sample.

To distinguish between the opportunistic and deliberate paths of attack, we performed three separate analyses on the signatures. First, we looked for significant differences in attack patterns between the targeted and nontargeted subgroups using simple parametric statistical tests. Second, we estimated the well-known Bass diffusion model (Bass 1969) to identify differences in diffusion patterns between the two subgroups as the attempts spread. Third, to understand differences between the two subgroups based on qualitative factors, we utilized several qualitative indicator variables as predictors in a logit regression with the targeted/nontargeted indicator as the dependent variable. If the deliberate and opportunistic paths are distinct, we expect significant differences in attack or diffusion patterns between the signature categories.

Table 7 reveals significant and interesting differences in attack patterns for targeted and nontargeted signatures. As expected, nontargeted signatures generate significantly greater number of alerts per signature (235,524 for each nontargeted signature compared to 46,772 for each targeted signature). The number of source addresses for nontargeted attacks is also significantly higher (2,291 per nontargeted

Table 7 Differences in Attack Patterns Between Targeted and Nontargeted Signatures

		Per signature statistics				
	No. of signatures	Alerts	Firms affected (out of 821)	Alerts per firm	Source addresses	Destination addresses
Overall	1,586	141,266	55	0.272	1,287	847
Targeted	792	46,772	52	0.330	281	1,267
Nontargeted	794	235,524	59	0.214	2,291	425
Mean difference		188,752**	7***	0.116***	2,010***	842
(standard errors)		(84,086)	(4.83)	(0.018)	(786)	(926)

Notes. Alerts per client are calculated for only those clients where a signature is present. Significance based on 2-tailed t-test of difference in mean. Standard errors are shown in parenthesis.

*($p < 0.1$), **($p < 0.05$), ***($p < 0.01$).

signature compared to 281 per targeted signature). On the other hand, targeted attacks are more thorough, with more alerts generated for each firm where they are present and reaching a greater number of destination addresses even though the number of alerts per signature is less. Thus, nontargeted attacks appear to be broad-brush, originating from more sources, exhibiting less expertise, and reaching the same limited set of destination addresses, while targeted attacks are less voluminous, originate from fewer sources, are more thorough, and penetrate each firm more deeply.

To examine differences in diffusion patterns between targeted and nontargeted signatures, we performed the following analysis. To capture the beginning of the diffusion pattern and reduce truncation problems, we selected only those signatures that had no alerts for any firm during the first two months of the year 2006. We also restricted our analysis to only those signatures that reached at least 50% of the clients in the one-year time period of the analysis, so that our results are not confounded by the many historical signatures that remain in the MSSP database (signatures are never removed) but infrequently generate attacks. We then aligned the signatures based on the first date when an alert appeared in our database for each selected signature and designated that date as day 0. We then calculated the number of new firms that each signature affected on subsequent days after day 0, and we estimated the Bass diffusion model (Bass 1969) with these values. The model we estimate is

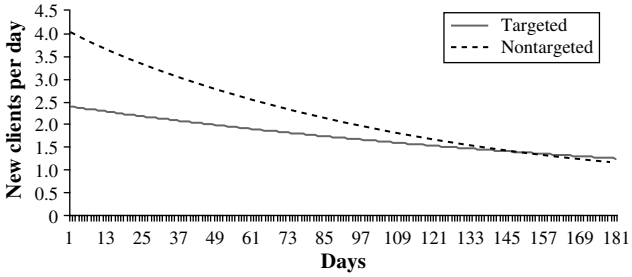
$$\frac{f(t)}{(1-F(t))} = p + \beta_p * T + q * F(t) + \beta_q * T * q * F(t), \qquad (1)$$

where $f(t)$ is the rate of change in the fraction of firms affected at time t, $F(t)$ is the fraction of firms affected at time t, p is the coefficient of innovation in the Bass model, q is the coefficient of imitation in the Bass model, and T is an indicator variable that is set to one for targeted signatures. In our context, p estimates the constant rate of change in the fraction of f affected by a signature, while q estimates the effect of a larger installed base on the rate of change (such as for propagating worms that spread faster as the affected population increases). The parameters β_p and β_q estimate whether there are significant differences in the p and q coefficients of the Bass model for targeted and nontargeted signatures.

Figure 3 Diffusion of Attacks for the Targeted and Nontargeted Signatures

	P	Q	β_p	β_q
Estimate	0.005***	−0.004***	−0.002***	0.003***
(standard error)	(0.0003)	(0.0005)	(0.0006)	(0.001)

$R^2 = 1\%$, $F = 21.96^{***}$, $N = 7{,}903$



Note. Significance $^{*}(p < 0.1)$, $^{**}(p < 0.05)$, $^{***}(p < 0.01)$.

Figure 3 shows the results of estimating of Equation (1) using ordinary least squares (OLS) estimation of parameters. The parameter β_p is significant and negative, indicating that the p parameter of the Bass diffusion model is significantly lower (by about 40%) for targeted attacks when compared to nontargeted attacks. The q parameter for nontargeted attacks is negative, while the same parameter for targeted attacks ($q + \beta_q$) is close to zero, with β_q significant and positive. The implications of these parameter estimates are clear in the plot of new firms (for our set of 821 firms) affected per day for the two types of signatures in Figure 3. Nontargeted signatures have higher rates of diffusion in general, but the number of firms affected per day is high in the first few days and decreases quickly over time. For targeted attacks, the rate is lower but remains almost constant or only slightly decreasing over time. The low R^2 results from the fact that while the targeted and nontargeted signatures are different in terms of diffusion patterns, there is significant variation in diffusion patterns within each group, and a more finer-grained analysis of diffusion that also considers other factors remains a future research issue.

Finally, to understand the differences between the two attack categories based on qualitative factors, we performed the following analysis. For each signature,

we had access to three qualitative variables: (a) the protocol used by the signature (e.g., http, sql, ssl, ftp, telnet, etc.), (b) the communication layer exploited (e.g., network, transport, session, etc.), and (c) the signature type (e.g., virus, worm, Trojan horse, dos command, backdoor, etc.). We created 31 indicator variables to represent the different protocol types, four indicator variables to represent the communication layer exploited, and 17 indicator variables to represent the different signature types. We performed a logit regression with the T variable ($T =$ one for targeted, zero otherwise) as the dependent variable, and the protocol, communication layer, and signature-type indicators as independent variables. The logit regression was highly significant ($\chi^2 = 1{,}738.97$; pseudo-$R^2 = 79\%$). Twenty six of the 31 protocol indicators were perfect predictors (belonged completely to either targeted or nontargeted categories) and the remaining five were highly significant ($p < 0.05$) in the logit regression. Likewise, one of the communication layer indicators was a perfect predictor and two of the remaining three were highly significant ($p < 0.05$); 15 of the 17 signature-type indicators were perfect predictors and the remaining two highly significant ($p < 0.05$) in the logit regression.

Overall, the empirical analysis in this section provides evidence that targeted and nontargeted attacks are significantly different in terms of attack patterns, attack diffusion rates, and several qualitative factors such as the protocol used and communication layer exploited.

Convergence of Opportunistic and Deliberate Paths

To examine the convergence of the opportunistic and deliberate paths, we built an unbalanced panel data set with the number of alerts of each type in the typology (Figure 1) for each client and for each day in 2006. The targeted/nontargeted classification was based on the expert assessments explained earlier. To classify signatures based on the reconnaissance/attempted compromise dimension (Figure 1), we found that traffic from all signatures is not necessarily stopped by the MSSP; rather, some signatures can be themselves potentially benign and legitimate, but are still logged because, combined with other activity, indicate attempts to gain information about the client systems (Cuppens and Miege 2002). Therefore, we used the information on whether or not the alert was filtered to classify the alert as information gathering or attack. Then, using both the targeted and informational dimensions, we classify each signature into one of the four categories in the typology (Figure 1). Thus, our unbalanced data set contains the number of alerts for each of the four types, for each of the 821 client firms, and for each of the 365 days of the year, resulting in over 299,000 observations. To examine the convergence of the opportunistic and deliberate paths of attack, we evaluate whether information scans lead to targeted probes through the following firm and time fixed-effects model:

$$\begin{aligned}\text{Model A1: } \ln(\text{TP}_{it}) &= \beta_0 + \beta_{\text{IS}} * \ln(\text{IS}_{it}) \\ &\quad + \beta_{\text{TP}} * \ln(\text{TP}_{i,t-1}) + \sum_i \beta_i * \text{FD}_i \\ &\quad + \sum_t \beta_t * \text{TD}_t, \qquad (2)\end{aligned}$$

where TP_{it} is the number of targeted probes for firm i on day t, IS_{it} is the number of information scans for firm i on day t, $\text{TP}_{i,t-1}$ is the lagged dependent variable, FD_i are firm dummies (820), and TD_t are week dummies (51). The model controls for unobserved firm-specific heterogeneity in the number of attacks through a fixed-effects model by using the 820 firm dummies. This controls for factors in the conceptual model such as target attractiveness and Internet presence that can affect attack volume. Likewise, we include 51 weekly indicator variables to control for changes in attack volume over the course of the study year because we observed significant variability over time in the total volume of attacks. Further, to control for unobserved events at a firm that may temporarily drive the number of attacks, we include a one-day lagged dependent variable in the model. Our primary independent variable of interest is $\text{Ln}(\text{IS}_{it})$.

Table 8, Panel A shows the results of the analysis using hierarchical regression. Model A0 includes all the control variables, while Model A1 introduces the $\text{Ln}(\text{IS}_{it})$ variable. The coefficient of the $\text{Ln}(\text{IS}_{it})$ variable is significant and positive, indicating that the number of targeted probes increases with an increase in the number of information scans. The coefficient of the $\text{Ln}(\text{IS}_{it})$ variable indicates that about 5% of the information scans are converted to targeted probes.

Table 8 OLS Regression on Unbalanced Panel of Alert Data

	Panel A Convergence of paths		Panel B Progression of attacks		
Model	Model A0	Model A1	Model B0	Model B1	Model B2
Dependent variable	Targeted probes (TP_{it})	Targeted probes (TP_{it})	Targeted attacks (TA_{it})	Targeted attacks (TA_{it})	Targeted attacks (TA_{it})
Constant	0.074*** (0.008)	0.051*** (0.008)	1.386*** (0.023)	1.353*** (0.023)	1.329*** (0.023)
Lagged dependent variable	0.462*** (0.002)	0.461*** (0.002)	0.405*** (0.002)	0.405*** (0.002)	0.400*** (0.002)
Information scans $Ln(IS_{it})$		0.056*** (0.001)		0.087*** (0.003)	0.067*** (0.003)
Targeted probes $Ln(TP_{it})$					0.321*** (0.005)
Time fixed-effects (weekly)	Included (52)	Included (52)	Included (52)	Included (52)	Included (52)
Client fixed-effects (821 firms)	Included (821)	Included (821)	Included (821)	Included (821)	Included (821)
Observations	224,884	224,884	224,884	224,884	224,884
F	1,236.28***	1,276.05***	1,335.70***	1,329.22***	1,392.74***
R^2 (within firms)	22.3	23.2	23.7	23.9	25.1
R^2 (between firms)	98.1	95.0	94.9	94.0	89.5
R^2 (overall)	50.7	50.8	48.3	48.5	48.8

Note. Standard errors in parentheses; $^{*}p < 0.05$, $^{**}p < 0.001$, $^{***}p < 0.001$.

The models explain about 51% of the variance overall, but as expected, most of the variance is explained through the firm fixed-effect variables (indicated by the high between-firms R^2). The within-firm R^2 is of particular interest because it indicates the fraction of within-firm variance explained by our models. The week dummies and lagged dependent variable explain 22% of the variance in targeted probes for the same firm. The introduction of the $Ln(IS_{it})$ variable increases the within-firm R^2 by approximately 1% to 23%. Even though only a small percentage (5%) of the information scans lead to targeted probes based on the estimates, they lead to compromise attempts that are more serious. Overall, we find preliminary evidence that a greater number of information scans lead to a greater number of targeted probes, after controlling for firm-specific and time-specific factors.

Progression from Information Gathering to Attack

To examine the progression of activity from information gathering to attack in the conceptual model in Figure 2, we test for the *mediating effect* of targeted probes between nontargeted information scans and targeted attacks (Baron and Kenny 1986). Specifically, we evaluate the following two models:

$$\text{Model B1: } \ln(TA_{it}) = \beta_0 + \beta_{IS} * \ln(IS_{it}) + \beta_{TA} * \ln(TA_{i,t-1}) + \sum_i \beta_i * FD_i + \sum_t \beta_t * TD_t, \quad (3)$$

$$\text{Model B2: } \ln(TA_{it}) = \beta_0 + \beta_{IS} * \ln(IS_{it}) + \beta_{TP} * \ln(TP_{it}) + \beta_{TA} * \ln(TA_{i,t-1}) + \sum_i \beta_i * FD_i + \sum_t \beta_t * TD_t, \quad (4)$$

where TA_{it} is the number of targeted attacks for firm i on day t, $TA_{i,t-1}$ is the corresponding lagged variable, and the other variables are as explained in the previous section.

Table 8, Panel B shows the results of OLS estimation of the parameters. Model B0 is a control model for targeted attacks with all variables highly significant. In Model B1, we test the impact of nontargeted information scans on targeted attacks and find the coefficient to be highly significant. Model B2 introduces the $LN(TP_{it})$ variable and finds the coefficient to

be highly significant also. Although the coefficient for $\text{Ln}(\text{IS}_{it})$ remains significant in Model B2, the magnitude of the coefficient is reduced (from 0.087 to 0.067) after the introduction of the $\text{Ln}(\text{TP}_{it})$ variable, indicating partial mediation (Baron and Kenny 1986). Further, we use the Sobel test (Baron and Kenny 1986, Sobel 1982) and find the results to be highly statistically significant ($T = 38.90$, $p < 0.001$), indicating the mediating role of the $\text{Ln}(\text{TP}_{it})$ variable. The within-firm R^2 increases from 23.9% to 25.1% in Model B2. Overall, our results provide preliminary evidence of progression from information gathering to attacks.

Additional Analysis with Alert Data

In addition to the empirical analysis described above, we performed two additional analyses using the alert data that are reported in an online appendix. First, as additional empirical support for the conceptual model, we demonstrate that larger passive Internet presence (measured by the number of reachable IP addresses) has a positive effect on the number of information scans and targeted probes. Second, for robustness, we considered the source IP address in the analysis of convergence and progression of attacks. Specifically, we segregate attacks to a target firm by their source IP address, thereby following attacks from the same source to the same destination, and we demonstrate similar results. The online appendix also provides correlations between the variables in the model.

5. Summary, Discussion, and Conclusions

In this research, we develop a conceptual model of the ISCP through a grounded approach that depicts two separate attack paths, deliberate and opportunistic, that merge as antecedents to information security compromise. The model also recognizes the moderating (rather than direct) role of organizational countermeasures in reducing the progression of attacks and their ultimate conversion to information security compromise. Our empirical results validate the existence of the two paths, the merging of the paths from opportunistic to deliberate, and the progression of attacks from informational to compromise attempts.

Limitations

We identify several limitations of this study. First, although we took care to differentiate alerts along the targeted/nontargeted dimension and the empirical analysis demonstrated significant differences, there remains ambiguity in classification because we have created dichotomous variables from underlying continuous classifications. Second, although we recognize that our study context is dynamic because signatures can evolve from targeted to nontargeted as they are packaged into tools, we are not able to observe this temporal dimension in our secondary data. Third, the alert data we use in the empirical analysis is inherently noisy because the signature-based identification scheme is imperfect and there is distinct randomness in the data. Fourth, we have used imprecise measures for each of the constructs in our conceptual model based on the data that was available. Finally, although we provide empirical support for the key contributions of our conceptual model, portions of the model related to target attractiveness and countermeasures remain untested in our analysis.

Managerial Implications

From a practical perspective, our results highlight four messages for managers. First, although it may have been previously safe to assume that an organization not intrinsically attractive to attackers was immune from attacks, the opportunistic path illustrates that all systems are potential victims. We see a high volume of nontargeted attacks (98% of all attacks) across all targets, irrespective of target attributes. Although these attacks are indiscriminate, broad-brush, and often require less expertise, the convergence of attack paths imply that many of these opportunistic attacks will become more serious targeted compromise attempts.

Second, we find evidence of progression of attacks from simple information scans to serious targeted attacks. Organizational countermeasures halt the progression of an incident by reducing the number of information scans converted to targeted probes, and the number of targeted probes converted to targeted attacks. Thus, effective vulnerability control and feature control countermeasures (e.g., patching, virus protection, disabling insecure protocols) that halt the progression of attacks at an early stage are important

because later stage countermeasures such as traffic filtering are often imprecise and imperfect (Cavusoglu et al. 2005).

Third, active presence on the Internet leads to more attacks through the targeted path. Although reducing active presence may be contrary to business goals, managers should consider its effects on information security. Similarly, reducing the dimensions of target attractiveness, such as shrinking the customer base or reducing visibility, may be infeasible or undesirable, leading to the reality of residual risk.

Finally, the conceptual model presented in Figure 2 can be used as an effective teaching tool to educate managers and students about IS security. It provides a comprehensive, cogent, and nontechnical model to understand the information security compromise process from the perspective of a target organization.

Implications for Research

Several areas of future research emerge from the conceptual model and empirical analysis.

Measurement Instruments. The development of measurement instruments that accurately capture each construct (organizational countermeasures, attractiveness, and presence) is a research topic in itself. Although we have identified the dimensions of each construct, we have not focused on measurement issues. As is common with secondary data analysis, we are limited to proxies that can be measured through the available data. However, development of detailed measurement instruments will have several benefits. It will help managers to accurately measure various aspects of their information security environment. The measurement instrument can also serve as a theory-driven audit and benchmarking tool.

Empirical Validation. Siponen (2005) points to the paucity of empirical research in this area. One area of empirical research that is likely to be of significant practical significance is the efficacy of different organizational countermeasures in the two attack paths, deliberate and opportunistic. Specifically, evaluating the trade-off between early and later stage countermeasures, balancing the ability of countermeasures to halt the progression of an attack versus the negative consequences of reduced access, and measuring the false positives and false negatives of later stage countermeasures are important topics. Empirical validation is also important to establish the antecedents of each path in the conceptual model (target attractiveness, active and passive presence), so that managers can better control or at least consider these antecedents during IS and business planning. Further, we have attempted a partial validation of the conceptual model, and a more complete empirical validation remains a future research opportunity.

Finer-Grained Analysis of Alert Data. Alert data is voluminous, complex, and extraordinarily difficult to synthesize. We have attempted a broad analysis of the alert data in this research, but there is significant scope for finer-grained analysis of this important data source. Four types of analysis are possible, among others: (a) discovery of attack patterns associated with various types of attacks, (b) analysis of the impact of specific countermeasures, (c) discovery of changing attack characteristics and trends over time, and (d) examination of the impact of security-relevant events (such as the release of a vulnerability or patch) on attack volume. Although the computer science community has focused on methods to aggregate alert data and to identify attacks in progress (Cuppens and Miege 2002), there is significant scope for analysis from organizational and policy perspectives.

Theoretical Extensions. Two fundamental theoretical extensions are possible. First, future research can focus on the antecedents and consequents of the constructs identified in this research. Within this theme, four topics emerge that will be of significant practical relevance: (a) What managerial, organizational, and environmental factors lead to better organizational countermeasures? (b) What managerial actions reduce the three dimensions of perceived attractiveness? (c) What are the business consequences of IS security compromise? and (d) What can managers do to reduce passive and active Internet presence and their impact? Second, future research can also modify the proposed relationships and dimensions, and identify additional constructs beyond those in Figure 2. For example, research can start with an alternative categorization of attacks and generate different constructs that affect such categories. Alternatively, research could identify additional constructs that affect the attack categories described in this paper.

Concluding Discussion

The conceptual model and empirical analysis highlights three key differences between the ISCP and general crime contexts examined in the literature. First, the existence of two separate paths of attack and the importance of the opportunistic path are distinctive characteristics of the ISCP. The proliferation of tools and the lack of enforcement have created a unique environment where the cost of attack is negligible and the expertise required to exploit vulnerabilities is low, resulting in the opportunistic path being dominant in terms of attack volume. The antecedents of the two attack paths are also distinct. In the opportunistic path, mere presence drives attacks and firms can do little to control the antecedents. For the deliberate path, there are two antecedents—one which is intrinsic to the firm (target attractiveness) and the other which the firm can partially control (active presence). Second, the opportunistic path leads to the targeted path, creating a new way of searching for targets that is often independent of target attractiveness or its active presence. In this method, attackers find targets by chance and then follow a more deliberate approach. Third, the progression of attacks from information gathering to compromise attempts is also a distinctive feature of the ISCP that has some parallels in the crime literature on repeat victimization (Bowling 1993, McShane and Williams 1997). However, in the ISCP context, the initial attempts fall within the boundaries of legitimate activity that cannot often be stopped by the target organization without hindering other critical activities. If there are weaknesses in countermeasures, then such holes will be discovered and exploited.

Finally, although we did not empirically investigate the issue in this paper, the conceptual model highlights a moderating rather than a direct role for organizational countermeasures in the ISCP. This distinction is subtle but important. The rational choice models of crime (Ehrlich 1996) indicate that higher levels of deterrence lead to lower levels of crime in general. In the Internet environment, the low cost of attacking systems creates an environment where countermeasures do not necessarily reduce attack volume, but reduce the progression of attacks from information gathering to compromise attempts, and subsequently to information security compromise.

Acknowledgments

The authors thank SecureWorks, Inc., and Jon Ramsey, Chief Technology Officer, for their assistance with this research by providing expert consultation, a detailed explanation of their Security Operations Centers, and thorough grounding in the reality of the current security environment. The authors are especially appreciative that a summarized abstract of their database of security alert data was made available to them. Thanks to the senior editor, the associate editor, three anonymous reviewers, Luis Martins, Christina Shalley, and Detmar Straub for their comments on earlier drafts of this manuscript. All errors are the responsibility of the authors. The first author gratefully acknowledges financial support from the Alan & Mildred Peterson Foundation.

References

Akers, R. L., M. Krohn, L. Lanza-Kaduce, M. Radosevich. 1979. Social learning and deviant behavior: A specific test of a general theory. *Amer. Sociol. Rev.* **44**(4) 636–655.

Arora, A., R. Telang, H. Xu. 2004. Timing disclosure of software vulnerability for optimal social welfare. *Proc. Third Workshop Econom. Inform. Systems*, Minneapolis, 1–47.

Bailey, K. D. 1994. *Typologies and Taxonomies*: *An Introduction to Classification Techniques*. Sage Publications, Thousand Oaks, CA.

Banerjee, D., T. P. Cronan, T. W. Jones. 1998. Modeling IT ethics: A study in situational ethics. *MIS Quart.* **22**(1) 31–60.

Baron, R. M., D. A. Kenny. 1986. The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *J. Personality Soc. Psych.* **51**(6) 1173–1182.

Baskerville, R. 1993. Information systems security design methods: Implications for information systems development. *ACM Comput. Surveys* **25**(4) 375–414.

Bass, F. 1969. A new product growth for model consumer durables. *Management Sci.* **15**(5) 215–227.

Becker, G. 1968. Crime and punishment: An economic approach. *J. Political Econom.* **76**(2) 169–217.

Boockholdt, J. L. 1989. Implementing security and integrity in micro-mainframe networks. *MIS Quart.* **13**(2) 134–144.

Bowen, P., J. Hash, M. Swanson. 2005. *Guide for Developing Security Plans for Federal Information Systems*. National Institute of Standards and Technology Special Publication 800-18, Revision 1, Gaithersburg, MD, 1–45.

Bowling, B. 1993. Racial harrassment and the process of victimization. *British J. Criminology* **33**(2) 231–250.

Braithwaite, J. 1989. *Crime, Shame and Reintegration*. Cambridge University Press, Cambridge, UK.

Brancheau, J., B. Janz, J. Wetherbe. 1996. Key issues in information systems management: 1994–1995 SIM Delphi results. *MIS Quart.* **20**(2) 225–242.

Cavusoglu, H., B. Mishra, S. Raghunathan. 2004. The impact of Internet security breach announcements on market value of breached firms and Internet security developers. *Internat. J. Electronic Commerce* **9**(1) 69–104.

Cavusoglu, H., B. Mishra, S. Raghunathan. 2005. The value of intrusion detection systems in information technology security architecture. *Inform. Systems Res.* **16**(1) 28–46.

Chakrabarti, A., G. Manimaran. 2002. Internet infrastructure security: A taxonomy. *IEEE Network* **16**(6) 13–21.

Cohen, A. K. 1955. *Delinquent Boys*: *The Culture of the Gang*. Free Press, New York.

Cohen, L. E., M. Felson. 1979. Social change and crime rate change: A routine activity approach. *Amer. Sociol. Rev.* **44**(4) 588–608.

Coleman, J. W. 1987. Toward an integrated theory of white-collar crime. *Amer. J. Sociol.* **93**(2) 406–439.

Corbin, J., A. Strauss. 1990. Grounded theory research: Procedures, canons and evaluative criteria. *Qualitative Sociol.* **13**(1) 3–21.

Cuppens, F., A. Miege. 2002. Alert correlation in a cooperative intrusion detection framework. *Proc. 2002 IEEE Sympos. Security Privacy*, Oakland, CA, 202–215.

DeLooze, L. L. 2004. Classification of computer attacks using a self-organizing map. *Proc. 2004 IEEE Workshop Inform. Assurance*, U.S. Military Academy, West Point, NY, 365–369.

Dhillon, G., J. Backhouse. 2001. Current directions in IS security research: Towards socio-organizational perspectives. *Inform. Systems J.* **11**(2) 127–153.

Dickersen, J. E., J. Juslin, O. KouKousoula, J. A. Dickersen. 2001. Fuzzy intrusion detection. *Proc. Joint 9th IFSA World Congress and 20th NAFIPS Internat. Conf., 2001*, Vancouver, Canada, 1506–1510.

DiPietro, R., L. V. Mancini. 2003. Security and privacy issues of handheld and wearable wireless devices. *Comm. ACM* **46**(9) 74–79.

Dutta, A., K. McCrohan. 2002. Management's role in information security in a cyber economy. *California Management Rev.* **45**(1) 67–87.

Ehrlich, I. 1973. Participation in illegitimate activities: A theoretical and empirical investigation. *J. Political Econom.* **81**(3) 521–565.

Ehrlich, I. 1996. Crime, punishment and the market for offences. *J. Econom. Perspectives* **10**(1) 43–67.

Embar-Seddon, A. 2002. Cyberterrorism: Are we under siege? *Amer. Behavioral Scientist* **45**(6) 1033–1043.

Gattiker, U. E., H. Kelley. 1999. Morality and computers: Attitudes and differences in moral judgments. *Inform. Systems Res.* **10**(3) 233–254.

Glaser, B. G., A. L. Strauss. 1967. *The Discovery of Grounded Theory*: *Strategies for Qualitative Research*. Aldine De Gruyter, New York.

Gordon, L. A., M. P. Loeb. 2002. The economics of information security investment. *ACM Trans. Inform. System Security* **5**(4) 438–457.

Gottfredson, M. R., T. Hirschi. 1990. *A General Theory of Crime*. Stanford University Press, Stanford, CA.

Halbert, D. 1997. Discourses of danger and the computer hacker. *Inform. Soc.* **13**(4) 361–374.

Harrington, S. J. 1996. The effect of codes of ethics and personal denial of responsibility on computer abuse judgements and intentions. *MIS Quart.* **20**(3) 257–278.

Howard, J. D. 1998. *An Analysis of Security Incidents on the Internet 1989–1995*. Carnegie Mellon University, Pittsburgh.

Julisch, K. 2003. Clustering intrusion detection alarms to support root cause analysis. *ACM Trans. Inform. System Security* **6**(4) 443–471.

Kannan, K., R. Telang. 2005. Market for software vulnerabilities? Think again. *Management Sci.* **51**(5) 726–740.

Kemmerer, R. A., G. Vigna. 2002. Intrusion detection: A brief history and overview. *IEEE Comput.* **35**(4) 27–30.

Loch, K. D., H. H. Carr, M. E. Warkentin. 1992. Threats to information systems: Today's reality, yesterday's understanding. *MIS Quart.* **16**(2) 173–186.

Lohmeyer, D. F., J. McCrory, S. Pogreb. 2002. Managing information security. *McKinsey Quart.* Special Edition(2) 12–16.

McShane, M., F. P. Williams. 1997. *Victims of Crime and the Victimization Process*, Vol. 6. Garland Publications, New York.

Miethe, T. D., R. F. Meier. 1994. *Crime and Its Social Context*: *Toward an Integrated Theory of Offenders, Victims, and Situations*. State University of New York Press, New York.

Ning, P., Y. Cui, D. S. Reeves, D. Xu. 2004. Techniques and tools for analyzing intrusion alerts. *ACM Trans. Inform. System Security* **7**(2) 274–318.

Sandhu, R., P. Samarati. 1996. Authentication, access control, and audit. *ACM Comput. Surveys* **28**(1) 241–243.

Sarathy, R., K. Muralidhar. 2002. The security of confidential numerical data in databases. *Inform. Systems Res.* **13**(4) 389–403.

Schechter, S. E., M. D. Smith. 2003. How much security is enough to stop a thief? The economics of outsider theft via computer systems and networks. G. Davida, Y. Frankel, O. Rees, eds. *Proc. Seventh Financial Cryptography Conf.*, January 27–30, 2003, *Lecture Notes in Computer Science*, **2742**, LCNS 2437. Springer-Verlag, New York, 7–10.

Schultz, E. 2004. Sarbanes-Oxley: A huge boon to information security in the US. *Comput. Security* **23**(5) 353–354.

Siponen, M. 2005. Analysis of modern IS security development approaches: Towards the next generation of social and adaptable ISS methods. *Inform. Organ.* **15** 339–375.

Sobel, M. E. 1982. Asymptotic confidence intervals for indirect effects in structural equation models. *Sociol. Methodology* **13** 290–312.

Speers, T., S. Wilcox, B. Brown. 2004. The privacy rule, security rule, and transaction standards: Three sides of the same coin. *J. Health Care Compliance* **6**(1) 11–14.

Straub, D. W. 1990. Effective IS security: An empirical study. *Inform. Systems Res.* **1**(3) 255–276.

Straub, D. W., W. D. Nance. 1990. Discovering and disciplining computer abuse in organizations: A field study. *MIS Quart.* **14**(1) 45–60.

Straub, D. W., R. J. Welke. 1998. Coping with systems risk: Security planning models for management decision making. *MIS Quart.* **22**(4) 441–469.

Sutherland, E. 1947. *Principles of Criminology*. Lippincot, Philadelphia.

Voiskounsky, A. E., O. V. Smyslova. 2003. Flow-based model of computer hacker's motivation. *Cyber Psych. Behav.* **6**(2) 171–180.

Weber, R. 2002. Theoretically speaking. *MIS Quart.* **27**(3) iii–xii.

Whetten, D. A. 1989. What constitutes a theoretical contribution? *Acad. Management Rev.* **14**(4) 490–495.

Willison, R. A. 2002. *Opportunities for Computer Abuse: Assessing a Crime Specific Approach in the Cast of Barings Bank*. London School of Economics and Political Science, London.

Zmud, R. 1998. Editor's comments. *MIS Quart.* **22**(2) 7–10.