ACQUISITION AND DIFFUSION OF TECHNOLOGY INNOVATION

A Thesis
Presented to
The Academic Faculty

by

Samuel B. Ransbotham III

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy in the
College of Management

Georgia Institute of Technology
March 2008

ACQUISITION AND DIFFUSION OF TECHNOLOGY INNOVATION

Approved by:

Associate Professor Sabyasachi Mitra,
Committee Chair
College of Management
Georgia Institute of Technology

Associate Professor Frank Rothaermel
College of Management
Georgia Institute of Technology

Associate Professor Vivek Ghosal
School of Economics
Georgia Institute of Technology

Professor Sandra Slaughter
College of Management
Georgia Institute of Technology

Professor Sridhar Narasimhan
College of Management
Georgia Institute of Technology

Date Approved: 24 March 2008

ACKNOWLEDGEMENTS

Acknowledgement sections are typically casually glossed over. Please don't do that now! Each name represents countless hours of active and behind-the-scenes support. And for each person mentioned, dozens of other people should have been mentioned as well.

I first offer thanks to my committee members— Saby, Vivek, Sri, Frank and Sandy. By tradition, students should be frustrated with their committee; I am not. At every stage they helped not hindered. I am grateful to the faculty and staff who helped make my third (and final?) degree from Georgia Tech a wonderful experience– Terry Blum, Mike Cummins, Rui Dai, Chris Forman, Stuart Graham, Matt Higgins, Ishwar Murthy, Eric Overby, Ann Scott, Vinod Singhal, Samit Soni, Marie Thursby, D. J. Wu, and Han Zhang. I thank my student cohort of Anne Fuller, Drew Hess, Jim Kroes, Jifeng Luo, Zhe Qu, and Fang Zhong. Further, much of this dissertation would not have been possible without the generous assistance of Jon Ramsey, Mike Vandiver and the SecureWorks organization. I am also appreciative of the assistance of the TI:GER program and the Alan & Mildred Peterson Foundation.

On a personal note, I again thank Saby Mitra who has been so much more than an advisor as a true model of intellectual excellence with an "enviable writing style". I also thank my friend Robert Martin for encouraging geeky curiosity. I am blessed by my parents, Ben and June Ransbotham, and my sister, LeAnn, who have been constant supporters. And finally, I thank Stephanie Jernigan who just makes everything fun and the newest rookie on our team, Ava, whose recent arrival has already changed everything.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

SUMMARY

My dissertation research involves three focal questions within the broad topic of technology innovation with a focus on information security. The questions examined are:

1. When should an acquirer buy an emerging technology innovation?
2. How do negative innovations diffuse through the economic environment?
3. How effective are the reward-based mechanisms in restricting the diffusion of negative innovations through the economic environment?

Chapter 2 addresses the first question with an empirical analysis of technology innovation acquisitions in the telecommunications industry from 1995 to 2001.

Chapter 3 addresses the second question with a cross industry analysis of security alert data generated by intrusion detection systems during 2006.

Chapter 4 addresses the third question with a large scale empirical analysis of vulnerabilities disclosed by both reward-based and non-reward-based mechanisms.

CHAPTER I

INTRODUCTION

My dissertation research involves three focal questions within the broad topic of technology innovation. The questions examined are:

1. When should an acquirer buy an emerging technology innovation?
2. How do negative innovations diffuse through the economic environment?
3. How effective are reward-based mechanisms in restricting the diffusion of negative innovations through the economic environment?

Acquisition: In the first essay, I examine value created through the external acquisition of nascent technology innovation. External acquisition of new technology is a growing trend in the innovation and product development process, particularly in high technology industries, as firms complement internal research and development efforts with aggressive acquisition programs. Yet, despite its importance, there has been little empirical research on the timing of acquisition decisions in high technology environments. Building on a real options perspective, I examine the impact of target age on value created for the buyer. Applying an event study methodology to technology acquisitions in the telecommunications industry from 1995 to 2001, empirical evidence supports acquiring early in the face of uncertainty. Furthermore, both target intellectual property and the target's public/private status moderate the impact of target age on value created for the buyer. In summary, the equity markets reward the acquisition of younger companies and penalize the acquisition of older targets that do not own patents or are publicly traded.

Diffusion: In sharp contrast to the first essay, the second essay examines the diffusion of *negative* innovations. While destruction can be creative (Schumpeter, 1934), certainly not all destruction is creative. Some is just destruction. Rogers (2003, p. 106) claims that "one of the most serious shortcomings of diffusion research is its pro-innovation bias". While in the previous essay, innovation is considered beneficial; this essay focuses on negative innovation. Specifically, I examine two fundamentally different paths to information security compromise— an opportunistic path and a deliberate path. Through a grounded approach using interviews, observations, and secondary data, I advance a model of the information security compromise process from the perspective of the attacked organization. Using one year of alert data from intrusion detection devices, empirical analysis provides evidence that these paths follow two distinct, but interrelated diffusion patterns. Although distinct, I find empirical evidence that these paths both converge and escalate. Beyond the specific findings in the Internet security context, the study leads to a richer understanding of the diffusion of negative technological innovation.

Reward-based Mechanisms: In the third essay, I build on the second essay by examining the effectiveness of reward-based mechanisms in restricting the diffusion of negative innovations. There are has been considerable general debate about the disclosure of vulnerabilities and recent specific debate about the creation of market-type mechanisms to reward benign disclosure. In particular, concerns have been raised that vulnerability markets introduce the opportunity for information leakage which decreases social welfare (Kannan and Telang, 2005). Using two years of alert data for vulnerabilities disclosed through reward-based and non-reward-based mechanisms, I find evidence of vulnerability market effectiveness despite any leakage which may be occurring. While disclosures through reward-based mechanisms are just as likely to be exploited as non-reward-based disclosures, exploits from reward-based disclosures are less likely to occur in the first week after disclosure. Further the overall volume

of alerts is reduced. This research helps determine the effectiveness of reward-based mechanisms and provides guidance for security policy makers.

CHAPTER II

TARGET AGE AND THE ACQUISITION OF INNOVATION IN HIGH TECHNOLOGY INDUSTRIES

2.1 Introduction

The importance of new product development is highlighted through a vast literature on the topic in operations management (Krishnan and Ulrich, 2001; Terwiesch et al., 1998), marketing (Hauser et al., 2006; Wind and Mahajan, 1997), strategy (MacMillan and McGrath, 2002; McGrath and Nerkar, 2004) and organizational behavior (Brown and Eisenhardt, 1995). Typical issues examined in this literature include concept development and product definition (Ulrich and Ellison, 1999), supply chain design (Lee and Tang, 1997), organizational practices (Brown and Eisenhardt, 1995), development process management (Bhuiyan et al., 2004; Terwiesch and Loch, 1999), and intellectual property (Ziedonis, 2004). Recent surveys appear in Shane and Ulrich (2004) and Krishnan and Ulrich (2001). Barring a few exceptions (Ahuja and Katila, 2001; Higgins and Rodriguez, 2006; Lambe and Spekman, 1997), the primary focus of this research stream has been on the product development and innovation process internal to the firm.

In high technology industries, external acquisition of new technology plays a vital role in the product development process (Higgins and Rodriguez, 2006). Since time-to-market pressures often render internal development too slow (Lambe and Spekman, 1997), firms like Microsoft and Cisco augment internal research and development (R&D) with aggressive acquisition programs that are becoming increasingly

important as a way for "maturing strategic buyers to access new growth opportunities" and to place "bets on new ideas or technologies" (Anonymous, 2006). Acquisitions also add a key exploratory component to product development, allowing access to technologies that fill gaps or correct blind spots (Chesbrough, 2003). Further, technology acquisitions foster a strong market for ideas, providing incentives for entrepreneurs to sweat, to risk and, maybe, to exit wealthy (Gans and Stern, 2003). However, despite its importance, technology acquisitions have received limited attention in the product development literature, and value creation through acquisitions is not well understood in high technology environments where acquisitions foster innovation rather than conglomerate diversification (Chaudhuri and Tabrizi, 1999).

In this paper, we focus on the effect of a fundamental characteristic of a target, specifically target age, on value creation for the buyer in high technology environments. Target age is an objective, observable (even for small, private startups) and critical differentiator that has received considerable media and industry attention, but limited research consideration. From the perspective of the buyer, the emergence of an early stage company begins an inherent conflict between risk and safety. Should organizations wait until more information is available about the target, its technology, its product, and the market so that a better valuation can be obtained? Or should the target be acquired early to preempt others and gain early access to key technologies? Even conventional proverbs offer conflicting advice as managers may choose to "look before they leap" or alternatively they may believe that "he who hesitates is lost". This ambiguity is also reflected in the trade literature, where target age is a frequent focal point (Anonymous, 2006; Wysocki, 1999). Diametrically opposed opinions are espoused such as emphasizing that "the important thing is, the bets are being placed on younger companies" (Wysocki, 1999), while others find lessons in the difficulties that acquirers like Cisco and Lucent have had with acquiring early stage companies (Schiesel, 2000). Clearly the role of target age in value creation is unclear.

Recent acquisition research has focused on some related aspects of timing, although not specifically on the effect of target age on value creation for the buyer. In a study of acquisitions in the context of industry waves, positive effects on acquirer value are seen from acquisitions that are made towards the beginning of an acquisition wave (Carow et al., 2004). In a study on the effects of structural integration on innovation outcomes, Puranam et al. (2006) find that increased target age decreases the hazard rate of acquirer new product introductions. When accounting based performance measures are used, increasing target age increases the benefits from an acquisition (Chaudhuri et al., 2005). In a study of the telecommunications industry, Warner et al. (2006) find that acquisitions are more likely to occur before the establishment of a formal standard when the target firm has standards relevant intellectual property.

The product development literature highlights a similar dilemma between the use of proven technologies and unproven (but promising) technologies in developing new products (Bhattacharya et al., 1998; Chaudhuri and Tabrizi, 1999; Iansiti, 1995). Analytical models demonstrate that selecting only proven technologies for inclusion in product design, may not be optimal in dynamic environments (Krishnan and Bhattacharya, 2002; Loch and Terwiesch, 2005). Likewise, forcing early finalization of specifications may result in a firm getting locked into an incorrect position (Bhattacharya et al., 1998). The fundamental insight from the analytical models is that flexibility is valuable in dynamic environments because it affords managers the ability to change course as better market and customer information become available. However, flexibility comes at a cost, since firms may have to invest in parallel technologies, over-design the product to work with alternative technologies, and monitor the product development process closely to terminate ineffective paths (Bhattacharya et al., 1998).

In this research, we examine acquisitions made by equipment manufacturers within

the telecommunications industry during 1995-2001 because of the industry's emerging standards, deregulation, numerous innovations, acquisition volume, and uncertainty during that period (Warner et al., 2006). These features indicate that the telecommunications industry fit the definition of high velocity during this period since there was "rapid and discontinuous change in demand, competitors, technology and/or regulation, such that information [was] often inaccurate, unavailable, or obsolete" (Bourgeois and Eisenhardt, 1988, p. 816). Evaluation of acquisition opportunities is particularly difficult in these environments since it is not clear which technologies will dominate or how the markets will evolve. We develop our hypotheses through a real options perspective that is particularly relevant to the valuation of opportunities in the high velocity environment of the telecommunications industry. A real options framework adds a fresh perspective on technology acquisitions with considerable explanatory power in uncertain environments (McGrath, 1997).

We use standard event study methods (Brown and Warner, 1985) to measure value creation through acquisitions by examining the abnormal stock market reaction to acquisition announcements by equipment manufacturers in the telecommunications industry. The use of event study methods has three advantages in our context. First, the event study method effectively isolates the impact of the acquisition on the acquiring firm better than aggregate measures based on annually reported accounting data (MacKinlay, 1997), particularly when firms make several acquisitions within the same year (Fuller et al., 2002). Second, for acquisitions of early stage targets, immediate impact on accounting indicators may be insignificant or even negative and will depend more on the stage of development of the innovation rather than its future value. Further, intangible values inherent in technology acquisitions (such as intellectual property and knowledge assets) are difficult to value through traditional productivity metrics, while equity prices include a capitalization of all future benefits. Third, event studies are well established in the literature as a method for assessing

value created through acquisitions. Utilizing a metric that has been frequently used in the literature enables us to exploit previous findings in our model.

There are two primary contributions of this research. First, theoretical underpinnings of previous empirical research on value creation through acquisitions have focused on the financial drivers of acquisitions, such as economies of scale and cost savings (Lambrecht, 2004), managerial mis-incentives (Moeller, 2004), equity misvaluations (Shleifer and Vishny, 2003), and free cash flow (Jensen, 1986). While these variables have considerable explanatory power in the traditional environments analyzed, they do not capture the primary drivers of acquisitions in the high technology industries, such as time-to-market pressures, capability enhancement in new technologies, and exploratory resource configurations (Chaudhuri and Tabrizi, 1999; Iansiti, 1995). The real options framework and empirical analysis in this paper provides a fresh perspective and a new set of value drivers in the technology acquisition context. Second, we empirically investigate the impact of an observable and objective characteristic of the target (specifically target age) that has been the source of considerable debate in the trade literature, but has received scant attention in the academic literature. Further, we identify and evaluate conditions that moderate the impact of this critical differentiator on value creation for the acquirer.

The rest of this chapter is organized as follows. In the next section, we develop our hypotheses on the impact of target age on value creation for the buyer. Then, we detail the data and methodology used to test the hypotheses. Next, we discuss the results of the analysis. Finally, we summarize the findings of the research and outline future research directions.

2.2 Theory and Hypotheses Development

2.2.1 The Real Options Perspective

Two fundamental and counter-intuitive principles underlie the real options perspective on the valuation of technology investments that make it suitable for the context examined here. First, it is uncertainty that drives the value of real options (McGrath, 1997), since options are characterized by a limit on the potential loss (the cost of the option) with a variable, but potentially large return. This is similar to the acquisition of technology, where the loss is limited to the cost of the acquisition, but the potential benefits are large if the right environmental conditions develop. Second, the initial investment in an option gives a firm the ability to select subsequent actions only if their outcomes are favorable. This possibility of abandonment is a key feature of the real options approach (Adner and Levinthal, 2004), and is also characteristic of a technology acquisition where subsequent investments to develop the technology and market are made only if profitable. Explicit recognition and valuation of this flexibility is a key feature of the real options approach. Consequently, many authors have prescribed the real options perspective as an alternative approach for the valuation of investments in uncertain environments (Amram and Kulatilaka, 1999; Michel, 2007; Fichman et al., 2005; Luehrman, 1998).

2.2.2 Acquisitions through a Real Options Perspective

Two key points underlie our application of the real options perspective in the context of technology acquisitions in a high velocity industry. First, we view the target as a combination of mature operations and growth options that have yet to be explored. Targets vary in the level of growth options that are present. The price of the target reflects the value of its existing operations and the value of its growth options that it is likely to exploit on its own, since a rational target will not accept a price that is lower. In this sense, the acquisition can be viewed not as the strike of an option,

but instead as the initial purchase of an option. In summary, the addition of the real options perspective helps to decompose an acquisition into two parts—an acquisition in the market for products and an acquisition in the market for ideas. In the former, the acquisition focuses on existing operations; in the latter, the focus is on future growth options.

Second, in the real options perspective on acquisitions, the synergistic value comes from the growth options that the acquirer can better exploit than the target can on its own. Value creation from the acquisition is dependent on the magnitude of this synergistic value. A key point is that if the target could fully exploit its innovation on its own, then this would be reflected in the price paid for the target. Value is created when the combination of acquirer and target resources allow possibilities that neither could realize alone (Capron and Pistre, 2002). Acquirers are typically larger than targets — in our data set, we found acquirers to be an average of two orders of magnitude larger than their targets (the average ratio of acquirer assets to price paid for the target was 117 to 1). Consequently, acquirers have more complementary assets than their targets, such as access to capital, established distribution networks, or manufacturing operations necessary for the innovation of a target to be useful (Tripsas, 1997).

2.2.3 Target Age through a Real Options Perspective

Table 1 summarizes the impact of target age on several sources of value creation (organized along two dimensions) in the technology acquisition context, when viewed through a real options perspective. First, younger targets have fewer mature operations and more growth options than older targets. By acquiring a target early at lower costs, more technology acquisitions can be done within a given budget, and the acquirer is then able to build a portfolio of growth options (Girotra et al., 2006), enabling flexibility. Rather than acting merely as a substitute for internal innovation,

the creation of a portfolio of technologies allows an acquirer to evolve its product portfolio opportunistically and to experiment (Rindova and Kotha, 2001). In uncertain environments, this flexibility is valuable in multiple ways. It allows the firm to defer technology choices to a time when more information is available about customer preferences (Bhattacharya et al., 1998), enables a firm to pursue alternative product development paths (Krishnan and Bhattacharya, 2002), achieve time-to-market objectives without sacrificing product quality (Cohen et al., 1996), and avoid the negative effects of being late to market (Hendricks and Singhal, 1997).

Second, target firms vary in the level of uncertainty inherent in its technology and market. It is exactly the substantial market and technological uncertainty associated with the growth options in a younger target that drives value from a real options perspective, since "the greater the variance in net revenues that might be accessed by commercializing the technology, the greater the option value" (McGrath, 1997, p. 979). In the acquisition context, downside losses are limited to the price paid for the target. On the margin, younger companies cost less and this serves to limit potential downside losses. At the same time, younger companies often possess newer technology whose upside potential is high, particularly in winner-take-all industries. The idiosyncratic risk associated with a young target reduces its valuation and price, but when part of a portfolio of options for the acquirer, this idiosyncratic risk is reduced through diversification (Goyal and Santa-Clara, 2003). As a target gets older, its inherent uncertainty is reduced, lowering its option value, and increasing the price paid for the target.

Finally, older targets have also had time to develop more infrastructure and take advantage of growth options on their own. Therefore, they benefit less from the complementary assets (Tripsas, 1997), commercialization expertise, or managerial experience (King and Tucci, 2002) in the acquiring firm. The increased ability to function independently shows, on the margin, that there is less potential for synergy

and value creation. Further, integration difficulties increase as targets grow older, creating pressure to retain their original identity and staff (Ranft and Lord, 2002), and reducing synergistic value. Thus, we empirically test the preceding reasoning through the following hypothesis.

Hypothesis 1 *In high velocity environments, value creation for the buyer will be negatively associated with target age.*

Table 1: Real Options Perspective on Value Creation through Technology Acquisitions

Source of Value	**Explanation**	**Primary Effect**	**Moderating Effects**	
		Target Age	**Target Patents**	**Target Private Status**
Growth Options	A target is viewed as a combination of mature operations and unexplored growth options	Young targets have less mature operations and more growth options, enabling a portfolio of options for the acquirer, for opportunistic evolution and experimentation. This flexibility is valuable in dynamic environments. (Bhattacharya et al., 1998; Cohen et al., 1996; McGrath, 1997; Rindova and Kotha, 2001) Higher uncertainty associated with the growth options of a young target generates greater option value for the acquirer. Also, idiosyncratic risk inherent in a young target reduces target valuation and price (Goyal and Santa-Clara, 2003; McGrath, 1997; McGrath and Nerkar, 2004)	Patents indicate the presence of R&D that creates growth options even for older targets, reducing the negative effect of target age (Griliches, 1990; McGrath and Nerkar, 2004; Sorensen and Stuart, 2000) Patents disclose information about growth options and reduce the perceived idiosyncratic risk inherent in young targets, thereby raising its valuation, and reducing the benefits of acquiring early (Austin, 1993; Hall et al., 2005)	
Synergy	Unexplored growth options benefit from the superior resources of a large acquirer	Young targets lack infrastructure to exploit growth options, thereby increasing synergy from acquisition. Young targets have less rigid operations that reduce integration difficulties (King and Tucci, 2002)(Tripsas, 1997).		Public status provides access to resources, enabling even public young targets to develop infrastructure, reducing synergy from acquiring early(Capron and Shen, 2007; Chang, 1998; Faccio et al., 2006; Fuller et al., 2002; Officer, 2007)

2.2.4 The Moderating Role of Target Intellectual Property

A key difference in some target companies lie in the intellectual property (IP) they possess, protected through patents. While the value of the patent can be incorporated in the price paid for the target, we argue in Table 1 that patents mitigate the negative effects of increased target age. The table focuses on this moderating role of target patents, rather than their direct impact on value creation. The table identifies two mechanisms through which patents reduce the negative effects of increased target age.

First, patents signal the presence of research and development activity in the target (Griliches, 1990). These activities produce on-going innovation, reducing concerns about aging and a lack of innovation (Sorensen and Stuart, 2000), and creates unexplored growth options that make an older target more akin to a young company. Even for older targets, patented technologies benefit from the commercialization expertise of a larger acquirer and subsequent "amplifying" investments that increase the value of the technology (McGrath, 1997), such as lobbying to enact favorable legislation, participating in industry organizations to promote compatible standards, and exploiting existing customer relationships to generate demand (McGrath, 1997). Thus, patents indicate growth options even in an older target, and reduce the negative impact of target age.

Second, patents provide protection from imitation and disclose information about the target's technology (Hall et al., 2005). Patents are awarded after a review of originality and uniqueness by the patent office and this independent review partially reduces the uncertainty associated with the technology of a young target. Patents also raise visibility of young targets among potential bidders. This increases its valuation and its price (Austin, 1993), and consequently reduces the benefits of early acquisition.

In summary, patents mute the negative effect of target age for older targets and information disclosure reduces the benefits of early acquisition. Therefore, we further hypothesize that:

Hypothesis 2 *In high velocity environments, the presence of intellectual property in the target mitigates the negative effect of the target age on value created for the buyer.*

2.2.5 Acquiring Private Targets

Another key observable difference is that some targets are public while others remain private at the time of acquisition. Prior research has found significant differences between the two sub-groups and have documented a direct positive effect of target private status on acquirer value (Capron and Shen, 2007; Faccio et al., 2006; Fuller et al., 2002; Officer, 2007). Along lines of reasoning that are similar to that of Hypothesis 2, we argue that a target's private status mutes the negative impact of target age on value creation for the acquirer. As before, we focus on this moderating role of target private status, rather than its direct impact on value creation.

Consider an older target that is privately held. Due to its limited access to the capital markets, in spite of its age, its unexplored growth options can benefit from the superior resources of a public acquirer in multiple ways. The prominence and greater resources of the public acquirer will enable it to make effective amplifying investments (McGrath, 1997) that increase the value of the unexplored growth options. Commercialization of growth options require access to resources for manufacturing, marketing and distribution that can benefit from access to the capital markets. Thus, private status of the target retains the synergy gains from acquisition, even for older private targets. Conversely, public status provides access to resources, enabling even public young targets to develop infrastructure, reducing synergy from early acquisitions. Therefore, we test the preceding logic through the following hypothesis.

Hypothesis 3 *In high velocity environments, privately held status of the target mitigates the negative effect of the target age on value created for the buyer.*

2.3 Data and Methodology

2.3.1 Data Sources

To build our data set, we searched the *Wall Street Journal*, *Business Wire*, *PR Newswire* and *Dow Jones News Service* to identify 361 acquisition announcements by publicly traded buyers in the telecommunications industry from 1995 to 2001. Of these 361 announcements, 249 announcements were by equipment manufacturers (such as Cisco, Nortel and Lucent), while 112 were acquisition announcements by service providers (such as Verizon, Cingular and MCI). Equipment manufacturers made acquisitions to obtain new products and technology, while a majority of the acquisitions by service providers related to the acquisition of new customers, new geographic coverage areas, new licenses and consolidation for economies of scale. To focus on the acquisition of products and technology in a high velocity industry, we concentrated on the 249 technology acquisition announcements by equipment manufacturers. The dataset was further augmented with information from the Securities Data Company (SDC) Mergers & Acquisitions database. First, we checked for any acquisitions by equipment manufacturers in the SDC database during this time period to ensure that no relevant acquisitions were missed from the search for announcements. Additionally, though announced, some acquisitions were later withdrawn. After removing withdrawn acquisitions, and those for which insufficient market trading data was available, 238 acquisitions remained.

Because of the importance of the exact date that the market learns of the acquisition (McWilliams and Siegel, 1997), we searched all publications included in the Factiva database for a one year period preceding the announcement date, to check for leakage of information regarding the acquisition. We adjusted the announcement date to the earliest date when the acquisition was announced or reported in the media. When the announcement was made after 4 p. m. or on a day the equity market was closed, we adjusted the announcement date to the next trading date.

Table 2: Descriptive Statistics and Pearson Product Moment Correlations between Variables

Variable	**Mean**	**Std. Dev.**	**1**	**2**	**3**	**4**	**5**	**6**
1. Abnormal Return	-0.009	0.056	1.00					
2. Buyer Market Value	0.092	0.115	0.057	1.00				
3. Buyer Free Cash	0.140	0.191	-0.018	0.214	1.00			
4. Buyer R&D Intensity	0.155	0.097	-0.067	0.023	-0.633	1.00		
5. Buyer Leverage	0.279	0.142	0.009	-0.039	-0.154	-0.133	1.00	
6. Buyer Acq. Exp.	29.709	33.057	0.064	0.776	0.249	-0.066	-0.070	1.00
7. Target Age	8.355	8.968	-0.153	-0.122	-0.017	-0.076	0.218	-0.087
8. Target Employees	533.043	1187.071	-0.189	-0.120	-0.025	-0.144	0.226	-0.053
9. Target Private	0.667	0.473	0.195	0.115	-0.014	0.085	-0.136	0.145
10. Patent Presence	0.518	0.501	-0.037	-0.039	0.051	-0.079	0.140	-0.025
11. Patent Stock	150.924	431.711	-0.243	-0.020	0.048	0.036	0.073	0.044
12. Acquisition Weight	117.292	293.628	-0.153	-0.273	-0.211	-0.004	0.037	-0.279
13. Acquisition Value	1.255	3.658	-0.222	0.044	0.023	0.312	0.019	-0.022
14. Payment Method	0.738	0.442	-0.030	0.050	-0.077	0.205	-0.069	-0.102
15. Prior Relationship	0.234	0.425	-0.097	0.122	-0.018	0.021	0.073	0.123
16. Post Bubble	0.348	0.478	0.079	0.252	-0.060	0.140	-0.064	0.243
17. Early Mover	0.043	0.203	0.003	-0.160	0.040	-0.137	0.062	-0.156
18. S&P Index (scaled)	1.071	0.224	0.010	0.415	-0.113	0.258	-0.011	0.294

	7	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
8.	0.656	1.00									
9.	-0.479	-0.393	1.00								
10.	0.341	0.324	-0.390	1.00							
11.	0.485	0.582	-0.286	0.382	1.00						
12.	0.233	0.502	-0.329	0.137	0.126	1.00					
13.	0.184	0.365	-0.248	0.237	0.492	0.218	1.00				
14.	-0.123	-0.041	0.048	-0.133	0.020	0.010	0.136	1.00			
15.	0.196	0.208	-0.226	0.279	0.280	0.076	0.294	-0.072	1.00		
16.	-0.073	-0.181	0.145	-0.037	-0.091	-0.110	0.046	0.047	0.022	1.00	
17.	0.121	0.057	-0.170	0.045	-0.012	0.014	-0.054	0.106	-0.048	-0.162	1.00
18.	-0.093	-0.080	0.142	-0.013	0.012	-0.099	0.122	-0.002	0.031	0.434	-0.510

Sample size is 141 and includes the firms in the final sample for which we had abnormal returns, and the values for all control variables.

2.3.1.1 Determining the age of the target

Unfortunately, the age of the target at the time of acquisition was not readily available through public data sources. To determine the company inception date, several sources were consulted. First, in some cases, the press release about the acquisition noted the start date of the target company. Also, news articles profiling the company or company founders sometimes noted the start date. By searching through news archives and company filings, start dates were obtained for 185 of the 238 companies in our sample. In 47 cases, both the month and year were available; in the remaining 138 cases, only the year was available and the beginning of the year was used to determine target age. The age of the target at the time of acquisition ranged from 2 months to 61 years with a mean of 8.4 years.

2.3.1.2 Calculating Abnormal Returns

We use the event study methodology to estimate the change in stock price (the abnormal return) for the acquirer attributable to the acquisition announcement by adjusting the stock price changes for market-wide movements (Brown and Warner, 1985). Abnormal returns are calculated using both the Market Model as well as the Market Adjusted Return model.

The Market Model posits a linear relationship between the return on a stock and the return on the market portfolio over a given time period. This relationship is expressed as: $r_{i,t} = \alpha_i + \beta_i r_{m,t} + \varepsilon_{i,t}$, where $r_{i,t}$ is the return of stock i on day t; $r_{m,t}$ is the return of the market portfolio on day t; α_i is the intercept of the relationship for stock i; β_i is the slope of the relationship for stock i; and $\varepsilon_{i,t}$ is the error term for stock i on day t. The term $\beta_i r_{m,t}$ is the return to stock i on day t that can be attributed to market wide movements, while $\varepsilon_{i,t}$ is the unexplained part of the return that captures the effect of firm specific events on day t. For each firm, we estimate $\hat{\alpha}_i$ and $\hat{\beta}_i$ using ordinary least squares (OLS) regression over an estimation period

of 200 trading days ending 10 days prior to the acquisition announcement, with the equally weighted Center for Research in Security Prices (CRSP) index as a proxy for the market portfolio. A minimum of 40 return observations in the estimation period is required for the estimation procedure. The abnormal return ($A_{i,t}$) for stock i on day t is: $A_{i,t} = r_{i,t} - \hat{\alpha}_i - \hat{\beta}_i r_{m,t}$, where $r_{i,t}$ is the actual return on stock i on day t. In the absence of any abnormal return, the return for the stock can be predicted by the Market Model parameters and any excess return (error term) can be attributed to firm specific events on that day.

Our primary results and discussion are based on the Market Adjusted Return model as recommended when frequent acquisitions overlap the estimation period used in the Market Model, reducing confidence in the Market Model estimated parameters (Fuller et al., 2002). In the Market Adjusted Return model, the abnormal return ($A_{i,t}$) for stock i on day t is calculated as $A_{i,t} = r_{i,t} - r_{m,t}$. The rationale is that in the absence of any abnormal return, the return for the stock can be predicted by the market return. For short-window event studies, any gain in estimation from including the Market Model parameters may be lost by overlap of other acquisitions during the model parameter estimation period (Fuller et al., 2002). Therefore, we focus on the Market Adjusted Returns in our analysis; the Market Model results are included to demonstrate the robustness of the results. To summarize the average valuation impact of acquisition announcements on the market value of firms in our sample, we focus on the abnormal returns ($A_{i,0}$) on the event day ($t = 0$). The use of a one day window allows us to isolate the effects of the acquisition announcement (McWilliams and Siegel, 1997). Consistent with other research, we use the abnormal returns ($A_{i,0}$) as the dependent variable in the regressions (Asquith et al., 1983; Chang, 1998).

2.3.2 Control Variables

Due to the vast literature on acquisitions, it is critical to control for known effects on the abnormal returns associated with acquisitions, to isolate the impact of target age. Four types of control variables were used in the following regressions— buyer characteristics, target characteristics, acquisition characteristics, and environmental characteristics. All monetary values are converted to the January 1995 equivalent using the U.S. Department of Labor, Bureau of Labor Statistics, consumer price index.

2.3.2.1 Buyer Characteristics

For buyer characteristics, we incorporated the *total market value* of the buyer immediately prior to the announcement because firm size has been found to influence acquirer valuation (Moeller et al., 2004) and because abnormal returns are expressed as percentages of market value. The buyer market value ranges from 104 million US$ to 430 billion US$ with a mean of 92 billion US$. The *buyer free cash intensity* (defined as the net income for the prior year minus income taxes minus preferred and common dividends divided by revenue) is included to control for excess free cash leading to low-benefit acquisitions (Jensen, 1986) and ranges from -1.25 to 0.44 with a mean of 0.14. The *buyer R&D intensity* (defined as the expenditure for the prior year on R&D divided by revenue) is included to control for absorptive capacity (Cohen and Levinthal, 1990) and ranges from 0.01 to 0.84 with a mean of 0.15. The *buyer leverage* (defined as the prior year debt divided by assets) is included to account for possible improvements in managerial decision making due to high leverage and subsequent oversight by the debt providers (Jensen, 1986). Buyer leverage ranges from 0.03 to 0.70 with a mean of 0.28. Further, we include the *number of prior acquisitions* that a firm has done at the time of the announcement to control for learning from prior experiences (Hayward, 2002). This data is calculated from the SDC database

of mergers and acquisitions. Finally, we include *firm fixed effects* for seven acquirers with five or more acquisitions, to control for unobserved heterogeneity from a small number of frequent acquirers that could affect the results (the results are robust to including, excluding or changing the threshold of this frequent acquirer set).

2.3.2.2 Target Characteristics

Next, because private firms were 67% of our sample, we were limited to data available for private firms. For target characteristics, we use the *total number of employees* at the target at the time of the acquisition to control for the target firm size. Because our independent variable is target age, it is important to distinguish between specific age related effects and those due to target size (Sorensen and Stuart, 2000). Target employees range from 17 to 7800 with a mean of 533. To determine the number of employees, we combined information from SDC, press releases about the acquisition, news articles about the target, and required filings. Because of the difficulty in accurately determining the number of employees, 28 acquisitions were excluded; however, excluded acquisitions range across all ages and acquisition values. The *public/private status* (defined as 1 if the target was private, 0 if public) is included to control for previously documented public versus private effects (Fuller et al., 2002; Officer, 2007, e.g.).

2.3.2.3 Target Patents and Patent Citations

To determine if the target company held any patents, we consulted data directly available from the U.S. Patent and Trademark Office and created a dataset of 2,264 individual patents for the target firms including filing date and grant date as well as a detailed list of the patents which cited patents within the dataset. Based on this data, we incorporated a *target patent indicator* variable that was set to 1 if the target held one or more patents at the time of acquisition and 0 otherwise (Puranam et al., 2006). Only 52% of the targets in our sample had filed for a patent at the time

of acquisition. This dichotomous indicator variable provides a good abstraction and representation of the knowledge available to the market at the time of acquisition (Puranam et al., 2006).

In addition to the patent indicator variable, we also incorporated a measure of patent quality defined in Hall et al. (2005) that calculates the citation weighted total number of patents of the target depreciated to the time of the acquisition (*patent stock*). The detailed procedure to calculate the patent stock variable can be found in Hall et al. (2005) . Thus, this measure calculates the value of a patent based on the number of citations it received in subsequent years and how recent the patent is. Hall et al. (2005) demonstrate that this citation weighted measure is a better indicator of the value of the patent portfolio than other measures. However, this measure has a significant limitation in our sample because the citations of later patents are significantly truncated. We use a procedure outlined in Hall et al. (2005) to extrapolate the citation weighted count of the patents to a consistent 30 year lag period from the date of issuance. We include the depreciated patent stock to control for heterogeneity in patent quality. We also test the regressions after excluding the patent stock variable and find no difference in our main results.

2.3.2.4 Acquisition Characteristics

Next, we include characteristics of the acquisition as control variables in the model. The *total value of the acquisition* is included to control for the size of the transaction. The transaction values, as reported by the SDC database, range from 3.1 million US$ to 36 billion US$ with a mean of 1.25 billion US$. Further, the *weight of the acquisition* (defined as the ratio of acquisition value to the buyer market value) is included to control for the impact of the acquisition on the buyer because of the size difference between the buyer and the target (Moeller et al., 2004). A large size difference can impact bargaining and allow the buyer to extract more of the

total acquisition value from the target. Acquisition weights range from 0.001% to 220% with a mean of 11.7%. The source of funds for the acquisition (*cash versus stock*) as reported in the SDC database is included to control for the method of payment (Andrade et al., 2001). A few acquisitions were not completely cash or stock. When the payment form was mixed, we coded it based on the largest source of funds used to complete the transaction. Because of the importance of acquirer knowledge about the target assets (Coff, 1999), we also include an indicator variable if a significant *prior relationship* existed between the acquirer and target. To determine the existence of a prior relationship, we read all press releases prior to the acquisition announcement available through *Factiva* that mentioned both the acquirer and the target, and found evidence of significant prior relationships (such as joint product development, or equity investment) in 23% of the cases.

2.3.2.5 Environmental Characteristics

Finally, we include characteristics of the economic environment. We include the *Standard & Poor's 500 Index* on the day of the acquisition announcement to control for high market valuations on the day of the announcement. Further, we include a *post-bubble indicator* variable if the acquisition occurred after the technology "bubble" using March 2000 as the cutoff date (Brunnermeier and Nagel, 2004; Uhlenbruck et al., 2006). Further, prior research indicates the presence of acquisition waves in many industries and highlights certain advantages for acquisitions that are made in the early phases of an industry acquisition wave (Carow et al., 2004). Following the procedure in Carow et al. (2004), we identify pre-1996 as the early part of the acquisition wave in the telecommunications industry, and we include an indicator variable (*early mover*) if the acquisition occurred prior to 1996, to ensure the results found are due to target age and not early mover advantages in an acquisition wave (Carow et al., 2004).

2.3.3 Regression Model

Based on data availability for the independent and control variables, a sample of 141 acquisitions remain for the regression models. Our empirical analysis is based on the following equation:

$$\begin{aligned} AR &= \beta_0 + \beta_1 * M + \beta_2 * F + \beta_3 * I + \beta_4 * L \\ &\quad + \beta_5 * J + \beta_6 * E + \beta_7 * V + \beta_8 * P + \beta_9 * K \\ &\quad + \beta_{10} * W + \beta_{11} * D + \beta_{12} * S + \beta_{13} * R + \beta_{14} * B \\ &\quad + \beta_{15} * Y + \beta_{16} * N + \beta_{17} * A + \beta_{18} * A * P \\ &\quad + \beta_{19} * A * V + \varepsilon \end{aligned}$$

where AR is the day 0 ($A_{i,0}$) abnormal market reaction (%); M is the buyer market value (US$); F is the buyer free cash intensity; I is the buyer R&D intensity; L is the buyer leverage; J is the buyer prior acquisition experience; E is the natural log of the number of target employees; V is an indicator variable that is set to 1 if the target is private; P is an indicator variable that is set to 1 if the target company had patents; K is the natural log of the patent stock (depreciated, citation weighted sum of patents); W is the acquisition weight (acquisition value divided by the buyer market value); D is the total value of the deal (US$); S is an indicator variable that is set to 1 if the transaction was primarily paid through stock and 0 otherwise; R is an indicator variable that is set to 1 if the dyad had a prior relationship and 0 otherwise; B is an indicator variable that is set to 1 if the acquisition occurred after March 2000 and 0 otherwise; Y is an indicator variable that is set to 1 if the acquisition occurred during the early mover phase (pre 1996) of the acquisition wave in the telecommunications industry, and 0 otherwise; N is the S&P 500 Index value on the date of the acquisition; A is the natural log of the target age (to evaluate Hypothesis 2); $A * P$ is the interaction of target age and target patents (to evaluate Hypothesis 2); $A * V$ is the interaction of target age and private/public status variable

(to evaluate Hypothesis 3); and ε is unexplained error.

Summarized descriptive statistics and correlations for the variables are shown in Table 2. We also mean centered the continuous variables in the model (total acquisition value D, patent stock K and target age A) to reduce multi-collinearity effects when interaction terms are present (Aiken and West, 1991).

2.4 Results and Discussion

2.4.1 Abnormal Returns

Table 3 shows the both the Market Model and Market Adjusted abnormal returns in the whole sample of 141 firms and specific sub-samples. The results presented in Panel A for the whole sample are consistent with earlier results in the literature and exhibit a strong negative abnormal return from acquisition announcements. The mean abnormal return is -1.01 % for day 0 and the t-statistics and Wilcoxon signed rank test statistic are significant. Interestingly, the other panels show that the day 0 negative abnormal return in the whole sample are muted for younger companies, providing preliminary support for Hypotheses 1, that we further investigate through the regression analysis reported below.

Table 3: Cumulative Buyer Abnormal Returns for the Whole Sample and Specific Sub-Samples

	Market Model				**Market Adjusted Return**			
	Days -1 to 1	**Days -1 to 0**	**Days 0 to 0**	**Day 0 to 1**	**Days -1 to 1**	**Days -1 to 0**	**Days 0 to 0**	**Day 0 to 1**
Panel A: Whole Sample of 141 acquisition announcements								
Mean abnormal return (%)	-1.14	-1.13	-1.18	-1.19	-0.56	-0.6	-1.01	-0.96
T-statistics	-2.071**	-2.508***	-3.691***	-2.638***	-0.971	-1.289*	-3.055***	-2.060**
Signed-rank test Z-statistic	-1.523	-1.612	-2.566	-2.068	-1.493	-1.506	-2.716	-2.243
Panel B: Sample of 70 acquisitions: target age is below median (younger targets)								
Mean abnormal return (%)	0.02	-0.29	-0.57	-0.26	0.44	0.01	-0.41	0.01
T-statistics	0.031	-0.442	-1.233	-0.392	0.537	0.019	-0.878	0.018
Signed-rank test Z-statistic	-0.118	0.053	-0.605	-0.625	0.106	0.071	-0.435	-0.249
Panel C: Sample of 71 acquisitions: target age is above median (older targets)								
Mean abnormal return (%)	-2.29	-1.96	-1.77	-2.11	-1.53	-1.21	-1.6	-1.92
T-statistics	-2.953***	-3.088***	-3.950***	-3.322***	-1.880**	-1.812**	-3.385***	-2.884***
Signed-rank test Z-statistic	-2.081	-2.38	-3.098	-2.359	-2.227	-2.211	-3.439	-2.949
Panel D: Sample of 73 acquisitions: the target company owns patents								
Mean abnormal return (%)	-1.42	-1.63	-1.39	-1.18	-0.95	-1.35	-1.26	-0.86
T-statistics	-2.033**	-2.854***	-3.449***	-2.075**	-1.291*	-2.259**	-2.981***	-1.430*
Signed-rank test Z-statistic	-1.902	-2.749	-3.04	-1.729	-2.214	-3.062	-3.346	-2.015
Panel E: Sample of 68 acquisitions: the target company does not own patents								
Mean abnormal return (%)	-0.84	-0.59	-0.94	-1.19	-0.14	0.2	-0.74	-1.08
T-statistics	-1.034	-0.892	-2.002**	-1.789**	-0.165	0.304	-1.550*	-1.602*
Signed-rank test Z-statistic	-0.34	0.375	-0.734	-1.31	0.072	0.938	-0.58	-1.26
Panel F: Sample of 47 acquisitions: target is publicly traded								
Mean abnormal return (%)	-3.29	-3.22	-2.63	-2.7	-2.81	-2.73	-2.68	-2.76
T-statistics	-3.618***	-4.334***	-5.015***	-3.644***	-2.988***	-3.557***	-4.952***	-3.604***
Signed-rank test Z-statistic	-3.381	-3.97	-4.251	-3.177	-3.634	-4.093	-4.921	-3.837
Panel G: Sample of 94 acquisitions: target is private								
Mean abnormal return (%)	-0.07	-0.09	-0.45	-0.43	0.57	0.46	-0.17	-0.06
T-statistics	-0.104	-0.16	-1.165	-0.792	0.833	0.825	-0.432	-0.11
Signed-rank test Z-statistic	0.45	0.746	-0.237	-0.364	0.655	0.956	0.026	-0.136

One-tailed significance: $^{*}(p < 0.05)$; $^{**}(p < 0.01)$; $^{***}(p < 0.001)$; Signed-rank statistic is the Wilcoxon signed-rank test Z-statistic

2.4.2 Cross Sectional Regression Analysis

To test the three hypotheses, five hierarchical regression models were analyzed based on Equation 1. The results are shown in Table 4 for the Market Adjusted Return and Table 5 for the Market Model returns; both sets of regressions use the single day (day 0) abnormal return as the dependent variable. The results are similar in both models; because of the presence of acquirers with multiple acquisitions overlapping the estimation period, we focus on the results based on the Market Adjusted Returns in Table 4, as explained in Fuller et al. (2002).

In the first model (Model 1), only the control variables were entered. In Model 1 only the patent presence ($\beta_8 = 0.045$, $t = 2.30$) and patent stock ($\beta_9 = -0.008$, $t = -1.74$) are significant. In the second model, the age of the target (using a natural log transformation) was entered in the regression model. Consistent with a diminishing marginal effect of target age (Hypothesis 1), the natural log of target age ($\beta_{17} = -0.012$, $t = -1.69$) is significant. Patent presence and patent stock remain significant with approximately the same coefficients as in Model 1.

In the third model, we investigate the moderating effect of the existence of target patents on the relationship between buyer abnormal returns and target age. In Model 3, the interaction of age and patent presence is significant ($\beta_{18} = 0.032$, $t = 2.54$) and supports Hypothesis 2. Patent presence and patent stock remain significant with approximately the same coefficients as in prior models. In Model 4, the interaction of age and private status is not significant ($\beta_{19} = 0.020$, $t = 1.54$; however, in the full model (Model 5) of Equation 1, the parameter estimates for age ($\beta_{17} = -0.046$, $t = -3.64$), for the interaction of age and patent presence ($\beta_{18} = 0.037$, $t = 2.92$) and for the interaction of age and private status ($\beta_{19} = 0.027$, $t = 2.10$) are significant. In all models, the variance inflation factor values remain well below the cut-off value of 10, suggesting that multi-collinearity is not a significant problem in the data (Neter et al., 1990). The Market Model (in Table 5) exhibits results that are similar to those

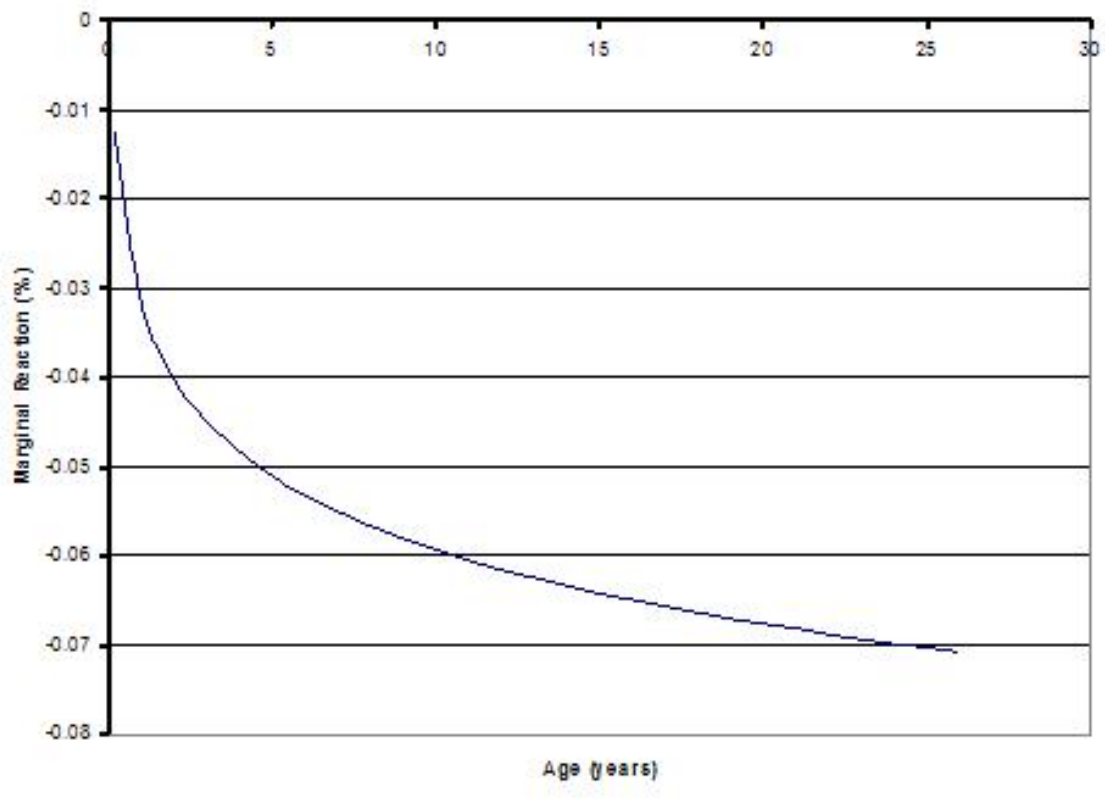


Figure 1: Marginal Impact of Target Age on Abnormal Reaction

in Table 4.

The results support Hypothesis 1. In all models that include the natural log of the target age, we find support for early acquisition of new technology. Figure 1 plots the abnormal returns in the sample as a function of target age based on the parameter estimates in Table 4. The figure illustrates the positive reaction to the acquisition of young firms, with rapid loss of value for the buyer as the target ages.

The results in Table 4 also support Hypothesis 2. The coefficient for the patent interaction term is significant in Model 3 for both the Market Model and the Market Adjusted Returns. Overall, we find that the presence of target patents mutes the negative impact of target age on value created for the buyer. To further analyze the relationships between target age, patents and value creation for the acquirer, we separated the data points into two groups based on the patent presence variable

Table 4: Hierarchical Regression for Day 0 Abnormal Market Adjusted Returns

Variable	**Model 1**	**Model 2**	**Model 3**	**Model 4**	**Model 5**
β_0: Intercept	-0.040	-0.052	-0.042	-0.016	0.007
	(-0.74)	(-0.96)	(-0.80)	(-0.28)	(0.12)
β_1: Buyer Market Value	0.015	0.020	0.011	0.002	-0.014
(billion US$)	(0.16)	(0.23)	(0.13)	(0.02)	(-0.17)
β_2: Buyer Free Cash Intensity	-0.014	-0.020	-0.036	-0.021	-0.041
(Free Cash/Sales)	(-0.42)	(-0.58)	(-1.08)	(-0.63)	(-1.23)
β_3: Buyer R&D Intensity	0.026	0.026	0.002	0.043	0.021
(R&D/Sales)	(0.34)	(0.35)	(0.03)	(0.57)	(0.29)
β_4: Buyer Leverage	0.088	0.087	0.090	0.076	0.075
(Debt / Assets)	(1.55)	(1.54)	(1.63)	(1.34)	(1.37)
β_5: Buyer Acquisition Experience	-0.282	-0.405	-0.557	-0.253	-0.375
(prior acquisitions x 10^{-3})	(-0.70)	(-1.00)	(-1.39)	(-0.61)	(-0.93)
β_6: Log of Target Employees	-0.001	0.004	0.002	0.004	0.002
	(-0.18)	(0.57)	(0.34)	(0.54)	(0.26)
β_7: Target Private	0.009	0.009	0.012	0.003	0.005
(1 if yes, 0 if no)	(0.63)	(0.58)	(0.84)	(0.20)	(0.37)
β_8: Target Patent Presence	0.045**	0.050**	0.057***	0.043**	0.048**
(1 if yes, 0 if no)	(2.30)	(2.56)	(2.93)	(2.13)	(2.44)
β_9: Target Patent Stock	-0.008*	-0.008*	-0.008*	-0.006	-0.006
(log depreciated cites)	(-1.74)	(-1.76)	(-1.90)	(-1.41)	(-1.47)
β_{10}: Acquisition Weight x 10^3	-0.022	-0.025	-0.031	-0.021	-0.027
(Acq. Val. / Buyer Val.)	(-1.00)	(-1.13)	(-1.44)	(-0.95)	(-1.24)
β_{11}: Acquisition Value	-0.002	-0.002	-0.002	-0.002	-0.002
(billion US$)	(-0.91)	(-1.07)	(-0.88)	(-1.17)	(-1.00)
β_{12}: Payment Method	0.003	-0.001	-0.003	-0.002	-0.006
(1 if stock, 0 if cash)	(0.20)	(0.01)	(-0.25)	(-0.12)	(-0.47)
β_{13}: Prior Relationship	-0.006	-0.002	-0.004	-0.003	-0.006
(1 if yes, 0 if no)	(-0.44)	(-0.13)	(-0.29)	(-0.25)	(-0.48)
β_{14}: Post Bubble (March 2000)	0.017	0.019	0.022*	0.018	0.020
(1 if yes, 0 if no)	(1.34)	(1.53)	(1.74)	(1.43)	(1.64)
β_{15}: Early Mover	-0.002	0.003	0.013	0.004	0.014
(1 if yes, 0 if no)	(-0.08)	(0.12)	(0.46)	(0.13)	(0.53)
β_{16}: S&P 500 Index	-10.985	-5.210	13.546	-10.867	8.801
(/1000)	(-0.33)	(-0.16)	(0.41)	(-0.33)	(0.27)
Fixed Effects	yes	yes	yes	yes	yes
(for frequent acquirers)					
β_{17}: Log of Target Age		-0.012*	-0.028***	-0.024**	-0.046***
(years)		(-1.69)	(-2.98)	(-2.29)	(-3.64)
β_{18}: Patent*log Target Age			0.032**		0.037***
			(2.54)		(2.92)
β_{19}: Private*log Target Age				0.020	0.027**
				(1.54)	(2.10)
R^2	16.6 %	18.6 %	22.9 %	20.2%	25.8 %
F	1.01	1.10	1.37	1.17	1.52
F (significant controls only)	2.09	2.64	3.13	2.86	4.72

OLS, (t-values in parenthesis). Two-tailed significance: $^*(p < 0.10)$; $^{**}(p < 0.05)$; $^{***}(p < 0.01)$.

Dependent variable day 0 buyer Market Adjusted abnormal returns; n = 141

Table 5: Hierarchical Regression for Day 0 Abnormal Market Model Returns

Variable	**Model 1**	**Model 2**	**Model 3**	**Model 4**	**Model 5**
β_0: Intercept	-0.023	-0.034	-0.024	0.001	0.024
	(-0.45)	(-0.66)	(-0.48)	(0.01)	(0.44)
β_1: Buyer Market Value	0.003	0.009	-0.001	-0.009	-0.026
(billion US$)	(0.04)	(0.10)	(-0.01)	(-0.11)	(-0.31)
β_2: Buyer Free Cash Intensity	-0.023	-0.028	-0.045	-0.029	-0.049
(Free Cash/Sales)	(-0.69)	(-0.85)	(-1.38)	(-0.90)	(-1.54)
β_3: Buyer R&D Intensity	0.015	0.015	-0.010	0.032	0.009
(R&D/Sales)	(0.20)	(0.21)	(-0.13)	(0.43)	(0.13)
β_4: Buyer Leverage	0.087	0.085	0.088*	0.074	0.074
(Debt / Assets)	(1.58)	(1.57)	(1.66)	(1.36)	(1.40)
β_5: Buyer Acquisition Experience	-0.163	-0.276	-0.428	-0.128	-0.251
(prior acquisitions x 10^{-3})	(-0.42)	(-0.71)	(-1.11)	(-0.32)	(-0.65)
β_6: Log of Target Employees	-0.001	0.004	0.002	0.003	0.001
	(-0.20)	(0.51)	(0.27)	(0.48)	(0.19)
β_7: Target Private	0.006	0.005	0.009	-0.001	0.002
(1 if yes, 0 if no)	(0.42)	(0.36)	(0.63)	(-0.01)	(0.15)
β_8: Target Patent Presence	0.045**	0.050**	0.056***	0.042**	0.048**
(1 if yes, 0 if no)	(2.38)	(2.62)	(3.02)	(2.18)	(2.52)
β_9: Target Patent Stock	-0.008*	-0.008*	-0.008**	-0.006	-0.007
(log depreciated cites)	(-1.85)	(-1.87)	(-2.03)	(-1.51)	(-1.58)
β_{10}: Acquisition Weight x 10^3	-0.024	-0.026	-0.032	-0.022	-0.028
(Acq. Val. / Buyer Val.)	(-1.10)	(-1.23)	(-1.55)	(-1.04)	(-1.35)
β_{11}: Acquisition Value	-0.002	-0.002	-0.001	-0.002	-0.002
(billion US$)	(-0.80)	(-0.94)	(-0.75)	(-1.04)	(-0.87)
β_{12}: Payment Method	0.002	-0.001	-0.003	-0.002	-0.006
(1 if stock, 0 if cash)	(0.18)	(-0.00)	(-0.27)	(-0.14)	(-0.50)
β_{13}: Prior Relationship	-0.008	-0.004	-0.006	-0.006	-0.009
(1 if yes, 0 if no)	(-0.62)	(-0.33)	(-0.50)	(-0.46)	(-0.70)
β_{14}: Post Bubble (March 2000)	0.018	0.020	0.022*	0.019	0.021*
(1 if yes, 0 if no)	(1.45)	(1.62)	(1.85)	(1.53)	(1.75)
β_{15}: Early Mover	-0.008	0.002	0.007	-0.002	0.009
(1 if yes, 0 if no)	(-0.28)	(-0.09)	(0.26)	(-0.08)	(0.33)
β_{16}: S&P 500 Index	-24.555	-19.303	-0.412	-24.799	-5.060
(/1000)	(-0.28)	(-0.61)	(-0.01)	(-0.78)	(-0.16)
Fixed Effects	yes	yes	yes	yes	yes
(for frequent acquirers)					
β_{17}: Log of Target Age		-0.011	-0.027***	-0.022**	-0.044***
(years)		(-1.60)	(-2.99)	(-2.24)	(-3.69)
β_{18}: Patent*log Target Age			0.032***		0.026**
			(2.66)		(2.14)
β_{19}: Private*log Target Age				0.019	0.037***
				(1.56)	(3.05)
R^2	18.5 %	20.3 %	24.9 %	21.9%	27.8 %
F	1.16	1.23	1.53	1.29	1.69
F (significant controls only)	2.01	2.65	3.33	2.52	4.87

OLS, (t-values in parenthesis). Two-tailed significance: $^*(p < 0.10)$; $^{**}(p < 0.05)$; $^{***}(p < 0.01)$.

Dependent variable day 0 buyer Market Model abnormal returns; n = 141

and performed the hierarchical regressions separately for each group. The results are reported in Table 6 (Models 1, 2, 3 and 4). As predicted by Hypothesis 2, there is a strong negative relationship between target age and acquirer value when the patent indicator is 0 (target has no patents), and there is no such relationship when the target has patents. Interestingly, the control variables predict a significantly higher percentage of the variance for the sub-group of data points where the target has patents, and the R^2 of the regression is much higher for that sub-group. Figure 2 illustrates the differing returns for targets with and without patents based on the parameter estimates in Table 6 (Models 2 and 4). While the abnormal market reaction for targets with patents is independent of age, the abnormal market reaction for targets without patents exhibits significant loss of value for the buyer as the target age increases.

The results in Table 4 and Table 5 also show support for Hypothesis 3. The coefficient for the interaction term is not significant in Model 4 for both the Market Model and the Market Adjusted Returns.; however, we do see significance in the complete model. Overall, we see evidence that private status mutes the negative impact of target age on value created for the buyer. To further analyze the relationships between target age, private status and value creation for the acquirer, we separated the data points into two groups based on the private status indicator variable and performed the hierarchical regressions separately for each group. The results are reported in Table 7 (Models 5, 6, 7 and 8). As predicted by Hypothesis 3, there is a strong negative relationship between target age and acquirer value when the private indicator is 0 (target is public) despite limited statistical power due to the reduce sample size (n = 47), and there is no such relationship when the target is private. Figure 2 illustrates the differing returns for private and public targets based on the parameter estimates in Table 7 (Models 6 and 8). While the abnormal market reaction for private targets is independent of age, the abnormal market reaction for public targets exhibits

Table 6: Hierarchical Models of Day 0 Market Adjusted Returns for Patent Split Sample Analysis

	Without Patents		**With Patents**	
Variable	**Model 1**	**Model 2**	**Model 3**	**Model 4**
β_0: Intercept	-0.045	-0.054	-0.084	-0.083
	(-0.38)	(-0.49)	(-1.17)	(-1.14)
β_1: Buyer Market Value	0.072	0.056	0.149	0.139
(billion US$)	(0.62)	(0.51)	(0.98)	(0.90)
β_2: Buyer Free Cash Intensity	0.017	-0.034	-0.058	-0.058
(Free Cash/Sales)	(0.25)	(-0.50)	(-1.51)	(-1.50)
β_3: Buyer R&D Intensity	0.013	-0.033	0.117	0.110
(R&D/Sales)	(0.10)	(-0.27)	(1.09)	(1.01)
β_4: Buyer Leverage	0.343***	0.337***	0.009	0.008
(Debt / Assets)	(3.55)	(3.70)	(0.13)	(0.11)
β_5: Buyer Acquisition Exp.	0.063	-0.498	-1.005	-0.939
(prior acquisitions x 10^{-3})	(0.10)	(-0.82)	(-1.59)	(-1.44)
β_6: Log of Target Employees	0.003	0.010	0.013*	0.011
	(0.21)	(0.62)	(1.73)	(1.24)
β_7: Target Private	-0.004	-0.008	0.027 (1.63)	0.028
(1 if yes, 0 if no)	(-0.12)	(-0.23)		(1.66)
β_8: Target Patent Presence				
(1 if yes, 0 if no)				
β_9: Target Patent Stock			-0.005	-0.005
(log depreciated cites)			(-1.29)	(-1.24)
β_{10}: Acquisition Weight x 10^3	0.104	0.081	-0.053**	-0.052**
(Acq. Val. / Buyer Val.)	(1.64)	(1.36)	(-2.34)	(-2.24)
β_{11}: Acquisition Value	-0.006	-0.010	-0.004**	-0.004*
(billion US$)	(-0.60)	(-1.08)	(-2.07)	(-1.92)
β_{12}: Payment Method	0.016	0.003	-0.021	-0.020
(1 if stock, 0 if cash)	(0.58)	(0.12)	(-1.42)	(-1.35)
β_{13}: Prior Relationship	0.005	0.010	-0.001	-0.002
(1 if yes, 0 if no)	(0.22)	(0.45)	(-0.02)	(-0.13)
β_{14}: Post Bubble	0.012	0.024	0.041**	0.040**
(1 if pre-Mar 2000, 0 if not)	(0.59)	(1.20)	(2.54)	(2.49)
β_{15}: Early Mover	-0.033	-0.014	0.030 (1.04)	0.030
(1 if yes, 0 if no)	(-0.48)	(-0.21)		(1.03)
β_{16}: S&P 500 Index	112.226*	-73.066	22.170	21.832
(/1000)	(-1.92)	(-1.29)	(0.56)	(0.55)
Fixed Effects	yes	yes	yes	yes
(for frequent acquirers)				
β_{17}: Log of Target Age		-0.031**		0.004
(years)		(-2.67)		(0.45)
N	68	68	73	73
R^2	34.6 %	43.3 %	44.8 %	45.0%
F	1.24	1.68	1.84	1.74
F (significant controls only)	0.31	5.58	3.46	0.17

OLS, (t-values in parenthesis). Two-tailed significance: $^*(p < 0.10)$; $^{**}(p < 0.05)$; $^{***}(p < 0.01)$.

Dependent variable day 0 buyer Market Adjusted abnormal returns

Table 7: Hierarchical Models of Day 0 Market Adjusted Returns for Private Split Sample Analysis

	Public		**Private**	
Variable	**Model 5**	**Model 6**	**Model 7**	**Model 8**
β_0: Intercept	-0.009	-0.151	-0.013	-0.004
	(-0.06)	(-1.03)	(-0.17)	(-0.05)
β_1: Buyer Market Value	0.316	0.086	0.002	-0.001
(billion US$)	(0.78)	(0.23)	(0.03)	(-0.01)
β_2: Buyer Free Cash Intensity	0.003	-0.057	0.003	0.003
(Free Cash/Sales)	(0.05)	(-0.94)	(0.04)	(0.04)
β_3: Buyer R&D Intensity	0.050	0.184	0.014	0.017
(R&D/Sales)	(0.26)	(1.02)	(0.12)	(0.15)
β_4: Buyer Leverage	0.064	0.097	0.092	0.088
(Debt / Assets)	(0.46)	(0.77)	(1.15)	(1.09)
β_5: Buyer Acquisition Exp.	-1.216	-0.977	-0.321	-0.277
(prior acquisitions x 10^{-3})	(-0.84)	(-0.74)	(-0.70)	(-0.58)
β_6: Log of Target Employees	0.010	0.029*	-0.012	-0.014
	(0.74)	(2.02)	(-1.23)	(-1.19)
β_7: Target Private				
(1 if yes, 0 if no)				
β_8: Target Patent Presence	0.026	0.014	0.080***	0.078***
(1 if yes, 0 if no)	(0.44)	(0.25)	(3.45)	(3.22)
β_9: Target Patent Stock	-0.008	0.004	-0.016***	-0.016***
(log depreciated cites)	(-0.66)	(0.35)	(-2.80)	(-2.71)
β_{10}: Acquisition Weight x 10^3	-0.073	-0.063	0.141**	0.141**
(Acq. Val. / Buyer Val.)	(-1.72)	(-1.64)	(2.57)	(2.55)
β_{11}: Acquisition Value	-0.003	-0.006	-0.002	-0.001
(billion US$)	(-0.72)	(-1.62)	(-0.24)	(-0.14)
β_{12}: Payment Method	-0.025	-0.045	0.005	0.004
(1 if stock, 0 if cash)	(-0.85)	(-1.61)	(0.30)	(0.24)
β_{13}: Prior Relationship	0.005	0.001	-0.008	-0.010
(1 if yes, 0 if no)	(0.18)	(0.01)	(-0.49)	(-0.56)
β_{14}: Post Bubble	0.018	0.025	0.017	0.017
(1 if pre-Mar 2000, 0 if not)	(0.56)	(0.86)	(1.16)	(1.12)
β_{15}: Early Mover	-0.028	0.007	0.017	0.015
(1 if yes, 0 if no)	(-0.51)	(0.13)	(0.40)	(0.36)
β_{16}: S&P 500 Index	-50.815	25.707	-6.066	-8.473
(/1000)	(-0.45)	(0.24)	(-0.17)	(-0.22)
Fixed Effects	yes	yes	yes	yes
(for frequent acquirers)				
β_{17}: Log of Target Age		-0.043**		0.003
(years)		(-2.55)		(0.31)
N	47	47	94	94
R^2	27.8%	43.7%	27.8%	28.9 %
F	0.42	0.78	1.24	1.18
F (significant controls only)	0.85	7.75	1.30	0.12

OLS, (t-values in parenthesis). Two-tailed significance: $^{*}(p < 0.10)$; $^{**}(p < 0.05)$; $^{***}(p < 0.01)$.

Dependent variable day 0 buyer Market Adjusted abnormal returns

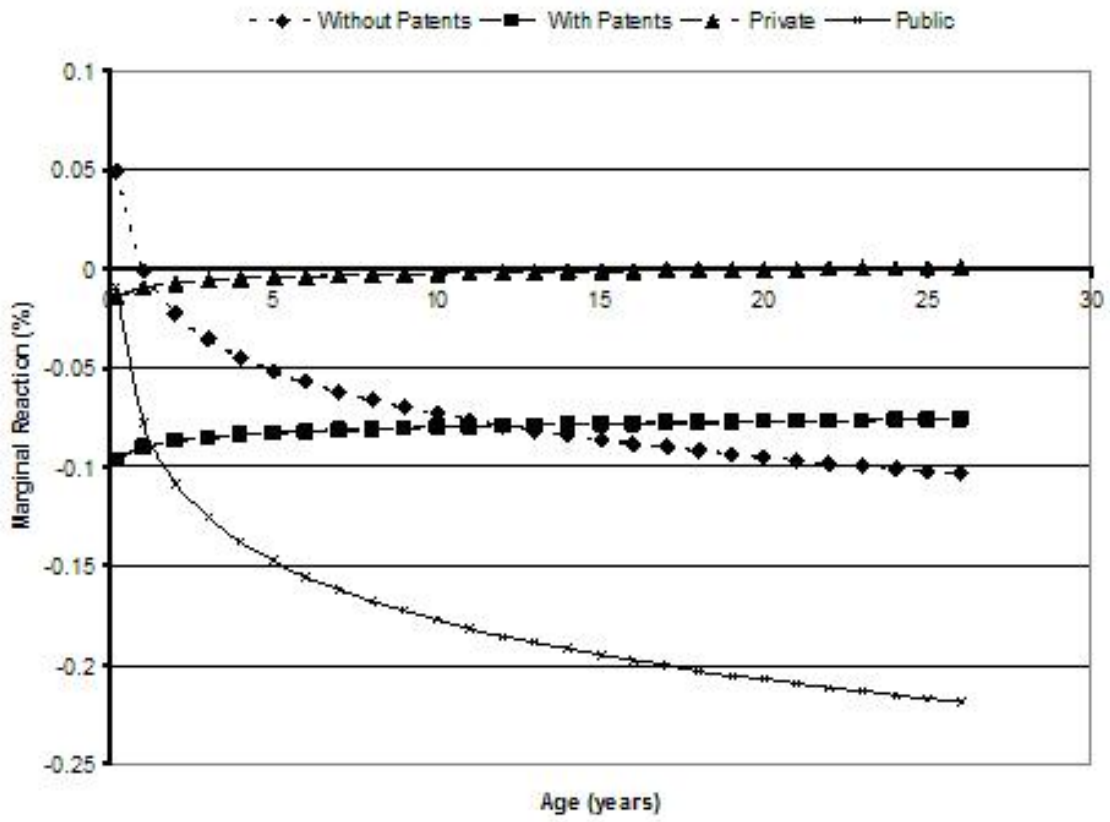


Figure 2: Marginal Impact of Target Age and Intellectual Property on Abnormal Reaction

significant loss of value as the target ages.

Another interesting observation arises from the negative and significant coefficient associated with the patent stock variable in all results reported. There are two explanations for this. First, highly cited patents indicate highly visible technologies, increasing the likelihood of a higher price for the target. The correlation between acquisition value and patent stock in Table 2 is 0.492. Second, higher patent stock values are associated with older clients with mature R&D processes and consequently less synergy from the acquisition. The correlation between patent stock and target age is 0.485 in Table 2.

In the results reported in Table 4, Table 5, Table 6 and Table 7, the large number of non-significant controls included in the regressions result in lower F values. It is important to include the controls to account for known effects on value creation and accurately evaluate our hypotheses. However, to evaluate model fit, we dropped the non-significant controls from the regressions and recalculated the F values. The coefficients and significance of model variables remain similar and the resulting F values are also reported in the tables.

2.5 Summary and Implications

In the high velocity environment of the telecommunications industry, the equity markets reward the acquisition of younger companies. However, patent ownership by the target mutes the negative impact of target age on value creation for the buyer, indicating strategic renewal of older targets through the presence of R&D. Thus, the equity markets strongly penalize the acquisition of older companies that do not own patents. Similarly, a target's privately held status mutes the negative impact of target age, indicating synergistic value for even older private targets from the superior resources of a publicly held buyer. Thus, the equity markets penalize the acquisition of older public companies. The results are robust under alternative definitions of

abnormal returns, are not based on a few frequent acquirers, and are consistent with a real options perspective on value creation in high velocity industries.

Beyond the main findings of the research outlined above, our empirical results also provide another interesting insight. None of the financial variables in the model are significant in the regression results in Table 4, Table 5, Table 6 and Table 7. Empirical research on acquisitions in other industries has consistently demonstrated lower acquirer returns for public targets (Chang, 1998; Fuller et al., 2002) and when equity is used to finance the transaction (Shleifer and Vishny, 2003). However, both of these variables are not significant in any of the regression models; however the private status of a target reduces the negative impact of target age. In addition, in contrast to earlier findings Andrade et al. (2001), the variables related to free cash flow and debt are also not significant. The only control variables that are significant in the model are related to target patent ownership and intellectual property. The low explanatory power of traditional control variables indicate that the drivers of acquisitions in the high technology industries are not captured through these variables, emphasizing the need for a fresh perspective.

Our empirical results also confirm the value of flexibility highlighted in the product development literature Bhattacharya et al. (1998); Krishnan and Bhattacharya (2002). Acquisition of younger targets enables the creation of a portfolio of technologies that allows for opportunistic evolution and experimentation, as more information becomes available about evolving market needs. In dynamic environments, this flexibility is valuable and is reflected in the higher valuation attached to the acquisition of younger targets and the role of target patents in muting the negative impact of target age.

2.5.1 Limitations

It is also important to emphasize two limitations of this study that indicate opportunities for future research. First, while event study methods utilized in this research demonstrate the advantages of acquiring early, market evaluations are imperfect measures of true value, even in efficient markets. Thus, it remains to be seen if the advantages of acquiring early translate to long term and sustainable competitive advantage. The use of detailed accounting or survey data on long term acquisition performance will provide additional insights. However, since firms make many acquisitions in a year, it will be difficult to separate out the effects of each acquisition on long term performance.

Second, our data is limited to acquisitions made by equipment manufacturers within the telecommunications industry. While the single industry focus has advantages, it also behooves us to analyze the boundary conditions of our findings. The rationale for the hypotheses examined here is rooted in the technical and market uncertainties prevalent in some environments. Conditions that foster technical uncertainties include a high rate of technological innovation, disruptive technologies, and emerging standards. Conditions that foster market uncertainties include time-to-market pressures, unpredictable demand, low switching costs, emerging markets, and hypercompetitive environments with multiple players. The convergence of both of these uncertainties creates a high velocity environment where the benefits of acting quickly outweigh the risks of such action. It is to such environments that may evolve in other industries at later times that our results can be extended.

CHAPTER III

CHOICE AND CHANCE: A CONCEPTUAL MODEL OF PATHS TO INFORMATION SECURITY COMPROMISE

3.1 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., 2004b; 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). 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 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 towards 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 chapter on the organizational perspective of information security. Our purpose is to develop a conceptual model of

[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 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 dataset 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 as 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 inter-relationships 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 datasets 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 model of the attack process developed from the perspective of a target organization.

The rest of the chapter is organized as follows. Section 3.2 briefly describes the research methodology. Section 3.3 discusses the results of interviews, observations, and document reviews, and presents our conceptual model. Section 3.4 describes the analysis of alert data to validate empirically the key concepts in our model. Section 3.5 concludes the chapter and outlines its implications for future research.

3.2 Research Methodology And Conceptual Model

3.2.1 Information Security Research Environment

The connection of individual computers and systems into a global network has created unprecedented opportunities for electronic commerce and information sharing.

Unfortunately, it also has created unprecedented opportunities for attack. As networks and applications have grown, so too have the variety and volume of attacks, including both automated and manual threats. For example, viruses attached to files and e-mails replicate to take over systems and networks. Similarly, worms spread quickly through systems and, even if they do not intrinsically cause damage, can encumber network resources. In contrast, individual attackers may try to gain access to specific resources through, for example, SQL injection, in which they pass along Structured Query Language (SQL) statements in response to Web input requests to compromise underlying databases. From a low-tech angle, attackers engaged in social engineering attempt to exploit weaknesses in people rather than in systems by, for example, pretending to be an IT support worker and asking a user to verify his or her password.

Like frantic Pandoras, systems professionals attempt to contain the risks of attack without destroying the opportunities for electronic commerce and information sharing. For example, they partition networks with firewalls (analogous to physical barriers that prevent fire from spreading from one part of a building to another), mandate the use of antivirus software, and constantly balance operational concerns while updating systems with patches to address vulnerabilities. The complexity and scope of the problem have led to the specialization of dedicated security professionals.

Similar to many other IT services, security services frequently are outsourced, which has led to the development of managed security service providers (MSSP). An MSSP takes responsibility for some of the information security functions that organizations need and provides these services to many organizations. Because it often can take advantage of economies of scale, an MSSP provides expertise and experience that may be difficult or expensive to maintain internally. Thereby, MSSPs gain invaluable experience from their exposure to compromise attempts on a wide variety of potential victims.

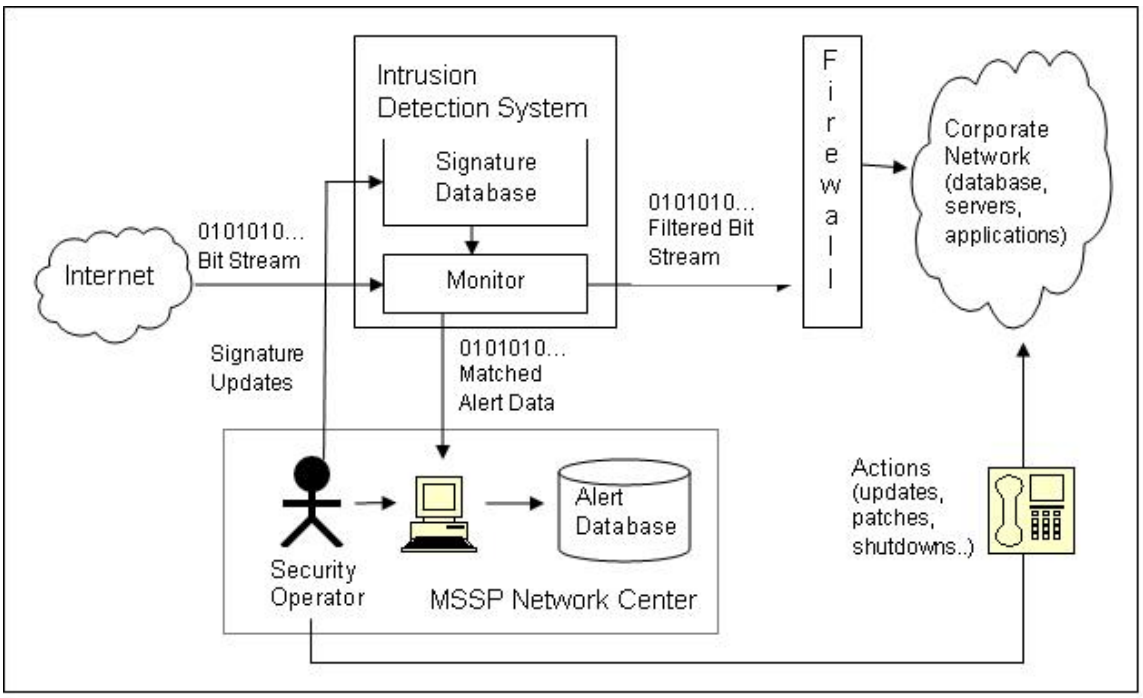


Figure 3: The Information Security Research Environment

A specific action that security professionals often take is to install monitoring devices that monitor and stop unwanted network traffic. Figure 3 shows a sample network configuration that includes an MSSP whose network monitors are designed to identify potential attacks and suspicious activity. Such identification, a key component of protection, frequently occurs through signatures, which are data traffic patterns that indicate a possible problem. As new threats and vulnerabilities appear, they are distilled into signatures that are distributed to the network monitors, which in turn improves the monitors' ability to analyze and respond to threats. Not all signatures correspond to definite attacks; some may indicate simply suspicious activity or activity that could be benign in isolation but be considered an attack when combined with another activity. For example, a request for a Web page is usually a benign activity. However, combined with many similar requests in a short period of time, it could indicate a denial of a service attack. Signatures are classified along a continuum from definitively benign to definitively problematic.

Another key component of the security environment involves the security professionals who monitor the traffic on the network using the signature-based classification generated by the network monitors. On the basis of their prior experience, current information about viruses and attacks, and similar activity at other sites, the security professionals make decisions about possible actions that might mitigate risk. Security professionals also use data from the monitors to improve signatures and signature classifications, storing suspicious bit streams in a database for later analysis.

3.2.2 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 chapter; instead, we focus on the relevance and limitations of the traditional theories in the context of the ISCP (Table 8).

Table 8: 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 pre-requisites 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 & 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" sub-culture 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 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.

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 pre-requisites 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 sub-groups.

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, since 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.

3.2.3 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 multi-jurisdictional 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 re-integrative 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.

3.2.4 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, 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 9 and Figure 4 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.

3.3 A Conceptual Model Of The ISCP

3.3.1 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: DNS

Table 9: 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	A 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 non-intrusive 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, 2X2 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*) and the other major constructs (*Countermeasures, Internet Presence and Attractiveness*).		The complete conceptual model in Figure 6 with the dimensions of each construct.	

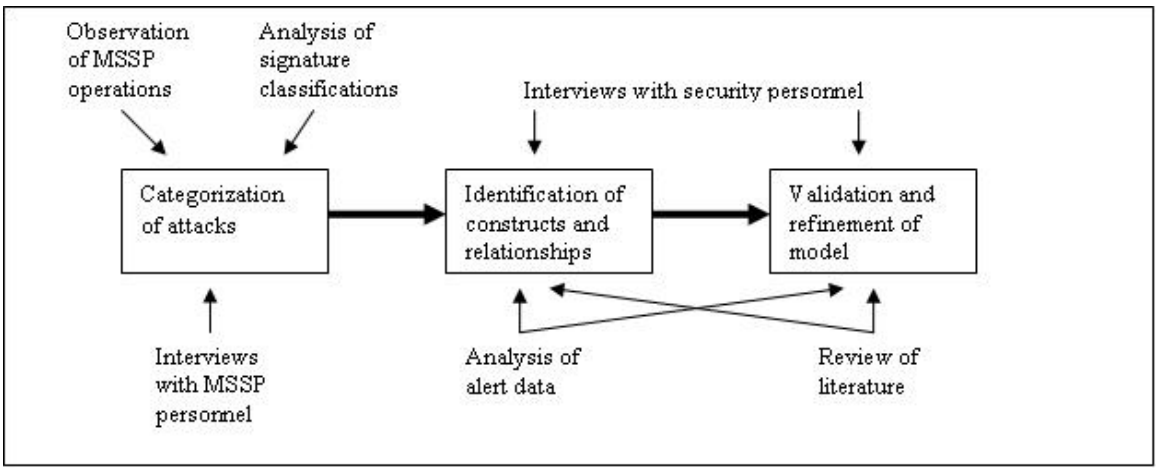


Figure 4: Research Process Summary

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 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

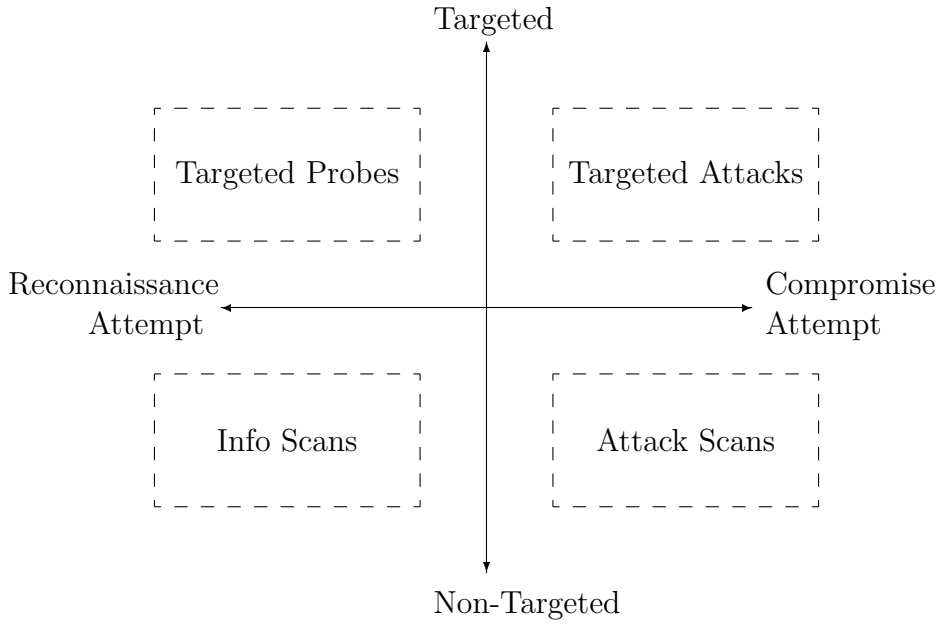


Figure 5: A Typology of Information Security Alerts

to separate out two paths of attack that have distinct antecedents in the conceptual model.

Using these two dimensions, we developed a typology (Figure 5 and Table 10) with the four possible permutations. First, non-targeted 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, non-targeted 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.

Table 10: Attack Typology 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 unauthorized database account

3.3.2 The Primary Constructs in the Conceptual Model

We conducted unstructured interviews with a 30 IS security staff from 8 organizations of four different types (3 North American financial institutions, 2 managed security providers, 2 large Western European based non-governmental organizations, and 2 universities). We explained to the participants that the fundamental question of our study was "Why are some organizations attacked more than others?" and we asked them to base their responses on their professional expertise without revealing any firm-specific information.

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*.

3.3.3 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 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 11 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.

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

Table 11: 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..." "...there are hackers who take over a machine to sell it to spammers." "machines...can be collected to form large collections with malware"	"If the corporation has top level documents, such as... NASA, it is cool to acquire them." "a real hacker will be tempted by the most impenetrable sites" "...whoever's the first one to break in [will] be recognized by his peers as the 'Top Dog' in hackerdom"	"I just hacked into the hardest system on the web...that was being run by child rapists" "Most people cannot cancel the phone service of those who upset them...to a proficient hacker this is not a difficult problem"

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 & Labeling theories of crime in Table 8 (Akers et al., 1979; Cohen and Felson, 1979). Thus, interviews, discussion group postings, and criminology literature support the following proposition.

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

3.3.4 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

Table 12: 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 non-targeted 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	Email Marketing campaigns and online ads Participation in discussion groups & 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 *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.	*Code breaking* tools decipher encrypted transmission and passwords. Larger active presence leads to more transmission that can be deciphered. *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.

by attackers and their methods of operation. We conducted a search on the Usenet discussion groups with 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 12. 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 12) 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 12. 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.

Proposition 2 *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 systems control tools described in Table 12 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 *Larger active Internet presence of the target firm is associated with a larger number of targeted probes.*

3.3.5 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 a 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 12 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 *Larger number of info scans at a target firm is associated with a larger number of targeted probes.*

3.3.6 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 a 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, foot printing tools in Table 12 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 *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., 2005a). Second, as new vulnerabilities are discovered and exploited, there is often a time lag in developing remedial countermeasures (Arora et al., 2004b). 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 *Larger numbers of (A) targeted attacks and (B) attack scans at a target firm are associated with a larger number of IS security compromises.*

3.3.7 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).

Table 13: 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 & inventory of software / devices Automatic discovery of devices and software **Logging** Logging and management of activity records

We categorized the guidelines into five dimensions (Table 13) 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 improve the other countermeasures over time through monitoring and learning. The following propositions reflect the moderating role of deterrence. Figure 6 summarizes the conceptual model.

Proposition 7 *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 *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).*

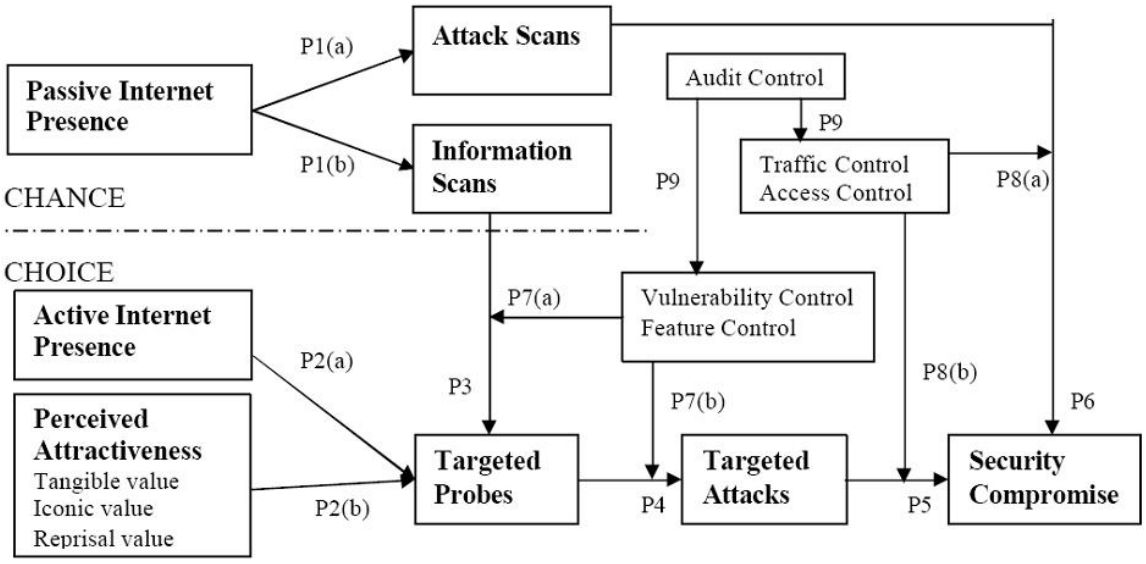


Figure 6: Conceptual Model of the ISCP

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

3.4 Emprical Examination Using Alert Data

3.4.1 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 1 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 1 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 non-targeted viruses and worms.

3.4.2 Purpose of the Empirical Analysis

While the data set is rich and unique, it has three key limitations with respect to our conceptual model in Figure 6. 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, since 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

Table 14: Correlation between the Main Variables of the Model

	Info Scans (ln)	**Attack Scans** (ln)	**Targeted Probes** (ln)
Info Scans (ln)	1.000		
Attack Scans (ln)	0.031	1.000	
Targeted Probes (ln)	0.136	0.142	1.000
Targeted Attacks(ln)	0.096	0.186	0.172

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?

In Table 14, we provide the correlations between the main variables in the model. As noted in the table, the correlations between the variables are low, indicating that multi-collinearity was not a major issue in the analysis. Further, the variance inflation factors (VIF) in the regression analysis in Table 16 are well below the cut-off value of 10.

3.4.3 Opportunistic and Deliberate Paths

Experts from the MSSP independently classified the signatures into targeted and non-targeted sub-groups 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 non-targeted ("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 non-targeted sub-groups 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 sub-groups as the attempts spread. Third, to understand differences between the two sub-groups based on qualitative factors, we utilized several qualitative indicator variables as predictors in a logit regression with the targeted / non-targeted 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 15 reveals significant and interesting differences in attack patterns for targeted and non-targeted signatures. As expected, non-targeted signatures generate significantly greater number of alerts per signature (235,524 for each non-targeted signature compared to 46,772 for each targeted signature). The number of source addresses for non-targeted attacks is also significantly higher (2,291 per non-targeted 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, non-targeted 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, more thorough and penetrates each firm more deeply.

Table 15: Differences in Attack Patterns between Targeted and Non-targeted Signatures

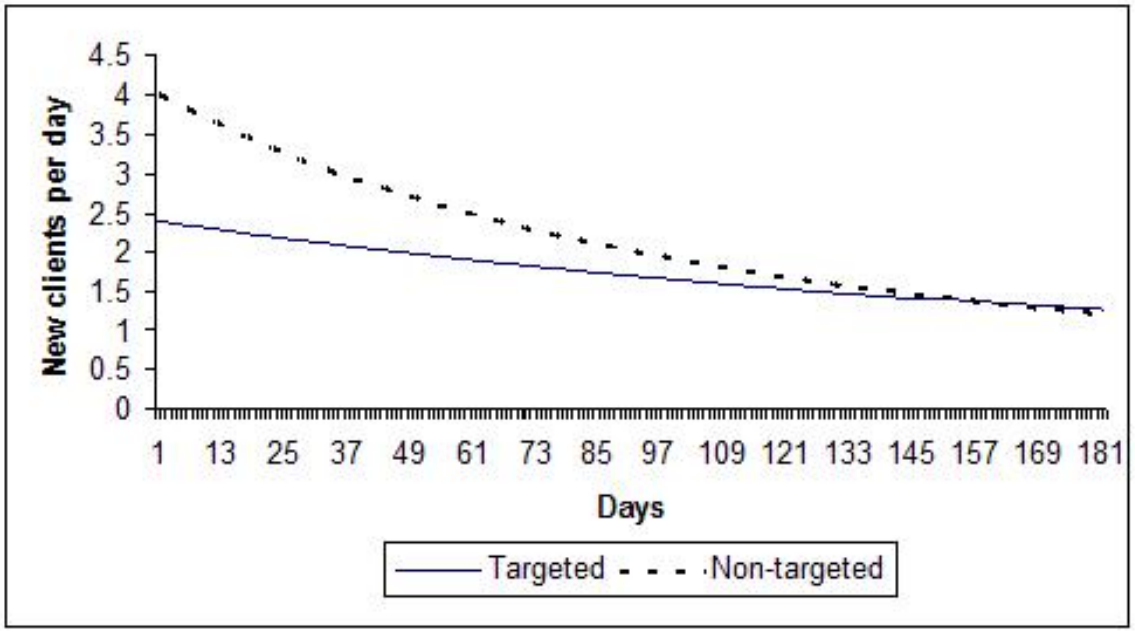
		Per Signature Statistics				
	No. of signatures	**Alerts**	**Firms affected (out of 821)**	**Alerts per firm**	**Source addresses**	**Destination Addresses**
Overall	1586	141,266	55	0.272	1,287	847
Targeted	792	46,772	52	0.330	281	1,267
Non-targeted	794	235,524	59	0.214	2,291	425
Mean Difference (standard errors)		188,752** (84,086)	7*** (4.83)	0.116*** (0.018)	2,010*** (786)	842 (926)

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

To examine differences in diffusion patterns between targeted and non-targeted 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

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

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 1 for targeted signatures. In our context, p estimates the constant rate of



	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

$R^2 = 1\%$, $F = 21.96^{***}$, $N = 7903$

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

Figure 7: Diffusion of Attacks for the Targeted and Non-targeted Signatures

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 which 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 non-targeted signatures.

Table 15 shows the results of estimating of Equation 1 using 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 non-targeted attacks. The q parameter for non-targeted 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 Table 15. Non-targeted 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 non-targeted 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, 4 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 ($T = 1$ for targeted, 0 otherwise) as the dependent variable, and the protocol, communication layer and signature type indicators as independent variables. The logit regression was highly significant ($\chi^2 = 1738.97$; pseudo-$R^2 = 79\%$). 26 of the 31 protocol indicators were perfect predictors (belonged completely to either targeted or non-targeted categories) and the remaining 5 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 ($p < 0.05$); and 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

non-targeted 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.

3.4.4 Convergence of Opportunistic and Deliberate Paths

To examine the convergence of the opportunistic and deliberate paths, we built an unbalanced panel dataset with the number of alerts of each type in the typology (Figure 5) for each client and for each day in 2006. The targeted / non-targeted classification was based on the expert assessments explained earlier. To classify signatures based on the reconnaissance / attempted compromise dimension (Figure 5), 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 since, 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 5). 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.

$$\ln(TP_{it}) = \beta_0 + \beta_{IS} * \ln(IS_{it}) + \beta_{TP} * ln(TP_{i,t-1}) + \sum_i \beta_i * FD_i + \sum_t \beta_t * TD_t \quad (2)$$

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, $TP_{i,t-1}$ 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, since 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 $\ln(IS_{it})$.

Table 16: Alert Data Analysis of Convergence and Progression

	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

OLS Regression; Standard errors in parentheses; $^{***}p < 0.001$, $^{**}p < 0.001$, $^{*}p < 0.05$

Table 16 Panel A shows the results of the analysis using hierarchical regression. Model A0 includes all the control variables, while Model A1 introduces the $\ln(IS_it)$ variable. The coefficient of the $\ln(IS_{it})$ 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 $\ln(IS_{it})$ variable indicates that about 5% of the information scans are converted to targeted probes. 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 as 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 $\ln(ISit)$ 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.

3.4.5 Progression from Information Gathering to Attack

To examine the progression of activity from information gathering to attack in the conceptual model in Figure 6, we test for the *mediating* effect of targeted probes between non-targeted information scans and targeted attacks Baron and Kenny (1986). Specifically, we evaluate the following two models.

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

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

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 16 Panel B shows the results of OLS estimation of the parameters. Model B0 in is a control model for targeted attacks with all variables highly significant. In Model B1, we test the impact of non-targeted information scans on targeted attacks and find the coefficient to be highly significant. Model B2 introduces $\ln(TP_{it})$ variable and find the coefficient to be highly significant also. Although the coefficient for $\ln(IS_{it})$ remain significant in model B2, the magnitude of the coefficient is reduced (from 0.087 to 0.067) after the introduction of the $\ln(TP_{it})$ 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 $\ln(TP_{it})$ 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.

3.4.6 Additional Analysis with Alert Data

In addition to the empirical analysis described above, we performed two additional analyses using the alert data. 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.

3.4.6.1 The Effect of Passive Internet Presence

The conceptual model hypothesizes that the effect of passive Internet presence on Targeted Probes is not direct; instead, the effect is mediated by Information Scans (Proposition 2 and Proposition 4). We are constrained by the information we have on each target firm; however, we can estimate the total number of distinct Internet addresses that are associated with the target firm by counting the distinct destination IP addresses of alerts generated for a target firm during the entire year. The number of IP addresses is one measure of the passive Internet presence of the target firm. We use this metric to provide support for Proposition 2B and Proposition 4.

First, we investigated the effect of passive Internet presence on Information Scans. The coefficient for the number of IP addresses in Model C (Table 17) with Information Scans as the dependent variable is positive and significant ($p < 0.01$). Thus, consistent with Proposition 2B, we find that the Passive Internet Presence of a target firm positively affects the number of Information Scans. Second, we investigated the mediating role of Information Scans on the relationship between passive Internet presence and Targeted Probes. Model D in Table 17 shows that the coefficient for IP addresses in the regression reduces from $1.98x10^{-6}$ to $1.65x10^{-6}$ after the introduction of Information Scans. The coefficient for Information Scans is positive and significant ($p < 0.01$). Further, a Sobel test supports the mediating role of Information Scans in the relationship between passive Internet presence and Targeted Probes ($t = 17.118$, $p < 0.01$). Because the number of IP addresses does not vary across time for the same firm, we are unable to include firm fixed effects in the models in Table 17. However, a lagged dependent variable is included to partially account for firm specific characteristics.

Table 17: Alert Data Analysis for the Effect of Passive Internet Presence

	Effect of Passive Internet Presence			
Model	**Model C0**	**Model C1**	**Model D0**	**Model D1**
Dependent Variable	**Info Scans** (IS_{it})	**Info Scans** (IS_{it})	**Targeted Probes** (TP_{it})	**Targeted Probes** (TP_{it})
Constant	0.152^{***} (0.016)	0.146^{***} (0.016)	0.035^{***} (0.008)	0.021^{**} (0.008)
Lagged Dependent Variable	0.627^{***} (0.002)	0.624^{***} (0.002)	0.707^{***} (0.001)	0.701^{***} (0.001)
Number of IP Addresses ($\times 10^{-6}$)		3.30^{***} (0.180)	1.98^{***} (0.094)	1.65^{***} (0.094)
Information Scans Ln ($\mathbf{IS}_{it}$)				0.041^{***} (0.001)
Time Fixed Effects (weekly)	Included (52)	Included (52)	Included (52)	Included (52)
Observations	224,884	224,884	224,884	224,884
F	2812.38	2,769.81	4418.76	4423.32
R^2	39.4	39.5	51.0	51.5

OLS regression; Standard errors in parentheses; $^{***}p < 0.001$, $^{**}p < 0.001$, $^{*}p < 0.05$

3.4.6.2 Analysis with Source IP Address

In the empirical analysis of convergence and progression of attack paths in the paper, we pooled all alerts for a given date so that the unit of analysis was the target firm and date set. That is, for each target firm and date, we calculated the volume of attacks for each of the four categories. For robustness, we repeated the same analysis after segregating the attacks for each target firm based on the source IP address. In this analysis, the unit of analysis is the target firm, date, and source IP addresses set. That is, for each target firm, source IP address and date combination, we calculated the volume of attacks for each of the four categories, and repeated the regressions. Thus, in this analysis, we effectively follow attacks from the same IP source to a specific target firm, to look for evidence of convergence and progression. Within this dataset, there are 8,024,697 distinct records for target firm, date, and source IP address combination. However, the dataset was extremely sparse since most source IP addresses generated attacks on a single date for a specific target, and never appeared again. To keep the problem tractable, we included the 10 source IP addresses for each target firm that generated the highest number of attacks during the entire year. Of course, the set of top 10 source IP addresses may be different for each client.

It is important to note that the results of this analysis should be interpreted with caution because source IP addresses are inherently unreliable. There are four reasons that a single attacking entity could have different source IP addresses while following the conceptual model of the information security compromise process. First, many of the higher volume alerts may be generated by zombies or botnets where an attacker uses multiple comprised computers to perform the early stages of the attack process (information search), then uses a different single machine for more targeted attacks. Second, attackers can be expected to change source IP addresses to reduce the likelihood of detection. Third, we expect that organized groups of attackers have division of responsibility where less experienced attackers channel information

gathered to more experienced attackers. Finally, given the criminal nature of the activities, attackers mask their actual source IP address to reduce the possibility of detection. Given these limitations, any empirical support found is a conservative estimate of the real effects.

Table 18 summarizes the results of the analysis. We find continued support for the convergence of paths with the information scans coefficient significant ($p < 0.01$) and indicating that 2% of the information scans are converted to targeted probes. However, support for the progression of attacks is less clear. The introduction of targeted probes as a mediator of the relationship between information scans and targeted attacks does not significantly reduce the coefficient on information scans, but the coefficient on the targeted probes variable is positive and significant. The associated Sobel test for mediation finds only weak indication ($t = 1.41$, $p < 0.160$) of any mediating role. In summary, when considering the source IP address of the alert, we find continued support for convergence, but weak evidence of progression. Since source IP addresses are inherently unreliable, the results represent a lower bound on the support for progression.

Table 18: Alert Data Analysis Considering Source of Alert

	Panel E Convergence of Paths		**Panel F Progression of Attacks**		
Model	**Model E0**	**Model E1**	**Model F0**	**Model F1**	**Model F2**
Dependent Variable	**Targeted Probes** (TP_{it})	**Targeted Probes** (TP_{it})	**Targeted Attacks** (TA_{it})	**Targeted Attacks** (TA_{it})	**Targeted Attacks** (TA_{it})
Constant	0.360^{***} (0.030)	0.342^{***} (0.030)	0.388^{***} (0.027)	0.373^{***} (0.028)	1.329^{***} (0.023)
Lagged Dependent Variable	0.478^{***} (0.004)	0.478^{***} (0.005)	0.417^{***} (0.005)	0.417^{***} (0.005)	0.417^{***} (0.005)
Information Scans Ln (IS_{it})		0.021^{***} (0.003)		0.018^{***} (0.003)	0.018^{***} (0.003)
Targeted Probes Ln(TP_{it})					0.013^{*} (0.007)
Time Fixed Effects (weekly)	Included (52)	Included (52)	Included (52)	Included (52)	Included (52)
Client – Source Fixed Effects (821x10)	Included (8210)	Included (8210)	Included (8210)	Included (8210)	Included (8210)
Observations	37,288	37,288	37,288	37,288	37,288
F	219.87^{***}	216.70^{***}	152.26^{***}	150.17^{***}	147.46^{***}
R^2	73.3	73.5	71.9	72.0	72.1

OLS regression; Standard errors in parentheses; $^{***}p < 0.001$, $^{**}p < 0.001$, $^{*}p < 0.05$. Note that the fixed effect is now on the client-source combination variable; thus, we cannot report the R^2 (within firm and between firms) provided in Table 16.

3.5 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 its 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.

3.5.1 Limitations

We identify several limitations of the study. First, while care was taken to differentiate alerts along the targeted/non-targeted dimension and the empirical analysis demonstrated significant differences, there remains ambiguity in classification since we have created dichotomous variables from underlying continuous classifications. Second, while we recognize that our study context is dynamic because signatures can evolve from targeted to non-targeted 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 to us. Finally, while 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.

3.5.2 Managerial Implications

From a practical perspective, our results highlight four messages for managers. First, while 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 non-targeted attacks (98% of all attacks) across all targets, irrespective of target attributes. While 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, since later stage countermeasures such as traffic filtering are often imprecise and imperfect (Cavusoglu et al., 2005b).

Third, active presence on the Internet leads to more attacks through the targeted path. While 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 6 can be used as an effective teaching tool to educate managers and students about IS security. It provides a comprehensive, cogent and non-technical model to understand the information security compromise process from the perspective of a target organization.

3.5.3 Implications for Research

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

3.5.3.1 Measurement Instruments

The development of measurement instruments that accurately capture each construct (organizational countermeasures, attractiveness and presence) is a research topic in itself. While 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 accurately measure various aspects of their information security environment. The measurement instrument can also serve as a theory-driven audit and benchmarking tool.

3.5.3.2 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.

3.5.3.3 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. While 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.

3.5.3.4 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 6. 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.

3.5.4 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, while 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 leads 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 reduces the progression of attacks from information gathering to compromise attempts, and subsequently to information security compromise.

CHAPTER IV

ARE REWARD-BASED DISCLOSURE MECHANISMS EFFECTIVE?

4.1 Introduction

The unfortunate reality of widespread security vulnerabilities in technology products is an important topic not only to security and information systems professionals but also to consumers, business and policy makers. While business commerce depends on information systems, security vulnerabilities pose ever-present risks which are no longer isolated to technical staff. In fact, policy decisions are increasing important as "incentives are becoming as important as technical design" (Anderson and Moore, 2006, p. 610). Much of the incentive debate has focused on the discovery and disclosure of vulnerabilities and the associated incentives for provision of research effort towards discovery.

Historically the security community relied on the others in the community to disclose vulnerabilities when found. In this sense, vulnerability research can be considered a public good– consumption of security information does not preclude others from using the information as well. Like other public goods, without additional incentives, security will be insufficiently provided (Garcia and Horowitz, 2007). Therefore, vulnerability markets have been proposed to encourage researchers to provide this public good (Schechter, 2004). Several private vulnerability markets are currently in existence, including iDefense and the Zero Day Initiative. Figure 8 depicts the overall vulnerability disclosures by both reward-based and non-reward-based mechanisms for each quarter since 2000. While reward-based disclosures remain a small fraction of the total disclosures, the vulnerability markets are being used.

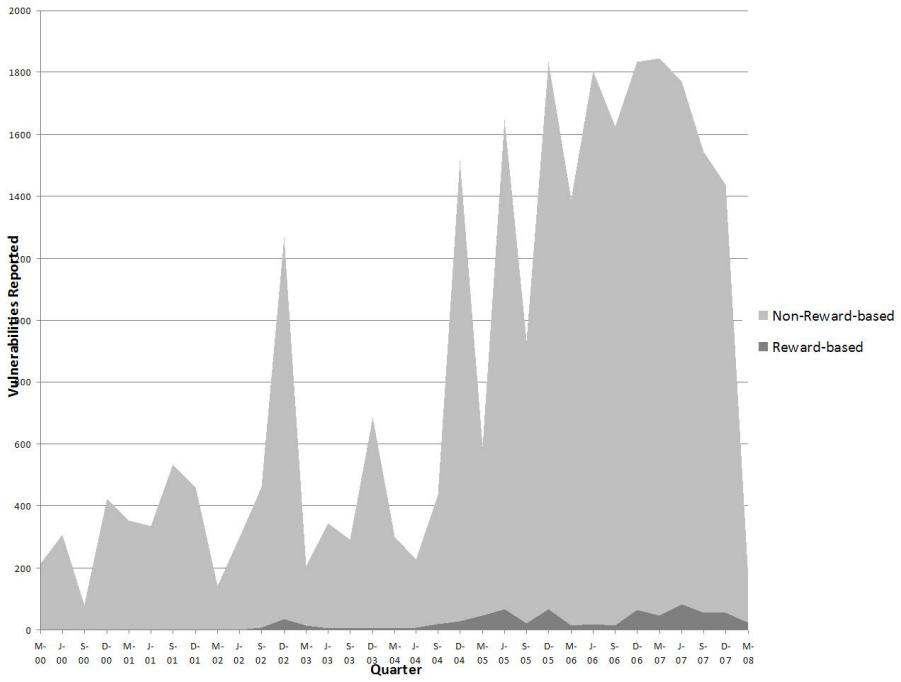


Figure 8: Vulnerability Reports by Quarter

Despite their use, the impact of these reward-based mechanisms is far from clear. While reward mechanisms create incentives for research and discovery, they have some limitations. Because the private vulnerability markets focus on their own profit maximizing strategy, they have an incentive to leak vulnerability information and therefore decrease social welfare (Kannan and Telang, 2005). Rather than having the desired effect of increasing security, they may instead be contributing to an overall decrease in security.

Thus, the fundamental question remains open— "are reward-based disclosure mechanisms for vulnerabilities effective?" My research addresses this question through a large scale empirical study of vulnerabilities disclosed through both reward-based and non-reward-based mechanisms. To gauge effectiveness, I examine three measures of effectiveness.

Risk Does reward-based disclosure affect the likelihood of a vulnerability being exploited?

Speed Does reward-based disclosure affect the speed of exploitation of a vulnerability?

Volume Does reward-based disclosure affect the volume of attacks based on the vulnerability?

Through the empirical study of more than 2.4 billion billion alerts generated by intrusion detection systems from 2006 and 2007, I provide evidence that vulnerability markets using reward-based mechanisms are effective.[1] First, while the overall exploitation of vulnerabilities is the same for reward-based and non-reward-based mechanisms, reward-based disclosures decrease the likelihood that the vulnerability will be exploited quickly. This allows more time for the security community to defend against the exploit through patching or developing countermeasures. Second, I find that reward-based disclosure reduces the volume of alerts resulting from a vulnerability.

The rest of this chapter is organized as follows. Section 4.2 provides background on the vulnerability disclosure environment. Section 4.3 reviews the recent literature regarding vulnerability disclosure in general and vulnerability market formation in particular. Section 4.4 describes the data and methods used to evaluate reward-based disclosure effectiveness. Section 4.5 examines the factors leading to selection of disclosure through reward-based or non-reward-based channels. Section 4.6 discusses the results of the empirical analysis of the effectiveness of the existing vulnerability markets. Section 4.7 provides a summary of the key findings along with guidance for future research.

[1]I would like to thank SecureWorks, Inc., and Jon Ramsey, Chief Technology Officer, for their assistance with this research by providing expert consultation, detailed explanation of their extensive Security Operations Centers, and thorough grounding in the reality of the current security environment. I am especially appreciative that they made a summarized abstract of their database of security alert data available to me. The views expressed in this thesis are my own. Any errors remain the responsibility of the author.

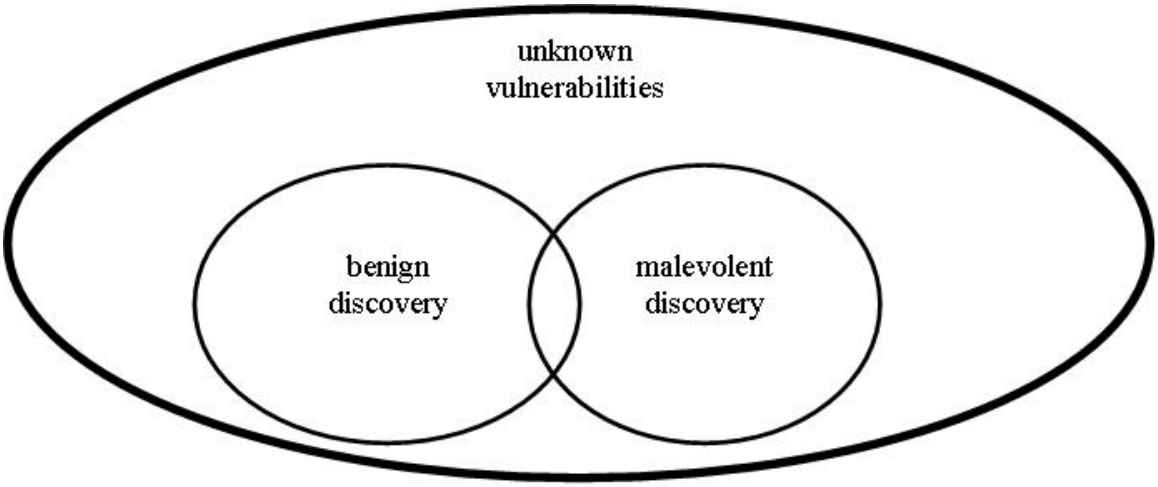


Figure 9: Discovery of Vulnerabilities

4.2 Disclosure Environment

Vulnerabilities exist in all systems whether they are known or unknown. Of the unknown vulnerabilities, there are two methods that a vulnerability can be discovered—labeled malevolent and benign. The defining distinction between the malevolent researcher and the benign researcher is the researcher action upon discovery of the vulnerability. Figure 9 depicts the relationships between the sets of vulnerabilities.

First, a vulnerability can be found by a malevolent researcher. This researcher is rewarded through exploiting the vulnerability (or, alternatively, selling the vulnerability to others who will exploit the vulnerability.) The total value of this reward is the expected value of the sum of the successful exploitations of the vulnerability. In the case of malevolent discovery, the discover benefits most if the vulnerability is kept secret and also is not discovered by a benign researcher. Second, a vulnerability can be found by a benign researcher. With vulnerability markets, the researcher is paid a reward by the market for their effort. (Without the vulnerability market, there is no monetary reward.)

These methods work independently, but are related. Benign researchers can find vulnerabilities that malevolent researchers have not found. However, to be useful

for protection, a benign discoverer must make use of the vulnerability information. Leakage occurs when malevolent researchers learn of the vulnerability as a result o fthe benign discovery. This leakage may be intentional, as private markets have incentives to leak information and increase the value of their services (Kannan and Telang, 2005), or it may occur inadvertently through reverse engineering of protection systems. Similarly, malevolent researchers may find vulnerabilities that benign researchers have not already found. In parallel to leakage of benign findings, the malevolent researcher must use the vulnerability to realize value. Usage of the vulnerability in an exploit may increase the likelihood of benign discovery.

4.3 Literature Review

Research is active in understanding the underlying economics of information security. Earlier work focused on topics such as risk management (Straub and Welke, 1998), and handling abuse (Straub and Nance, 1990). More recently, Anderson and Moore (2006) and Gordon and Loeb (2006) provide overviews of the key complexities surrounding the misaligned incentives, negative externalities, and general challenges for information systems professionals. Patching issues such as user incentives (August and Tunca, 2006), restricted distribution (Rahman et al., 2006), and piracy (August and Tunca, 2008) have been of recent research interest.

Recognizing that vulnerabilities are inevitable, research surrounding disclosure of vulnerabilities has been particularly active. While disclosure announcements can affect the value of software vendor (Telang and Wattal, 2005), public disclosure can, under some conditions, promote social welfare (Nizovtsev and Thursby, 2007). Further, disclosure itself has several options, each of which has their own strengths and weakness (Arora et al., 2004b), particularly regarding the pressure that disclosure places on vendors. Vendors have been shown empirically to respond to disclosure (Arora et al., 2005) especially under certain competitive conditions (Arora et al.,

2006a). Disclosure and patching has also been found to affect the volume of attacks seen in controlled research networks called *honeypots* (Arora et al., 2006b, 2004a). However, while there is great value in the controlled environment that honeypots provide, my research is among the first empirical analysis using real, multi-firm alert data.

A significant issue in information systems security is the incentives for investment. Research has shown that security can be considered a public good and tends to be under-provisioned (Garcia and Horowitz, 2007). Investment in IT security deterrence has been shown to be effective within a firm (Straub, 1990). However, because of externalities, under-investment is likely. Regulation has been suggested to improve social welfare but faces significant challenges (Garcia and Horowitz, 2007).

As an alternative, reward-based mechanisms have been proposed to address the under-investment. Specifically, rather than depending on the security community to freely contribute vulnerability research, payments can be used to encourage research (Schechter, 2004). This approach recognizes the reward structure for vulnerabilities available in the black market (Radianti and Gonzalez, 2007) and seeks to offset it. These markets for vulnerabilities have been suggested as an interesting economic model for exploration (Sutton and Nagel, 2006; Anderson and Moore, 2006). In addition to straight payment structures, auctions have been proposed but they, along with reward mechanisms, have implementation difficulties (Ozment, 2004). In fact, a recent vulnerability auction has been implemented (WabiSabiLabi). Yet, interest in reward-based mechanisms remains the most active with two vulnerability markets (iDefense and the Zero Day Initiative) in active use over the past couple of years.

Unfortunately, the impact of such reward-based mechanisms is not clear. The presence of private infomediaries introduces additional complexity to the disclosure and patch cycle (Li and Rao, 2007). A specific concern is that private infomediaries have an incentive to leak information. In an analytical model, Kannan and Telang

(2005) have shown that private infomediaries can actually reduce social welfare due to information leakage rather than increase welfare through incentives. Further, the information leak does not have to be intentional by the private infomediaries. Instead, by reverse engineering signatures on intrusion detection systems, firms providing protection to their clients can inadvertently disclose vulnerabilities to potential attackers. Adding further complexity, Kumar et al. (2007) find differential effects from different types of information leaks such as vulnerabilities which reveal confidential information. In an abstract sense, much like there are concerns that weapon buy-back programs may actually increase the number of guns (Mullin, 2001), vulnerability purchase programs may increase the number of vulnerabilities.

Overall, the effects of reward-based private infomediaries are ambiguous as increased incentives may be offset by information leakage. To examine the effectiveness of reward-based disclosures for vulnerabilities, I consider three possibilities.

- Does disclosure through a reward-based mechanism affect the likelihood of a vulnerability being exploited?
- Does disclosure through a reward-based mechanism affect the speed by which a vulnerability is exploited?
- Does disclosure through a reward-based mechanism affect the volume of alerts seen by from a vulnerability?

First, not all vulnerabilities disclosed are exploited. Attackers may find some vulnerabilities more attractive or more rewarding than others. One measure of effectiveness of a reward-based mechanism would be if vulnerabilities disclosed through the mechanism were more or less likely to be exploited. Based on the preceding concerns about leakage of information from private infomediaries, I hypothesize that:

Hypothesis 1 *Disclosure through reward-based mechanisms will* increase *the likelihood that a vulnerability will be exploited.*

In contrast, based on the preceding benefits from information sharing among benign researchers, a competing hypothesis is:

Hypothesis 2 *Disclosure through reward-based mechanisms will* decrease *the likelihood that a vulnerability will be exploited.*

Second, the discovery mechanisms of reward-based private infomediaries get information to the defenders more quickly, increasing the time available for the deployment of countermeasures. Accordingly, I hypothesize that:

Hypothesis 3 *Disclosure through reward-based mechanisms will* decrease *the likelihood that a vulnerability will be seen soon after the vulnerability is published.*

Third, the discovery of vulnerabilities through reward-based private informediaries may decrease the usage of the vulnerability by attackers by the preceding reasoning. Therefore, I hypothesize that:

Hypothesis 4 *Disclosure through reward-based mechanisms will* decrease *the number of alerts that are seen for a vulnerability.*

4.4 Data and Methodology

4.4.1 Data

To investigate the effectiveness of reward-based mechanisms, my primary datasource is a summarized database of alerts generated from intrusion detection systems. An intrusion detection system (IDS) is installed to protect a network by filtering bad or potentially bad traffic from getting into the network. One way that an IDS works is by looking for sequences of data in a packet that match a known sequence associated with a vulnerability. These known sequences are called *signatures*. (The basic role and function of intrusion detection systems are described in more detail in Chapter 3.) Each time a signature is seen, an alert is generated and saved for further analysis.

The alert database is provided by SecureWorks, a managed security service provider. The dataset provides a unique forum for research analysis both because it contains real alert data (as opposed to data from a research setting) and because the data is from several thousand clients across many industries. These characteristics allow me to examine the actual effectiveness of markets using real data that is not specific to any single client. The following analysis is based on a summarized set of alerts covering 2006 and 2007.

The key variable of interest is whether or not a vulnerability was disclosed through a reward-based mechanism (market) or through a non-reward-based mechanism. During 2006 and 2007, there were two vulnerability markets providing incentives for researchers to discover and disclose vulnerabilities through their service (iDefense and the Zero Day Initiative). During that same period, there were many other options which did not reward researchers directly. The most common of these are CERT, Security Focus, XForce, Secunia, Bugtraq and Internet Security Systems X-Force. I include an indicator variable if a vulnerability was disclosed through one of the two reward-based mechanisms.

4.4.2 Control Variables

I match the signatures for a vulnerability with the detailed information available primarily through the National Vulnerabilities Database (NVD, 2008). Each vulnerability in the National Vulnerabilities Database (NVD) is assessed using a Common Vulnerability Scoring System (CVSS). Through this uniform scoring, I am able to control for specific attributes of the vulnerability. Details on version 2 of the scoring system are in Mell and Romanosky (2008). From the scoring, I include the following:

Access Required This metric describes the proximity required to exploit the vulnerability. Proximities are scored as *local* if the attacker must have local access to the potential target, *adjacent* if attacker must be closely located or *remote*

if the attacker can be across a non-local network.

Complexity Once the attacker has access, vulnerabilities have varying degrees of complexity to exploit and are categorized as *low*, *medium*, or *high* complexity.

Authentication Required Some vulnerabilities may be exploited anonymously; others require authentication. I include an indicator if the attacker must pass some authentication step to exploit the vulnerability. While the CVSS indicates the number of authentications required (either *None*, *Single*, or *Multiple*), I use an indicator variable *Authentication Required* if any authentication is required due to a low number of multiple authentication vulnerabilities reported.

Impact The potential impact of a vulnerability is categorized as affecting the disclosure of confidential information (*Confidentiality*), the integrity of data (*Integrity*) or the availability of system resources (*Availability*). For each of these, the CVSS reports impacts of None, Partial, or Complete. However, for my analysis I use an indicator variable for each category if the impact is present. (There are few partial impact vulnerabilities.)

Beyond the scoring, there are other aspects of the vulnerability for which I am able to control. First, the NVD includes seven different types of vulnerabilities. They are incorrect allowance of privileges (Access Validation), failure to handle incorrect input (Input Validation), shortcomings in design of software (Design Error), insufficient response to unexpected conditions (Exception Error), weak configuration of settings (Configuration Error), errors due to sequencing of events (Race Condition), or uncategorized (Other). Indicator variables are included for these categories. Second, I include an indicator variable, *Patch Available*, if a patch was available at the time that the vulnerability was disclosure. Next, I include an indicator variable, *Signature Available*, if a signature was available at the time that the vulnerability was disclosed. Further, I also include the age of vulnerability measured as the number of days since

the vulnerability was disclosed. Finally, in several of the following analyses, I am also able to control for changes in trends over time using fixed effects.

4.4.3 Methodology

First, in my sample of 1252 vulnerabilities for which we had full data with alert signatures matched into the NVD database, only 153 (12%) were exploited by attackers. To examine the difference that reward-based mechanism disclosure makes in the likelihood of exploitation, I use the logit regression, $\ln\left(\frac{e_i}{1-e_i}\right) = \beta x_i + \beta_{market} x_{market,i}$. The variable e_i takes the value of 1 when an exploit of vulnerability i is observed. Vector β is the control variables listed in Section 4.4.2 and variable $x_{market,i}$ is 1 if the reward-based mechanism for disclosure was used. Further, because of the potential for censoring caused by the end of the study, I use a Cox proportional hazard model (Cox, 1972) to provide further support. In the proportional hazard model, the risk of failure (exploitation of a vulnerability) at time t for vulnerability i is given by $\lambda(t) = \lambda_0(t_i)e^{(-x_i\beta)}$. These analyses allow an empirical answer to the competing hypotheses that reward-based either increase or decrease the likelihood of exploitation of a vulnerability (Hypothesis 1 and Hypothesis 2).

Second, I use another logit model to examine the risk of exploitation shortly after the vulnerability is published. The risk of exploitation in the prior analysis only evaluated the risk of exploitation during the entire study period. For comparison, I use similar logit regression to determine the risk of exploitation within one month and one week of disclosure. This analysis allows an empirical answer to the hypothesis that reward-based disclosures decrease the likelihood that an exploit will be seen soon after disclosure (Hypothesis 3).

Third, I built a panel dataset which contains the daily count of alerts for each type of vulnerability for the period from 2006 to 2007. I use a random effects panel regression to estimate the impact of market disclosure on the natural log of the

number of alerts, $a_{i,t}$ for vulnerability i. The model estimated is $\ln(a_{i,t}) = x_{i,t}\beta + alpha_i + u_{i,t}$ where $x_{i,t}$ is the vector of independent and control variables, $alpha_i$ are the random effects, and $u_{i,t}$ is the error term. This analysis allows an empirical answer to the hypothesis that reward-based disclosures decrease the overall volume of alerts generated (Hypothesis 4).

4.5 Selection of Disclosure to Reward-Based or Non-Reward-Based

Before examining the effectiveness of the reward-based mechanisms, I first compare the vulnerabilities disclosed through the two mechanisms. For this comparison, I use the entire set of vulnerabilities contained in the NVD. While there are several repositories of vulnerability information, the NVD contains a large cross sections of vulnerabilities consistently reported. Similar large scale analysis have been done of vulnerabilities (Frei et al., 2006), but have not focused on the selection of disclosure mechanism. During 2006 and 2007, the NVD published information about 13,249 vulnerabilities. Of these, 345 (2.6%) were initially reported by one of the two vulnerability reward-based mechanisms. Table 19 shows descriptive statistics about all of the vulnerabilities disclosed during 2006 and 2007.

I use a logit model to analyze the selection of disclosure through the reward-based or non-reward-based mechanism. Table 20 shows the influence of vulnerability attributes on the likelihood of being disclosed through a reward-based mechanism versus a non-reward-based mechanism. The logit analysis indicates that vulnerabilities which only require network access are associated with non-reward-based disclosure. Similarly, vulnerabilities based on access violation, input validation errors, and design omissions are also associated with non-reward-based disclosure. Conversely, reward-based disclosures are associated vulnerabilities of medium complexity or which impact system confidence or availability. Overall, the analysis suggests that there are distinct associations between some vulnerability attributes and resultant disclosure

Table 19: Sample Descriptive Statistics

Variable		**Percentage**	**Count**
Total		100.00%	13,249
Reward-Based		2.60%	345
Non-Reward-Based		97.40%	12,904
Access	Requires Local	9.53%	1,262
	Requires Adjacent	0.44%	58
	Network	90.04%	11,929
Complexity	Low	62.84%	8,326
	Medium	29.41%	3,897
	High	7.74%	1,026
Authentication	Not required	93.52%	12,391
	Required	6.48%	858
Confidentiality Impact	No	28.30%	3,750
	Yes	71.70%	9,499
Integrity Impact	No	21.40%	2,835
	Yes	78.60%	10,414
Availability Impact	No	28.40%	3,763
	Yes	71.60%	9,486
Vulnerability	Access	4.95%	656
	Input	51.13%	6,774
	Design	11.85%	1,570
	Exception	5.35%	709
	Environmental	0.24%	32
	Configuration	0.87%	115
	Race Condition	0.62%	82
	Other	1.05%	139
Contains Signature	No	97.28%	12,888
	Yes	2.72%	361
Patch Available	No	66.89%	8,862
	Yes	33.11%	4,387

mechanism.

Table 20: Selection of Reward-based or Non-Reward-based Disclosure

Variable	**Model 0**	**Model 1**	**Model 2**	**Model 3**	**Model 4**	**Model 5**	**Model 6**
Constant	-5.9814***	-1.8711***	-5.9938***	-5.9888***	-7.1940***	-5.1101***	-5.9267***
	(1.0013)	(0.2383)	(1.0024)	(1.0015)	(1.0137)	(1.0052)	(1.0267)
Access: Adjacent		-0.0252					-0.0783
		(0.4732)					(0.4897)
Access: Network		-1.1539***					-0.8516***
		(0.1333)					(0.1526)
Complexity: Medium			0.0273				0.3057**
			(0.1207)				(0.1331)
Complexity: High			0.2623				0.1256
			(0.2311)				(0.2398)
Authentication				0.1694			-0.3179
				(0.2001)			(0.2165)
Confidence Impact					0.5191***		0.6293***
					(0.2037)		(0.2127)
Integrity Impact					-0.1333		0.2080
					(0.1966)		(0.2148)
Availability Impact					1.2411***		0.8335***
					(0.2032)		(0.2097)
Vuln: Access						-0.6798***	-0.6842***
						(0.2542)	(0.2547)
Vuln: Input Validation						-1.9849***	-1.7928***
						(0.1676)	(0.1757)
Vuln: Design						-0.7530***	-0.6565***
						(0.1966)	(0.2029)
Vuln: Exception						-0.2745	0.1371
						(0.2129)	(0.2153)
Vuln: Config						-1.0329	-1.1215
						(0.7379)	(0.7343)
Vuln: Race						0.2214	-0.1099
						(0.4560)	(0.4733)
Vuln: Other						-1.0338**	-0.9215*
						(0.5269)	(0.5282)
Fixed Effects	month	month	month	month	month	month	month
Log likelihood	-1525.2518	-1492.871	-1524.6379	-1524.9153	-1486.8923	-1426.7713	-1377.6206
Pseudo R^2	4.62	6.64	4.65	4.64	7.02	10.73	13.80
Wald χ^2	110.23***	180.77***	110.03***	111.95***	183.13***	278.89***	378.67***

Logit model (1=reward-based), robust standard errors in parenthesis. Two-tailed significance: $^{*}(p < 0.10)$; $^{**}(p < 0.05)$; $^{***}(p < 0.01)$. n = 13,249

Table 21 shows a similar analysis to Table 20, but examines changes in attribute influence through 2006 to 2007. Based on the logit analysis, none of the explanatory variables shift their influence from reward-based to non-reward-based during the time period. However, the magnitude of some of the coefficients changes significantly. For example, while vulnerabilities which require only network access (instead of local access) to exploit are consistently more often reported through non-reward-based mechanisms, their association with non-reward-based disclosure increases in strength during the period of the study. Also, which input validation based vulnerabilities are initially strongly associated with non-reward-based disclosure in early 2006, by the end of 2007, they are as likely to be disclosed though one mechanism as the other. Overall, this suggests there are some minor changes in the attributes of vulnerabilities which are being disclosed through each type of mechanism.

4.6 Empirical Examination of Reward-based Disclosure Effectiveness

First, I examine how reward-based or non-reward-based disclosure affects the risk of the vulnerability being exploited. The logit regressions in Model 1 and Model 2 (Table 22) indicate that disclosure through a reward-based mechanism does not significantly affect the likelihood of a vulnerability being exploited. Interestingly, medium complexity vulnerabilities are less likely to be exploited than low complexity, but high complexity are not. Attackers also appear to be more likely to exploit vulnerabilities impacting system integrity. As expected, the availability of patches reduces the likelihood of exploit as attacker may feel that their chances of success are diminished. The availability of a signature increases the likelihood of exploitation providing some evidence that attackers gain information about how to exploit a vulnerability by examining a signature. Because the sample is censored at the end of 2007, a similar analysis was done using a proportional hazard model (Table 23). In

Table 21: Selection of Reward-based or Non-Reward-based Disclosure Over Time

Variable	**Jan-Jun 2006**	**Jul-Dec 2006**	**Jan-Jun 2007**	**Jul-Dec 2007**
Constant	-4.9775***	-3.9975***	-3.3216***	-3.9254***
	(0.9244)	(0.6021)	(0.5055)	(0.4265)
Access: Adjacent	—-	—	0.9347	-0.0201
			(0.6304)	(1.1797)
Access: Network	-0.7876*	-0.6035*	-0.3068	-1.4280***
	(0.4640)	(0.3343)	(0.2776)	(0.2437)
Complexity: Medium	1.2863	0.3036	0.2694	0.3071
	(0.8560)	(0.3605)	(0.1947)	(0.2115)
Complexity: High	0.1003	0.1407	0.0909	0.0458
	(0.5322)	(0.3743)	(0.4728)	(0.6339)
Authentication	-0.2378	0.4300	-0.4736	-0.7969*
	(0.8243)	(0.3512)	(0.3586)	(0.4677)
Confidence Impact	1.0001	0.4754	0.2709	1.0937***
	(0.8318)	(0.4759)	(0.3581)	(0.3482)
Integrity Impact	0.1989	-0.2622	0.4775	0.5036
	(0.8843)	(0.4731)	(0.3766)	(0.3699)
Availability Impact	1.3898*	1.2638***	0.5847*	0.6368*
	(0.7941)	(0.4660)	(0.3453)	(0.3579)
Vuln: Access	-1.2168	-0.9925	-0.3530	-0.4414
	(0.9957)	(0.7308)	(0.3133)	(0.7252)
Vuln: Input Validation	-2.7317***	-1.3152**	-2.0968**	-0.4571
	(0.7664)	(0.3198)	(0.2775)	(0.3176)
Vuln: Design	-1.3637**	-0.1658	-0.7064**	0.0125
	(0.6355)	(0.3873)	(0.2972)	(0.4022)
Vuln: Exception	-0.0785	0.3863	0.0828	0.3608
	(0.6864)	(0.3977)	(0.3115)	(0.6182)
Vuln: Race	0.4436	—	0.3627	0.1672
	(1.1025)		(0.6664)	(0.7678)
Vuln: Other	—	0.5145	—	0.2072
		(1.1557)		(0.6116)
Vuln: Config	—	—	-0.5226	-0.2785
			(1.0262)	(1.2070)
Observations	3112	3381	3574	2980
Log likelihood	-139.26106	-335.76698	-485.92231	-433.99179
Pseudo R^2	17.65	7.65	11.42	9.09
Wald χ^2	110.23 ***	75.18***	113.78***	98.92***

Logit model (1=reward-based), robust standard errors in parenthesis. Two-tailed significance: $^{*}(p < 0.10)$; $^{**}(p < 0.05)$; $^{***}(p < 0.01)$. n = 13,249

both estimations, I see no evidence that reward-based disclosure increases the likelihood that a vulnerability will be exploited. Based on these results, I find no support for Hypothesis 1 that reward-based mechanisms increase the risk of exploitation or for the competing Hypothesis 2 that reward-based mechanisms decrease the risk of exploitation.

Next, I examine how reward-based or non-reward-based disclosure affects the speed with which a vulnerability is exploited. The logit regressions in Model 3 and Model 4 (Table 22) indicate that disclosure through a reward-based mechanism does not significantly affect the likelihood of a vulnerability being exploited within one month of disclosure. However, Model 5 and Model 6 do indicate that reward-based disclosure decreases the likelihood of exploitation during the week after publication. (Similar models using time periods shorter than one week show similar results, but lack statistical power primarily due to the reduced number of exploitations in general as the time period shrinks.) This is important because decreasing the likelihood of exploitation in the short term allows for IT infrastructure professionals to implement countermeasures such as patching. Based on these results, I find support for Hypothesis 3 that reward-based disclosure decreases the risk of exploitation shortly after disclosure.

Finally, I examine the volume of alerts generated by a vulnerability. The panel regression in Table 24 is based on 139,347 daily observations of each vulnerability for 960 clients locations. Model 1 shows that the volume of alerts increases as the age increases. Model 2 finds no evidence that the availability of a patch reduces the volume of alerts. Model 3 finds that the availability of a signature increases the volume of alerts. Finally, Model 4 and Model 5 show that disclosure through a reward-based mechanism significantly reduces the volume of alerts seen. Based on these results, I find support for Hypothesis 4 that reward-based disclosure decreases the volume of alerts from a vulnerability.

Table 22: Choice of Exploitation of Vulnerabilities

	Within Sample		Within One Month		Within One Week	
Variable	**Model 1**	**Model 2**	**Model 3**	**Model 4**	**Model 5**	**Model 6**
Constant	-2.3932***	-2.3716***	-4.1762***	-4.1280***	-3.2629***	-3.1895
	(0.3871)	(0.3842)	(0.6517)	(0.6466)	(0.7053)	(0.7018)
Complexity:	-0.9509***	-0.9468***	-0.7935**	-0.7877**	-1.1818***	-1.2041***
Medium	(0.2368)	(0.2366)	(0.3248)	(0.3261)	(0.4789)	(0.4837)
Complexity: High	0.1557	0.1494	0.3835	0.3735	0.5078	0.4738
	(0.2614)	(0.2620)	(0.3233)	(0.3236)	(0.4342)	(0.4367)
Confidence Impact	0.3541	0.3566	0.2254	0.23821	-1.5491**	-1.5984**
	(0.3048)	(0.3048)	(0.5327)	(0.5342)	(0.6785)	(0.7135)
Integrity Impact	0.9716***	0.9706***	1.4507**	1.4515**	—	—
	(0.3238)	(0.3227)	(0.6129)	(0.6115)		
Availability Impact	-0.2330	-0.2287	0.2674	0.2682	1.3606*	1.4296*
	(0.2605)	(0.2590)	(0.4763)	(0.4723)	(0.7424)	(0.7740)
Vuln: Access	-0.8830	-0.8600	-0.7107	-0.6484	0.3110	0.4770
	(0.7604)	(0.76128)	(1.0447)	(1.0470)	(1.1211)	(1.1406)
Vuln: Input Validation	0.4081**	0.3894*	0.3344	0.2913	0.9179***	0.8800***
	(0.2069)	(0.2054)	(0.2664)	(0.2632)	(0.3551)	(0.3555)
Vuln: Design	-0.0996	-0.1259	0.2170	0.1520	0.1777	0.0723
	(0.2946)	(0.2943)	(0.3773)	(0.3769)	(0.5332)	(0.5299)
Vuln: Exception	-0.1688	-0.1923	-0.7212	-0.7923	-0.4856	-0.6495
	(0.3856)	(0.3848)	(0.6391)	(0.6402)	(0.8335)	(0.8475)
Vuln: Config	0.5444	0.5410	-0.0297	-0.0460	—	—
	(0.6993)	(0.7073)	(1.0526)	(1.0555)		
Vuln: Race	-0.3283	-0.3260	—	—	—	—
	(0.9724)	(0.9537)				
Vuln: Other	-0.0101	-0.0512	0.8282	0.7252	0.1974	0.0002
	(0.7050)	(0.7058)	(0.7301)	(0.7308)	(1.2151)	(1.2061)
Patch Available	-0.5976***	-0.5701***	-0.4687*	-0.4074	-0.4770	-0.3960
	(0.1871)	(0.1917)	(0.2596)	(0.2641)	(0.3706)	(0.3720)
Signature Available	1.1066***	1.1228***	1.2743***	1.3161***	2.1340***	2.2411***
	(0.2412)	(0.2413)	(0.2984)	(0.3000)	(0.3996)	(0.4056)
Reward-based Disclosure		-0.2598		-0.6691		-1.3421*
		(0.3089)		(0.4507)		(0.7609)
Observations	1055	1055	1047	1047	804	804
Log likelihood	-397.2295	-396.8439	-239.6904	-238.4691	-132.3755	-130.2724
Pseudo R^2	9.05	9.14	10.36	10.82	15.17	16.52
Wald χ^2	70.91***	72.37***	52.28***	54.45***	52.85***	54.37***

Logit model (1=exploited), robust standard errors in parenthesis.

Two-tailed significance: $^{*}(p < 0.10)$; $^{**}(p < 0.05)$; $^{***}(p < 0.01)$.

Table 23: Risk of Exploitation of Vulnerabilities

	Complete Sample		Within One Month		Within One Week	
Variable	**Model 0**	**Model 1**	**Model 0**	**Model 1**	**Model 0**	**Model 1**
Complexity: Medium	1.3984	1.4638	2.1970**	2.5432**	3.1766***	3.8307***
	(0.3379)	(0.3622)	(0.8030)	(1.0007)	(1.4843)	(1.9330)
Complexity: High	1.5224*	1.5025*	2.3322***	2.2943***	3.0749**	2.8543**
	(0.3636)	(0.3616)	(0.7704)	(0.7626)	(1.4226)	(1.3638)
Confidence Impact	1.2940	1.3229	1.1187	1.1713	0.9751	1.0393
	(0.3951)	(0.4066)	(0.6510)	(0.6981)	(0.4746)	(0.4953)
Integrity Impact	2.1233**	2.0968**	4.0060**	3.9278**	—	—
	(0.6877)	(0.6798)	(2.4923)	(2.4886)		
Availability Impact	0.8873	0.8906	1.3789	1.4021	2.0654	1.9934
	(0.2320)	(0.2326)	(0.7347)	(0.7641)	(1.1147)	(1.1286)
Vuln: Access	0.3363	0.3249	0.4599	0.4129	1.1256	0.8777
	(0.2591)	(0.2521)	(0.5178)	(0.4770)	(1.3714)	(1.1387)
Vuln: Input Validation	1.2037	1.1858	1.2414	1.1759	1.8313	1.7122
	(0.2453)	(0.2404)	(0.3682)	(0.3487)	(0.7413)	(0.7048)
Vuln: Design	0.9082	0.8900	1.2300	1.1580	1.1447	0.9937
	(0.2666)	(0.2604)	(0.4986)	(0.4713)	(0.7084)	(0.6318)
Vuln: Exception	1.1981	1.1569	0.8330	0.7629	0.8323	0.7372
	(0.4327)	(0.4170)	(0.5469)	(0.5003)	(0.7051)	(0.6193)
Vuln: Config	1.3376	1.3081	0.7641	0.7047	—	—
	(0.7560)	(0.7420)	(0.9162)	(0.8577)		
Vuln: Race	0.3786	0.3695	—	—	—	—
	(0.3808)	(0.3750)				
Vuln: Other	1.0330	0.9846	1.9560	1.7355	1.9394	1.5847
	(0.9639)	(0.9207)	(1.9384)	(1.7282)	(2.5105)	(2.0910)
Patch Available	0.4740***	0.4800***	0.4855	0.4846**	0.6048	0.6013
	(0.0924)	(0.0939)	(0.1460)	(0.1483)	(0.2732)	(0.2816)
Signature Available	2.3354***	2.3783***	3.0832**	3.1719***	5.2960***	5.6997***
	(0.5133)	(0.5254)	(0.953)	(1.0081)	(2.0603)	(2.3434)
Reward-based Disclosure		0.7259		0.4513*		0.2662*
		(0.2133)		(0.2174)		(0.2061)
Failures	153	153	74	74	39	39
Log likelihood	-859.405	-858.665	-380.595	-378.633	-189.239	-186.9790
Wald χ^2	49.86***	50.86***	2643.01***	2192.94***	6984.87***	5729.36***

Cox proportional hazard model, robust standard errors in parenthesis.

Two-tailed significance: $^{*}(p < 0.10)$; $^{**}(p < 0.05)$; $^{***}(p < 0.01)$. Observations = 1252.

Table 24: Volume of Alerts based on Reward-based or Non-Reward-based Disclosure

Variable	Model 0	Model 1	Model 2	Model 3	Model 4	Model 5
Constant	-0.4666*	-0.4980	-0.4699	-0.4784*	-0.4870*	-0.5252*
	(0.2830)	(0.2805)	(0.3186)	(0.2816)	(0.2821)	(0.3163)
Access: Network	0.4205	0.4120	0.4223	0.4606*	0.4636*	0.4933*
	(0.2608)	(0.2580)	(0.2652)	(0.2591)	(0.2606)	(0.2619)
Complexity:	-0.1359	-0.0918	-0.1358	-0.1604	-0.1017	-0.0809
Medium	(0.1229)	(0.1232)	(0.1230)	(0.1227)	(0.1220)	(0.1218)
Complexity: High	0.3640*	0.3559*	0.3638*	0.2801	0.3523*	0.2614
	(0.2155)	(0.2156)	(0.2157)	(0.2174)	(0.2153)	(0.2173)
Authentication	-0.4927***	-0.4908***	-0.4929***	-0.4461***	-0.4827**	-0.4337***
	(0.0780)	(0.0788)	(0.0780)	(0.0775)	(0.0772)	(0.0776)
Confidence Impact	0.0560	0.0505	0.0560	0.0156	0.0608	0.0157
	(0.1912)	(0.1911)	(0.1914)	(0.1905)	(0.1907)	(0.1896)
Integrity Impact	0.0568	0.0454	0.0561	0.0542	0.0896	0.0779
	(0.1929)	(0.1926)	(0.1894)	(0.1921)	(0.1938)	(0.1891)
Availability Impact	0.0186	0.0222	0.0189	-0.0226	0.0211	-0.0162
	(0.1735)	(0.1734)	(0.1744)	(0.1744)	(0.1730)	(0.1749)
Vuln: Access	0.0188	0.0252	0.0184	0.0718	0.0366	0.0964
	(0.1764)	(0.1763)	(0.1750)	(0.1756)	(0.1759)	(0.1732)
Vuln: Input Validation	0.1068	0.0975	0.1071	0.1105	0.0651	0.0577
	(0.1375)	(0.1376)	(0.1394)	(0.1367)	(0.1382)	(0.1389)
Vuln: Design	-0.0406	-0.0347	-0.0402	-0.0781	-0.0647	-0.0972
	(0.1691)	(0.1694)	(0.1703)	(0.1693)	(0.1690)	(0.1704)
Vuln: Exception	-0.0288	-0.0154	-0.0296	-0.1314	-0.0180	-0.1040
	(0.2933)	(0.2931)	(0.2948)	(0.2920)	(0.2931)	(0.2919)
Vuln: Config	-0.2393	-0.2601	-0.2380	-0.1843	-0.2412	-0.2098
	(0.3600)	(0.3599)	(0.3633)	(0.3588)	(0.3591)	(0.3604)
Vuln: Race	0.2657	0.2084	0.2659	-0.0669	0.1940	-0.1933
	(1.2573)	(1.2597)	(1.2586)	(1.2710)	(1.2552)	(1.2732)
Vuln: Other	-0.3946	-0.3618	-0.3927	-0.7191	-0.4516	-0.7435
	(1.1531)	(1.1646)	(01.156)	(1.1582)	(1.1502)	(1.1696)
Age (ln)		0.0421***				0.0419***
		(0.0055)				(0.0055)
Patch Available			0.0033			-0.0053
			(0.1181)			(0.1206)
Signature Available				0.4224**		0.4160**
				(0.2081)		(0.2100)
Reward-based Disclosure					-0.3179***	-0.3287***
					(0.1199)	(0.1246)
Fixed Effects	month	month	month	month	month	month
Within R^2	1.22	1.26	1.22	1.22	1.22	1.26
Between R^2	2.95	3.44	2.95	4.56	3.90	5.90
Overall R^2	2.77	3.00	2.78	3.11	3.28	3.83
Wald χ^2	1680.39***	1708.44***	1686.00***	1689.74***	1680.74***	1725.99***

Panel regression; dependent variable = log of the number of alerts; n = 139,347; 343 vulnerabilities robust standard errors in parenthesis. Two-tailed significance: $^{*}(p < 0.10)$; $^{**}(p < 0.05)$; $^{***}(p < 0.01)$.

4.7 Summary and Conclusions

Overall, the theoretical impact of reward-based-based mechanisms for disclosure are not clear. While rewards increase incentives for security research, they may have a negative impact due to the likelihood of information leakage from the private infomediaries (Kannan and Telang, 2005). Based on a large scale empirical study of real alerts from intrusion detection systems across 960 clients for two years, I find evidence of effectiveness of reward-based mechanisms.

First, while reward-based disclosure does not increase or decrease the likelihood that a vulnerability will be exploited, it does decrease the likelihood of exploitation during the one week period after disclosure. This decrease is important for practitioners in that it allows more time to implement countermeasures. Further, it indicates that while leakage may happen, there are potentially positive aspects of leakage. Second, reward-based disclosure does reduce the volume of alerts. Because of the overwhelming number of alerts, mechanisms which reduce the volume of alerts can help administrators better allocate resources.

In general, while information leakage may be occurring, the loss in welfare may be offset not only by incentive gains but also by positive aspects of leakage as others in the security community are made aware of vulnerabilities. This aspect points to opportunities for research to model and to quantify both the benefits and costs of information leakage. Future research could also help quantify the impact of specific incentive levels in increasing the vulnerabilities discovered. Research would also be valuable that helped understand if reward-based mechanisms are truly providing incentives or are just compensating those would be researching and disclosing anyway.

A key insight from this study is that private infomediaries incorporate two distinct aspects of vulnerability management. First, private infomediaries are able to provide rewards to encourage researchers. Second, the private nature of the infomediaries and their subscription mechanisms restrict access to information. While the rewards

offered may be encouraging research and discovery, the underlying effectiveness of these vulnerabilities markets may be due more to the restricted access to vulnerability information rather than the incentives provided.

Finally, the evidence of effectiveness is encouraging for both policy makers and the security community. Rewards can be effective. Mechanisms that combine the incentive structures and positive aspects of information sharing while restricting the negative consequences of leakage could positively impact social welfare. It is towards these mechanism designs that my research provides encouragement.

Bibliography

Adner, R. and Levinthal, D. (2004). What is not a real option: Considering boundaries for the application of real options to business strategy. *Academy of Management Review*, 29(1):74–85.

Ahuja, G. and Katila, R. (2001). Technological acquisitions and the innovation performance of acquiring firms: A longitudinal study. *Strategic Management Journal*, 22(3):197.

Aiken, L. S. and West, S. G. (1991). *Multiple Regression: Testing and Interpreting Interactions*. Sage Publications.

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

Amram, M. and Kulatilaka, N. (1999). Disciplined decisions: Aligning strategy with the financial markets. *Harvard Business Review*, 77(1):95.

Anderson, R. and Moore, T. (2006). The Economics of Information Security. *Science*, 314(5799):610–613.

Andrade, G., Mitchell, M., and Stafford, E. (2001). New evidence and perspectives on mergers. *Journal of Economic Perspectives*, 15(2):103–120.

Anonymous (2006). U.S. Technology M&A - Lex Column. *Financial Times*, page 14.

Arora, A., Forman, C., Nandkumar, A., and Telang, R. (2006a). Competition and Quality Restoration: An Empirical Analysis of Vendor Response to Software Vulnerabilities.

Arora, A., Krishnan, R., Nandkumar, A., Telang, R., and Yang, Y. (2004a). Impact of vulnerability disclosure and patch availability— an empirical analysis. Workshop on the Economics of Information Security.

Arora, A., Krishnan, R., Telang, R., and Yang, Y. (2005). An empirical analysis of vendor response to disclosure policy. Workshop on the Economics of Information Security.

Arora, A., Nandkumar, A., and Telang, R. (2006b). Does information security attack frequency increase with vulnerability disclosure? An empirical analysis. *Information Systems Frontiers*, 8(5):350–362.

Arora, A., Telang, R., and Xu, H. (2004b). Optimal policy for software vulnerability disclosure. Workshop on the Economics of Information Security.

Asquith, P., Bruner, R. F., and Mullins, Jr., D. W. (1983). The gains to bidding firms from merger. *Journal of Financial Economics*, 11:121–139.

August, T. and Tunca, T. (2008). Let the Pirates Patch? An Economic Analysis of Software Security Patch Restrictions. *Information Systems Research*, 19(1).

August, T. and Tunca, T. I. (2006). Network software security and user incentives. *Management Science*. Forthcoming.

Austin, D. H. (1993). An event-study approach to measuring innovative output: The case of biotechnology. *The American Economic Review*, 83(2):253.

Bailey, K. D. (1994). *Typologies and Taxonomies: An Introduction to Classification Techniques*. Quantitative Applications in the Social Sciences. Sage Publications.

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

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

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

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

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

Bhattacharya, S., Krishnan, V., and Mahajan, V. (1998). Managing new product definition in highly dynamic environments. *Management Science*, 44(11):S50.

Bhuiyan, N., Gerwin, D., and Thomson, V. (2004). Simulation of the new product development process for performance improvement. *Management Science*, 50(12):1690.

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

Bourgeois, III, L. J. and Eisenhardt, K. M. (1988). Strategic decision processes in high velocity environments. *Management Science*, 34(7):816–835.

Bowen, P., Hash, J., and Swanson, M. (2005). Guide for developing security plans for federal information systems. *National Institute of Standards and Technology Special Publication*, 800-18(revision 1):1–45.

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

Braithwaite, J. (1989). *Crime, Shame and Reintegration*. Cambridge University Press, Cambridge, U.K.

Brancheau, J., Janz, B., and Wetherbe, J. (1996). Key issues in information systems management: 1994-95 SIM Delphi results. *MIS Quarterly*, 20(2):225–242.

Brown, S. J. and Warner, J. (1985). Using daily stock returns: The case of event studies. *Journal of Financial Economics*, 14:3–31.

Brown, S. L. and Eisenhardt, K. M. (1995). Product development: Past research, present findings, and future directions. *Academy of Management Review*, 20(2):343–378.

Brunnermeier, M. K. and Nagel, S. (2004). Hedge Funds and the Technology Bubble. *The Journal of Finance*, 59(5):2013–2040.

Capron, L. and Pistre, N. (2002). When do acquirers earn abnormal returns? *Strategic Management Journal*, 23(9):781–794.

Capron, L. and Shen, J.-C. (2007). Acquisitions of private vs. public firms: Private information, target selection, and acquirer returns. *Strategic Management Journal*, 28:891–911.

Carow, K., Heron, R., and Saxton, T. (2004). Do Early Birds Get The Returns? An Empirical Investigation Of Early-Mover Advantages In Acquisitions. *Strategic Management Journal*, 25(6):563–585.

Cavusoglu, H., Cavusoglu, H., and Raghunathan, S. (2005a). Emerging issues in responsible vulnerability disclosure. Workshop on the Economics of Information Security.

Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal Of Electronic Commerce*, 9(1):69–104.

Cavusoglu, H., Mishra, B., and Raghunathan, S. (2005b). The Value of Intrusion Detection Systems in Information Technology Security Architecture. *Information Systems Research*, 16(1):28–46.

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

Chang, S. (1998). Takeovers of privately held targets, methods of payment, and bidder returns. *Journal of Finance*, 53(2):773–784.

Chaudhuri, S., Iansiti, M., and Tabrizi, B. (2005). The multilevel impact of complexity and uncertainty on the performance of innovation-motivated acquisitions. Working Paper.

Chaudhuri, S. and Tabrizi, B. (1999). Capturing the real value in high-tech acquisitions. *Harvard Business Review*, 77(5):123–130.

Chesbrough, H. W. (2003). *Open Innovation*. Harvard Business School Publishing Corporation.

Coff, R. W. (1999). How buyers cope with uncertainty when acquiring firms in knowledge-intensive industries: Caveat emptor. *Organization Science*, 10(2):144.

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

Cohen, L. and Felson, M. (1979). Social change and crime rate change: A routine activity approach. *American Sociological Review*, 44(4):588–608.

Cohen, M. A., Eliashberg, J., and Ho, T.-H. (1996). New product development: The performance and time-to-market tradeoff. *Management Science*, 42(2):173.

Cohen, W. M. and Levinthal, D. A. (1990). Absorptive capacity: A new perspective on learning and innovation. *Administrative Science Quarterly*, 35(1):128–152.

Coleman, J. W. (1987). Toward an integrated theory of white-collar crime. *The American Journal of Sociology*, 93(2):406–439.

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

Cox, D. R. (1972). Regression models and life tables. *Journal of the Royal Statistical Society, Series B*, 34:187–202.

Cuppens, F. and Miege, A. (2002). Alert correlation in a cooperative intrusion detection framework. In *Proceedings of the 2002 IEEE Symposium on Security and Privacy*, pages 202–215.

DeLooze, L. (2004). Classification of computer attacks using a self-organizing map. In *2004 IEEE Workshop on Information Assurance*, pages 365–369, US Military Academy, West Point, NY.

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

Dickersen, J., Juslin, J., KouKousoula, O., and Dickersen, J. (2001). Fuzzy intrusion detection. In *Proceedings of the Joint 9th IFSA World Congress and 20th NAFIPS International Conference*, pages 1506–1510, Vancouver, Canada.

DiPietro, R. and Mancini, L. V. (2003). Security and privacy issues of handheld and wearable wireless devices. *Communications of the ACM*, 46(9):75. 00010782.

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

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

Ehrlich, I. (1996). Crime, punishment and the market for offences. *Journal of Economic Perspectives*, 10(1):43–67.

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

Faccio, M., McConnell, J. J., and Stolin, D. (2006). Returns to acquirers of listed and unlisted targets. *Journal of Financial and Quantitative Analysis*, 41(1):197–220.

Fichman, R. G., Keil, M., and Tiwana, A. (2005). Beyond Valuation: "Options Thinking" In IT Project Management. *California Management Review*, 47(2):74.

Frei, S., May, M., Fiedler, U., and Plattner, B. (2006). Large-scale vulnerability analysis. *Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense*, pages 131–138.

Fuller, K., Netter, J., and Stegemoller, M. (2002). What Do Returns to Acquiring Firms Tell Us? Evidence from Firms That Make Many Acquisitions. *Journal of Finance*, 57(4):1763–1793.

Gans, J. S. and Stern, S. (2003). The product market and the market for "ideas": Commercialization strategies for technology entrepreneurs. *Research Policy*, 32(2):333–350.

Garcia, A. and Horowitz, B. (2007). The potential for underinvestment in internet security: implications for regulatory policy. *Journal of Regulatory Economics*, 31(1):37–55.

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

Girotra, K., Terwiesch, C., and T., U. K. (2006). Valuing R&D Projects In A Portfolio: Evidence From The Pharmaceutical Industry. Working Paper.

Glaser, B. G. and Strauss, A. L. (1967). *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago: Aldine.

Gordon, L. and Loeb, M. (2006). Economic aspects of information security: An emerging field of research. *Information Systems Frontiers*, 8(5):335–337.

Gordon, L. A. and Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4):438 – 457.

Gottfredson, M. R. and Hirschi, T. (1990). *A General Theory of Crime*. Stanford University Press, Stanford, California.

Goyal, A. and Santa-Clara, P. (2003). Idiosyncratic risk matters! *The Journal of Finance*, 58(3):975.

Griliches, Z. (1990). Patent statistics as economic indicators: A survey. *Journal of Economic Literature*, 28(4):1661–1707.

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

Hall, B., Jaffe, A., and Trajtenberg, M. (2005). Market value and patent citations. *Rand Journal of Economics*, 36(1):783–804.

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

Hauser, J., Tellis, G. J., and Griffin, A. (2006). Research on innovation: A review and agenda for marketing science. *Marketing Science*, 25(6):687.

Hayward, M. (2002). When do firms learn from their acquisition experience? Evidence from 1990–1995. *Strategic Management Journal*, 23(1):21–39.

Hendricks, K. B. and Singhal, V. R. (1997). Delays in new product introductions and the market value of the firm: The consequences of being late to the market. *Management Science*, 43(4):422.

Higgins, M. J. and Rodriguez, D. (2006). The outsourcing of R&D through acquisitions in the pharmaceutical industry. *Journal of Financial Economics*, 80(2):351–383.

Howard, J. (1998). *An Analysis of Security Incidents On the Internet*. PhD thesis, Carnegie Mellon University. http://www.cert.org/research/JHThesis/Start.html.

Iansiti, M. (1995). Shooting the rapids: Managing product development in turbulent environments. *California Management Review*, 38(1):37–58.

Jensen, M. C. (1986). Agency costs of free cash flow, corporate finance, and takeovers. *The American Economic Review*, 76(2):323–329.

Julisch, K. (2003). Clustering intrusion detection alarms to support root cause analysis. *ACM Transactions on Information and System Security*, 6(4):443–471.

Kannan, K. and Telang, R. (2005). Market for Software Vulnerabilities? Think Again. *Management Science*, 51(5):726–740.

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

King, A. A. and Tucci, C. L. (2002). Incumbent entry into new market niches: The role of experience and managerial choice in the creation of dynamic capabilities. *Management Science*, 48(2):171.

Krishnan, V. and Bhattacharya, S. (2002). Technology selection and commitment in new product development: The role of uncertainty and design flexibility. *Management Science*, 48(3):313.

Krishnan, V. and Ulrich, K. T. (2001). Product development decisions: A review of the literature. *Management Science*, 47(1):1.

Kumar, V., Telang, R., and Mukhopadhyay, T. (2007). Optimally securing interconnected information systems and assets.

Lambe, C. J. and Spekman, R. E. (1997). Alliances, external technology acquisition, and discontinuous technological change. *Journal of Product Innovation Management*, 14(2):102–116.

Lambrecht, B. (2004). The timing and terms of mergers motivated by economies of scale. *Journal of Financial Economics*, 72:41–62.

Lee, H. L. and Tang, C. S. (1997). Modelling the costs and benefits of delayed product differentiation. *Management Science*, 43(1):40–53.

Li, P. and Rao, H. (2007). An examination of private intermediaries roles in software vulnerabilities disclosure. *Information Systems Frontiers*, 9(5):531–539.

Loch, C. and Terwiesch, C. (2005). Rush and be wrong or wait and be late: A model of information in collaborative processes. *Production and Operations Management*, 14(3):331–343.

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

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

Luehrman, T. A. (1998). Strategy as a portfolio of real options. *Harvard Business Review*, 76(5):89–99.

MacKinlay, A. C. (1997). Event studies in economics and finance. *Journal of Economic Literature*, 35(1):13–39.

MacMillan, I. C. and McGrath, R. G. (2002). Crafting R&D project portfolios. *Research Technology Management*, 45(5):48–59.

McGrath, R. G. (1997). A real options logic for initiating technology positioning investments. *Academy of Management Review*, 22(4):974–996.

McGrath, R. G. and Nerkar, A. (2004). Real options reasoning and a new look at the R&D investment strategies of pharmaceutical firms. *Strategic Management Journal*, 25(1):1–21.

McShane, M. and Williams, F., editors (1997). *Victims of Crime and the Victimization Process*, volume 6 of *Criminal Justice - Contemporary Literature in Theory and Practice*. Routledge, New York, NY.

McWilliams, A. and Siegel, D. (1997). Event studies in management research: Theoretical and empirical issues. *Academy of Management Journal*, 40(3):626–657.

Mell, P. and Romanosky, S. (2008). A complete guide to the common vulnerability scoring system version 2.0. http://www.first.org/cvss/cvss-guide.html, Accessed 8 March 2008.

Michel, S. (2007). The upside of falling flat. *Harvard Business Review*, 85(4):21.

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

Moeller, S. B., Schlingemann, F. P., and Stulz, R. M. (2004). Firm size and the gains from acquisitions. *Journal of Financial Economics*, 73:201–228.

Moeller, T. (2004). Let's make a deal! How shareholder control impacts merger payoffs. *Journal of Financial Economics*, 76:167–190.

Mullin, W. (2001). Will gun buyback programs increase the quantity of guns? *International Review of Law & Economics*, 21(1):87–102.

Neter, J., Wasserman, W., and Kutner, M. H. (1990). *Applied Linear Statistical Models*. Irwin, Boston, MA, 3rd edition edition.

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

Nizovtsev, D. and Thursby, M. (2007). To disclose or not? An analysis of software user behavior. *Information Economics and Policy*, 19:43–64.

NVD (2008). National vulnerability database. http://nvd.nist.gov/, Accessed 8 March 2008.

Officer, M. S. (2007). The price of corporate liquidity: Acquisition discounts for unlisted targets. *Journal of Financial Economics*, 83:571–598.

Ozment, A. (2004). Bug auctions: Vulnerability markets reconsidered. *Third Workshop on the Economics of Information Security*.

Puranam, P., Singh, H., and Zollo, M. (2006). Organizing For Innovation: Managing The Coordination-Autonomy Dilemma In Technology Acquisitions. *The Academy of Management Journal*, 49(2):263–280.

Radianti, J. and Gonzalez, J. (2007). Understanding Hidden Information Security Threats: The Vulnerability Black Market. *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*.

Rahman, M., Kannan, K., and Tawarmalani, M. (2006). The Countervailing Incentive of Restricted Patch Distribution: Economic and Policy Implications.

Ranft, A. L. and Lord, M. D. (2002). Acquiring new technologies and capabilities: A grounded model of acquisition implementation. *Organization Science*, 13(4):420.

Rindova, V. P. and Kotha, S. (2001). Continuous 'morphing': Competing through dynamic capabilities, form, and function. *Academy of Management Journal*, 44(6):1263–1280.

Rogers, E. M. (2003). *Diffusion of innovations*. Free Press, New York, 5th edition.

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

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

Schechter, S. (2004). *Computer Security, Strength and Risk: A Quantitative Approach*. PhD thesis, Harvard. http://www.eecs.harvard.edu/ stuart/papers/thesis.pdf.

Schechter, S. E. and Smith, M. D. (2003). How Much Security is Enough to Stop a Thief? The Economics of Outsider Theft via Computer Systems and Networks. In *Proceedings of the Seventh Financial Cryptography Conference*.

Schiesel, S. (2000). Acquisitions by the technology companies of start-up small-fry offer a sampler on how deals can go wrong. *The New York Times*. 5 June 2000, p. 3.

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

Schumpeter, J. A. (1934). *The Theory of Economic Development*. Harvard University Press, Cambridge, MA, 7th edition.

Shane, S. and Ulrich, K. (2004). Technological innovation, product development, and entrepreneurship in management science. *Management Science*, 50(2):133–144.

Shleifer, A. and Vishny, R. W. (2003). Stock market driven acquisitions. *Journal of Financial Economics*, 70(3):295.

Siponen, M. (2005). Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods. *Information and organization*.

Sobel, M. (1982). Asymptotic Confidence Intervals for Indirect Effects in Structural Equation Models. *Sociological Methodology*, 13:290–312.

Sorensen, J. B. and Stuart, T. E. (2000). Aging, obsolescence, and organizational innovation. *Administrative Science Quarterly*, 45(1):81–112.

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

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

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

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

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

Sutton, M. and Nagel, F. (2006). Emerging economic models for vulnerability research. In *The Fifth Workshop on the Economics of Information Security*.

Telang, R. and Wattal, S. (2005). Impact of software vulnerability announcements on the market value of software vendors— an empirical investigation. Workshop on the Economics of Information Security.

Terwiesch, C., Loch, C., and Niederkofler, M. (1998). When product development performance makes a difference: A statistical analysis in the electronics industry. *The Journal of Product Innovation Management*, 15(1):3.

Terwiesch, C. and Loch, C. H. (1999). Measuring the effectiveness of overlapping development activities. *Management Science*, 45(4):455.

Tripsas, M. (1997). Unraveling the process of creative destruction: Complementary assets and incumbent survival in the typesetter industry. *Strategic Management Journal*, 18(Summer Special Issue):119–142.

Uhlenbruck, K., A., H. M., and Semadeni, M. (2006). Market value effects of acquisitions involving internet firms: A resource-based analysis. *Strategic Management Journal*, 27:899–913.

Ulrich, K. and Ellison, D. (1999). Holistic customer requirements and the design-select decision. *Management Science*, 45(May):641–658.

Voiskounsky, A. E. and Smyslova, O. V. (2003). Flow-based model of computer hacker's motivation. *CyberPsychology & Behavior*, 6(2):171–180.

Warner, A. G., Fairbank, J. F., and Steensma, H. K. (2006). Managing uncertainty in a formal standards-based industry: A real options perspective on acquisition timing. *Journal of Management*, 32(2):279–298.

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

Whetten, D. A. (1989). What constitutes a theoretical contribution? *Academy of Management Review*, 14:490–495.

Willison, R. A. (2002). *Opportunites for computer abuse: Assessing a crime specific approach in the cast of Barings Bank*. PhD thesis, London School of Economics and Political Science.

Wind, J. and Mahajan, V. (1997). Issues and opportunities in new product development: An introduction to the special issue. *JMR, Journal of Marketing Research*, 34(1):1.

Wysocki, Jr., B. (1999). Europeans snap up U.S. high-tech firms— they realize it's faster and cheaper to buy technology. *The Wall Street Journal Europe*. 18 August 1999, p. 4.

Ziedonis, R. H. (2004). Don't fence me in: Fragmented markets for technology and the patent acquisition strategies of firms. *Management Science*, 50(6):804.

Zmud, R. (1998). Editor's comments. *MIS Quarterly*, 22(2).