VIRGINIA COMMONWEALTH UNIVERSITY

Virginia Commonwealth University
VCU Scholars Compass

Theses and Dissertations | Graduate School

2006

An Integrative Approach for Examining the Determinants of Abnormal Returns: The Cases of Internet Security Breach and Ecommerce Initiative

Francis Kofi Andoh-Baidoo
Virginia Commonwealth University

Follow this and additional works at: http://scholarscompass.vcu.edu/etd

 Part of the Management Information Systems Commons

© The Author

Downloaded from
http://scholarscompass.vcu.edu/etd/1249

This Dissertation is brought to you for free and open access by the Graduate School at VCU Scholars Compass. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of VCU Scholars Compass. For more information, please contact libcompass@vcu.edu.

© Francis Kofi Andoh-Baidoo 2006
All Rights Reserved

AN INTEGRATIVE APPROACH FOR EXAMINING THE DETERMINANTS OF ABNORMAL RETURNS: THE CASES OF INTERNET SECURITY BREACH AND ELECTRONIC COMMERCE INITIATIVE

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Business at Virginia Commonwealth University

By:

Francis Kofi Andoh-Baidoo
MS, Information Technology & Management, University of North Carolina, Greensboro, NC, 2000
MBA, University of North Carolina, Greensboro, NC, 1999
BS (Honors), Materials Engineering, Kwame Nkrumah University of Science & Technology, Kumasi, Ghana, 1992

Directors:

Dr. Kweku-Muata Osei-Bryson (Chair)

Dr. Ojelanki K. Ngwenyama (Co-Chair)

Virginia Commonwealth University
Richmond, Virginia
April 2006

ACKNOWLEDGEMENT

I am grateful to the Almighty God for bringing me to this far. I also want to thank my committee members for all what they have done for me. My special thanks goes to my major Advisor, Dr. Osei-Bryson for his insight and direction. I deeply appreciate the extensive attention and support that I received from him. I would also like to thank Dr. Ojelanki Ngwenyama, my dissertation Co-Chair, for his invaluable insights that enhanced my understanding on some issues. Dr. Redmond always showed confidence in me even when I did not so feel so. Dr. Weistroffer spent several hours reviewing this work. He also provided timely advice. Dr. Dula's kind words were full of encouragement. I am grateful to Dr. Kasper for his emotional support. I thank the faculty, staff and students of the information systems department of Virginia Commonwealth University for providing the necessary assistance that I really needed. I am thankful to Drs. Dubofsky and Dhillon through whom the research topic emerged. To my family members and my friends who contributed to my success in the PhD program, I say big thank you. Most importantly, I am grateful to my wife, Rosemarie and my children, Kwabena Ntim, Afua Pomaah, Kofi Danso and Akosua Amoako for their sacrifice, understanding, spiritual, physical and moral support. I cherish you all. God bless you all!!

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

AN INTEGRATIVE APPROACH FOR EXAMINING THE DETERMINANTS OF ABNORMAL RETURNS: THE CASES OF INTERNET SECURITY BREACH AND ECOMMERCE INITIATIVE

by
Francis Kofi Andoh-Baidoo, Ph.D.

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at Virginia Commonwealth University

Virginia Commonwealth University, 2006

Major Director: Kweku-Muata Osei-Bryson, Professor, Information Systems Department

Researchers in various business disciplines use the event study methodology to assess the market value of firms through capital market reaction to news in the public media about the firm's activities. Capital market reaction is assessed based on cumulative abnormal return (sum of abnormal returns over the event window). In this study, the event study methodology is used to assess the impact that two important information technology activities, Internet security breach and ecommerce initiative, have on the market value of firms. While prior research on the relationship between these business activities and cumulative abnormal return involved the use of regression analysis, in this study, we use decision tree induction and regression.

For the Internet security breach study, we use negative cumulative abnormal return as a surrogate for damage to the breached firm. In contrast to what has been

reported in the research literature, our results suggest that the relationship between cumulative abnormal return and the independent variables for both the Internet security breach and ecommerce initiative studies is complex, often involving conditional interactions between the independent variables. We report that the incomplete contract theory is unable to effectively explain the relationship between cumulative abnormal return and the organizational variables. Other ecommerce theories provide support to the findings from our analysis. We show that both attack and firm characteristics are determinants of damage to breached firms.

Our results revealed that the use of decision tree induction presents additional insight to that provided by regression models. We illustrate that there is value in using data mining techniques to study the market value of e-commerce initiative and Internet security breach and that this approach has applicability in other domains and that Decision Tree can enhance the event study methodology.

We demonstrate that Decision Tree induction can be used for both theory building and theory testing. We specifically employ Decision Tree induction to test and enhance ecommerce theories and develop a theoretical model for cumulative abnormal return and ecommerce. We also present theoretical models for Internet security breach and damage to the breached firm. These models can be used by decision makers in Internet security and ecommerce investments strategic formulations and implementations.

CHAPTER1
INTRODUCTION

1.1 Overview of the Research Topic

> "Much has been learned from the body of research based on event study methodology... As one moves forward, it is expected that event studies will continue to be a valuable and widely used tool in economics and finance" (Mackinlay 1997, p.38).

Over the past three decades, businesses made tremendous investments in information and communication technologies to enhance operational efficiencies and to gain competitive advantage or maintain competitive parity (Larsen and Bloniarz 2000; Rosen and Howard 2000). What is even more important and remarkable is that during the last two decades of the twentieth century, incumbent firms that operate in traditional brick and mortar markets and new firms invested in electronic markets because of the potentials of electronic commerce to transform organizational activities and to support the global reach of firms.

Ecommerce is one of the most important business phenomena that has attracted the interest of researchers, practitioners and the public (Coltman et al. 2001). On the one hand, computer hardware, software, and networks that support electronic commerce became cheaper enabling small and large as well as existing and start up firms make IT investments in the electronic commerce environment. However, because there is little

control over these networks as they span over the globe, they expose firms to serious security threats.

As firms move their operations to the Internet and new firms start up Internet businesses, the public is bombarded regularly with news of variant virus attacks and other security threats to software applications and networks. These security threats inhibit the successful deployment and application of Internet-enabled technologies. Just before the end of the twentieth century, at about the mid April of 2000, the hype and hopes of electronic commerce dwindled forcing several businesses especially Internet firms to fold up resulting in what has been termed the "Internet bubble".

The Internet bubble has necessitated intensive inquiry by businesses and academic researchers into whether electronic commerce initiatives provide value to firms and to examine the factors that determine market value of electronic commerce investments. At the same time several researchers have examined whether firms that experience Internet security attacks are marked with decline in market value and to investigate the determining factors.

In this study, we define Internet security in terms of the preservation of confidentiality, integrity and availability of a firm's network and data resources. Hence a security breach occurs if confidentiality, integrity or availability of a firm's network or computer system is compromised (Bishop 2003). An Internet security breach could have negative impacts on the firm's performance including lower sales revenues, higher expenses, a decrease in future profits and dividends, and a reduction in market value (Gordon et al. 2003a; Power 2003). Although information security researchers and

practitioners recognize the seriousness of Internet security breaches, the relationship between security incidents and economic impact and valuation of the firm is not well understood. Measuring the economic impact of Internet security breaches will help in risk management and information security planning. However, making information systems security investment decision is very complex and difficult (Gordon and Loeb 2002).

The event study methodology has been employed to address the question of market value of firms with respect to electronic commerce initiatives and Internet security breaches (e.g., Campbell et al. 2003; Cavusoglu et al. 2004a; Hovav and D'Arcy 2003; Hovav and D'Arcy 2004; Subramani and Walden 1999; Subramani and Walden 2000; Subramani and Walden 2001). This methodology is a common approach that has been used in Finance, Accounting and Information Systems (IS) disciplines to study several events (e.g., Ball and Brown 1968; Binder 1998; Dos Santos et al. 1993; Fama et al. 1969).

The market value of a firm measures the confidence that investors have in that firm. Hence measuring the market value of a firm that has been compromised is one way of calculating the impact of Internet security breaches and augments other economic studies (Gordon and Loeb 2002; Gordon et al. 2003a). Firm damage can be operationalized as the observed cumulative abnormal return (CAR) that is attributed to the announcement of Internet security breach over the event window. For the Internet security breach analysis, we use CAR as a measure of firm damage.

Similarly, the market value of the firm's equity can be effectively used to measure information technology (IT) investments and such a measure can help mitigate the problems with measuring tangible and intangible benefits of electronic commerce. The current market value of the firm depicts investors' perception of the present value of all future benefits (both long term and short term) to the firm. While productivity related measures require observations of several months, measuring an event's economic impact can easily be computed using stock prices observed over a relatively short period using the event study approach. Thus the use of market value can minimize the time lag between ecommerce implementation and when productivity and or profitability improvements are realized which may require observations of several months or years (Mackinlay 1997), a situation that intensifies the productivity paradox (Brynjolfsson and Hitt 1996; Brynolfsson 1993; Hitt and Brynjolfsson 1996).

The Event study methodology typically has two goals: (1) to determine whether an event such as the announcement of Internet security breach, leads to CAR; and (2) to examine the factors that influence the observed CAR. Traditionally, regression is used for achieving the second goal.

1.2 Motivation for the Research

While prior event studies report that Internet security breach leads to negative CAR, they differ on the factors that impact CAR. These inconsistencies hinder the ability of organizations to develop effective strategies to minimize Internet security breaches.

Likewise, a review of the literature reveals that results on CAR and ecommerce initiatives are mixed (Dehning et al. 2004; Subramani and Walden 1999; Subramani and Walden 2000; Subramani and Walden 2001; Subramani and Walden 2002). Business researchers in fields such as Finance, Accounting and Information Systems traditionally use regression to assess the factors that impact CAR when conducting event studies. However, in some situations the number of potential variables could be so large that developing and testing of hypotheses may be extremely difficult or impossible. In such cases, the researcher may be unable to identify important relationships existing in the data that are not specified in the hypotheses. In addition, regression analysis is unable to handle variables with missing values. This implies that either the relevant observation has to be excluded, or that some approach must be used for imputing these values. Data mining techniques, such as decision tree induction have means of addressing missing values more effectively (Berry and Linoff 2004).

Decision-driven research suggests that accounting information influences investors' decision-making process (Lee 2001). More so, Lee cites interdisciplinary research concept to support his argument that accounting information is not the only economic factor which investors base their decisions on. This notion has support in the event study literature. The event study methodology has been used to show that, beyond the firm's past financial performance data, other factors influence the observed CAR resulting from the announcements of some events in the public media.

Investors' perception of a firm's current and future financial performance in response to announcements published in the public media will be influenced by the

investors' interpretation of the event and some specified characteristics of the firm whose stock is under consideration. For instance, if there is announcement in the public media on Internet security breach, an investor's reaction could be influenced by the attack and firm characteristics. The investor may respond differently based on his or her belief on the potential impact that the attack may have on that firm (Gupta et al. 2000). If the investor's past experience influences his or her decision, then he or she would assess the new event based on a similar event that has occurred in the past. In doing so, the event characteristics and the nature of the firm or organization or the industry in which the firm operates may be relevant variables. Thus the investors' perception of the firm's market value, as a result of the event, would be influenced by some characteristics of the firm and the event.

Similarly, firms would be interested in knowing which combinations of firm and event characteristics determine whether the event would lead to positive CAR or negative CAR, whichever is of interest. From past records, firms that make ecommerce investments can learn about the event and firm characteristics reported in the announcement and how these parameters affect CAR or how firm and attack characteristics of Internet security breach influence CAR.

Knowledge gained from the relationship between CAR and the firm and event characteristics could enhance an organization's understanding of favorable ecommerce characteristics and so focus on such ecommerce initiatives, or to understand the characteristics of Internet security breaches that lead to negative CAR so that they can

develop effective strategies to minimize damage that can result from attacks based on the attack characteristics and their specific firm characteristics.

Given a set of events that have been classified by some kind of dichotomous or nominal categorical variables with one of the variables assigning an event as either Abnormal (positive CAR or negative CAR depending on the event) or Normal based on other predictor variables, we can use DT induction to generate set of rules that can be employed to assign new events as Abnormal or Normal. These set of rules and outcomes can provide understanding of the relationships between firm and event characteristics and CAR. Thus while regression analysis determines how much the specific variables influence the level of CAR, DT induction is used to measure the likelihood that the event would lead to positive CAR or negative CAR.

We propose an integrative approach where both regression and data mining techniques would be employed to analyze the event data to present comprehensive understanding and explanation of the determinants of CAR in event studies in general through the illustration of the potentials of this approach from our study on ecommerce initiatives and Internet security breaches. It has been shown that the use of both data mining and regression for data analysis present additional insights that were not detected by the regression models alone (Ko 2003; Murphy 1998; Osei-Bryson and Ko 2004).

> Analysis with linear regression identified only one significant attribute...the induced decision trees revealed useful patterns... (Murphy 1998, p. 189).

Further, we seek to use DT induction to develop theoretical models that explain investors' behavior to the announcements of Internet security breaches influenced by firm and attack characteristics, and to test and enhance existing theories on electronic commerce initiatives and CAR. An additional motivational factor is that the results of prior research findings on Internet security breaches have been inconclusive. One of the main reasons for the disparity in the results is the inconsistency in the factors employed in the various studies. In this study, we use a comprehensive set of attack variables based on a theoretical model (Howard 1997).

Studying the market value of electronic commerce investments and Internet security breaches using an alternative approach is necessary, and has great potential to enhance existing theories and present new ways of looking at these two important and critical business activities in the IS discipline.

1.3 Research Questions

The research objective is to determine whether the use of our integrative approach consisting of regression analysis and data mining techniques in event studies provides better understanding on factors that influence CAR. Using Internet security and ecommerce, two business issues that have received extensive attention by both academic researchers and business practitioners, we seek to answer the following questions:

1. Does the announcement of Internet security breach in the public media lead to negative CAR?
2. Does the announcement of ecommerce initiative in the public media lead to positive CAR?
3. Using the Internet security sample data, does the use of Decision Tree Induction provide additional insight that is not presented by regression models?
4. Using the ecommerce sample data, does the use of Decision Tree Induction provide additional insight that is not presented by regression models?
5. Do theory-based factors enhance the understanding of the determinants of CAR for Internet security breach announcements?
6. Does the incomplete contract theory effectively explain the relationship between CAR and organizational variables?

We propose that the use of our integrative approach would provide more insight into understanding the determinants of CAR for ecommerce initiative and Internet security breach than with traditional regression models alone.

1.4 Significance of Research

The study has both academic and practical applications as it seeks to enhance theory and methodology. The proposed approach is applicable to IS and other business researchers. We make methodological contribution by providing a new approach to

solving the problem of market valuation of ecommerce initiatives and Internet security breaches. We also enhance the event study methodology in general since the integrated solution provides additional insights to what traditional regression-based event study alone may present. We are not aware of any paper that employs data mining technique to examine determinants of abnormal return in event studies in any discipline. This is the first time that a data mining technique is used to elucidate the variables that explain the observed abnormal return in event studies.

Giving that prior research on the market valuation of Internet security breach provide inconsistent results due to the variant and atheoretic factors that have been used to represent attack characteristics, we have broken new ground in exploring a range of attack variables that affect the market's reaction to Internet security breach announcements. This is achieved by using detailed theory-based taxonomy that represents the characteristics of the attack to examine the impact of attack and firm characteristics on CAR. This is the only single study where both firm and attack characteristics are found to be determinants of CAR. We also provide a theoretical understanding of the factors that determine negative CAR for breached firms by presenting theoretical propositions that can be used for further examination of the relationships between attack characteristics, firm characteristics, time lag and damage, which is operationalized as the observed CAR.

This integrative approach has the capability to provide more information and guiding principles to help decision makers make informed decisions on ecommerce investments and IT security management and investments. Some IS researchers show that

juxtaposing data mining and traditional regression presents additional useful insights that were not detected by the regression analysis alone (Ko 2003; Murphy 1998; Osei-Bryson and Ko 2004). Our work corroborates those findings. We show from our study that there is value in the use of data mining in the market valuation of Internet security breaches and ecommerce initiatives, and that data mining is useful for event study in other business domains.

With respect to the ecommerce initiative, we use DT induction to test the incomplete contract theory. Using DT induction, our data provides support to the existing literature that *Transformational* ecommerce initiatives are rewarded while *Executional* ecommerce initiatives are not. Beyond that, we also demonstrate that other variables (i.e. *Customer Type*, *Governance*) are predictors only when an ecommerce *Initiative* is *Transformational*. Since the incomplete contract theory is unable to effectively explain the relationship between the organizational variables and CAR, we use other ecommerce theories to provide justification for the observation. In fact, the ecommerce theories and the incomplete contract theory collaborate to provide a more effective explanation for the relationship between CAR and the organizational variables.

We demonstrate from this work that DT induction can be used for both theory building and theory testing. First, we use the theoretical model to develop a set of hypotheses to be tested. We then use DT induction to generate models that describe the relationship between CAR and the independent variables. We verify whether the findings are consistent with the theoretical model. Where there are discrepancies between the theoretical model and the empirical analytical results from the DT induction, we employ

other theories to explicate the observed relations. We then refine the theoretical model or state our findings, where we show whether the theory is able to explain the proposed relationships based on our sample data. We specifically employ DT induction to test and enhance ecommerce theories and to make theoretical propositions in the Internet security breach domain.

DT induction is also a proven technique for enhancing existing statistical approaches. We illustrate how DT induction is a valuable technique that enhances the event study methodology. Finally, we present sets of theoretical propositions for the relationships between the announcements of Internet security beach and CAR and the announcements of ecommerce initiative and CAR. These relationships can be further tested using different data sets.

With the growing interest in ecommerce investments and Internet security breaches, research that focuses on market valuation of these activities and effectively explicates the determinants of CAR is likely to significantly advance knowledge in this research topic. Using two case situations, we show that our approach has applications for research in other business disciplines.

1.5 Organization of the Study

The rest of the study is organized as follows. Chapter 2 is an overview of prior event study research on ecommerce initiative and Internet security breach. We also discuss risk management which is relevant to investment and management of Internet security breach. In chapter 3, we present the research methods that we employ in this

work with special treatment of the event study methodology and decision tree induction. Chapter 4 discusses theories, data description and the results of Internet security breach. First, we present two theoretical models that serve as the foundation for the hypotheses development. We present the data collection, data cleaning and coding of the events.

We present and discuss the results of the regression and DT induction analysis. We also present theoretical propositions for understanding the determinants of CAR for Internet security breach. Chapter 5 presents the theories, data set and findings for ecommerce initiatives. Here, we discuss the theories we employ to develop our hypotheses and also for explaining our empirical analysis. We also develop a set of hypotheses for the study. We then describe our data highlighting the collection process, data cleaning and coding. We discuss the findings from the ecommerce initiatives and present theoretical propositions that show how existing theories collaborate to explain the findings. In chapter 6 we conclude the paper by listing the limitations, presenting the highlights on the findings, and discussing theoretical, methodological and practical contributions, and suggesting potential future research.

CHAPTER 2
REVIEW OF THE LITERATURE

The event study methodology has been accepted in the information systems discipline as a useful approach for examining the market value of firms. In this section, we present a review of event studies in the field of information systems. We look at those studies on Internet security breach and ecommerce initiative in greater depth. Before we do that we provide some background information on electronic commerce. We also discuss security risk management which is relevant to how information security investments decisions are made.

2.1 Electronic Commerce

The importance of electronic commerce to the success of businesses in the modern information age is unquestionable. Relatively cheaper networks, hardware, software and new technologies, such as XML, make it easy for firms to not only have web presence for disseminating informational assets, but to develop better relationships with customers and suppliers. Traditional brick and mortar firms leverage online channel adding choice, flexibility and savings to the consumer.

In recent years, the worldwide ecommerce has experienced remarkable growth with corresponding significant increase in spending. For instance, it is reported that ecommerce worldwide reached a high $1.3 trillion in 2003 (Mahmood et al. 2004) and

that net spending during the holiday season in 2003 alone was 35% higher than that in the same period in 2002 (Sachs et al. December 2003). Ecommerce enables new approaches to marketing, retail transactions, knowledge distribution and other support activities (Applegate et al. 1996; Kardaras and Papathanassiou 2000).

The ecommerce market is classified into two main types: business-to-business (*B2B*) and business-to-consumer (*B2C*)(Chen and Siems 2001; Kauffman and Walden 2001; Subramani and Walden 2001). Noticing that there was no formal definition for the two main categories of ecommerce operations, *B2B* vs. *B2C*, Subramani and Walden make such distinction by stating that the former requires multiple firms to develop strategic joint actions in operations and especially in IT investments (Subramani and Walden 2000). From this view, a *B2B* initiative focuses on strategic investment decisions that enhance relationships with customers and suppliers and requires multiple firms. Later, the authors treated *B2B* vs. *B2C* as a *Customer Type* variable which consequently changed the original definition (Subramani and Walden 2002).

In the revised definition, *B2B* relationships are those where the ecommerce initiative promises some sort of benefits to business customers whereas *B2C* ecommerce seeks to generate benefits for the individual consumer or customer. In this study, *B2B* ecommerce involves electronic exchange between two or more business entities while *B2C* ecommerce involves at least one business entity and individual consumers. Our definition is in line with Subramani and Walden's later work where the benefits promised to the *Customer Type* is more critical than the number of participants involved with the initiative. This is important because we recognize that both *B2B* and *B2C* ecommerce

could either be a unilateral initiative, or a joint initiative, involving an alliance or partnership of multiple business firms. *B2B* initiatives tend to focus on improvement in the processes and systems that enable flow of information between organizations (Gebauer and Shaw 2002).

With the uncertainties in the ecommerce environment resulting from the dot.com crash, businesses have higher responsibility in making the "right" investment decisions in general and in ecommerce in particular. Firms have to understand the business value associated with strategic ecommerce initiatives. Any study that provides insight into understanding the investments in ecommerce will add to the knowledge of this interesting and challenging topic. Studies on the market valuation of *B2B* initiative for instance is of great interest due to the tremendous investments being made and the daunting projections of ecommerce in the very near future. It was proposed that *B2B* transactions alone could soar to about $7.3 trillion in 2004 (Subramani and Walden 2000).

Recently, Subramani and Walden used a set of binary variables to develop a theoretical understanding of ecommerce (Subramani and Walden 2002). The results showed that ecommerce investments provide market value when they involve complementary investments in intangible assets. The specific variables that were employed are *Customer Type, Firm Type, Product Type, Innovativeness*, and *Governance*. We seek to add to the literature on event study on ecommerce by extending Subramani and Walden's work on electronic commerce (Subramani and Walden 2000; Subramani and Walden 2001) using the variables employed in their recent work but we use an expanded period of study covering 1998 through 2003. This extension enables us

to look beyond the period where there was great volatility in the market so we can develop a more theoretical understanding over a wider period. In this way, our results would be less influenced by the market return fluctuations that occurred during the period of their study.

2.2 Internet Security Breach

Research shows Internet security as one of the critical issues that determine successful implementation of ecommerce solutions and operations (Chang et al. 2004; Torkzadeh and Dhillon 2002). Also in a 2000 Financial Times report, the director of the National Consumer Council was quoted as saying, "Unless the total online shopping environment – sites and payment mechanisms – is made more secure, some consumers will never have confidence to explore the opportunities" (Mackintosh, 2000, p2).

The CERT®/CC report shows continual increase in the number of incidents reported to the center. This number has grown from 21, 756 in 2000 to about 137, 529 in 2004 (Cert 2004). Further, businesses have been hit by several attacks including Denial of Service attacks and virus attacks such as "I love You", and "Melissa". In 2003, virus attacks alone cost businesses an estimated $55 billion (Tan 2004). Prior estimates were $30 billion for 2002 and $13 billion for 2001. On April 11, 2005 for instance, Lexis-Nexis made an astonishing revelation that about 310, 000 of its customers may have had their personal information stolen (Ewalt 2005).

Gordon and Loeb (2002) lament about the limited economic research on Internet security breach and assert that most of the research in that domain is primarily focused on behavior aspects and technical solutions. Within the technical solutions are those that provide encryption, access control, and firewalls (Amoroso 1994; Denning and Branstad 1996; Muralidhar et al. 1995; Osborn et al. 2000; Peyravian et al. 1996; Pfleeger 1997; Sandhu et al. 1996; Simmons 1994; Wiseman 1986); and those on intrusion detection systems (Axelsson 2000; Brown et al. 2000; Daniels and Spafford 1999; Denning 1987; Frincke 2000; Stillerman et al. 1999).

These studies focus on technical solutions to prevent security incidents in networks whiles the attack is underway. Some of these systems prevent intruders from getting into corporate networks while others have the capabilities to inform operators about security threats or automatically shut down systems when security threats are "highly" suspected. In performing these functions, the systems sometimes provide "false alarm" alerting responsible individuals of security threats when there is none. Some behavior research discuss management systems necessary to mitigate security breaches (Loch et al. 1992; Straub 1990; Straub and Welke 1998).

In response to the lack of economic studies on information security, Gordon and Loeb (2002) developed an economic model for estimating the optimal amount to invest in information security. The model asserts that firms need to invest a relatively small fraction of the expected loss due to security breach "Our analysis also indicates that, even within the range of justifiable investments in information security, the maximum amount

a risk-neutral firm should spend is only a fraction of the expected loss due to security breaches" (Gordon and Loeb 2002, p. 440).

While this model seeks to provide effective resource allocation, it could be difficult to implement since it requires firms to classify threats into three levels, an exercise that the authors do not provide guidelines for. Further, although the study has potential benefit, it has an inherent deficiency due to its limited focus on information type and vulnerability without consideration of the characteristics of the organization, which are critical variables when firms make IT investment decisions.

A game theoretic approach for IT security investments has been proposed (Cavusoglu et al. 2004b). This approach assumes relationships among: (1) firm's payoff from security investments, (2) hacker's payoff from hacking, (3) the likelihood of the hacker being caught, and (4) the likelihood of the firm being hacked. The model that computes monetary loss and benefits has inherent weakness since the Internet security *Attacker* may be motivated by non-monetary factors (Gupta et al. 2000; Howard 1997).

2.3 Risk Management Issues

Acknowledging that Internet security breach is a specific case of the risk management problem, we provide a brief review of the relevant risk management issues to position our discussion of Internet security breach in that literature. Straub and his research partners have used the deterrence theory to study information systems security (Hoffer and Struab 1989; Straub 1990; Straub et al. 1993; Straub et al. 1992; Straub and

Nance 1990; Straub and Welke 1998). The precursor of these studies is the model developed by Nance and Straub (1988). In general, this stream of research argues that actions taken by management can deter potential computer abusers from violating organizational security policies. Further, the theoretical models from these studies assert that security actions taken by managers actually lead to lower systems risk.

In particular, Straub and Welke (1998) provide a theoretical framework including: use of a security risk planning model, education and training in security analysis, and countermeasure matrix analysis that can be used to manage and minimize systems risk. Their research reveals that (1) managers are not aware of all the actions that can be taken to reduce systems risk; and (2) if managers are exposed to theory-grounded security planning techniques, they would be encouraged to employ them in their planning process. Their model seeks to demonstrate that managers can successfully deter, prevent, and detect abuse as well as pursue remedies and or punish offenders for abuse.

Clearly, Straub and Welke (1998) seek to advance the systems risk body of research. Systems risks deals with the conceptual belief that an organization's information systems are insufficiently protected against certain kinds of damage or loss. However, they allude to the fact that the deterrence theory was ineffective. Moreover, the increasing reports about security breaches suggest that management systems and policies are not effective in preventing security breaches. It is important that, with limited resources, management take the necessary steps to leverage risk and resources, and to implement the most effective and well informed Internet security investment strategies. The findings from Straub and Welke's model exemplify how our research could be

valuable to practitioners. We seek to develop a well-grounded theory-based understanding of Internet security and firm damage that we believe managers could incorporate into security planning, investments analysis and implementation strategies.

Generally, risk assessment deals with the cost-benefit analysis of security investments to ensure that systems are secured while managing the costs of the investments. In this section, we present some theoretical models on how firms and organizations manage security risk. In fact, information security implementation involves risk assessment and risk management (Bener 2000; Blakley et al. 2001).

Several approaches have been proposed for assessing risk in information security. Bener (2000) for instance discusses cultural and psychological theories of risk management. Dillon (2003) presents a framework that addresses technical failure, security, and management risks. The theoretical base for this framework is probabilistic (PRA) and decision analysis (DA). The assumption of these concepts is that there are potential alternative actions from which management can take to minimize risks. PRA is therefore used to quantify such risks. The DA, on the other hand, analyzes the potential benefits by using values and preferences to determine whether the potential benefits are favorable compared to the associated risks. Further, decision analysis seeks to select the best alternative that maximizes decision maker's utility.

The economic approach is generally used to justify investments of information systems security design and implementation. Fitzgerald and Courtney are among the pioneers who developed risk analysis methods (Courtney 1977; Fitzgerald 1978). Courtney defines risk as the product of risk probabilities and loss estimates. Generally

information security risk management involves risk assessment, procedures to minimize and maintain risk at an acceptable level. For instance, the National Institute of Standards and Technology defines information security risk management as:

> Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk (NIST 1995, p. 71).

In recent years, cyber risk insurance is used in managing Internet security threats in ecommerce environments. Firms such as America International Group, Chubb, and Fidelity provide various cyber risk insurance products (Gordon et al. 2003c). These companies have developed ways to address pricing, adverse selection and moral hazard problems. For instance, due to the lack of data on Internet security, it is impractical to use actuarial tables employed in traditional insurance products. In response, insurance companies have managed to develop pricing schemes but they question whether they are charging the right premium for their products (Gordon et al. 2003c).

Adverse selection problem results when the insurance firm has no information about the security vulnerability of the firm or how likely the firm seeking insurance can be breached. Accordingly, insurance companies require firms seeking cyber-risk insurance to have information security audit submitted before being issued with security policies (Gordon et al. 2003c). This allows insurance firms to issue different premiums to match the policy holder's level of vulnerability. Moral hazard deals with the situation where the insured firm has no incentive to develop actions to minimize the possibility of cyber-risk. Insurance firms address this problem by: (1) requiring firms that desire cyber-

risk insurance to have minimum deductibles; and (2) offering premium reductions for firms that take actions to reduce the loss probability.

Figure 2.1 represents a framework proposed for firms that seek to balance the mix of cyber-risk insurance and investment against security breaches (Gordon et al. 2003c).

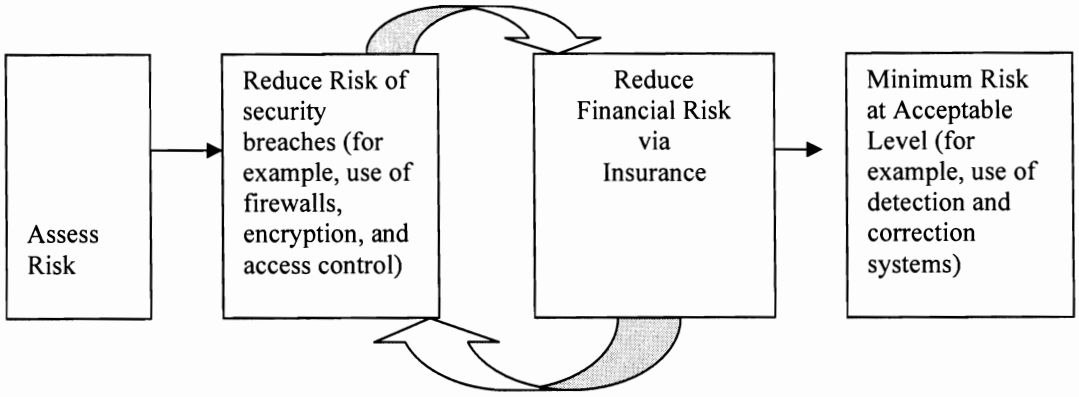

Figure 1: Cyber-risk Insurance Framework (Gordon et al. 2003c)

The researchers also suggest a four step cyber-risk insurance plan:

1. Conduct an Information security risk audit
2. Assess current insurance coverage
3. Examine and evaluate available policies
4. Select a policy

Information sharing has been suggested as an effective mechanism to reduce costs of information security investments while providing the necessary infrastructure to

minimize security breaches (Gordon et al. 2003b). The authors, however, recognize that without economic incentive mechanisms that can stimulate and facilitate the sharing of security information, the sharing of information cannot be effective and the expected benefits may not be achieved.

The authors argue that without these incentives, some firms will rather choose to free ride on the expenditures of other firms. The goal of most of the participating firms would be to falter on a sharing agreement, and in some cases provide less information to other participating firms and seek to reap individual benefits (Gordon et al. 2003b). The US Federal government has been involved with formation of several information sharing organizations including the CERT®/CC, INFRAGARD, Secret Service Electron Crimes Task Force, Information Sharing Analysis Centers, and Security Officers Round Tables in support of the information sharing initiative. Gordon et al. propose ways that firms can be motivated to share information as participants of information sharing groups. The strategies include providing subsidies to firms that join these organizations, providing government subsidized insurance and enabling favorable government regulations. The authors are quick to add that incentives should encourage and not discourage firms from participating in information sharing groups.

On the other side of cooperation is competition. In this case, Gordon and others have suggested that a firm's response to competitive analysis systems can be used to provide security (Gordon and Loeb 2001). According to this model, firms typically use competitive analysis systems to gather information about sensitive and strategic competitive information from competitors. Hence, the authors argue that if a firm can

determine what information its competitors would be interested in, then an approach to preventing the competitor to gain access to this useful informational asset would also serve as security for the firm.

A Simulation and Analysis (SEAS) laboratory at the Krannet Graduate school of management at Purdue provides synthetic economic set up for the modeling of effective strategies to counter threats facing Online financial institutions (Gupta et al. 2000). According to the researchers, the approach used presents several advantages over traditional simulation approach. The authors argue that simulation seeks to model rational behavior of humans which is not always true especially in the environment that was modeled. The synthetic economy, they state, allows human players to capture the decision making process of humans. The synthetic economy also creates search space that facilitates the monitoring, analysis and interpretation of the human behavior acted by the human players.

Our review on risk management suggests that firms have difficulty in addressing Internet security breach. In fact, some researchers argue that the economic approach of information security risk assessment is inadequate (Ansell and Wharton 1992; Baskerville 1998; Baskerville 1993; Baskerville 1991). Yet others suggest that it requires judgment "Quantification tools if applied prudently, can assist in the anticipation, budgeting, and control of direct and indirect computer security costs" (Mercuri 2003, p.15). With the scarce resource devoted for IT investments in risk management and that firms cannot ensure 100% security due to economic and technical problems (Gordon et al. 2003c), firms need the most relevant information to make the most informed decision

on Internet security investments. In this study, we seek to contribute to the risk management problem by providing new approach that can be used to understand the ramification of Internet security breaches in terms of market value and to provide a new way of establishing relationship between firm and attack characteristics and CAR. Knowledge from these relationships can be used by decision makers in security investment management strategies.

2.4 Event Studies in the Information Systems Discipline

The event study methodology has been widely used in the information systems literature. Dos Santos, Peffers, and Mauer (1993) used the event study methodology to assess the impact of the announcement of information technology investments on the market value of firms. Recently, the application of the event study methodology in the information systems discipline has been more prevalent including research involving: IT investments (Chatterjee et al. 2002; Dehning et al. 2004; Dehning et al. 2002; Im et al. 2001; Oh and Kim 2002), ecommerce investments (Dehning et al. 2004; Dehning et al. 2002; Subramani and Walden 2000; Subramani and Walden 2002; Subramani and Walden 2001), IT failures (Bharadwaj and Keil 2001), Dot.com name changes (Cooper et al. 2001), newly created CIO positions (Chatterjee et al. 2001), ERP implementation (Hayes et al. 2000), information systems outsourcing (Hayes et al. 2001), board of director nominations of Internet companies (Richardson and Zmud 2002), and Internet

security breaches (Campbell et al. 2003; Cavusoglu et al. 2002; Cavusoglu et al. 2004a; Ettredge and Richardson 2001; Hovav and D'Arcy 2003; Hovav and D'Arcy 2004).

These studies examine the business value of management activities and how CAR can be used to explain the future market value of firms. They also provide some theoretical understanding of the factors that determine the level of abnormal returns resulting from announcements of those activities in the public media.

2.4.1 Event Studies on Electronic Commerce Initiative

Some researchers have used the event study methodology to assess the economic impact of ecommerce initiatives (Dehning et al. 2004; Subramani and Walden 1999; Subramani and Walden 2000; Subramani and Walden 2002; Subramani and Walden 2001). Table 1 presents the various studies with highlights of the major differences. Subramani and Walden (1999) looked at 305 announcements of ecommerce initiative between October and December of 1998. Their motivation is that Internet technologies present strategic and operational benefits to organizations and thus capital markets would reward firms that seek to incorporate ecommerce operations into existing systems or new firms that seek to operate solely in the ecommerce environment.

Using the efficient market hypothesis as the basis, the authors argue that the announcement of ecommerce will lead to positive CAR. The results of the empirical study provide support for the hypothesis. The CAR from the analysis ranges from 3% to 11%. In particular, CAR of 11% and 10.5% were reported for the day of the event, and a 11 day window respectively. The authors also compared CAR for: (1) *Net* and *Non-Net* firms; and (2) *B2B* and *B2C*. Given that this is the first time the event study methodology

was used to assess the impact of ecommerce initiative on CAR, their study advanced knowledge in the market valuation of IT investments in the ecommerce environment.

Table 1: Event Studies on Ecommerce Initiative

Author (s)	Period of Analysis	Main Focus	Variables	Some Major Findings
Subramani &Walden (1999)	10/1998 – 12/1998	ecommerce initiatives	*Firm Type*[1], *Customer Type*[2]	o Firms reported CAR of 3-11 % within event window o Results on difference in CAR between *Net* and *Non-Net* firms did not support hypothesis o CAR for *B2C* was greater than that of *B2B* supporting hypothesis
Subramani & Walden (2000)	10/1998 – 12/1998	Empirically test the incomplete contract theory[3] on *B2B* firms	*Product Type*[4] (*Digital* v. *Tangible*) *Firm Type*	o CAR for *Net* firms is significant and that of *Non-Net* firms is not o There is no significant difference in CAR for *Tangible* v. *Digital* goods
Subramani & Walden	10/1998 –	ecommerce initiatives; sample	*Firm Type* *Customer Type*	o CAR for *Tangible* goods higher than

[1] *Firm Type* has two classes: *Net* firm v. *Non-Net* firm. The classification mechanism is based on resource-based view. *Net* firms are conventional firms that operate in the traditional brick and mortar market and *Net* firms are firms whose operations are mainly through the Internet.

[2] Firms are classified as either *B2B* or *B2C*.

[3] The incomplete contract theory is discussed in a latter section.

[4] *Product Type* can be *Digital* or *Tangible*; further discussion on this variable is presented in the paper

(2001)	12/1998	sample size less		that of *Digital* goods o *Firm Type* results are similar to 1999 study
Dehning et al. (2004)	1/1998 – 6/2002	Reexamine Subramani and Walden (2001) for 1998 and 2000 (Time lag effect)	*Firm Type* *Customer Type* *Time Lag* (2000 v. 1998) *Product Type*	o Positive and significant CAR in 1998 but not in 2000 o CAR for *Digital* goods was higher than that of *Tangible* goods in 2000 but not in 1998 o Initiatives involving *B2B*, *Tangible* products and *Net* firms had higher CAR in 1998 than in 2000
Subramani and Walden (2002)	1/1998-12/2000	Use long event window; develop comprehensive ecommerce theory	*Firm Type*, *Customer Type*, *Product Type*, *Governance*[5], *Innovativeness*[6]	o Results for short event window were not consistent o Results for long event window (1 year) are consistent o CAR for *Net* firms is 11.38% o CAR for *B2B* initiatives is 20.55% o CAR for *Tangible* goods is 13.39% o CAR for *Transformational* initiatives is 11.43%.

Subramani and Walden (2001) extend their 1999 work but includes *Product Type* as an additional variable: *Tangible* versus *Digital* goods. Other differences between the

[5] *Governance* deals with whether the initiative was through an alliance or was done unilaterally.

[6] *Innovativeness* refers to whether the initiative was transformational or executional (small changes in strategic direction). The distinction between the two categories is discussed in chapter 5.

two studies are that the estimation window is expanded and stocks with price less than $1 were eliminated from the statistical analysis reducing the usable events from 305 in the 1999 studies to 251. The results show significant CAR of 7.5 percent over a 5-day window and 16.2 percent during a 21 day window for ecommerce announcements. The resource-based view that suggests that the CAR for *Non-Net* firms was greater than *Net* firms was not supported by the *Firm Type* results. This was consistent with the results from the 1999 study. The CAR for *B2C* announcements was higher than that for *B2B* announcements. The results confirm the hypothesis that the CAR due to the announcements of ecommerce initiative is higher for *Tangible* goods than *Digital* goods.

In furthering research in this domain, Subramani and Walden (2000) used the event study methodology to test the incomplete contract theory, which is explicated in the next section, on the market value of *B2B* ecommerce. The event window was reduced to 45 days arguing that it reflects short time nature of the event that was measured. More so, they did not find any significant difference for the market returns between 270 days and 45 days.

The authors distinguish a *B2B* relationship from a *B2C* relationship by the way participants do business rather than pure descriptions. Similar to the 1999 work, the authors propose that the announcements of *B2B* initiatives would lead to positive CAR. Beyond this, the authors use the incomplete contract theory to develop four more hypotheses: (1) abnormal return attributed to the announcements of *B2B* initiative by *Non-Net* firms is not different from zero; (2) abnormal return attributed to the announcements of *B2B* initiative by *Net* firms is positive; (3) abnormal return attributed

to the announcements of *B2B* initiative by firms engaged in tangible goods is positive; and (4) abnormal return attributed to the announcements of *B2B* initiatives by firms engaged in *Digital* goods is not different from zero.

The regression tests confirm the researchers' proposition concerning Net firms and *Non-Net* firms. However, the authors did not see any significant difference between the returns of firms that deal with *Digital* goods from those that deal with *Tangible* goods. This is interesting since the 2001 study found significant difference in abnormal return between *Tangible* and *Digital* goods.

Recently, value relevance of ecommerce initiatives was reexamined (Dehning et al. 2004). The variables used were time period (4^{th} Qtr of 1998, 4^{th} Qtr of 2000), ecommerce type (*B2B* v. Non *B2B*), *Product Type* (*Tangible* v. *Digital*), and *Firm Type* (Pure-play (*Net*) and Non pure-play (*Non-Net*)). Dehning and his coworkers (Dehning et al. 2004) extend the work of Subramani and Walden (2001) by: (1) examining the announcements of ecommerce initiative for the 4^{th} quarters of 1998 and 2000; (2) proposing a new event study methodology appropriate for high volatile markets; and (3) testing Subramani and Walden's regression variables.

In addition to the traditional event study approach, the authors employ an alternative methodology. They argue that in high volatile markets, the abnormal returns can be exaggerated and suggest that researchers verify that the abnormal returns are actually due to the events by comparing the abnormal return on event dates to abnormal return on random dates. They argue from the results of their study that traditional methodology could not isolate abnormal return on ecommerce announcement dates from

abnormal return on other dates around the ecommerce announcement whereas the alternative methodology does. They assert that the alternate methodology is more reliable than the traditional methodology in highly volatile markets. However, they found that the methodology proposed lack statistical power when the event window was increased beyond three days and therefore urge researchers to continue to use the standard methodology for long event window. It must be noted that the concerns raised by these researchers are as a result of the market volatility with respect to the period of study (4^{th} quarters of 1998 and 2000).

Subramani and Walden (2002) argue that long event window provides better reflection of firm value creation capability for novel information technologies such as ecommerce than what short event window presents. This argument supports the resource based view of the firm where the usage of ecommerce is critical for realization of business value of ecommerce (Zhu and Xu 2004).

Subramani and Walden's latest research differs significantly from prior research. First, the authors use both short run and long run event study techniques. The authors argue that the variations in CAR during the period 1998 and 2000 are similar to the market variations suggesting that "extraneous, non-firm-specific factors may be very influential in determining short term abnormal returns than is recognized by researchers" (Subramani and Walden 2002, p.7). The authors champion longer event windows for novel technologies such as ecommerce initiatives.

> Event studies in the IS literature that use short term event windows assume that investors in capital markets make a comprehensive assessment of the value created by events within a short time and window after news of the firm's plans become public. This is a questionable assumption in the context of IT-enabled events involving novel technologies for several reasons (Subramani and Walden 2002, p.5).

One problem with long event window is that some firms make several announcements within this period. Since the motives for each announcement and the initiative are different and are however influenced by prior initiatives, using long event window could confound prior announcements or initiatives. In most cases, the second and or third event may have to be dropped because they confound the previous announcements. Since the first may involve *Executional* while the later may involve *Transformational* initiative, dropping the second because it confounds the first initiative diminishes the findings of the empirical analysis especially where the reason is because the event window has been intentionally prolonged.

In the same way, if the investor uses the information that they know in making investment decisions then the current knowledge that they have or the understanding that they get from the announcement is what will influence their decisions. Hence, for a firm that makes three ecommerce investment announcements, the investor's decision on the third announcement could be influenced by those of the first two but will be primarily based on the information that he or she gets from the last announcement.

Arguments for long event window are based on the assumptions that investors will wait for such a long time to make a buy or sell decision. Investors make their

decision anytime possible and revise their decision not only on that single event but on several other events involving the firm. There is no guarantee that the specific investor would remember the event that happened ten months ago in revising his or her decision based on a current event. In this study, we look at more prolonged period 1998 through 2003 which covers periods before, during and after the Internet bubble to alleviate some of the concerns that some researchers have on short event window. Second, Subrmani and Walden (2002) include business model as additional explanatory variable. The results of their study, however, show that the theory of primacy of intangible assets explains the observed CAR for electronic commerce initiatives better than predicted by business model. The authors observed CAR of 11.38%, 20.55%, 13.39%, and 11.43% over a 1-year window for *Net* firms, *B2B*, *Customer Type*, *Tangible* products, and *Transformational* electronic commerce initiatives respectively.

Again, using long event window could erase a benefit that event study methodology provides for understanding the business value of IT investments. Unlike the productivity and cost benefit methods, event study provides a short term stock market analysis of the reaction of investors to the firm's plan to develop ecommerce initiatives. By using a long event window, it may be difficult for the firm to detect whether investor's reaction is based on the specific initiative or other confounding effects that may have taken place during such a long period. Focusing on long event windows such as a year could "resurrect" the productivity paradox (Brynolfsson 1993) arguments with respect to the use of event studies for studying IT investments in general. Several research discuss how nonparametric analysis can be used to minimize the problems of

return variability (Aktas et al. 2004; Corrado 1989; Cowan 1992; Seiler 2000). The use of nonparametric statistical analysis can help mitigate some of the concerns that have been raised in support of long event windows for IT investments. We use the nonparametric statistical analysis in this study.

2.4.2 Event Studies on Internet Security Breach

Table 2 is a list of event studies on Internet security breach with the major findings and distinguishing features. One of the earliest studies on Internet security breach and (negative) CAR is that of Ettredge et al. (2001). Ettredge et al. focused on denial-of-service (DoS) attacks that occurred over a very short period - February 2000. Given that this was the first event study that focused on security breaches, the findings make a significant contribution to the literature.

The main limitation of this research however was its lack of consideration of effect of firm and attack characteristics as they relate to abnormal return. Firm characteristics and the nature of the attack were later studied by Cavusoglu et al. (2002; 2004a). In particular, firm characteristics considered were *Firm Size* and *Firm Type*. The nature of the attack was examined by categorizing the events into *Denial of Service* and non-Denial of Service attacks.

Cavusoglu et al. examined how firm characteristics, the nature of the attack, and time (considering that the interest of stakeholders in Internet security incidents has increased in recent years) affect CAR. These researchers also studied the impact of security breaches on firms that provide information security technologies. The results show that *Firm Type, Firm Size*, and *Time* are important factors that affect the abnormal

(negative) return. Cavusoglu et al.'s study also suggests that market value of breached firms decrease while those of security developers increase within two days of announcement of the security breach. On the average each firm in the sample lost 2.1 percent of its market value within two days of the announcement.

Table 2: Event Studies on Internet Security Breach

Author (s)	Period of Analysis	Main Focus	Variables	Some Major Findings
Ettredge et al. (2001)	February 2000	Denial-of-service attacks	*Firm Type* Firm's e-risk	o *B2C* firms experienced 7.9% lower CAR o Internet firms that disclosed controllable e-risk experienced more negative CAR
Cavusoglu et al. (2004a)	1/1996 – 12/2001	Internet security breaches in general and economic effect of attack on security developers	*Firm Size*[7] *Firm Type* Time lag The nature of the attack[8]	o Breached firms lost an average of 2.1% market value within 2 days of the announcement o Security developers gained 1.36 % within the same event window o The nature of the attack does not influence CAR o *Firm Size, Firm Type* and *Time* are determinants of CAR
Campbell et al. (2003)[9]	1/1995-12/2000	Confidential Information	The nature of the attack (*Confidential*	o The nature of the attack influences CAR

[7] In all the studies, *Firm Size* was categorized as small or large using financial market data.

[8] Measure of this variable varies across the studies.

[9] In all the studies, the hypothesis that Internet security leads to abnormal stock market return was

			v. *Non-confidential*)	○ *Confidential* information has more negative CAR than *Non-confidential* information
Hovav and D'Arcy (2003)	1/1998 – 6/2002	Denial-of-service attacks	The nature of the attack (*Denial-of service-attack* v. *non-denial-of-service attack*)	○ The stock market does not penalize firms that report *Denial of Service* attack, i.e. the nature of the attack is not a determinant of CAR ○ *Net* firms have more negative CAR than *Non-Net* firms
Hovav and D'Arcy (2004)	1/1998 – 12.2002	Virus attacks	The nature of the attack (*Virus attack* v. *non-virus attack*)	○ Virus attack is not a determinant of CAR, i.e., the nature of the attack is not a determinant of CAR

On the other hand, each security developer earned an abnormal return of about 1.36 percent for the two day of announcement with an average market gain of about $1.06 billion. The nature of the attack, however, was not found to have effect on the CAR. Clearly, Cavusoglu et al.'s work made a great stride in understanding the phenomenon. One aspect that this research did not, however, consider was whether investors' reaction to breaches involving confidential information impacts CAR. This factor is important since confidentiality, integrity and availability are the basic dimensions of information security. Confidentiality has always been considered as one of the main tenets of security (Bishop 2003).

---

significantly confirmed except Campbell et al. that was marginally significant (i.e., α=0.051)

Campbell et al. (2003) examined the confidentiality dimension that was not considered in Cavusoglu et al.'s study by classifying events as either confidential or non-confidential. Campbell et al.'s research covers the period January 1995 to December 31, 2000. Contrary to the findings by Cavusoglu et al., Campbell et al.'s study show that the nature of the attack influences CAR. One sharp distinction and perhaps the most probable reason for the difference in the findings between the two studies is that the variables representing the nature of the attack are completely different. While Cavusoglu et al. use *Denial of Service* and *non-Denial of Service* to represent the characteristics of attack, Campbell et al. classified attack as *Confidential* and *Non-confidential*.

Quite Recently, Hovav and D'Arcy performed two different event studies measuring the impact of *Denial of Service* attacks (2003), and virus attacks (2004) on the market value of firms. Their results show that there is significant impact of the announcement of virus attack on breached firms. With the study on *Denial of Service* attack, the researches found that although firms that are breached do not experience significant abnormal returns in general, *Net* firms have a more negative abnormal return than *Non-Net* firms. We find that for all the studies, although categories employed to represent the nature of the attack are components of attack characteristics, the categorization itself is atheoretic.

From a review of the event studies literature, we notice that the major problem with research focusing on Internet security breach and abnormal (negative) return is the inconsistencies in the factors used, particularly the attack characteristics. Attack characteristics are potential predictors that could influence CAR (Campbell et al. 2003;

Cohen et al. 1998; Howard 1997). Obviously, stockholders will not ignore the information that they read on Internet security breaches; they will surely assess the valuation impact of what they read. Hence in the absence of information asymmetry, the stock market reaction to Internet security breaches could be influenced by the specifics of the incident. Effective examination of this claim requires that well-defined factors be established. We use regression and DT induction to determine the relationships between CAR and the predictor variables: firm and attack characteristics. The potential predictors are informed by the literature (Campbell et al. 2003; Cavusoglu et al. 2002; Cavusoglu et al. 2004a; Cohen et al. 1998; Ettredge and Richardson 2001; Howard 1997; Im et al. 2001).

CHAPTER 3
RESEARCH METHODS

In this study, we use traditional event study methodology to assess the impacts that the announcements of Internet security breach and ecommerce initiative have on CAR. Two approaches are used to measure the factors that influence the observed CAR: decision tree induction (a data mining technique) and traditional regression. In this section, we review the event study methodology and decision tree induction in more detail. First, we describe the efficient market hypothesis which is the basis for the event study methodology.

We discuss the forms of the hypothesis stating specifically which form is related to the event study methodology. We then discuss the event study methodology where we describe the steps for the methodology and also discuss the statistical tests for examining the statistical significance of the claim that the event leads to abnormal return. Following these, we present an overview of data mining approach and decision tree induction where we describe the sibling rule. Finally we present a statistical test, the test for the significance of difference between independent proportions, for examining whether the predictor variables that play the role of discriminating predictor are statistically established to be predictors of CAR.

3.1 Efficient Market Hypothesis

The Efficient market hypothesis (EMH) posits that capital markets are efficient mechanisms for processing information available about firms (Fama et al. 1969). Investors, according to this hypothesis, process information about current and past activities of a firm to assess its current and future market value. The market's valuation of a firm is reflected in the firm's market price as measured by the present value of all expected future cash flows.

The hypothesis conveys the notion that stock price reflects all the available information about the firm. As new information about the firm becomes available, the price of the stock quickly adjusts so that at any time, the stock price equals the market consensus estimate of the value of the stock (Bodie et al. 2001).

3.1.1 Forms of the Efficient Market Hypothesis

Three categories of the EMH widely discussed and tested in the literature are weak, semi-strong, and strong forms. These versions of EMH are differentiated by the definition of the information set typically used in testing the hypothesis. Following, we present the distinctions between the three forms of the EMH.

3.1.1.1 The weak-form EMH

The weak form of the EMH considers its information set to be solely the information contained in the past price history of the market as of time *t*. The assertion of

this form of the hypothesis is that a firm's stock price reflects all the available information derived by examining market trading data such as history of past prices, trading volume, or short interest. According to this form of the EMH, there is no economic incentive for investors to perform trend analysis on past historical data as information from such activities is already reflected in the stock price.

3.1.1.2 The semi-strong-form EMH

The semi-strong form EMH takes as its information set those of the weak form in addition to publicly available information regarding the prospects of the firm at time *t*. The information include fundamental data on the firm's product line, quality of management, balance sheet composition, patents held, earnings forecasts, accounting practices, etc. (Bodie et al. 2001, p. 270). Clearly, the weak form EMH is a restricted form of the semi-strong form.

3.1.1.3 The strong-form EMH

The strong form EMH encompasses all kinds of information available at time *t* including information available only to company insiders. This definition makes it difficult to justify insider trading as a criminal offense. The reason is that all information that the insider knows, by which he or she is being charged has already been factored into the stock price. The argument put forth violates the belief that insiders have advantage in trading on information that the public is unaware of. The fundamental problem therefore

is a flaw in the definition and that a paradox may exist as a result of the discrepancy between this definition and justification for insider trading.

3.1.2 Tests of the Efficient Market Hypothesis

Different measures are used in testing the efficacy of the three forms of the EMH. The weak form EMH is tested by answering questions such as: is price efficient with respect to past prices? The predictability test is used to test the weak form EMH. Specifically, if investors or speculators could use trends on past stock prices to earn abnormal returns then the weak form EMH has failed.

Event study (which is discussed in detail in the next section and the methodology employed in this study) is used to test the semi-strong EMH. It answers the question: do prices adjust efficiently to public information? The semi-strong form EMH is the most accepted form of the EMH and generally implied in the literature when there is no specific qualification to the EMH. Perhaps the main reason for the high acceptability of the semi-strong EMH is its consistent test results, at least compared to the other forms (Jensen 1978). According to the semi-strong form EMH (with which empirical evidence is consistent), the market price fully reflects all publicly available information (Fama 1970). Finally, the strong form EMH is tested using performance evaluation methods. It answers questions such as: does anyone have private information not contained in market prices?

3.2 Overview of the Event Study Methodology

Recall from the previous section that the event study methodology is based on the efficient market hypothesis, which posits that capital markets are efficient mechanisms to process information available about firms (Fama et al. 1969). Specifically the event study methodology is the test for the semi-strong form of the efficient market hypothesis. This form of hypothesis states that investors process publicly available information about the activities of a firm that impact the firm's current and future performance. Further, as new information about the firm's activities that can potentially affect the firm's future earnings is publicized, the stock price changes relatively quickly to reflect the current assessment of the value of the firm.

Since the seminal works of Ball and Brown (1968) and Fama et al. (1969), the event study methodology has been very successfully used in the fields of Finance, Accounting and Information systems for empirical research in examining the effects of several events on the returns of a firm's common stock. "The event study methodology has...become the standard method of measuring security price reaction to some announcement" (Binder 1998). In the next section we discuss the steps of the original event study framework (Fama et al. 1969).

3.2.1 Steps of the Event Study Methodology

The typical event study methodology has the following steps: (1) determine the event of interest; (2) determine the announcement date; (3) determine event window, (4)

determine estimation window; (5) estimate parameters of event generating model; (6) compute the abnormal return, and the cumulative abnormal return; (7) average the abnormal returns on the sample; and (8) construct statistical test of significance.

The two events that we study are the announcements of Internet security breach in one of the major newspapers (Financial Times, New York Times, USA Today, Wall Street Journal and Washington Post) for the period 1997 to 2003, and the announcements of ecommerce initiative in PR Newswire or the Business wire for 1998 to 2003. The event window is the period over which the event occurs. Generally the event window is defined to be larger than the specific period of interest but should be short relative to the estimation period. Typical event window is 3 days covering a day before the announcement through the day after the announcement.

The estimated window is the period over which the normal stock market return is estimated. Typically this period is 120 days but 160 days has been used in some studies. Generally, the event period is not included in the estimation window to prevent the event from influencing the normal performance model.

Typically, a set of criteria is defined to select appropriate events to be included for analysis. The criteria include: (1) selecting the first announcement when a single event is reported multiple times in a single source or multiple sources, (2) including firms that were listed on the exchange from which market parameter estimates are obtained, and the firm listed in the specific database where stock prices are obtained; (3) ensuring that for firms included in the research database, the returns are available for at least a period equal to the estimation window; and (4) ensuring that where there are confounding

effects such as earning announcements, dividends or any major announcement in the event window involving a firm that is included in the sample, the event is dropped.

3.2.2 Return Generating Process

In order to compute abnormal returns, we need to first estimate what the normal return would be without the event. Two common approaches are employed in the estimation of normal returns: the constant mean return model and the market model. Of these two, the market model is the most frequently used. Some researchers have shown that the results of short term event studies are insensitive to the return generating model (Aktas et al. 2003; Brown and Warner 1980; Brown and Warner 1985).

Using the Market Model (Sharpe 1963), the return of a specific stock can be represented as:

$$R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it}$$

where R_{it} = return of stock i on day t; R_{mt} is the return of the market portfolio on day t, α_i, β_i are the intercept and slope parameters respectively for firm i, and ε_{it} is the disturbance term for stock i on day t.

For the Internet security breach, according to the semi-strong EMH, a firm that experiences Internet security breach will report a negative abnormal return (prediction error). This reflects the market reaction to the announcement which is quickly absorbed

into the firm's stock. We compute the daily abnormal return by subtracting the predicted normal return from the actual return for each of the days in the event window. The abnormal return is also referred to as the excess return.

We compute the abnormal return for firm *i* on day *t* of the event window as:

$$AR_{it} = R_{it} - (\hat{\alpha}_i + \hat{\beta}_i R_{mt})$$

where $\hat{\alpha}$ and $\hat{\beta}$ are the ordinary least square estimates of α and β. These parameters are estimated using the market model over the 120 day period ending with the day immediately preceding the first day of the event window, i.e. day (-2).

The summation of the daily abnormal returns over the event window is the cumulative abnormal return. The cumulative abnormal return for stock i over the event window $(T1, T2)$ is computed as:

$$CAR_{i(T1,T2)} = \sum_{t=T1}^{T2} AR_{it}$$

For a sample of *n* stocks the cumulative abnormal return over the event window is

$$CARR_{(T1,T2)} = \frac{1}{n} \sum_{i=1}^{n} CAR_{i(T1,T2)}$$

For the ecommerce initiatives, the abnormal return and the cumulative abnormal return (CAR) are expected to be positive. For Internet security breaches, the abnormal return as well as the cumulative abnormal return is expected to be negative.

3.2.3 Test of Significance

Eventus® software is used in the computation of abnormal return resulting from the announcements of Internet security breach and announcements of ecommerce initiative. Eventus® effectively interfaces with SAS and CRSP to generate test results. The generalized sign test is used for testing the statistical significance of the results. "The generalized sign test examines whether the number of stocks with positive cumulative abnormal returns in the event window exceeds the number expected in the absence of abnormal performance" (Cowan 1992, p.5). It is a nonparametric statistic.

Nonparametric tests have been shown to provide higher power in the detection of abnormal return than traditional parametric tests (Corrado 1989; Cowan 1992). Brown and Warner (1985) show that parametric tests report "false" price more often than nonparametric tests when there are event-related variances. The advantage of nonparametric tests over parametric tests is that nonparametric statistic is not subjected to stringent assumptions about return distributions as parametric does.

According to Seiler (2000), the generalized sign test alone is not powerful enough. Seiler suggests that the standardized cross sectional test, a hybrid of the standardized residual test and cross-sectional methods, enjoys the benefits of both methods. For the standardized cross-sectional test, he states that "...it prevents few

securities with large sample variances from driving the results" (Seiler 2000, p. 103). In this study, the standardized cross-sectional test is performed to cross validate the generalized sign tests results.

Other studies have used the time series standard deviation method (Brickley et al. 1991; Dopuch et al. 1986). Although the time series standard deviation method computes a single variance estimate for the entire portfolio without consideration of the unequal return variances across firms or events, it evades the potential problems of cross-sectional correlation of security returns.

Although the rank test is more powerful than the generalized sign test, in the case where the return variance increases, the generalized sign test offers the better choice (Cowan 1992). In particular, Cowan shows that when a single stock in a portfolio has extreme positive return, the generalized sign test is correctly specified while the rank test is not.

For the Internet security breach events, recall that we expect that the cumulative abnormal return will be negative. We therefore test the hypotheses:

$$H_A : CARR_{T1,T2} < 0$$

$$H_0 : CARR_{T1,T2} \geq 0$$

For the Internet security breach, if the null hypothesis is true then we would fail to reject it and accept that the announcements of Internet security breach have no impact on CAR. However, if the alternative hypothesis is true, then we reject the null hypothesis

and state that the announcements of Internet security breach in the public media have negative impact on CAR and for that matter, firm damage.

For the announcements of ecommerce initiative, we would test the following hypotheses:

$$H_A : CARR_{T1,T2} > 0$$

$$H_0 : CARR_{T1,T2} \leq 0$$

If the null hypothesis is true then we would fail to reject it and accept that the announcements of ecommerce initiative have no impact on CAR. However, if the alternative hypothesis is true, then we reject the null hypothesis and state that the announcements of ecommerce initiative in the public media have positive impact on CAR and, for that matter, market value.

3.3 Overview of Data Mining

Confirmatory and exploratory approaches can be used to analyze statistical data. With the confirmatory approach, the researcher develops and tests hypotheses, whereas with the exploratory approach, however, the researcher identifies useful patterns from the data via data analysis without any prior hypothesis.

Most of the prior event studies use confirmatory analysis, specifically regression and ANOVA, in examining the determinants of abnormal stock market return. In this

study we juxtapose both confirmatory and exploratory approaches where confirmatory approach we employ is regression analysis and exploratory approach involves the use of decision tree induction, a data mining technique.

While regression models have several advantages, the use of data mining is important in certain situations. For instance where data is large and the size of variables or factors is large, it could be difficult for the researcher to develop every hypothesis. Even more difficult would be the ability to develop the research design necessary to ensure that all possible hypotheses and models are tested and analyzed. In addition, the researcher may not be able to discover additional important relationships in the data among the variables that are not explicitly specified in the hypotheses. It is also acknowledged in the literature that confirmatory approaches do not effectively handle missing variables. For instance, when there are missing values, confirmatory approaches either exclude the variable, or estimate the variable using imputation. However, exploratory approach has been found to effectively address the missing value problem.

3.4 Overview of Decision Trees

A decision tree (DT) is a representation of a given decision problem in tree structure where every non-leaf node is associated with one of the decision variables, and every branch from a non-leaf node is associated with a subset of the values of the corresponding decision variable, and each leaf node is associated with a value of the target (or dependent) variable. If the target variable is discrete then the DT is considered

to be a classification tree and for each node the DT generation algorithm generates the relative frequencies (probabilities) for the classes of the target variable. At every leaf a class is assigned, with the winning class being the one that provides the largest class probability (even if the probability is less than 50%). If the target variable is continuous the DT is considered to be a regression tree. For every node, the DT algorithm associates the mean value of the target variable.

Generally a decision tree is generated in two phases: growth phase and a pruning phase (Kim and Koehler 1995). The growth phase involves inducting a DT from the training data (initial set used to generate tree structure and therefore the rules) in such a way that either each leaf node is associated with a single class or further partitioning of the given leaf would result in the number of cases in one or both child nodes being below some specified threshold. The pruning phase seeks the generalization of the DT generated from the training set so as to avoid over fitting the DT. Hence, in the pruning phase, the DT is evaluated against the validation dataset in order to generate a subtree of the DT generated in the growth phase with the lowest error rate against the validation dataset.

In the growth phase, DTs are built using greedy algorithms in a top-down manner. The algorithm involves a recursive class dependent partitioning (i.e. splitting) of the relevant training data. The splitting method is the component of the DT induction algorithm that determines both the attribute (variable) that is selected for a given node of the DT and also the partitioning of the values of the selected attribute into mutually exclusive subsets such that each subset uniquely applies to one of the branches that emanate from the given node. Various splitting methods have been proposed including

those based on information theory (e.g. entropy) and those based on distance between probability distributions (e.g. Gini) (Breiman et al. 1984; Quinlan 1993). It is established in the literature that there is no single splitting method that will give the best performance for datasets and that some datasets are sensitive to the choice of splitting methods while other datasets are insensitive to the choice of splitting methods (Osei-Bryson and Giles 2002).

Decision tree induction identifies those variables most significant in predicting the outcome. The most significant attribute is located at the root of the tree and succeeding attributes further discriminate between the outcomes. The sequence of attribute values in the decision tree can easily be converted to the rules of an expert system.

One of the strengths of decision tree induction is the excellent explanatory power of the rules generated. It is shown that decision tree is one of the few data mining techniques able to simultaneously handle both categorical and continuous variables in a classification problem (Quinlan 1990).

In this study we use classification trees to classify events using CAR as the categorical dependent variable (abnormal or normal). Thus while regression tree is an alternate approach to addressing linear regression models, classification trees can be used to answer questions that are traditionally answered by linear logistic models. More importantly, decision tree approach offers several benefits including:

1. DT presents more interpretable English rules and actions that are easily understood

2. When DTs are used, they may provide additional insights that confirmatory approaches such as regression are unable to identify
3. DTs can handle interaction among predictors that may be difficult for some confirmatory approaches.

In this study we use DT induction to generate strong rules & discriminating predictor variables. We test a set of hypothesis to verify the statistical significance of the discriminating variables as predictors of CAR. Strong rules provide evidence of conditions that are highly likely to lead to CAR. Even if the given input variable does not play the role of a discriminating predictor, its presence in such rules indicates that it could be an important predictor of CAR. For this study we focus on rules for which the relative frequency of a CAR is at least 80%.

3.5 Sibling Rules

Decision tree (DT) induction is used to partition the dataset into subsets based on input variables selected by the relevant splitting method. In a DT, Nodes that have the same non-root parent node (i.e. input variable) are referred to as sibling nodes, where each sibling is associated with a mutually exclusive subset of the values of the relevant input variable, and the relevant value of any higher ancestor node. Figure 2 below displays one obvious pair of sibling rules where all conditions are the same except for the one involving the given subject variable (i.e. *Governance*):

- IF *Innovativeness* is *Transformational & Governance* is *Unilateral* THEN *CAR* is *Positive* with probability 74.5% and N (i.e. Number of Cases) = 115;
- IF *Innovativeness* is *Transformational & Governance* is *Joint* THEN *CAR* is *Positive* with probability 84.3% and N = 97.

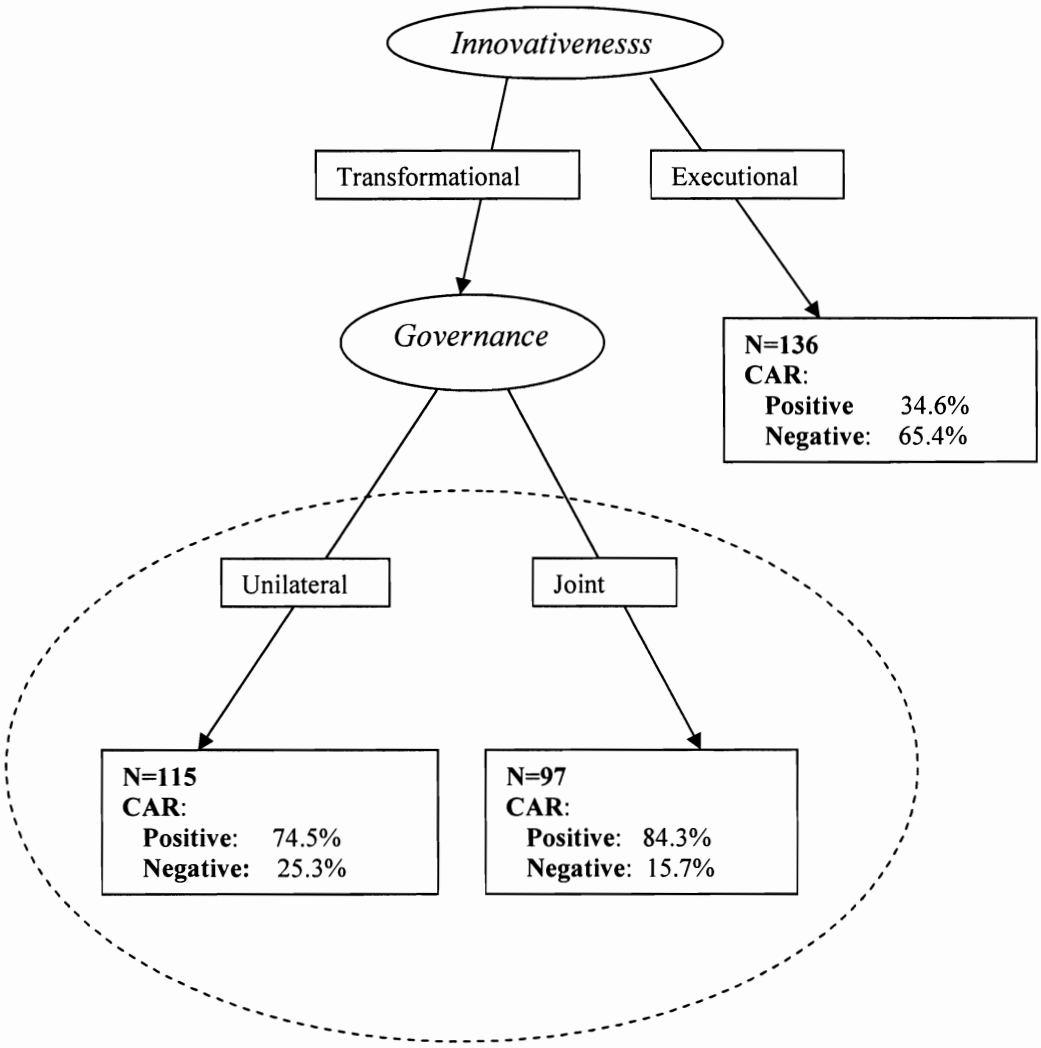

Figure 2: Set of Sibling Rules with *Governance* as the Subject Variable

In some cases there are other relevant embedded sibling rules that may be obtained by combining lower level 'sibling' nodes (see links & leaf nodes surrounded by dashed lines in Figure 2) that have the same value of the subject variable. Combining this pair of lower level sibling nodes (see Figure 3), a new pair of sibling rules is obtained in which the subject input variable is *Innovativeness*:

- IF *Innovativeness* is *Transformational* THEN *CAR* is *Positive* with probability 78.8% and N = 212;
- IF *Innovativeness* is *Executional* THEN *CAR* is *Positive* with probability 34.6% and N = 136.

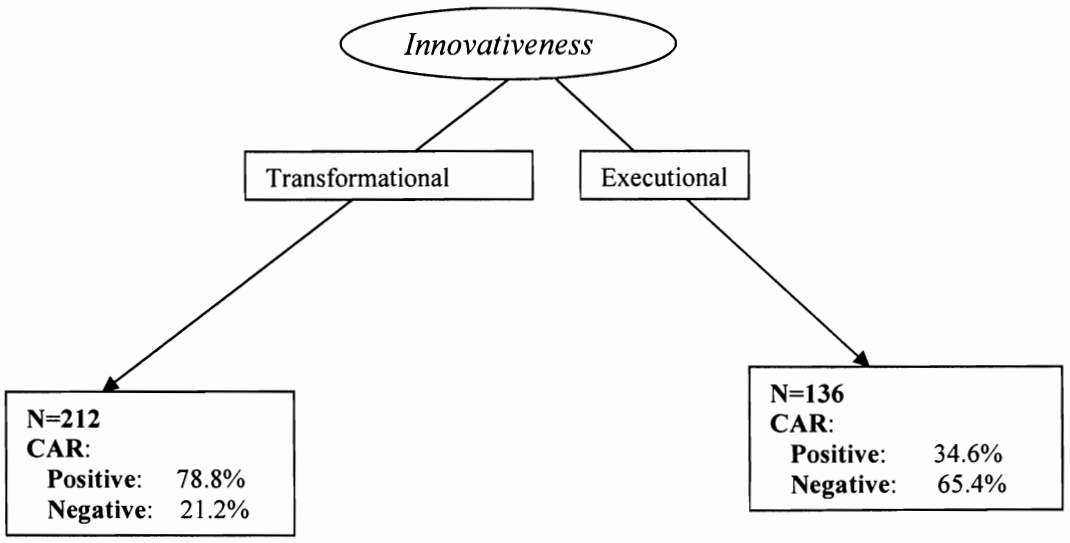

Figure 3: Set of Sibling Rules with *Innovativeness* as the Subject Variable

For the given target event (e.g. CAR is Abnormal), the posterior probabilities for each sibling node are compared. If for any pair of sibling nodes, the relevant posterior probabilities are very different, then this would suggest that the given variable is a predictor for the target event (Osei-Bryson and Ngwenyama 2004). In this manner a given set of sibling rules can be used to generate and test hypotheses that involve conjecturing that the given variable is a predictor of CAR. If the number of cases associated with a given set of sibling nodes is sufficiently large, then the hypothesis may be subjected to statistical hypothesis testing that is described in the next section.

3.6 Statistical Test for the Significance of Differences between Two Independent Proportions

We perform a proportion test to confirm that the difference in posterior probabilities (proportions or relative frequencies of the number of cases that are abnormal) for the sibling nodes of the subject variable are the same, and that the difference did not occur by chance. We test the difference of proportion at the 5% level. This is a t-test. The difference is between two population proportions (p_1-p_2) based on two independent samples of size n_1 and n_2 with sample proportions $\hat{p}_1$ and $\hat{p}_2$.

Our test statistic is given by

$$Z = \frac{\hat{p}_1 - \hat{p}_2}{\sqrt{\frac{\hat{p}_1(1-\hat{p}_2)}{n_1} + \frac{\hat{p}_2(1-\hat{p}_2)}{n_2}}}$$

The Z value for the *Innovativeness* variable depicted in Figures 2 and 3 is 8.926374 and corresponding probability of <0.001. Hence we can reject the null hypothesis that there is no difference in the proportion of cases that are abnormal for the *Executional* and *Transformational* ecommerce initiative and agree that there is significant difference in those proportions. We also use the result to suggest that the *Innovativeness* variable is statistically validated as a predictor of abnormal return for ecommerce initiative announcements. We discuss other sibling rules in the results section of the ecommerce initiatives.

CHAPTER 4
EFFECT OF INTERNET SECURITY BREACHES ON CUMULATIVE ABNORMAL RETURN

In this chapter, we first present the theoretical models that form the foundation for developing attack characteristics variables that impact CAR. Using those foundational theoretical models and the literature, we derive a set of hypotheses for Internet security breach and CAR. We subsequently test the hypotheses using traditional regression analysis and also using decision tree induction. We present the results from both the regression and decision tree induction techniques, and compare these results. Finally, we develop a set of propositions for the relationship between the independent variables and CAR, where CAR represents the damage that a breached firm suffers.

Recall that since Internet security breach is a negative event, we expect that the announcement of Internet security breach will lead to negative cumulative abnormal return. This means that the return as a result of the announcement of Internet security breach will be lower than expected. Hence the dependent variable that is of interest, as we develop the set of hypotheses, is negative CAR. We predict that the attack and firm characteristics would be related to negative CAR, where this negative CAR is the operationalization of damage to the breached firm.

4.1 Theoretical Background of Internet Security Breaches

Prior event study research on Internet security breach examined how the nature of the attack influences the observed CAR when Internet security breaches are announced in the public media. However, the factors considered as attack characteristics are atheoretic. In the following section, we discuss two models that provide means of presenting comprehensive theory-based attack characteristics.

4.1.1 Cause and Effect Model

Cohen and his research partners present an extensive list of sets of threats profiles, attack mechanisms, and consequences (effects)(Cohen 1997a; Cohen 1997b; Cohen et al. 1998). In particular, a model developed by the team of researchers '...assert that Causes (also called threats) use Mechanisms (previously published under the name Attacks and also called Attack Mechanisms) to produce Effects (also called consequences). Figure 4 depicts the threat profiles, attack mechanisms, protective mechanisms and consequences (effects) model.

The study identifies 37 various actors whose activities may pose threat or may cause failure to information systems, 94 mechanisms which cause failure to information systems, 140 mechanisms which can be used to reduce or limit the harm caused by attacks. Knowledge about these attacks and mechanisms can help mitigate the effects of attack mechanisms. Although this model can help organizations develop defense mechanisms to address specific threats, it is not appropriate for developing theoretical

models because the many-to-many relationships that the model presents makes it difficult to establish relationships between the categories of the actor, threat and mechanism entities, or potential independent variables.

However this model is important because it shows possible relationships between the various attackers, the attack mechanisms and the defense mechanisms. Another reason why this model is important is that it relates to Howard's taxonomy that we use in this paper to develop the hypotheses for the relationship between damage and attack characteristics. Cohen et al.'s work complements that of Howard (1997) who presents a more theoretical taxonomic framework for studying the threats, attack mechanisms and effect.

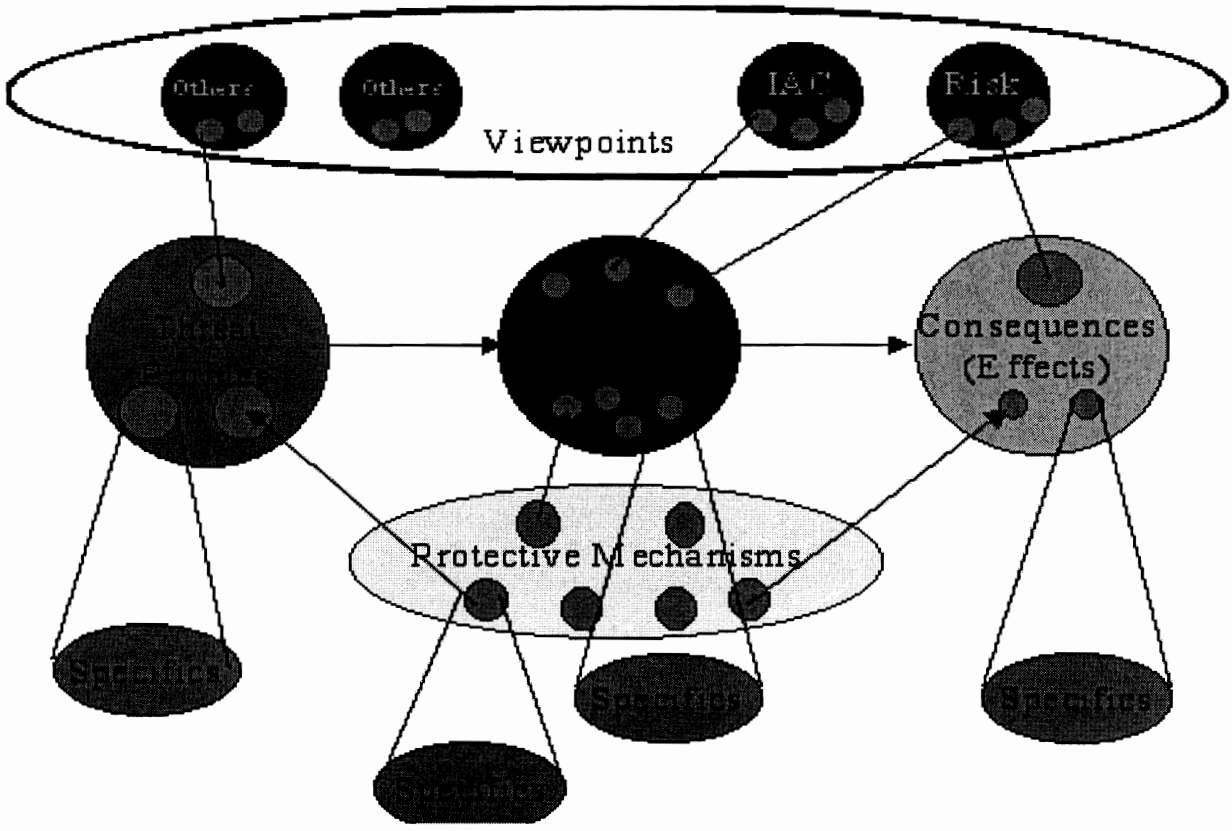

Figure 4: Cause and Effect Model (Cohen et al. 1998)

4.1.2 Internet Security Attack Characteristics Model

The Computer Emergency Response Team at the CERT® Coordination Center (CERT®/CC) of the Carnegie Mellon University has been involved with the tracking of Internet security incidents; it also provides recommendations to organizations to address Internet security breaches. In his PhD dissertation, Howard (1997) used the CERT®/CC database to study the characteristics of the attacks that occurred for the period 1989-1995. Howard's (1997) study and other reports that the CERT®/CC center provides annually suggest that the incident reports received at the center continues to grow. Howard (1997) suggests in his study that there are different types of *Attackers* each with different *Objective*. Each of these attackers takes advantage of the vulnerabilities in a firm's IT system to attack the firm's network or data in transition.

The study shows that a greater portion of security incidents were due to unauthorized use where individuals or a group of individuals, such as disgruntled employees, abuse their privilege by accessing corporate networks to perform illegal activities resulting in security breaches. Notwithstanding this, there are other categories of *Attackers* outside of the organization who attempt and often are successful in accessing corporate networks, data and information. This type of access is termed *Unauthorized Access*. Four main results of attacks were identified by the study. Howard indicates that the level of sophistication of the tools that are used to attack continues to grow. Howard's (1998) taxonomy is presented as Figure 5 below. "...Taxonomy is a classification system

where the classification scheme conforms to a systematic arrangement into groups or categories according to established criteria." (Undercoffer et al., 2003, p2).

Howard strengthens his taxonomy by demonstrating that it is "good" taxonomy and that it satisfies what the literature considers to be requisite properties of a sufficient and acceptable taxonomy for computer security (Amoroso 1994; Howard 1997; Lindquist and Jonsson 1997; Undercoffer et al. 2003). These properties are: mutually exclusive, unambiguous, repeatable, accepted, useful, comprehensible, conforming, objective, deterministic and specific.

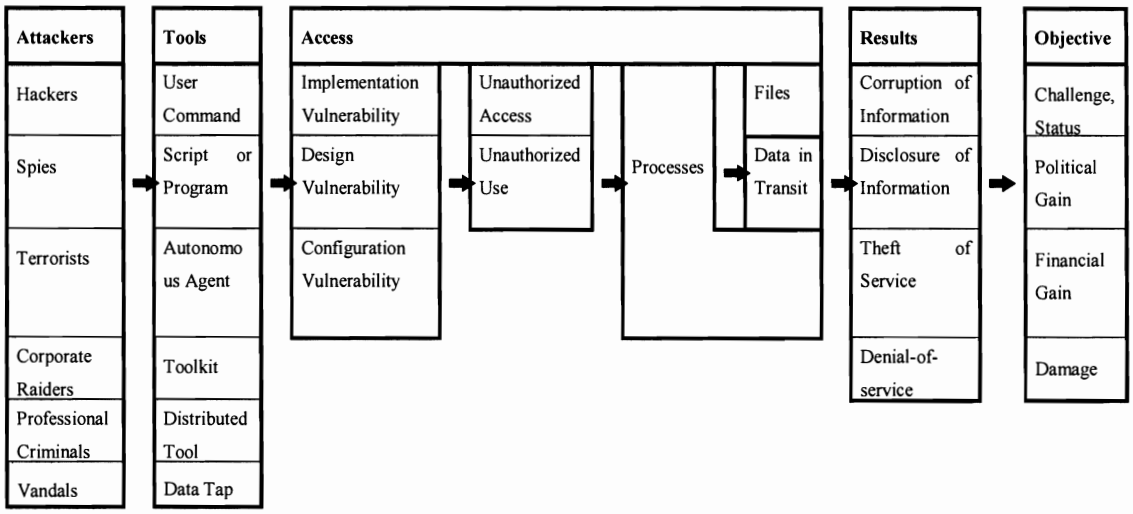

Figure 5: Computer and Network Attack Taxonomy – (Howard 1997)

We use Howard's taxonomy as a theoretical lens for investigating the determinants of abnormal return in Internet security breach. The five categories of the framework: *Attackers, Tools, Access, Results and Objective* serve as five variables that can be used to represent the nature of the attack. Using this taxonomy enables us to

present a more theory-based analysis of the determinants of abnormal returns, and also to provide a more comprehensive and solid understanding of Internet security breach and damage, operationalized as the CAR observed when Internet security breach is announced in the public media.

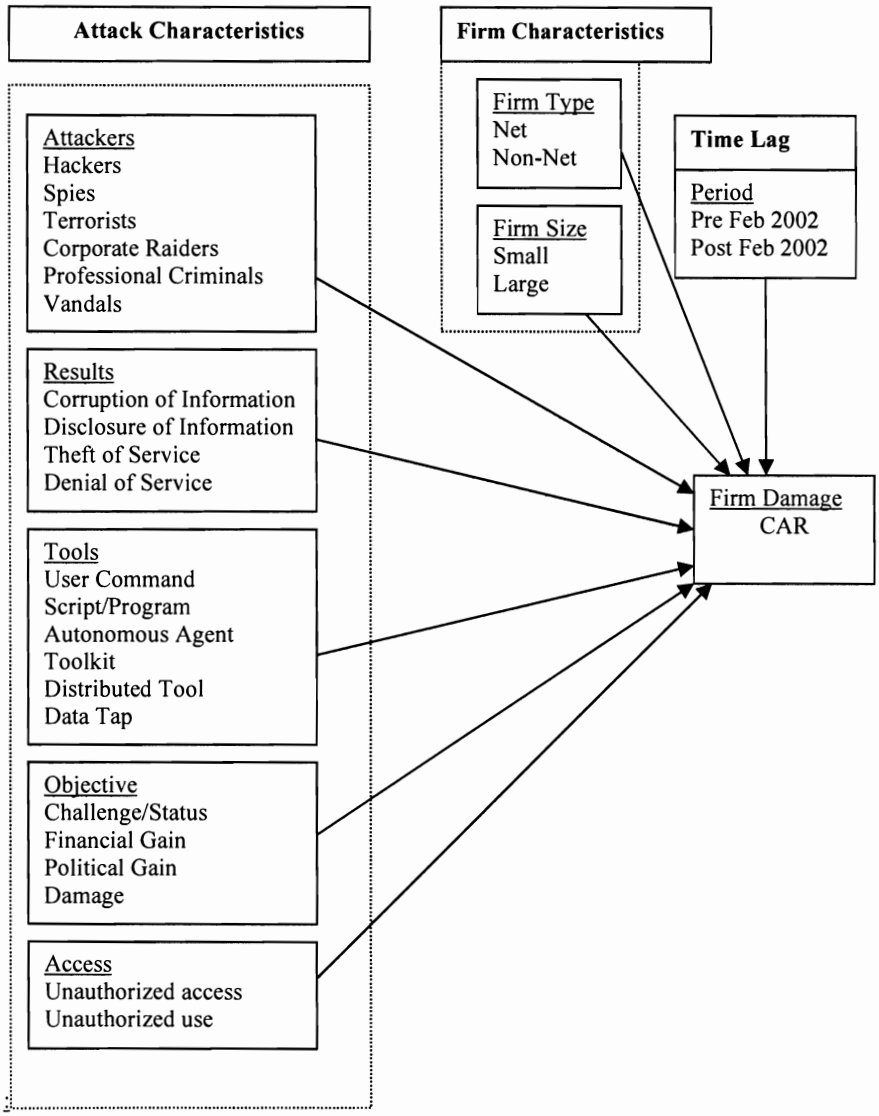

Figure 6: Framework for Firm Damage, Attack Characteristics, Firm Characteristics and Time lag

Figure 6 represents the list of variables and categories for the attack characteristics, firm characteristics and time lag variables. These variables are expected to influence the damage to the breached firm when Internet security breach announcements are made in the public media. We use these sets of variables to derive the hypotheses for Internet security breach announcements. We propose that these variables are determinants of negative CAR (firm damage).

4.2 Hypotheses for Internet Security Breach

Recall that for Internet security breach, we use firm specific factors (*Firm Type, Firm Size*), attack characteristics or the nature of the attack (*Attacker, Objective, Results, Tools, and Access*), and time lag (*Period*), as predictor variables, and CAR as the dependent variable for developing the set of hypotheses which are subsequently tested.

4.2.1 Impact of Internet Security Breaches on Market Returns

Internet security breach brings anxiety to businesses, governments, and the public. The havoc that Internet security breach can cause is enormous. Generally, investors lose confidence in a firm when it is involved with any security breach. Thus, Internet security breach is bad news to investors and our expectation is that investors will react negatively to any announcement of Internet security breach that affects a firm. We therefore state the first hypothesis as:

Hypothesis 1: The abnormal return attributed to the announcements of Internet security breach is negative.

Firm Type

Previous related studies and the information systems security literature suggest that firms that depend heavily on the Internet (referred to as "*Net*" firms, such as Amazon.com and eBay) are found to have greater interest in Internet security issues than do other firms (Cavusoglu et al., 2002). The *Net* firms (also known as pure-plays) rely solely on the Internet to perform market transactions, unlike conventional (click and mortar) firms that combine the Internet and existing brick and mortar operations, to conduct their business. In the case of *Net* firms, an incident that shuts down the network could result in no sales, whilst a conventional firm that suffers the same incident may generate sales from traditional markets. We extend this argument to hypothesize that *Net* firms will respond to Internet security incidents differently than *Non-Net* firms. We state this hypothesis as follows:

Hypothesis 2: All else being equal, the abnormal return attributed to the announcements of Internet security breach is more negative for Net firms than Non-Net firms.

Firm Size

Research shows that the influence of public announcement of accounting information is different for *Large* and *Small* firms (Cavusoglu et al. 2004a; Hayes et al. 2000; Im et al. 2001). When security breach announcement is made, abnormal return is

observed since investors process this new information which they were not aware before the announcement. *Large* firms may communicate security breaches internally such that the stock price would have reflected the news even before the public announcement is made. *Small* firms, on the other hand, may take time or may not communicate the security breach before the event date rendering the public announcement important information that needs to be incorporated into the valuation of the firm. Hence, we would expect that the abnormal (negative) return due to the announcements of Internet security breach in the public media would be larger for *Small* firms than for *Large* firms. This leads to the hypothesis that:

Hypothesis 3: All else being equal, the abnormal return attributed to the announcements of Internet security breach is more negative for Small firms than Large firms.

Time Lag

In February 2000, several major firms such as Yahoo, E-Bay, Amazon, and E-trade had their web sites shut down by a denial-of-service attack. This event according to Cavusoglu et al. (2002) could distinguish the "fallow" time where investors were more forgiving than later times where investors react to security breaches. On the one hand, firms whose sites are compromised and have responsibilities for the security breaches have taken major steps to prevent security incidents. On the other hand, investors would expect that, with time, firms would be better prepared to address security problems and thereby less forgiving than they have been in the past. From this discussion we hypothesize that:

Hypothesis 4: All else being equal, the abnormal return attributed to the announcements of Internet security breach is more negative for Post February 2000 announcements than Pre February 2000 announcements.

4.2.2 Attack Characteristics (The Nature of the attack)

The nature of the attack will impact the abnormal return because investors try to make sense of the information that they read concerning Internet security breaches. Here we develop the hypotheses for the characteristics of the attack. It is suggested that *Attackers*' perception of the risk of being caught influences their motivation to attack (Cohen et al. 1998; Gupta et al. 2000). Thus an *Attacker* group that believes that it is unlikely to be caught, and therefore has high tendency to attack, poses more threat. This suggests that investors' reaction to attack would be influenced by their perception on the likelihood that the firm would suffer such attacks again therefore using that information to value the firm's potential financial damage due to the attack and threats that the *Attacker* poses.

Gupta et al. (2000) suggest that groups of *Attackers* may have access to substantial financial resources leading to high capability to cause serious damage. For instance, business competitors (*Corporate Raiders*) may have financial support from their sponsors. We therefore assert that there is relationship between *Attacker Type* and firm damage (which can be operationalized as the negative cumulative abnormal return).

Attacker Type

In this paper, we define *Attacker* to mean an individual or group of individuals responsible for the Internet security incident. Howard (1997) identifies six categories of *Attackers*. In a particular announcement, the *Attacker* left a note telling the attacked firm about how vulnerable its systems were. Howard (1997) refers to this group of *Attackers* as *Hackers*. What motivates *Hackers* to attack is the desire to show their prowess and to raise their status in the community in which they operate. Truly, other kinds of *Attackers* could use the vulnerabilities resulting from hackers' activities to launch other attacks with more disastrous outcomes (Cohen et al. 1998). However, if a firm responds quickly to the *Hacker's* activities, those vulnerabilities could be eliminated, preventing further attacks.

Vandals aim at causing harm to the systems of the attacked firms, while *Professional Criminals* seek financial benefits from their activities. Gupta et al. (2000) indicate that each of these *Attacker Types* has different capabilities for using the specific tools to achieve its specific strategies and *Objectives*. It is believed that investors can distinguish between the different *Attackers* based on their capabilities to cause harm to a firm's resources. Thus the *Attacker Type* will influence the abnormal return. We therefore state the hypothesis for the *Attacker Type* as:

Hypothesis 5 (i): All else being equal, the abnormal return attributed to the announcements of Internet security breach is influenced by the Attacker Type.

Attacker's Objective

Corporate Raiders and *Professional Criminals* seek *Financial Gain* from their activities. *Corporate Raiders* are employees of an organization who break into the computer and network systems of competitors to seek information of strategic competitive importance. *Professional Criminals,* however, are individuals who operate on their own. *Vandals* break into computer systems mainly to cause damage. Gupta et al. (2000) show that different group of *Attackers* have different motivation to attack. According to these researchers, *Attackers*' motivation is influenced by the individual and collective psychology as well as the political and ideological background.

Attackers that perceive that they are likely to be caught may have far less impact on the firm damage than those that have confidence in their ability to act without being found out. Investors from past experience may notice which *Attacker Types* are likely to repeat the attack knowing that their activity are likely to continue as they are "protected" from being caught. Individual's response and behavior towards risks are influenced by what they have observed in the past (Bener 2000). Thus if investors know that in the past different *Attackers* have different impact on the firm then they would interpret the announcements on attacks by various *Attackers* differently.

Clearly, an attack geared towards *Financial Gain*, and another where the *Attacker* challenges the firm's claim that its system is secured will be interpreted differently by investors, and that the *Objective* of the *Attacker* will therefore have impact on abnormal return. In fact Gupta et al (2000) suggest that the *Attacker*'s capabilities and motivations determine the level of vulnerability that an *Attacker Type* poses. Certainly investors

would consider an *Attacker Type* that poses a higher threat to have more negative impact on the firm's future financial position than one with lower threats. We state the hypothesis for *Attacker*'s *Objective* as:

Hypothesis 5(ii): All else being equal, the abnormal return attributed to the announcements of Internet security breach is influenced by the Attacker's Objective.

Attack Results

Howard (1997) identifies four different results of attack: Corruption of *Information, Denial of Service, Theft of Service*, and *Disclosure of Information*. All the studies that have characterized Internet security attacks by variables such as the *Attacker Type*, attack mechanisms and *Results* have shown that the impact of the diverse attacks are different (Cohen 1997a; Cohen 1997b; Cohen et al. 1998; Howard 1997; Liu et al. 2005). Since each of these *Results* could have a different impact on the breached firms, investors will also react differently. Thus we develop the following hypothesis:

Hypothesis 5 (iii): All else being equal, the abnormal return attributed to the announcements of Internet security breach is influenced by the Results of the attack.

Attack Tools

Howard (1997) claims that the level of sophistication of the *Tools* used to attack, continues to increase. The kinds of destruction and the level of access that the *Attacker* can gain increase with the increased sophistication of tools employed. Thus, the *Tools* employed in the attack could impact the abnormal return. We develop the hypothesis:

Hypothesis 5 (iv): All else being equal, the abnormal return attributed to the announcements of Internet security breach is influenced by the Tools used to attack.

Access Type

Attacks can be internal or external. Internal attacks include disgruntled employees taking advantage of the access privilege to corporate networks to perform unauthorized activities. Outsiders usually take advantage of vulnerabilities to gain *Unauthorized Access* to corporate networks. There are differing opinions (Howard 1997) as to which type of *Access* is mostly used by *Attackers*. In spite of the different views, investors' reactions could depend on which *Access Type* was employed by the *Attacker*. On the one hand, investors may consider *Unauthorized Use* as an error and *Unauthorized Access* as an organization's failure to prevent intruders from getting access to "secured" data or network systems. On the other hand, investors could consider *Unauthorized Use* as betrayal by organization's employees and react more negatively to an attack using this kind of *Access*. In an asymmetric information environment, investors will be more concerned with one type of *Access* to another. This leads to the final hypothesis for security breach announcements:

Hypothesis 5 (v): All else being equal, the abnormal return attributed to the announcements of Internet security breach is influenced by the Access used to attack.

4.3 Data Description

In this section, we describe the data set for Internet security breach announcements. We describe the source of data, data cleaning and coding of the data for regression analysis as well for the DT induction.

4.3.1 Data Collection

We define an event as an announcement about a firm's Internet security breach in one of the major newspapers. Using Lexis-Nexis Academic online feature, we include in our sample all announcements in the Wall Street Journal, New York Times, Financial Times, Washington Post, and USA Today for the period 1997 through 2003. The list of keywords used for searching events include: virus names (e.g., love bug, soBig, and blaster worm); *Attacker Type* (e.g., hacker, vandal); *Results* of the attack (e.g., *Denial of Service, Theft of Service*), names of organizations reported in previous studies (e.g., Yahoo, eBay), or a term or combination of such terms (e.g., information security breach, computer system security, Internet security incident, and breach).

Initially, our search generated over 10,000 potential events. All events involving governmental, state, local and non-profit organizations were not considered. Only events involving publicly traded firms were considered in this study. We recorded 110 events. However, we eliminated some events using the following criteria: (1) some of the events were reported more than once in a single or in different newspapers. In such cases, we kept only the first announcement; (2) only firms that were listed on New York Stock Exchange (NYSE), NASDAQ, or American Stock Exchange (AMEX) and had return

data in the CRSP[10] database were included for analysis; (3) for firms in the CRSP database, the returns data had to be available for 120 days before the event for the computation of stock market return; and (4) where there were confounding effects such as earning announcements, dividends or any major announcement in the event window involving the breached firm that could impact return, the event was dropped. Table 3 shows the impact of the criteria listed on the event size. 41 events remained after event eliminations.

Table 3: Selection Criteria for the Internet Security Breach Events

Criterion	Reduction in Event size	Remaining Event size
Initial Number of Events	0	110
Repeated Announcement	37	73
CRSP data availability	29	44
Sufficient data for estimating returns (120 day estimation window)	1	43
Confounding event – e.g. earning announcement	2	41

[10] CRSP is a financial research center at University of Chicago. It generates and maintains leading historical US databases for stock (NASDAQ, AMEX, and NYSE), indices, bond, and mutual fund securities used by leaders in the academic and corporate communities for financial, economic, and accounting research.

4.3.2 Events and Estimation Period

A three-day event period covering the day before the event through the day after the event was used in this study. One of the previous studies used the same event window (Cavusoglu et al. 2004a). The rationale behind this length of period is that investors may have a "pre-announcement" hint ("leakage") about the security breach and may react before the market closes a day before the announcement. Similarly, breach announcement might have been made after 4PM on day *t*, which means that the entire reaction will occur on day *t+1*. We used 120 days before the event to estimate the expected stock market return. This is consistent with prior studies.

4.3.3 Coding

Time

We use February 2000 as the "cutoff date". This is the time when major firms were hit by the *Denial of Service* attack and most firms experienced security breach for the first time. This date is often referred to in the literature (Campbell et al. 2003; Cavusoglu et al. 2004a; Ettredge and Richardson 2001). In agreement with Cavusoglu, we believe that this period would be recognized as time that businesses and investors became more aware of security breaches. For the *Time*[11] dummy variable, *Pre February 2000* events were coded 0 and *Post Feb 2000* coded 1.

[11] *Time* and *Period* are used interchangeably in this paper.

Firm Type

The *Firm Type* dummy variable was coded as 1 for *Net* firms and 0 for *Non-Net* firms. This scheme is also consistent with that used in Cavusoglu et al.'s work. We used Internet Stock listing™ and Morgan Stanley Dean Witter's Internet Company list to identify "*Net*" and "*Non-Net*" firms (e.g., Cavusoglu et al. 2004b; Im et al. 2001).

Firm Size

The market value of the firm ten days before the event date was used for *Firm Size*. Specifically, we computed the market value as that day's stock price multiplied by the number of shares outstanding. For *Firm Size* dummy variable, firms with values greater or equal to the median value of the sample were classified as large, and those lower than the median value as *Small*. The *Firm Size* dummy variable was coded as 1 for *Large* firms and 0 for *Small* firms.

Attack Characteristics

In the hypotheses that we develop, we seek to find the magnitude of the effect of each of the categories on the abnormal (negative) return using regression. For each of the independent variables: *Attacker, Objective, Results, Tools, and Access,* we created dummy variables to test the effect of the specific category within the variable on the cumulative abnormal return.

Hypothesis 5 (i) *Attacker*: For the *Attacker* we created five dummy variables for the six categories in performing regression analysis. Here A1=1 if *Hackers* and 0 otherwise. A2 =1 if *Professional Criminals* and 0 otherwise. A3= 1 if *Vandals* and 0 otherwise. A4 = 1 if *Corporate Raiders* and 0 otherwise. A5 = *Terrorists* and 0 otherwise.

Hypothesis 5 (ii) *Objective*: Here we created three dummy variables. O1 = 1 if *Challenge* or *Status* and 0 otherwise. O2 = 1 if *Political Gain* and 0 otherwise. O3 = 1 if *Financial Gain* and 0 otherwise.

Hypothesis 5 (iii) *Results*: Here three dummy variables were developed. R1=1 if C*orruption of Information* and 0 otherwise. R2 = 1 if *Disclosure of Information* and 0 otherwise. R3 = 1 if *Denial of Service* and 0 otherwise.

Hypothesis 5 (iv) *Tools*: We developed 5 dummy variables. T1 =1 if *User Command* and 0 otherwise. T2 =1 if *Script* or *Program* and 0 otherwise. T3 = 1 if *Autonomous Agent* and 0 otherwise. T4 = 1 if *Toolkit* and 0 otherwise. T5 = 1 if *Distributed Tool* and 0 otherwise.

Hypothesis 5 (v) *Access*: With the *Access* dummy variable, *Unauthorized Use* was coded 1 and *Unauthorized Access* coded as 0.

4.3.4 Identification of Potential Predictor Variables

For the data mining analysis, we included all the variables used in the regression analysis. The potential predictor variables are: *Firm Size, Firm Type, Period, Attacker, Objective, Tools, Results,* and *Access.* The "Other" category depicts the situation where there was not enough information to determine the specific category. Interestingly, for the *Attacker* and *Objective* variables, only one event each had the "Other" category. The *Results* and *Access* variables had no event reporting "Other". The *Tools* variable had the highest number of events (ten) reporting the "Other" category. Appendix 5 includes the list of terms and definitions used in Howard's study. These terms informed the classification of the Internet Security breach attacks into the five variables listed above. The CAR values from the Eventus ® software analysis was used as the target variable or the dependent variable for the DT induction. It is also the dependent variable for the regression analysis.

4.4 Results & Discussions

In this section, we present and discuss the results for the Internet security breach sample. First, we present the results and discussion of the cumulative abnormal return attributed to the announcement of Internet security breach. We also discuss the results of the DT induction providing justification of some of the findings using existing literature. We also compare the results of the DT induction and regression and provide discussion about the findings. Finally, we make theoretical propositions on Internet security breach

that can serve as a theoretical foundation for further research in Internet security breach and damage.

4.4.1 Cumulative Abnormal Return

We present the results of the Eventus® analysis for the sample of events from the Internet security breach announcements. As we discussed in Chapter 3, we used the generalized sign test (see Panel A of Table 4) to test the significance of the results. However, to enhance the validity of our findings, we also use the time series standard deviation method (see Panel B of Table 4) to assess the significance of the results.

Table 4: Cumulative Abnormal Returns for Internet Security Breach Sample

Panel A: Generalized Sign Test Results

Days	Cumulative Average Abnormal Return		Median Cumulative Abnormal Return	Z	Positive: Negative	Generalized Sign Z
	Equally Weighted	Precision Weighted				
(-1, +1)	-3.18%	-1.75%	-1.45%	-1.94*	14:27	-1.72<

Panel B: Results for the Time Series Standard deviation method

Days	Average Abnormal Return	Cumulative Abnormal Return	Z	Positive: Negative	Generalized Sign Z
(-1, +1)	-3.18%	-1.45%	-2.48**	14:27	-1.72<

$, (,) significant at .10 *, <, > significant at .05

****, <<, >> significant at .01 ***, <<<, >>> significant at .001**

Since Internet security breach is a "negative event", the test statistic is significant if the ratio of positive CAR cases (abnormal) to negative CAR (normal) cases is low. As can be seen the ratio is 14:27 for both Panels A and B of Table 4. If the ratio is 1, we would fail to reject the null hypothesis and accept that Internet security announcements in the public media have no effect on CAR or firm damage.

Similarly, the generalized sign test (one–tail test) shows that the results are significant at the 5% level. There is no difference in the results given by the cross-sectional method, and hence are not reported here. In addition, there is no significant difference in the results given by the time series standard deviation method shown in Panel B of Table 4. Each of these tests shows that there is significant evidence that the abnormal (negative) return resulting from the announcements of Internet security breach did not occur by chance. Thus hypothesis 1 is confirmed by our data. Within a three day window of security breach announcement, firms on an average lost 3.18% of their market value.

4.4.2 DT Induction Results

In Chapter 3, we discussed how a potential predictor variable can perform two possible roles: (1) a discriminating predictor, and (2) a predictor in strong rule. In this section, we present the results and discussion of each variable as a discriminating predictor and also as a potential predictor in strong rules in which the variable participates. It is possible that for some of the input variables, one or more of these rules

may not apply. Using Osei-Bryson and Ngwenyama's (Osei-Bryson and Ngwenyama 2004) sibling rules computation method, we present in Appendix 2 several of these rules that are used in the Tables 5-10. Appendix 3 provides other relevant rules. Since the sample size for the Internet security breach was small, we did not perform the difference in proportion test for the discriminating predictor variable. We however compute this statistic for the ecommerce data set.

Firm Type

Table 5: Sets of Rules that include *Firm Type* as a Discriminating Predictor

Source	Rules	Comments

DT_EGa	IF **Firm Type** = 'NET' & **Results** ∈ {'THEFT OF SERVICE', 'CORRUPTION OF INFORMATION'} & **Attacker** ∈ {'CORPORATE RAIDERS', 'VANDALS'} THEN
	N = 3
	CAR: {POSITIVE: 0.0%; NEGATIVE: 100.0%}
	
	IF **Firm Type** = 'NON-NET' & **Results** ∈ {'THEFT OF SERVICE', 'CORRUPTION OF INFORMATION'} & **Attacker** ∈ {'CORPORATE RAIDERS', 'VANDALS'} THEN
	N = 9
	CAR: {POSITIVE: 44.4%; NEGATIVE: 55.6%}
		This pair of rules together suggests that when an attack by *Corporate Raiders* or *Vandals* results in *Theft of Service* or *Corruption of Information,* the likelihood that such attack will lead to negative CAR is higher for *Net firms* (100%) than for *Non-Net firms* (55.6%).

DT_Gc	IF **Firm Type** = 'NON-NET'& **Access** = 'UNAUTHORIZED USE' THEN
	N = 6
	CAR: {POSITIVE: 83.3%; NEGATIVE: 16.7%}
	
	IF **Firm Type** = 'NET' & **Access** = 'UNAUTHORIZED USE' THEN
		This pair of rules together suggests that when an attack is perpetrated by an

	N = 3 **CAR:** {POSITIVE: 33.3%; NEGATIVE: 66.7%}	Insider (i.e. *Unauthorized Use*) the likelihood of attack leading to negative CAR for *Net firms* is substantially higher than for *Non-Net firms* (i.e., 66.7% vs 16.7%).
	IF **Firm Type** = 'NET' & **Period** = 'PRE FEB 2000' & **Access** = 'UNAUTHORIZED ACC' THEN N = 5 **CAR:** {POSITIVE: 40.0%; NEGATIVE: 60.0%} IF **Firm Type** = 'NON-NET' & **Period** = 'PRE FEB 2000' & **Access** = 'UNAUTHORIZE ACC' THEN N = 3 **CAR:** {POSITIVE: 66.7%; NEGATIVE: 33.3%}	This pair of rules together suggests that *Net firms* have higher risk (60%) of observing Negative CAR than do *Non-Net firms* (33.3%) when an attack by an outsider (*Unauthorized Access*) occurred in *Pre February* 2000.

Based on Table 5, we state that the relationship between damage, operationalized by negative CAR, and the *Firm Type* is conditioned on other independent variables. Three different sets of conditions are identified. First, the conditional variables are *Results* and *Attacker*. Second, the variable is *Attacker* and finally the conditional variables are *Access* and *Period*. Irrespective of the conditional variables, *Net firms* are always more likely to suffer damage from security breach than *Non-Net firms*.

Table 6: Strong Individual Rules that include *Firm Type* as a Predictor

Source	Rules
DT_EGa	IF **Firm Type** = 'NET' & **Results** ∈ {'THEFT OF SERVICE', 'CORRUPTION OF INFORMATION'} & **Attacker** ∈ {'CORPORATE RAIDERS', 'VANDALS'} THEN N = 3 **CAR:** {POSITIVE: 0.0%; NEGATIVE: 100.0%}

The strong individual rule presented in Table 6 that includes *Firm Type* shows that it is highly likely that *Net firms* will suffer damage when attack by *Corporate Raiders* or *Vandals* results in *Theft of Service* or *Corruption of Information.* This rule also corroborates the sets of rules that include *Firm Type* as a discriminating predictor variable presented in Table 5 where we observe that *Net firms* are more likely to suffer damage than *Non-Net firms*. Thus both the discriminating predictor rules and the strong individual rules suggest that *Firm Type* is a predictor variable of damage to the firm when Internet security breach is announced in the public media.

Tables 5 and 6 reveal that the *Firm Type* variable interacts with four other independent variables: *Attacker, Access, Period,* and *Results*. Other independent variables: *Firm Size, Objective,* and *Tools* have no interactions with the *Firm Type* variable. We have shown that *Net* firms are more damaging than *Non-Net* firms and so we can develop and test hypothesis for *Firm Type* and CAR or damage.

Firm Size

Table 7: Sets of Rules that include *Firm Size* as a Discriminating Predictor

Source	Rules	Comments

DT_EGa	IF **Firm Size** = 'SMALL' & **Attacker** = 'HACKERS' THEN
	N = 3
	CAR: {POSITIVE: 33.3%; NEGATIVE: 66.7%}
	
	IF **Firm Size** = 'LARGE' & **Attacker** = 'HACKERS' THEN
	N = 6
	CAR: {POSITIVE: 0.0%; NEGATIVE: 100.0%}
		This pair of rules suggests that when the *Attacker* is a *Hacker*, negative CAR is more likely to occur if the *Firm Size* is *Large* than if it is *Small* (100% vs 66.7%).

DT_Eb	IF **Firm Size** = 'SMALL' & **Objective** = 'CHALLENGE/STATUS' THEN
	N = 3
	CAR: {POSITIVE: 33.3%; NEGATIVE: 66.7%}
	
	IF **Firm Size** = 'LARGE' & **Objective** = 'CHALLENGE/STATUS' THEN
	N = 7
	CAR: {POSITIVE: 0.0%; NEGATIVE: 100.0%}
		This pair of rules suggests that when the *Objective* is *Challenge/Status*, negative CAR is more likely to occur if the *Firm Size* is *Large* than if it is *Small* (100% vs 67%).

	IF **Firm Size** = 'SMALL' & **Objective** = 'DAMAGE' THEN
	N = 5
	CAR: {POSITIVE: 20.0%; NEGATIVE: 80.0%}
	
	IF **Firm Size** = 'LARGE' & **Objective** = 'DAMAGE' THEN
	N = 6
	CAR: {POSITIVE: 33.3%; NEGATIVE: 66.7%}
		This pair of rules suggests that when the *Objective* is *Damage*, negative CAR is more likely to occur if the *Firm Size* is *Small* than if it is *Large* (80% vs 67%).

DT_Gc	IF **Firm Size** = 'SMALL' & **Objective** ∈ {'DAMAGE', 'POLITICAL GAIN'} & **Period** = 'POST FEB 2000' & **Access** = 'UNAUTHORIZED ACC' THEN
	N = 5
	CAR: {POSITIVE: 20.0%; NEGATIVE: 80.0%}
	
	IF **Firm Size** = 'LARGE' & **Objective** ∈ { 'DAMAGE', 'POLITICAL GAIN'} & **Period** = 'POST FEB 2000' & **Access** = 'UNAUTHORIZED ACC' THEN
	N = 7
	CAR: {POSITIVE: 42.9%; NEGATIVE: 57.1%}
		This pair of rules suggests that for more recent events (attack occurring *Post February 2000*) through *Unauthorized Access* by an outsider where the *Attacker*'s *Objective* is *Damage* or *Political Gain*, negative CAR is more likely to occur if the *Firm Size* is *Small* than if it is *Large* (80% vs 57%).

Table 7 presents several sets of rules where *Firm Size* performs discriminating predictor role. The table shows that for an attack by a *Hacker* or an attack motivated by *Status* or *Challenge*, *Large* firms are more likely to suffer damage than *Small* firms. However, when the *Attacker's Objective* is to cause damage or where the conditional variables are *Period* and *Access*, *Small* firms are more likely to suffer damage than *Large* firms.

Table 8: Strong Individual Rules that include *Firm Size* as a Predictor

Source	Rules
DT_EGa	IF **Firm Size** = 'LARGE' & **Attacker** = 'HACKERS' THEN N = 6 **CAR:** {POSITIVE: 0.0%; NEGATIVE: 100.0%}

DT_Eb	IF **Firm Size** = 'LARGE' & **Objective** = 'CHALLENGE/STATUS' THEN
	N = 7
	CAR: {POSITIVE: 0.0%; NEGATIVE: 100.0%}
	
	IF **Firm Size** = 'SMALL' & **Objective** = 'DAMAGE' THEN
	N = 5
	CAR: {POSITIVE: 20.0%; NEGATIVE: 80.0%}

DT_Gc	IF **Firm Size** = 'SMALL' & **Objective** ∈ { 'DAMAGE', 'POLITICAL GAIN'} & **Period** = 'POST FEB 2000' & **Access** = 'UNAUTHORIZED ACC' THEN N = 5 **CAR:** {POSITIVE: 20.0%; NEGATIVE: 80.0%}

In Table 8, where *Firm Size* performs a strong rule role, further suggests concerning the *Firm Size* variable that, it is highly likely that attacks involving *Large* firms and *Hackers,* or attack on *Large* firms motivated by *Challenge* or *Status* would cause damage. *Small* firms are more likely to suffer damage when the *Objective* is to cause *damage* or *Political Gain,* and the attack occurred *Post February 2000* by *Unauthorized Access*. The strong rule and discriminating rules together suggest that *Firm Size* is a predictor of damage. However, the likelihood that Large or *Small* is more likely to suffer damage depends on the conditional variables. We cannot say whether attack on *Large* or *Small* firm is more damaging. We note that *Attacker, Objective, Period*, and *Access interact* with the *Firm Size* variable but *Firm Type, Results* and *Tools* do not.

Time

Table 9: Sets of Rules that include *Period (Time) as* a Discriminating Predictor

Source	Rules	Comments
DT_C	IF **Access** = 'UNAUTHORIZED ACC & **Period** = 'PRE FEB 2000' THEN N : 8 **CAR:** {POSITIVE: 50.0%; NEGATIVE: 50.0%} IF **Period** = 'POST FEB 2000' & **Access** = 'UNAUTHORIZED ACC' THEN N : 24 **CAR:** {POSITIVE: 16.7%; NEGATIVE: 83.3%}	This pair of rules suggests that for attacks involving *Unauthorized Access*, those that occurred *Pre February 2000* are less likely to lead to negative CAR than those that occurred *Post February 2000* (50% vs 83%).
DT_Eb	IF **Period** = 'PRE FEB 2000' & **Tools** = 'OTHER' & **Objective** ∈ {'FINANCIAL GAIN', 'OTHER', 'POLITICAL GAIN'} THEN N = 4 **CAR:** {POSITIVE: 25.0%; NEGATIVE: 75.0%} IF **Period** = 'POST FEB 2000' & **Tools** = 'OTHER' & **Objective** ∈ {'FINANCIAL GAIN', 'OTHER', 'POLITICAL GAIN'} THEN N = 5 **CAR:** {POSITIVE: 60.0%; NEGATIVE: 40.0%}	This pair of rules suggests that if the *Tools* used to attack is *Unknown* and the *Objective* of the *Attacker* is *Financial Gain, Political Gain* or *Unknown*, *Pre February* 2000 attack has a higher likelihood of negative CAR than *Post February 2000* attacks (75% vs 40%).

Table 9 suggests that prior to the widespread knowledge about Internet security breach in February 2000, investors did not link announcement on Internet security breach to market value (*Pre February 2000*) when the breach was perpetrated by *Unauthorized users*, i.e. the outsider, much as they do *Post February 2000* when many individuals and firms became more aware of security breach. However, it is observed that when *Tool* is unknown and the *Objective* is *Political Gain, Financial Gain* or *Unknown* then *Pre February 2000* announcements are more likely to lead to damage than *Post February 2000* announcements.

We note therefore that the effect of time on CAR is depended on *Objective* of the *Attacker* and *Tools* used to attack. Firms need to be aware of the importance of *Time* in determining damage of Internet security attacks. However, we cannot only look at time in isolation. We need to look at the conditional relations between the independent variables as well. As the general public becomes more aware of the information technology issues, they are better informed in interpreting the implications of Internet security and the impact Internet security breach have on market value of breached firms.

Table 10: Strong Individual Rules that include *Time (Period)* as a Predictor

Source	Rules
DT_C	IF **Period** = 'POST FEB 2000' & **Access** = 'UNAUTHORIZED ACC' THEN N : 24 **CAR:** {POSITIVE: 16.7%; NEGATIVE: 83.3%}
DT_Gc	IF **Objective** ∈ { 'CHALLENGE/STATUS', 'FINANCIAL GAIN'} & **Period** = 'POST FEB 2000' & **Access** = 'UNAUTHORIZED ACC' THEN N = 12 **CAR:** {POSITIVE: 0.0%; NEGATIVE: 100.0%} IF **Firm Size** = 'SMALL' & **Objective** ∈ { 'DAMAGE', 'POLITICAL GAIN'} & **Period** = 'POST FEB 2000' & **Access** = 'UNAUTHORIZED ACC' THEN N = 5 **CAR:** {POSITIVE: 20.0%; NEGATIVE: 80.0%}

From Table 10, we see that in recent times (Post February 2000), an attack with *Objective* of *Challenge/Status* or *Financial Gain* through *Unauthorized Access* is highly likely to cause damage. Our data does not tell us whether *Pre February 2000* is more damaging than *Post February 2000*. We note that *Period* interacts with *Access, Objective and Tools* but not *Attacker, Firm Type, Firm Size,* and *Results.*

Attacker

Table 11: Sets of Rules that include *Attacker Type* as a Discriminating Predictor

Source	Set of Rules	Comments
DT_EG	IF **Attacker** ∈ {'OTHERS', 'PROFESSIONAL CRIMINALS', 'TERRORISTS'} THEN N = 16 **CAR:** {POSITIVE: 56.2%; NEGATIVE: 43.8%} IF **Attacker** = 'HACKERS' THEN N = 9 **CAR:** {POSITIVE: 11.1%; NEGATIVE: 88.9%} IF **Attacker** ∈ {'CORPORATE RAIDERS', 'VANDALS'} THEN N = 16 **CAR:** {POSITIVE: 25.0%; NEGATIVE: 75.0%}	This set of rules suggests that the likelihood of the occurrence of negative CAR varies with the Attacker Type (e.g. 88.9% for *Hackers* vs 43.8% for Attacker ∈ {'OTHERS', 'PROFESSIONAL CRIMINALS', 'TERRORISTS'})

Table 11 suggests that, in general, for all the categories of *Attackers, Hackers* are the most damaging. This is very interesting because Howard and Cohen et al. (Cohen et al. 1998; Howard 1997) in their discussions on Internet security breach assert that a *Hacker*'s motivation is to challenge firms that profess to have secured systems. A *Hacker* wants to send a message to firms that their networks and systems are vulnerable. By doing so, hackers also prove their prowess to their peers in the cyber terrorism world. If *Hackers* have no intentions to damage, then why is it that investors penalize attacks by *Hackers* more than attacks by other *Attacker Types*? Cohen et al. suggest that although *Hackers* do not naturally have malicious intent, their *Tools* may create opportunities for other *Attackers*. Further, *Hackers* sometimes become afraid of their actions and in the process of covering their tracks may cause harm.

From these discussions, it seems that although *Hackers* do not often intend to cause damage to a firm's network and resources, it is possible that investors have witnessed in the past situations where *Hackers*' actions either caused damage to the firms that they attacked or the results were more harmful than was expected. Hence from these past experiences, investors' reactions to *Hackers*' actions are different from what we would expect based on the theoretical model that we are using to examine attackers' *Objective* on damage to the firm.

Table 12: Strong Individual Rules that include *Attacker Type* as a Predictor

Source	Rules
DT_EG	IF **Results** ∈ {'DENIAL OF SERVICE', 'DISCLOSURE OF INFORMATION'} & **Attacker** ∈ {'CORPORATE RAIDERS', 'VANDALS'} THEN N = 4 **CAR:** {POSITIVE: 0.0%; NEGATIVE: 100.0%} IF **Firm Type** = 'NET' & **Results** ∈ {'THEFT OF SERVICE', 'CORRUPTION OF INFORMATION'} & **Attacker** ∈ {'CORPORATE RAIDERS', 'VANDALS'} THEN N = 3 **CAR:** {POSITIVE: 0.0%; NEGATIVE: 100.0%}

Table 12, where *Attacker* participates in a strong rule, however, presents a more startling revelation that is different from what is observed in Table 11. Here, we observe that when the *Attacker* variable is conditioned on *Results* or on *Results* and *Firm Type*, *Corporate Raiders* and *Vandals* rather than *Hackers* are highly likely to cause damage. Putting both the discriminating rule and strong rule together, we see that when investors read about Internet security breach announcements two things happen with respect to the *Attacker* variable. If the investor notices that the attack is caused by a *Hacker*, then the

reaction is negative, and thus the likelihood for a negative impact on the returns leading to negative CAR and therefore damage to the firm is high. However, when the investor is aware of the results of the attack, then the type of results and firm type are conditions that influence the likelihood of negative CAR due to the *Attacker Type*.

We note from Table 12 that, if the attack results in *Denial of Service* or *Disclosure of Information*, investors react negatively if the attacker is *Corporate Raiders* or *Vandals*. The plausible reason is that *Denial of Service* by *Corporate Raiders* seems to suggest that the competitor is sabotaging the firm from using the Internet to perform business activities. Since *Vandals*, according to the literature, seek to damage the firm's network, investors look at this as a serious problem.

When the firm that suffers the attack is *Net*, then *Theft of Service* or *Corruption of Information* is seen as "serious" problems as well. One would have expected that *Corruption of Information* would be included in the first case even for *Non-Net* firms. One thing that we can say is that *Non-Net* firms may have time to clean up data before transmitting them when there is attack that corrupts the firm's operational information. However for the *Net* firm, the site is up 24/7 meaning that during the period of the attack, customers are more likely to receive inaccurate information, which investors may consider as very harmful to the customer and also to the future performance of the firm. Overall, our data clearly shows that the *Attacker* variable is a predictor of CAR when Internet security breach announcement is made.

Objective

Table 13: Sets of Rules that include *Objective* as a Discriminating Predictor

Source	Rules	Comments

DT_Eb	IF **Objective** = 'CHALLENGE/STATUS' THEN
	N = 10
	CAR: {POSITIVE: 10.0%; NEGATIVE: 90.0%}
	
	IF **Objective** = 'DAMAGE' THEN
	N = 11
	CAR: {POSITIVE: 27.3%; NEGATIVE: 72.7%}
	
	IF **Objective** ∈ {'FINANCIAL GAIN','OTHER','POLITICAL GAIN'} THEN
	N = 20
	CAR: {POSITIVE: 50.0%; NEGATIVE: 50.0%}
		This set of rules suggests that the likelihood of the occurrence of Abnormal return varies with the *Objective* of the attacker (e.g. 90% for '*Challenge/Status*' vs 50% for '*Financial Gain*', 'Other', or '*Political Gain*').

DT_Gc	IF **Objective** ∈ { 'CHALLENGE/STATUS', 'FINANCIAL GAIN'} & **Period** = 'POST FEB 2000' & **Access** = 'UNAUTHORIZED ACC' THEN
	N = 12
	CAR: {POSITIVE: 0.0%; NEGATIVE: 100.0%}
	
	IF **Objective** ∈ { 'DAMAGE', 'POLITICAL GAIN'} & **Period** = 'POST FEB 2000' & **Access** = 'UNAUTHORIZED ACC' THEN
	N = 12
	CAR: {POSITIVE: 33.3%; NEGATIVE: 66.7}
		This set of rules suggests that for *Post February 2000*, if the intrusion is by an outsider (i.e. '*Unauthorized Access*" then the likelihood of the occurrence of Abnormal return varies with the *Objective* of the attacker (e.g. 100% for '*Challenge/Status*' or 'Financial Gain vs 66.7% for *'Damage*', or '*Political Gain*').

The results presented in Table 13 suggests that in general, attack motivated by *Challenge/Status* is the most damaging of all the categories of attacker's *Objective.* Further, if the attack occurred recently (*Post February 2000*) through *Unauthorized*

Access, then those attacks that are either motivated by *Challenge/Status* or *Financial Gain* are highly likely to cause damage.

The interpretation of this finding is quite similar to what was said concerning *Hackers*. Here we see that investors take attack where firms are reminded of vulnerabilities seriously. It seems that investors would expect firms to have security mechanisms that enable them proactively act to prevent attacks (Cohen 1997a; Cohen 1997b; Cohen et al. 1998). For the investor, if someone else has to remind the firm of its vulnerability, then the firm has not effectively prepared against attacks and such actions are considered as security failures and therefore investors would react negatively to such announcements. We note from the findings that the *Objective* variable is an important predictor of attack as it influences investors' decision on the breached firm, which subsequently impacts the returns of the firm.

Table 14: Strong Individual Rules that include *Objective* as a Predictor

Source	Rules

DT_Eb	IF **Firm Size** = 'LARGE' & **Objective** = 'CHALLENGE/STATUS' THEN
	N = 7
	CAR: {POSITIVE: 0.0%; NEGATIVE: 100.0%}
	
	IF **Firm Size** = 'SMALL' & **Objective** = 'DAMAGE' THEN
	N = 5
	CAR: {POSITIVE: 20.0%; NEGATIVE: 80.0%}

DT_Gc	IF **Objective** ∈ { 'CHALLENGE/STATUS', 'FINANCIAL GAIN'} & **Period** = 'POST FEB 2000' & **Access** = 'UNAUTHORIZED ACC' THEN N = 12 **CAR:** {POSITIVE: 0.0%; NEGATIVE: 100.0%} IF **Firm Size** = 'SMALL' & **Objective** ∈ { 'DAMAGE', 'POLITICAL GAIN'} & **Period** = 'POST FEB 2000' & **Access** = 'UNAUTHORIZED ACC' THEN N = 5 **CAR:** {POSITIVE: 20.0%; NEGATIVE: 80.0%}

Table 14 provides support for the argument that has been presented concerning attacker's *Objective* from Table 13 above. Table 14, however, also shows that the problem of damage as a result of attackers' motivation to *Challenge/Status* is often associated with *Large* firms whereas attack with *Objective* to cause damage is often a problem with *Small* firms. What this means is that investors take *Challenge/Status* problems seriously when it involves *Large* firms, and they also take an attack that actually seeks to cause *Damage* more seriously for *Small* firms. Based on the above discussions, we can develop a proposition that states that the abnormal return attributed to the announcements of Internet security breach would be higher when the *Objective* variable is *Challenge/Status* than the other categories of *Objective*.

Results

Table 15: Sets of Rules that include *Results* as a Discriminating Predictor

Source	Rules	Comments
DT_EG	IF **Results** ∈ {'DENIAL OF SERVICE', 'DISCLOSURE OF INFORMATION'} & **Attacker** ∈{'CORPORATE RAIDERS','VANDALS'} THEN N = 4 **CAR**: {POSITIVE: 0.0%; NEGATIVE: 100.0%} IF **Results** ∈ {'THEFT OF SERVICE', 'CORRUPTION OF INFORMATION'} & **Attacker** ∈ {'CORPORATE RAIDERS', 'VANDALS'} THEN N = 12 **CAR:** {POSITIVE: 33.3%; NEGATIVE: 66.7%}	This set of rules suggests that if the *Attacker* is a *Corporate Raider* or *Vandal* then the likelihood of the occurrence of negative CAR varies with the *Results* of the attack.

We infer from Table 15 that if the *Results* variable is conditioned on the *Attacker* where the *Attacker* is *Corporate Raiders* or *Vandals*, then attacks that result in *Denial of Service* or *Disclosure of Information* are more damaging than those that result in *Corruption of Information* or *Theft of Service*. This finding corroborates what was found concerning the *Attacker* variable.

Table 16: Strong Individual Rules that include *Results* as a Predictor

Source	Rules
DT_EG	IF **Results** ∈ {'DENIAL OF SERVICE', 'DISCLOSURE OF INFORMATION'} & **Attacker** ∈ {'CORPORATE RAIDERS', 'VANDALS'} THEN N = 4 **CAR:** {POSITIVE: 0.0%; NEGATIVE: 100.0%} IF **Firm Type** = 'NET' & **Results** ∈ {'THEFT OF SERVICE', 'CORRUPTION OF INFORMATION'} & **Attacker** ∈ {'CORPORATE RAIDERS', 'VANDALS'} THEN N = 3 **CAR:** {POSITIVE: 0.0%; NEGATIVE: 100.0%}

Table 16 suggests that for *Net* firms however, *Theft of Service* or *Corruption of Information* has the same likelihood of damage as would be expected for *Denial of Service* and *Disclosure of Information* if it is conditioned on attack by *Corporate Raider or Vandals*. The strong rule and the discriminating rule together suggests that the *Results* variable is a good predictor of damage. This finding is contrary to what has been reported in the literature concerning the nature of the attack.

One of the earlier studies on Internet security breach indicated that only confidential information needs to be protected (Campbell et al. 2003). Here we have seen that all the categories of the *Results* of attack are likely to lead to damage and that firms need to

prevent attack in general. The findings seem to suggest that *Net* firms should be more concerned with all four categories of *Results* of attack, whereas *Non-Net* firms need to pay more attention to attacks that result in *Denial of Service* or *Disclosure of Information.*

Tools

Table 17: Sets of Rules that include *Tools* as a Discriminating Predictor

Source	Rules	Comments
DT_EGa	IF **Tools** = 'SCRIPTS/PROGRAMS' & **Attacker** ∈ {'OTHERS', 'PROFESSIONAL CRIMINALS', 'TERRORISTS'} THEN N = 4 **CAR:** {POSITIVE: 100.0%; NEGATIVE: 0.0%} IF **Tools** = 'OTHER' & **Attacker** ∈ { 'OTHERS', 'PROFESSIONAL CRIMINALS', 'TERRORISTS'} THEN N = 6 **CAR:** {POSITIVE: 50.0%; NEGATIVE: 50.0%} IF **Tools** = 'AUTONOMOUS AGENT' & **Attacker** ∈ {'OTHERS', 'PROFESSIONAL CRIMINALS', 'TERRORISTS'} THEN N = 6 **CAR:** {POSITIVE: 33.3%; NEGATIVE: 66.7%}	These rules suggest that when the *Attacker* is *Professional Criminals* or *Terrorists* or *Unknown*, the likelihood of negative CAR varies significantly with the *Tools* used by the *Attacker*. This ranges from 0 for *Scripts/Programs* to 66.7 for *Autonomous Agents.*

DT_Eb	IF **Tools** = 'AUTONOMOUS AGENT' **& Objective** ∈ {'FINANCIAL GAIN','OTHER','POLITICAL GAIN'} THEN N = 6 **CAR:** {POSITIVE: 33.3%; NEGATIVE: 66.7%} IF **Tools** = 'SCRIPTS/PROGRAMS' **& Objective** ∈{'FINANCIAL GAIN', 'OTHER', 'POLITICAL GAIN'} THEN N = 5 **CAR:** {POSITIVE: 80.0%; NEGATIVE: 20.0%} IF **Tools** = 'OTHER' **& Objective** ∈ {'FINANCIAL GAIN', 'OTHER', 'POLITICAL GAIN'} THEN N = 9 **CAR:** {POSITIVE: 44.6%; NEGATIVE: 55.6%}	These rules suggest that when the *Objective* is *Financial Gain, Political Gain* or *Unknown*, the likelihood of negative CAR varies significantly with the *Tools* used by the attacker.

Table 17 suggests that, *Autonomous Agents* are more likely to cause damage than any category of *Tools,* when the effect of *Tools* on damage is conditioned on *Objective* and the *Objective* is *Financial Gain* or *Political Gain.* In fact, when the security breach is due to *Faulty Programs/Scripts*, firms are highly likely to have normal returns, i.e. the likelihood of damage will be very low when the attack is conditioned on *Attacker*, and the *Attacker* is either *Professional Criminals* or *Terrorists*. The table also shows that *Tools* is an important variable as the likelihood value for the different *Tools* varies considerably. We notice that irrespective of the conditions, among the different categories of *Tools, Autonomous Agents* are highly likely to cause damage. We can develop a theoretical

model involving *Tools* and damage where we propose that *Autonomous Agents* would have higher likelihood of causing damage than other *Tools.*

Table 18: Strong Individual Rules that include *Tools* as a Predictor

Source	Rules
DT_EGa	IF **Tools** = 'SCRIPTS/PROGRAMS' & **Attacker** ∈ {'OTHERS', 'PROFESSIONAL CRIMINALS', 'TERRORISTS'} THEN N = 4 **CAR:** {POSITIVE: 100.0%; NEGATIVE: 0.0%}

Table 18 can be used to make the statement that security breach due to faulty programs and scripts are highly likely to cause no damage and that the announcements of Internet security breach caused by *Faulty Scripts/Programs* is highly likely to lead to normal returns. The strong rule that includes *Tools* supports what is presented when *Tools* performs a discriminating predictor role (see Table 17).

Access

Table 19: Set of Rules that include *Access* as a Discriminating Predictor

Source	Rules	Comments
DT_C	IF **Access** = 'UNAUTHORIZED USE' THEN N= 9 **CAR:** {POSITIVE: 66.7%; NEGATIVE: 33.3%} IF **Access** = 'UNAUTHORIZED ACC' THEN N= 32 **CAR:** {POSITIVE: 25.0%; NEGATIVE: 75.0%}	This set of rules suggests that *Unauthorized Access* (i.e. 75%) is more likely to result in negative CAR than *Unauthorized Use* (i.e. 33%).

From Table 19, we can say that *Unauthorized Access* (attack by intruders or outsiders) has almost twice likelihood to cause damage than by insiders (*Unauthorized Use)*. This is in direct contrast to what Howard observes from his data. It seems that investors are more concerned with intruders getting into corporate networks than employees using corporate networks and resources for *Unauthorized Use*. This is difficult to explain because one would have expected that investors would be concerned about insiders who are expected to be loyal to have abused their privileges to perform illegal activities that have potential to cause damage to the firm. It seems that Howard's database had more cases where the *Attackers* were insiders. However, the announcements in the public media include less of those where the *Attacker* is insider and so it is possible that investors think that insider attacks are rare, and therefore not very critical as opposed to attacks by intruders.

Table 20: Strong Individual Rules that include *Access* as a Predictor

Source	Rules
DT_C	IF **Period** = 'POST FEB 2000' & **Access** = 'UNAUTHORIZED ACC' THEN N= 24 **CAR:** {POSITIVE: 16.7%; NEGATIVE: 83.3%}
DT_Gc	IF **Objective** ∈ {'CHALLENGE/STATUS', 'FINANCIAL GAIN'} & **Period** = 'POST FEB 2000' & **Access** = 'UNAUTHORIZED ACC' THEN N = 12 **CAR:** {POSITIVE: 0.0%; NEGATIVE: 100.0%} IF **Firm Size** = 'SMALL' & **Objective** ∈ {'DAMAGE', 'POLITICAL GAIN'} & **Period** = 'POST FEB 2000' & **Access** = 'UNAUTHORIZED ACC' THEN N = 5 **CAR:** {POSITIVE: 20.0%; NEGATIVE: 80.0%}

We surmise from Table 20 where *Access* variable performs a strong rule role, that *Unauthorized Access* attacks that occurred *Post February 2000* are highly likely to cause damage. For these conditions, an attack that is motivated by *Financial Gain* or *Challenge/Status* is likely to be more damaging than those with *Objective* to cause *Damage* or for *Political Gain.*

4.4.3 Summary of Regression Results

Several regression models involving combinations of potential predictors were generated. Since our potential predictors are all categorical, each had to be represented by

one or more dummy variables. Thus for example, the variable *Tools* was represented by several dummy variables such as *Tool_Aut* for the *Autonomous Agent Tools*. We report the results for two models: (1) Model 1 that includes all the potential predictor variables; and (2) Model 2 that is significant at 5% level (See Table 21 Panels A-C). Model 1 is not significant at 5%, although the *Firm Type* variable is significant (See Table 21 Panel A). Model 2 includes *Tool_Aut, Firm Size, Firm Type,* and *Period* as potential predictors.

Table 21: Regression Models for Internet Security Breach

Panel A: Selected Parameters for Two Regression Models

Model	Variables tested	F	Significance	R^2	Adjusted R^2	Variables Significant at 5% level	
						Variable	p-value
1	All variables	1.393	0.225	0.553	0.222	*Firm Type*	0.011
2	Tool_Aut Firm Size Firm Type Time	2.770	0.042	0.235	0.15	*Firm Type*	0.016
						Tool_Aut	0.011

Table 21 Panel C shows the detailed parameters for the overall regression models and the individual predictor variables. We observe that only two independent variables were significant: *Firm Type* and *Tools* (specifically *Tool_Aut*, i.e., *Autonomous Agents*) with p-values of 0.016 and 0.011 respectively.

Panel B: Summary for the Statistical Significant Regression Model

Model	R	R^2	Adjusted R^2	Std. Error of the Estimate
2	.485(a)	.235	.150	6.50592

Predictors: (Constant), *TOOL_AUT, Firm Size, Time, Firm Type*

In summary, the results of the regression analysis suggest that only two of the possible predictor variables were found to have significant impact on CAR: *Firm Type* and *Tools* used to attack. Specifically, *Net* firms have more negative CAR than *Non-Net* firms, and the use of *Autonomous Agents* (that include virus and worms) lead to negative CAR.

Panel C: Coefficients for the Statistical Significant Regression Model

Model		Unstandardized Coefficients		Standardized Coefficients	T	p-value
		B	Std. Error	Beta		
2	(Constant)	4.602	3.604		1.277	.210
	Firm Type	-5.813	2.307	-.414	-2.519	**.016**
	Firm Size	-1.593	2.394	-.101	-.665	.510
	Time	-.975	3.155	-.049	-.309	.759
	Too_Aut	-5.798	2.164	-.415	-2.679	**0.011**

4.4.4 Comparison of Regression and DT Induction Results

We now compare the results of our regression analysis with that of the DT-based analysis (see Table 22). In Table 23, we provide arguments that could be used to justify the role of the given variable as a predictor of negative CAR.

Table 22: Comparative Analysis of Regression and DT Results

Variable	Hypothesis	Variable established as a Predictor?	
		Regression	**Decision Tree Induction**
Firm Type	H2[12]	Statistically established to be a predictor	Evidence suggests it to be a predictor
Firm Size	H3	Statistically established Not to be a predictor	Evidence suggests it to be a predictor
Time Period	H4	Statistically established Not to be a predictor	Evidence suggests it to be a predictor
Attacker Type	H5 (i)	Statistically established Not to be a predictor	Evidence suggests it to be a predictor
Attacker Objective	H5 (ii)	Statistically established Not to be a predictor	Evidence suggests it to be a predictor
Attack Results	H5 (iii)	Statistically established Not to be a predictor	Evidence suggests it to be a predictor
Tools Used to attack	H5 (iv)	Statistically established to be a predictor	Evidence suggests it to be a predictor
Access used to attack	H5 (v)	Statistically established Not to be a predictor	Evidence suggests it to be a predictor

From Table 22, we observe that only two variables: *Tools* and *Firm Type* are statistically established to be predictor variables according to the regression analysis. However, the DT analysis provides evidence to suggest that all the attack and firm characteristics variables are predictors. What we have shown is that the relationship between some of the predictor variables is not direct but through conditional interactions between the independent variables.

[12] H refers to Hypothesis, i.e. H2 = Hypothesis 2; Hypothesis 1 is used to examine the overall CAR.

What the DT analysis reveals therefore is that the relationship is more complex than predicted by the regression models. It shows that the DT analysis is revealing interactions among the independent variables that may induce damage, but these relationships are not predicted by the regression models. This finding supports our proposition that using data mining has the potential to provide additional insights that may not be revealed by the regression models alone.

Table 23: Justification of Results of DT Analysis

Variable	**Justifying Comments**
Firm Type	The information systems security literature suggests that *Net* firms, that depend heavily on the Internet (Cavusoglu et al., 2004), due to their open connectivity, are more susceptible to security attacks and therefore have high potential of recording negative CAR. For in the case of *Net* firms, an incident that shuts down the network could result in no sales, while a *Non-Net* firm that suffers security incident may be able to generate sales from the traditional market.
Firm Size	Results from previous research suggest that the influence of public announcement of accounting information is different for *Large* and *Small* firms (Hayes et al., 2000; Im et al., 2001). When security breach announcement is made, investors process this new information which they were not aware before the announcement. *Large* firms may communicate security breaches internally such that the stock price would have reflected the news even before the public announcement is made. *Small* firms on the other hand, may take time or may not communicate the security breach before the event date making the

	public announcement important information that needs to be incorporated into the valuation of the firm. Thus generally, attacks involving *Small* firms are likely to have more negative CAR than those involving *Large* firms. However, we realize that attack involving *Hackers* or where attacker's *Objective* is *Challenge/Status*, *Large* firms have larger negative CAR than *Small* firms. This shows that the relationship between CAR and *Firm Size* is conditioned on attacker's *Objective*. The probable reason may be that *Large* firms are expected to have in place security systems such that intruders may not be the first to inform them of vulnerabilities.
Time Period	In February 2000, several major firms such as Yahoo, E-Bay, Amazon, and E-trade had their web sites shut down by a denial-of-service attack. This event could distinguish the "fallow" time where investors were more forgiving than later times where investors react to security breaches. Investors would expect that with time firms would be better prepared to address security problems and thereby less forgiving than they have been in the past. It must, however, be noted that the *Objective* of the attacker is a conditional variable that influences the impact that time has on CAR.
Attacker Type	A major motivation for *Hackers* to attack is the desire to show their prowess and to raise their status in the cyber terrorism community in which they operate. Other types of *Attackers* could use the vulnerabilities resulting from *Hackers*' activities to launch other attacks with more disastrous outcomes. However, if a firm responds quickly to the *Hackers*' activities, those vulnerabilities could be eliminated, preventing further attacks. *Vandals* aim at causing harm to the systems of the attacked firms, while *Professional Criminals* seek financial benefits from their activities. Gupta et al. (2000) indicate that each of these *Attacker Types* has different capabilities for using

	the specific *Tools* to achieve its specific strategies and *Objectives*. It is believed that investors can distinguish between the different *Attackers* based on their capabilities to cause harm to a firm's resources. The results from the *Attacker* variable suggest that *Hackers* are the most damaging. This finding mandates critical review of Howard's taxonomy to ensure that the classification of *Attacker* variable is in line with what the public perceive the different *Attacker Types*.
Objective	An attack geared towards *Financial Gain* and another where the *Attacker* challenges the firm's claim that its system is secured will receive different reaction from investors and will therefore have different impacts on abnormal return.
Results	Howard (1997) identifies four different *Results* of attack: *Corruption of Information (violates integrity)*, *Denial of Service(prevents systems to be available)*, *Theft of Service*, and *Disclosure of Information (violates confidentiality)*. Since the different results will determine whether integrity, confidentiality and availability of the firm's systems have been breached, results will influence investor's reactions.
Tools	The kinds of damage to the firm and the level of access that the *Attacker* can gain increase with the increased sophistication of *Tools* employed. Thus, the *Tools* used to attack impact the cumulative abnormal return.
Access	Attacks can be internal or external. Internal attacks include disgruntled employees taking advantage of the access privilege to corporate networks to perform unauthorized activities. Outsiders usually take advantage of vulnerabilities to gain *Unauthorized Access* to corporate networks. Investors may consider *Unauthorized Use* as an error and *Unauthorized Access* as an organization's failure to prevent intruders from getting access to "secured" data or network systems, and thus may react more negatively to the latter.

4.4.5 Comparison with Results of Previous Research

While prior studies had conflicting results on whether the firm characteristics and the nature of the attack are determinants of CAR, the results of our study suggest that both the firm characteristics and the nature of the attack (attack characteristics) are determinants of CAR. It should be noted that while each of our results is consistent with that of at least one other study, no previous single study has provided evidence that both firm and attack characteristics are determinants of CAR.

One of the previous studies had suggested that only attack involving confidentiality leads to negative CAR (Campbell et al. 2003). Here, we have shown that compromise due to any or combination of confidentiality, integrity, and availability leads to negative CAR. Table 24 presents a comparison of some results of our study with those relevant previous studies that were presented in an earlier section.

Table 24: Comparison of Results of This Study with Results of Previous Studies

Previous Studies				This Study
Author (s)	**Main Focus**	**Variables**	**Some Major Findings**	
Ettredge et al. (2001)	Denial-of-service attacks	Firm Type, Firm's e-risk	• *B2C* firms experienced 7.9% lower CAR • Internet firms that disclosed controllable e-risk experienced more negative CAR	*Firm Type* , *Access* are determinants of CAR
Cavusoglu et al. (2004a)	Internet security breaches in	*Firm Size, Firm Type*, time lag,	• The nature of the attack does not	• Nature of attack is a determinant

	general and economic effect of attack on security developers	The nature of the attack	influence CAR • *Firm Size*, *Firm Type* and time lag are determinants of CAR	of CAR • *Firm Size*, *Firm Type* and *Period* are determinants of CAR
Campbell et al. (2003)	Confidential Information	The nature of the attack (*Confidential* v. *Non-confidential*)	• The nature of the attack influences CAR	• The nature of attack does influence CAR • It is not only loss of confidential data that leads to damage but any attack that result in lack of availability of computer system or network or loss of data integrity
Hovav and D'Arcy (2003)	Denial-of-service attacks	The nature of attack (*Denial-of service-attack* v. *Non-Denial-of-Service attack*)	• Market does not penalize firms that report *Denial of Service* attack, i.e. the nature of the attack is not a determinant of CAR • *Net firms* have higher negative returns than *Non- Net* firms	• The nature of the attack is a determinant of CAR • *Denial of Service* attack is a category of attack characteristics and this category has different impact than other categories on CAR, i.e. *Results* is a predictor of CAR
Hovav and D'Arcy (2004)	Virus attacks	The nature of the attack (*Virus attack* v. *non-virus attack*)	• Virus attack is not a determinant of CAR, i.e., the nature of the attack is not a	• The nature of the attack is a determinant of CAR • Virus attack is a

			determinant of CAR	category of attack characteristics and has different impact on CAR from other categories.

4.5 Theoretical Propositions

In the following section, we present the theoretical propositions of the relationship between the attack characteristics, firm characteristics and damage. This is based on the results of the DT induction. First we present the key terms, derived from the literature, which is used to represent the *Results* of the attack. We then use the DT induction results to propose the relationship between the independent variables and damage.

4.5.1 Key terms

The key terms (see Table 25) that form the foundations for understanding the relationship between the three tenets of information security and Howard's categories of *Results* of attack are presented. We use the terms to develop relationship between firm damage and *Results* of the attack. This is very important because it allows us to understand that beyond loss of confidential information, the other tenets of Information security are relevant variables for understanding the impact of attack characteristics on damage.

Table 25: Key Theoretical Terms

Term	Definition (s)
Confidentiality	(Secrecy) the principle that keeps information from being disclosed to anyone not authorized to access it (Howard 1997); Only authorized individuals have access to the databases and information systems (Bodin et al. 2005).
Integrity	Protection against forgery or tampering (Howard 1997); The information in the system is accurate, complete, and consistent, and only authorized individuals can change such information (Bodin et al. 2005). Corruption of information destroys the integrity of information (Howard, 1997).
Availability	Computers, networks and files are all working and available for use (Howard 1997); The information is available to authorized users in a timely manner.
Disclosure of Information	The dissemination of information to anyone who is not authorized to access that information (Howard 1997).
Corruption of Information	Unauthorized alteration of files stored on a host computer or data in transit across a network (Howard 1997).
Denial of Service	The intentional degradation or blocking of computer or network resources (Howard 1997).
Theft of service	The Unauthorized Use of computer or network services without degrading the service to other users (Howard 1997).

The confidentiality property of information resource is compromised by *Disclosure of Information* which permits anyone that is able to access such resources to have access to confidential information supposed to be held in secret and only made available to authorized users. *Denial of Service* attack bombards corporate networks with

Hence *Denial of Service* compromises data availability. When an attack on a corporate network corrupts data, data integrity is lost. Although *Theft of Service* by unauthorized users does not degrade networks, it could lead to *Disclosure of Information* or *Corruption of Information,* and consequently result in comprise of data confidentiality and data integrity.

Clearly, the *Results* variable in Howard's (1997) taxonomy (*Disclosure of Information, Corruption of Information, Denial of Service, and Theft of Service*) represents the three tenets of information security (confidentiality, integrity, and availability). Prior studies suggest that the nature of the attack does not affect CAR (Cavusoglu et al. 2004b; Hovav and D'Arcy 2003). Campbell et al. (2003) also note that only attacks that involve loss of confidential information lead to negative CAR.

In this study, we have shown that both attack and firm characteristics are determinants of damage to breached firms where damage is operationalized as the CAR. Using the literature we show that the three tenets of security are related to the *Results* of the attack in Howard's taxonomy. The DT induction reveals that attack due to any of the categories in the results variable leads to negative CAR. Hence we can make the argument that confidentiality, integrity and availability, the three tenets of security cause damage to the firm. For the minimum, firms that seek to protect their systems and networks should realize that investors will not only penalize attacks that result in loss of confidential data or information but any attack that prevents system availability, integrity and loss of confidential data will all be considered as bad news by investors.

The use of Decision tree induction enhances the understanding of the factors that determine the observed abnormal return when Internet security breaches are announced. We present general propositions that can be used to develop theories about Internet security breach and damage to breached firms.

Recall that we identified two roles that each of the predictor variables can play: discriminating role and participating in a strong rule. When a predictor variable is discriminating and is not conditioned on other independent variables, that variable has direct relationship with CAR, which in the case of Internet security is damage to the firm. However, if the variable is part of a strong rule then that variable could be a moderating variable for one or more of the independent variables that form the strong rules. Based on this discussion, we list below some general propositions from the DT induction that can further be tested.

1. We find that *Attacker Type* variable has direct relationship with damage where it is known that *Hackers* are the most damaging of all the *Attacker Types* (see Table 11).
2. Attacker's *Objective* has direct relationship with firm damage; i.e., *Challenge/Status* is the most damaging (Table 13).
3. *Access* used to attack has direct relationship with damage, *Unauthorized Access* is more likely to cause damage than *Unauthorized Use*, i.e. intruders are more likely to cause damage than insiders (Table 19).

*A*t the minimum, we can examine the predictor variables that have direct relationship with damage to develop theory about damage and attack and firm characteristics. For instance we can develop theoretical models involving *Attacker Type, Objective of the attacker,* and *Access* used to attack. Here we could test for the three hypotheses where we know that one specific category each of the 3 variables is either more damaging or the most damaging. Research on a large sample data can help validate the theoretical models that are presented in the following pages on firm characteristics, attack characteristics and damage.

4.5.2 Theoretical Models for Internet Security Breaches and CAR

We present in Figures 8 to 15, theoretical models for the relationships between the independent variables (firm characteristics variables, attack characteristics variables, and time lag variable) and the independent variable (CAR or damage). Each figure represents one of the predictor variables. Figure 7 is the legend for Figures 8-15.

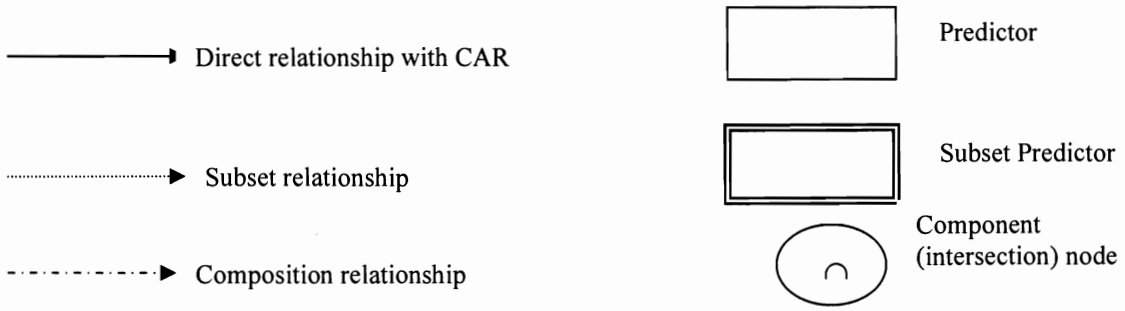

Figure 7: Legend for Theoretical Models

Depicted in Figure 7 are three nodes: the Predictor node, the Subset Predictor node, and the Composition (intersection) node. The Predictor node indicates a variable with all its possible categories or subsets. The Subset node represents the situation where a subset of the variable participates in the relationship. The composition or intersection node represents the intermediate variable that results from the interaction of the independence variables. This variable then has direct impact on CAR or damage.

The Prediction feeds directly into CAR. It is represented by directed unbroken line. For instance in the case where *Tools used to attack* has direct impact on CAR, we represent the relationship between the *Tools* variable and CAR with unbroken line. The Subset feeds directly into Subset node. This is represented by directed dotted line. The composition feeds directly into the intersection node. It is also represented by directed broken line but has large width than that of the Subset.

Firm Type Model

Figure 8 depicts the *Firm Type* Model. Here *Firm Type* variable has no direct relationship with CAR or firm damage. *Firm Type* interacts with the two components of *Access Type*: *Unauthorized Access* and *Unauthorized Use* in two different relationships. It interacts with the *Pre February 2000* subset of *Period* variable when *Access Type* used to attack is *Unauthorized Access* (Insider attack). *Firm Type* also interacts with *Results* used to attack and the *Attacker Type* variables but here only subsets of these variables participate in the relationship. The subset of *Attacker Type* variable includes *Corporate Raiders* and *Vandals* while the *Results* used to attack variable includes *Theft of Service* and *Corruption of Information.*

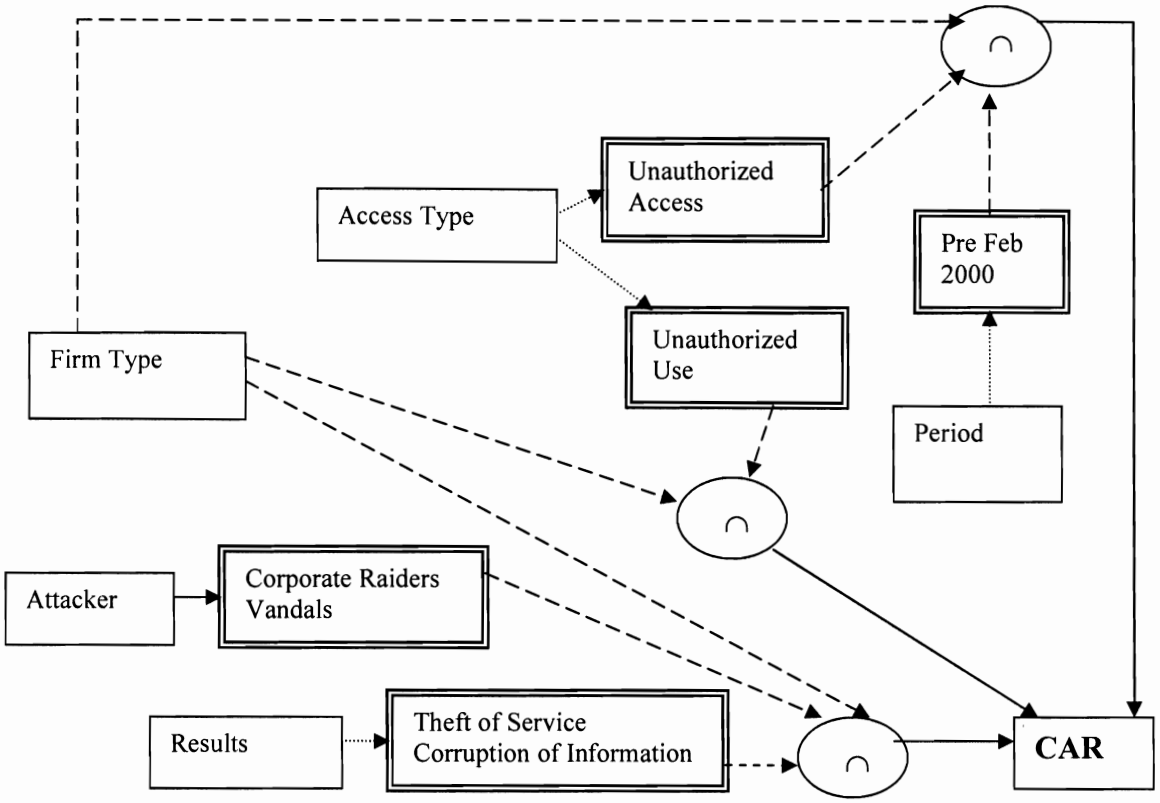

Figure 8: Firm Type Model

Firm Size Model

Figure 9 is the *Firm Size* model representing the relationship between Firm Size, CAR, and other independent variables. Firm Size interacts with the Hacker subset of the *Attacker Type* variable to impact CAR. The *Objective Type* variable interacts with *Firm Size* through two subsets: *Damage* and *Political Gain*; and *Challenge/Status*. The first subset also interacts with *Access Type* variable where access is *Unauthorized Access*. The second interacts with the *Post February 2000* subset of the *Period* Variable.

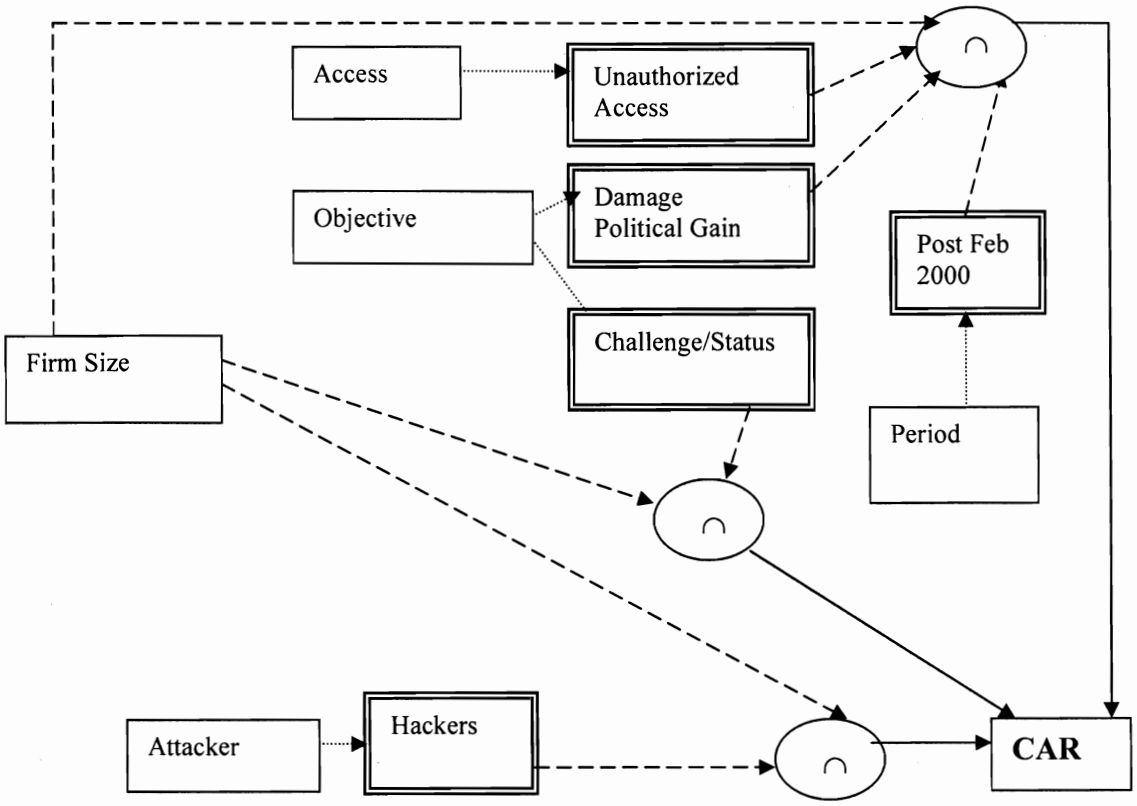

Figure 9: Firm Size Model

Period Model

In Figure 10, we present the *Period* (Time) theoretical model representing the relationships between *Period*, CAR, and other independent variables. The *Period* variable interacts with the *Objective* and *Tools* variables where the *Tools* subset is *Other* and the *Objective* subset includes *Financial Gain*, *Political Gain* and *Other*. The *Period* variable also interacts with *Unauthorized Access* subtype of the *Access Type* variable. *Period* has no direct relationship with CAR.

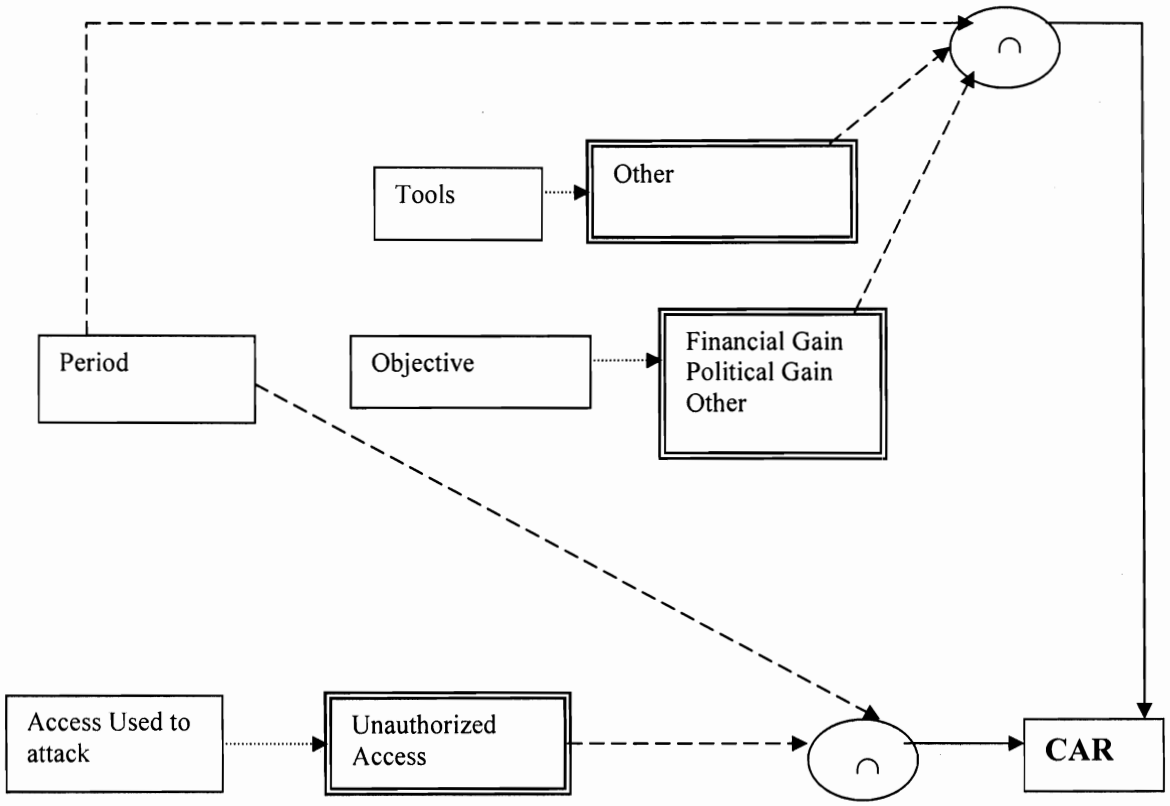

Figure 10: Period Model

Attacker Model

Figure 11 shows the *Attacker Type* Model. Here we observe two relationships. First, the Attacker *Type* variable has direct relationship with CAR. Second the *Attacker Type* variable interacts with the *Firm Type* variable to impact damage to the breached firm.

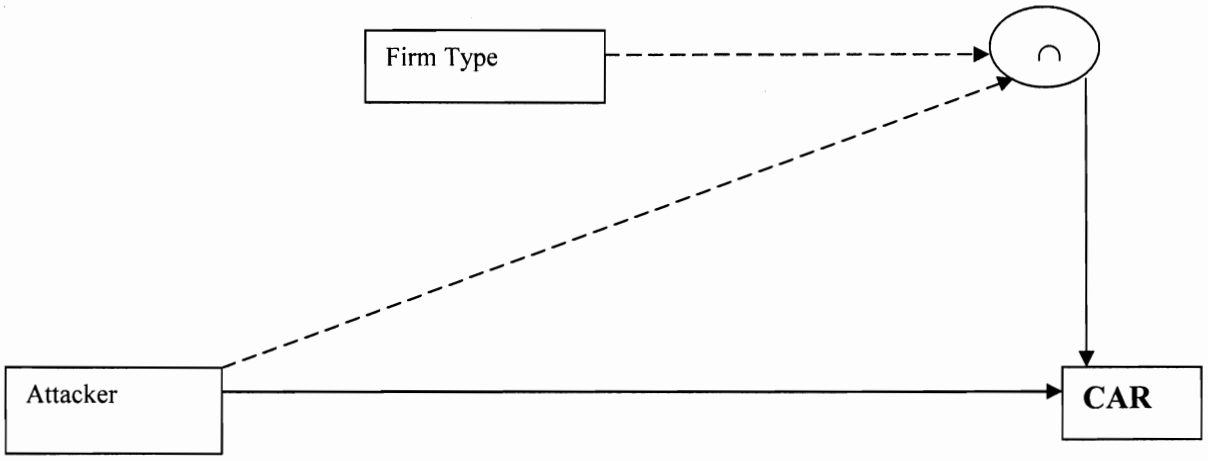

Figure 11: Attacker Type Model

Objective Model

The *Objective* variable has direct relationship with CAR. However, its impact on damage also depends on its interaction with other independent variables: *Period* and *Access Type.* Specifically, the *Access Type* subset is *Unauthorized Access* and *Period* subset is *Post February 2000.* The *Objective* model is presented in Figure 12.

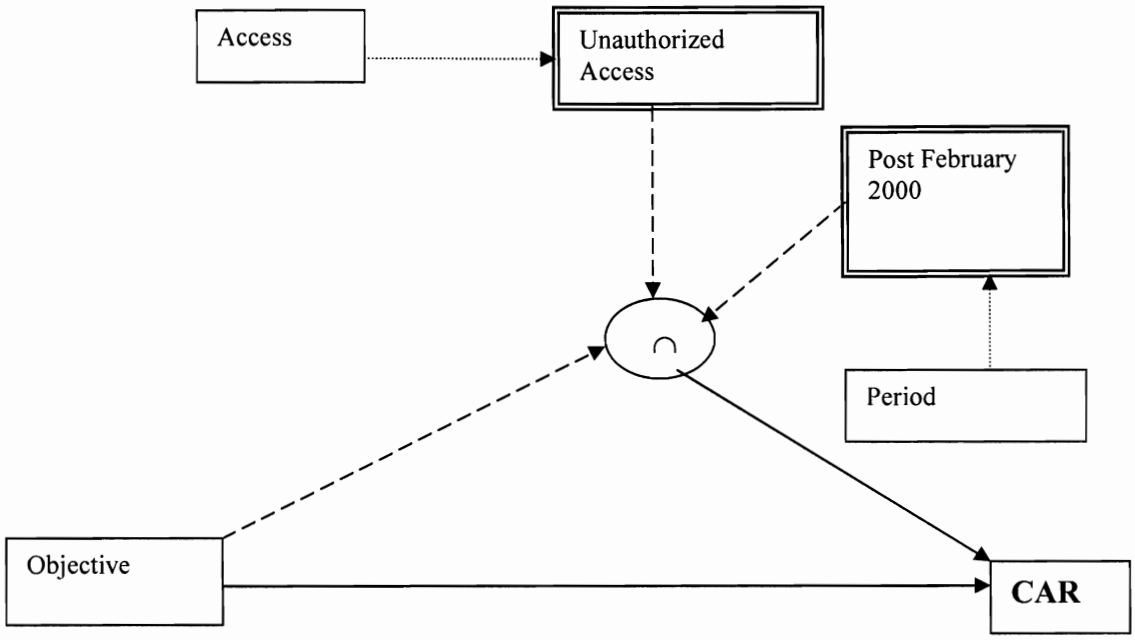

Figure 12: Objective Model

Results Model

The *Results* model is presented in Figure 13. The *Results* variable interacts with the *Attacker Type* variable through a subset. Specifically, the subset includes the *Corporate Raiders* and *Vandals* categories.

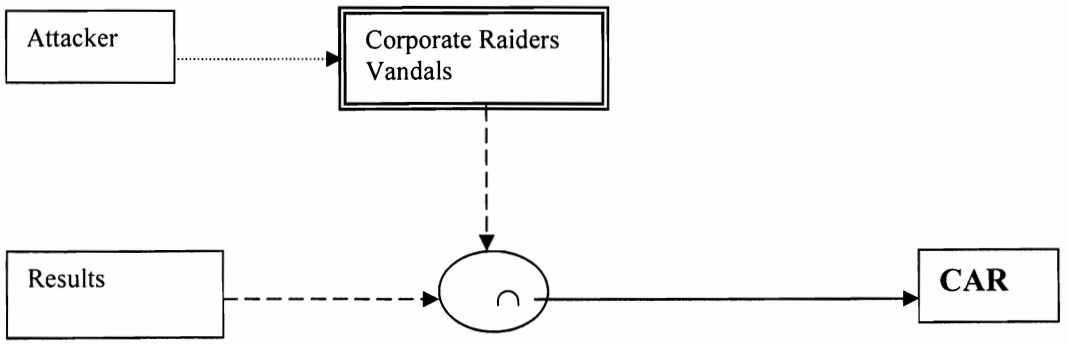

Figure 13: Results Model

Tools Model

Figure 14 depicts the *Tools* Model. First, the *Tools* variable has direct impact with CAR. Second, *Tools* interacts with subsets of the *Attacker Type* and the *Objective* variables. For the *Attacker Type* variable, the specific categories that participate in the interactive relationship are *Professional Criminals, Terrorists, a*nd *Other*. The *Political Gain, Financial Gain*, and *Other* categories of the *Objective* variable interacts with the *Tools* variable.

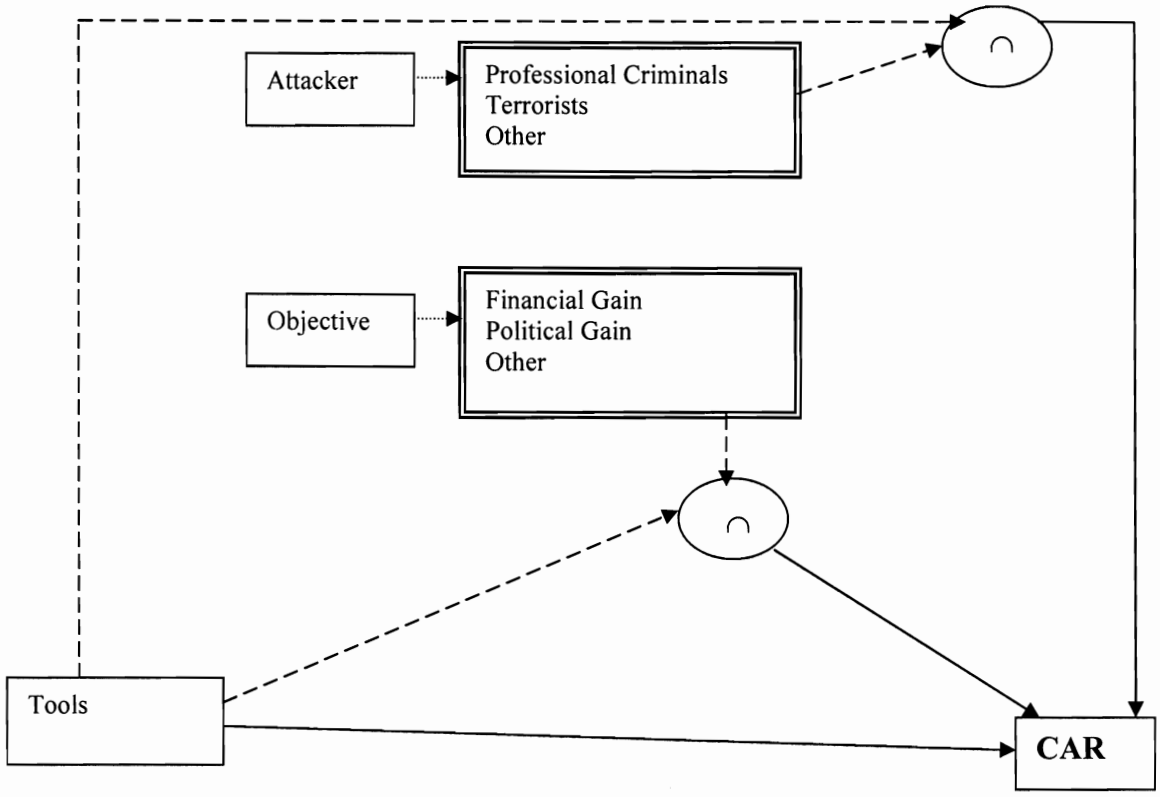

Figure 14: Tools Model

Access Type Model

The *Access Type* variable directly impacts CAR or firm damage. U*nauthorized Access* is more likely to lead to negative CAR than *Unauthorized Use*. Although Howard suggests that most of the attack is due to *Unauthorized Use*, here we find that *Unauthorized Access* is the most damaging.

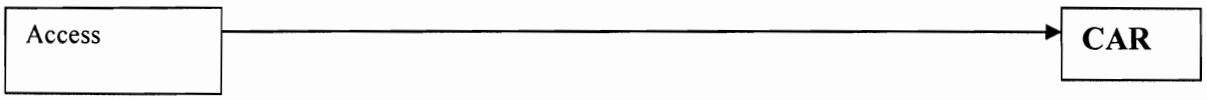

Figure 15: Access Model

CHAPTER 5
EFFECT OF ECOMMERCE INITIATIVES ON CUMULATIVE ABNORMAL RETURN

5.1 Theoretical Background of Ecommerce Initiatives

We discuss the theories used in deriving hypotheses for ecommerce initiatives. We use the incomplete contract theory to propose our set of hypotheses for ecommerce initiatives We also present other theories that have been discussed in the literature that may explain some of the findings from the DT induction. Specifically we use these theories to support or refute the incomplete contract theory and also provide comprehensive understanding of the impact of the announcements of ecommerce initiative on CAR. We present the approach for data collection, cleaning and coding. We discuss both the regression and data mining results and compare these sets of results. We also compare our results with prior research. Finally, we develop a set of theoretical propositions on firm value and organizational variables.

5.1.1 Transformational IT Investments

The importance of understanding the factors that determine the payoff of IT investments is well discussed in the literature (e.g., Barua and Mukhopadhyay 2000; Dehning et al. 2003). Further, the need for information technology investments to have strategic appeal have been noted elsewhere (e.g., Dehning et al. 2003). That research extends prior research (Chatterjee et al. 2001; Dos Santos et al. 1993; Im et al. 2001) by

including IT strategic role (transformative vs. non-transformative) as an additional explanatory variable. Dehning et al. (2003) suggest that prior studies fail to provide a common understanding of factors that lead to positive returns from IT investments. The authors propose that investors belief about the firm's future performance and for that matter its market value will be influenced by the characteristics of the firm, the IT investments and the contexts in which the investment is made.

The measurement of the strategic role of the IT investment is with respect to the announcement or the initiative which can be different from the firm's overall IT strategic role. The IT strategic role construct has three components: automate, informate-up, informate-down, and transform (Schein 1992; Wiseman 1986). A brief explanation of the dimensions of the IT strategic role construct is in order. *Automate* describes replacing human labor with IT by automating the business process. *Informate-up* refers to the use of IT to provide information on the organization's business process activities to senior management. *Informate-down* is in reference to the application of IT to provide information about the firm's business activities to its employees across the firm. *Transform* involves the use of IT for drastically redefining business and industry processes and relationships.

The authors provide empirical evidence that firms that make strategic transformative IT investments had higher positive CAR than those who made non-transformative IT investments. Dehning et al. (2003) also suggest that the use of IT for automation does not lead to CAR because such use of IT does not provide competitive advantage to the firm. The authors suggest that in the case where firms employ IT to

enhance organizational decision making at the lower and higher levels, .i.e., automate-down and automate-up respectively; there is a possibility that some firms would make radical changes in their decision structures and cultures. If the radical changes are maintained and enhanced, such firms are likely to achieve competitive advantage beyond what other industry participants may have. Such strategic use of IT is what is referred to as transform or transformative information technology investments (Dehning et al. 2003). The authors, therefore, propose that announcements made by firms that make transformative IT investments are more likely to lead to higher positive CAR than those made by firms that make non-transformative IT investments.

Further, the authors argue that the strategic role of IT within the industry influences how investors react to a firm's IT investment, and that IT investments by firms in industries where transformative IT strategic role is seen by investors to dominate, are likely to experience positive abnormal changes in market value. Based on the above discussion the authors developed and tested four propositions. They suggest that the announcements involving: firms making transformational IT investments, firms in industry in which transform IT strategic role dominates, and firms that make IT investments that lead their industry IT strategic role would lead to positive abnormal return while those involving firms making IT investments that lag their industry IT strategic role would lead to negative abnormal return. While the first three hypotheses were supported by the empirical analysis, the fourth was not. Thus, investors do not penalize firms that make IT investments that lag the dominant industry IT strategic role.

Quite recently other researchers have argued that the type of IT investment (transformation v. non-transformation) in the electronic markets is relevant in determining the market value of firms (Dehning et al. 2004). In support of other studies, the research confirmed prior studies that transformational IT investments results in higher returns than non-transformational investments.

5.1.2 Intangible Assets and the Complementarity Theory

Quantitative support is presented on the notion that IT investment has more value when coupled with complementary investments in intangible assets and resulting changes in organizational design (Brynjolfsson et al. 1998). The complementary intangible assets include new organizational form, new business process and new set of supplier relations. Other resources have been identified as complementary resources to IT. These include: tangible infrastructure, human resources, IT-related intangibles (Bharadwaj 2000), intangible assets – organizational capital (Brynjolfsson et al. 1998), IT infrastructure, human resource, and business resource (Zhu and Xu 2004).

Brynjolfsson et al. suggest that the cost of making these intangible organizational investments are substantially high. They indicate, however, that firms that make such investments can experience positive changes in market value because such investments provide competitive advantage as they are difficult to be duplicated by competitors. The authors state that the organizational assets and IT "create more value when used together than when used separately" (Brynjolfsson et al. 1998, p.4).

Other researchers have employed the complementarity theory to explain the importance of leveraging organizational variables. According to Migroms and Roberts, activities can be classified as complementary when increase in one of the activities leads to higher returns of the other activities (Milgrom and Roberts 1995). The authors proposed that organizational elements: structure, strategy and processes are linked to each other such that they coherently evolve over time. Barua et al have shown how complementary organizational variables can be leveraged to enhance business value (Barua et al. 1996). The complementarity theory has been used to explicate the complex relationship of IT investments in the healthcare industry (Ko 2003; Osei-Bryson and Ko 2004).

Subramani and Walden's work develops and tests a general theory of electronic commerce (Subramani and Walden 2002). They echoed Brynjolfsson et al (1998) by suggesting that critical success factor in IT investments in the electronic market environments is the creation of intangible, electronic commerce technology complementing assets. They assert from their empirical study that investments in intangible assets determine returns to electronic commerce initiatives. This the authors refer to as the theory of primacy of intangible assets.

5.1.3 Incomplete Contract Theory

The incomplete contract theory has been expounded to characterize relations between firms who have to invest in a first period and share benefits of the investments with partners in the second period (Grossman and Hart 1986; Hart and Moore 1988).

When firms expect to form relationships that would require them to share benefits from IT investments, they are motivated to delay investments till they form such partnerships (Subramani and Walden 2000). The Incomplete contract theory discusses benefit sharing between firms, a topic, which has received great attention (Iacovou et al. 1995; Riggins and Mukhopadhyay 1999; Seidmann and Sundararajan 1997; Truman 1998). In the ecommerce environment, firms that believe that they would have bargaining power during the negotiation of benefits accrued from initial IT investments are motivated to commit to the initial investment (Subramani and Walden 2002).

Subramani and Walden (2000) test the incomplete contract theory with ecommerce investment. In that study, the authors focus on *B2B* relationships arguing that *B2C* investments do not involve relationships. In a later work, the authors include *Governance* variable that deals with whether or not the initiative was done unilaterally or through strategic alliance. With the new variable the authors introduce a new definition for *B2B* and *B2C* as we have explained in Chapter 3. We believe that the incomplete contract theory is applicable to both *B2B* and *B2C* relationships. We seek to verify whether the *Customer T*ype influences the observed CAR.

5.1.4 Process and Resource Based Views on Ecommerce Value

Resource-based and process-oriented views have been suggested as possible theories for studying the value of electronic business investments (Zhu and Xu 2004). The process-oriented view proposes a multistage process from initial IT investment through IT usage before the final realization of the business value of IT (Cooper and

Zmud 1990; Soh and Markus 1995; Zhu and Xu 2004). The resource-based view links firm performance to its organizational valuable resources that are difficult to imitate (Barney 1991). Using the resource-based view model, Zhu and Xu (2004) suggest that e-business makes sense and provide business value only when there is effective implementation of e-business downstream, upstream and in internal processes.

Using the process view could be difficult and inappropriate when the interest is in determining whether periodic ecommerce initiatives either *Unilateral* or through strategic alliance provide business value. The reason is that by the time the initiative goes through the multistage process proposed by (Zhu and Xu 2004), there could be confounding effects that may make it difficult to attribute the business value measured during these periods to that specific initiative. This problem will hamper a firm's desire to assess the business value of the different initiatives that have been made during a year although it could effectively present the overall business value for all the various initiatives that have taken place in the organization for that period. The problem presented could hinder a firm's ability to take advantage of the specific initiatives that provide enhanced business value and differentiate those initiatives from others that may not be quite so good.

5.2 Hypotheses for Ecommerce Initiatives

In this section, we develop the hypotheses of the ecommerce announcements and market value. We employ the relevant theory from the literature in developing the ecommerce initiative hypotheses. Figure 8 shows the set of organizational variables that

is proposed to have relationship with the observed CAR when announcements of ecommerce initiative are made in the public media. Recall that ecommerce is considered as positive news, and investors are expected to react positively to ecommerce initiative announcements. In the hypotheses that we develop for ecommerce announcements and CAR, we consider positive CAR.

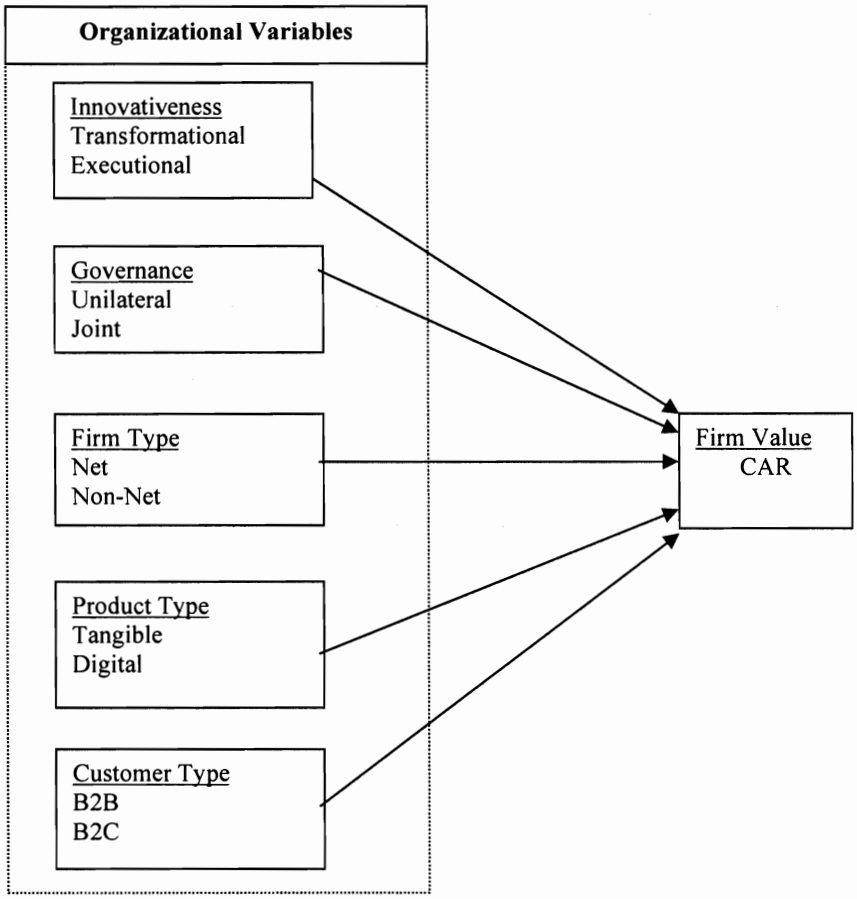

Figure 16: Framework for Examining CAR and Organizational Variables

5.2.1 Hypotheses for Ecommerce Initiative

We use the incomplete contract theory to develop the hypotheses. In explaining the empirical findings from the DT induction, we employ the incomplete contract theory but where the theory fails to provide effective justification, we use other theories from the literature to support the observation.

In deriving our first hypothesis, we remind ourselves that the hype in ecommerce is the belief that it provides opportunities for firms to enhance business operations, gain competitive advantage and eventually improve profits. Investors will therefore see ecommerce announcements as a way of improving both current and future value of the firm. Hence we put forward our first hypothesis as:

Hypothesis 1: The abnormal return attributed to the announcements of ecommerce initiative is positive.

Firm Type Variable

It is shown that where the number of participants in a partnership is few, firms have greater bargaining power and are thereby motivated to invest to generate more output (e.g., Hart and Moore 1988). Since *Net* firms (firms that derive most of their revenue from Internet commerce) focus only on one channel, i.e., the Internet, they are likely to have far less partnership and that firms that operate in these environments are motivated to invest since they do not anticipate having problems with sharing benefits from their initial investments. This leads to the following hypothesis:

Hypothesis 2: The abnormal return attributed to the announcements of ecommerce initiative by Net firms is positive.

Click-and-mortar firms (firms that operate in the traditional market as well as on the Internet) seeking ecommerce initiatives are often involved in multiple partners from both the Internet and traditional channels. Not knowing whether the Internet or the traditional channel provide the greatest promise, they are torn between the two channels and form much relatively larger partnerships, thus limiting their ability to bargain. Hence click-and-mortar firms have far lesser bargaining power than *Net* firms. There is, therefore, an incentive for click-and-mortar firms to under-invest. Thus we form the following hypothesis:

Hypothesis 3: The abnormal return attributed to the announcements of ecommerce initiative by click-and-mortar firms is not different from zero.

Product Type Variable

Tangible and *Digital* are discussed in the literature as two products that are offered by ecommerce (Jones 2003; Negroponte 1995; Shapiro and Varian 1999; Subramani and Walden 2002). Businesses producing *Tangible* products have the capability to hide their cost structures. During negotiations, the other parties do not have the necessary information to make meaningful estimates of the structure allowing the firm to have "strong" bargaining power. Hence firms that produce *Tangible* products can exercise post ante bargaining power from the results of their initial ecommerce investments. We therefore hypothesize that:

Hypothesis 4: The abnormal return attributed to the announcements of ecommerce initiative for Tangible products is positive.

Digital products are those produced by computers and are typically available for download from the Internet or for use online. It is easy to share a *Digital* goods and not able to make distinctions between the original and the copy. Just as it is easy to produce *Digital* products, it is relatively simple to determine the cost structure for making these products. In addition, there are incentives to under sell *Digital* products which reduces the bargaining power of firms that engage in *Digital* products. This leads to the following hypothesis:

Hypothesis 5: The abnormal return attributed to the announcements of ecommerce initiative for Digital products is not different from zero.

Customer Type Variable

With *B2C* investments, except for simple computers and networks, the supplier or firm that operates in this environment does not expect the buyers, the end customer or consumer, to make any huge investments to maintain the relationship. There is no incentive for the firm to undercut its initial investments knowing the potential Post ante bargaining power that it can gain from the resulting relationship. Thus we envisage that firms would provide the IT investments necessary to support the relationship and to enhance the firm's business value. We therefore put forward the following hypothesis:

Hypothesis 6: The abnormal return attributed to the announcements of B2C ecommerce initiative is positive.

We recognize that *B2B* which is based on the Electronic data interchange is made cheaper by new standards such as XML. At the same time, with better customer relationship management systems, firms engaged in *B2B* have lower operational costs making the *B2B* ecommerce venture more profitable. However, we expect that *B2B* sellers and buyers may under-invest because of the feeling of low bargaining power resulting from the seller or buyer's action. It is difficult for the individual partners in this relationship to determine effectively the benefits that they can get from the relationship with respect to the IT investments that need to be made to support the relation. This discussion leads to the following hypothesis:

Hypothesis 7: The abnormal return attributed to the announcements of B2B ecommerce initiative is not different from zero.

Governance Variable

The *Governance* variable has two categories: *Unilateral* and *Joint* (initiative through alliance). When a firm *unilaterally* initiates an ecommerce venture, there is great opportunity for it to hide its cost structure and therefore receive future post ante bargaining power. Thus, firms that operate unilaterally in an ecommerce initiative are likely to receive positive returns. This leads to the following hypothesis:

Hypothesis 8: The abnormal return attributed to the announcements of Unilateral ecommerce initiative is positive.

The incomplete contract theory suggests that when two firms form an alliance in ecommerce initiative, there is less opportunity for the firms to hide the cost structure and therefore have low future post ante bargaining power. Firms in partnership are motivated by this plight to undercut their initial investments in IT that supports the relationship. Hence the returns from such investment could be low. We hypothesize that:

Hypothesis 9: The abnormal return attributed to the announcements of Joint ecommerce initiative is not different from zero.

Innovativeness Variable

We have indicated in previous discussion that investors reward IT initiatives that have strategic intent. Thus *Transformational* investments are looked at as positive while non-transformational are not. When firms undertake ecommerce initiatives that change strategic direction or introduce new business opportunities and or new markets, investors translate that move as strategic and that it represents the desire to enhance the business value of the firm. We therefore hypothesize that:

Hypothesis 10: The abnormal return attributed to the announcements of Transformational ecommerce initiative is positive.

When firms make non-transformational investments, there is no strategic intent associated with such movements. Investors will not see greater benefit and may doubt its potential to transform business activities and enhance future business value. Thus *Non-transformational* investments or what is refereed to as *Executional* ecommerce initiatives would not create value for the firm. Hence, we put forward the following hypothesis:

Hypothesis 11: The abnormal return attributed to the announcements of Executional ecommerce initiative is not different from zero.

5.3 Data Description

Our data consists of 946 ecommerce announcements. For each event we read the announcement and assign it one of the predetermined categories for each of the five organizational variables. We describe the source of data and coding of the data for regression analysis and the DT induction.

5.31 Data Collection

Like Subramani and Walden (2000), we collected data on the announcements of ecommerce initiatives. Our data set, however, expands from 1998 through 2003. This allows us to test the incomplete contract theory on ecommerce investments for longer period rather than the short period that was studied by Subramani and Walden (2000). Our sources of data are PR Newswire and Business Wire using the online search features

of Lexis-Nexis. We use the search terms launch or announce which appear in the same sentence as the words online or ecommerce and ".com."

Over 12000 potential events were generated from the query. However, some of the events were eliminated for reasons shown in the Table 26. If the same announcement was repeated in the same media or multiple media, we kept only the first announcement. We also eliminated announcements that were confounding such as earning announcement around the event date. In addition only publicly traded firms and those with data in the CRSP database and with prices listed in the periods used for estimating market returns were included. We classify each of the 946 cases into one of the two categories of the five organizational variables. The detailed coding mechanism that follows Subramani and Walden (2002) is presented below. We also provide in the Appendix 6 a sample announcement and show how each categorical variable was coded.

Table 26: Selection Criteria for the Ecommerce Announcements

Criterion	**Reduction in Event size**	**Remaining Event size**
Initial Number of Events	0	1405
Repeated Announcement	48	1357
CRSP data availability	372	985
Sufficient data for estimating returns (120 day estimation window)	29	956
Confounding event – e.g., earning announcements	10	946

Firm Type

The *Firm Type* predictor variable was coded the same way we coded the *Firm Type* variable for the Internet security breach sample. For the regression analysis *Net* firms were coded as 1 and *Non-Net* coded as zero.

Customer Type Variable

For the *Customer Type* variable, our focus is on the initiative rather than the revenue generation. Hence if the value creation is primarily geared towards a business entity we coded that initiative as *B2B* whereas an initiative that promises value creation for the individual consumer is coded as *B2C*. For the regression analysis, B2B initiatives were coded 1 and *B2C* as 0.

Product Type Variable

As we discussed in an earlier section, *Digital* goods have low production cost and include products generated by computers and can be downloaded from the Internet. Products that are not available for downloads and are not available for use on the Internet are coded as *Tangible*. For regression, *Digital* products were coded as 1 and *Tangible* products as 0.

Governance Variable

If the announcement involved one business entity we coded it as *Unilateral*. We coded an announcement as *Joint* if two or more firms were involved through some kind

of partnership or alliance. *Joint* initiatives were coded as 1 and *Unilateral* initiatives coded as 0.

Innovativeness Variable

An announcement that portrays a firm or alliance making strategic investments such as moving into new lines of business or adopting new business models were coded as *Transformational.* Announcements that show some minor strategic changes or modifications were coded as *Executional. Transformational* initiatives were coded as 1 and E*xecutional* initiatives as 0 for the regression analysis.

5.3.2 Data Mining Predictor Variables

We use the five organizational variables: *Firm Type, Customer Type, Product Type, Governance,* and *Innovativeness* described above as our potential predictor variables for the DT induction. The CAR obtained from the Eventus ® software analysis is used as the target variable for the DT induction. Here we compute the test of difference in proportion for each sibling rule for the independent variables. This is used to statistically validate that a variable is a predictor, i.e., the difference in the impact of the different categories within the variable did not occur by chance.

5.4 Results & Discussions

We present our findings on both regression and DT induction for ecommerce initiatives. We compare the DT and regression results. We also compare our results to prior research with respect to both the overall sign of CAR when there is an announcement of ecommerce initiative, and also with respect to the predictor variables. We discuss how existing ecommerce theories can be used to explain the relationships between CAR and the predictor variables.

5.4.1 Cumulative Abnormal Returns

Table 27: Cumulative Abnormal Return for Ecommerce Sample

Panel A: Cumulative Abnormal return for 3-day

Days	Cumulative Average Abnormal Return		Z	Positive: Negative	Generalized Sign Z
	Equally Weighted	Precision Weighted			
(-1, +1)	1.83%	1.24%	5.844***	497:449	4.085***

Panel B: Abnormal Return for each of the 3-days in the event window

Days	Average Abnormal Return	Z	Positive: Negative	Generalized Sign Z
-1	0.37	1.115	452:494	1.149
0	1.60	7.699****	505:441	4.607***
1	-.14	1.309$	447:499	0.823

$, (,) significant at .10 *, <, > significant at .05

****, <<, >> significant at .01 ***, <<<, >>> significant at .001**

The CAR for the 3-day event window (-1, 1) is positive and significant at the 1% level (See Panel A of Table 27). We note that for the 3-day event window, the ratio of positive to negative events is greater than 1 (497:449) supporting the hypothesis that the announcements of ecommerce initiatives in the public media lead to positive CAR. The results also show that the return a day before and a day after the event date were not significant at the 5% level (See Panel B of Table 27). An interesting observation therefore, is that the reaction actually occurred on the event date.

Generally, our results were in contrast to other works, where it was reported that a short event window did not produce consistent CAR. Our work show that within 3 days of the event window, the announcement of ecommerce initiative leads to positive CAR and that the abnormal return is attributable to the announcement, and does not occur by chance. For 3-day event window, the CAR for the 946 events is about 1.83% and is significant.

5.4.2 DT Induction Results

For each predictor variable, we present the rule set that depicts the variable as a discriminating subject variable. We also perform statistical test to verify that the difference in the proportion of sample cases assigned to the abnormal and normal classes did not happen by chance. Specifically we perform difference in proportion test. Only those rules that are significant at the 5% level are shown in Tables 28, 31, 33, and 34. A list of other relevant rules is presented in Appendix 4.

Innovativeness

Table 28: Sets of Rules that include *Innovativeness* as a Discriminating Predictor

Source	Rules	**Statistical testing Results/Comments**[13]
DT_E	IF **Innovativeness** ='TRANSFORMATIONAL' N = 212 **CAR**: {POSITIVE: 78.8%; NEGATIVE: 21.2%)	Statistically Significant **p-value**: <0.001
	IF **Innovativeness** ='EXECUTIONAL' N = 136 **CAR**: {POSITIVE: 34.6%; NEGATIVE: 65.4%)	This pair of rules together suggests that the probability that a *Transformational* initiative leads to positive CAR is over twice that of *Executional* initiative having a positive CAR (i.e., 78.8%: 34.6%).

The results show that *Transformational* ecommerce initiative has high probability of positive CAR than *Executional* initiative. In particular, the likelihood of normal CAR for *Executional* initiatives is far higher than corresponding positive CAR for *Executional* initiative. In fact, Table 33 illustrates cases where the likelihood of *Executional* initiative to be normal are 90%, 95.5% and 100%. These are situations, where it is highly likely that the initiative will not create any market value. In essence, the findings of the DT induction with respect to the *Innovativeness* predictor variable are consistent with the incomplete contract theory. Investors reward *Transformational* initiatives but not *Executional* initiatives.

[13] The results of the difference in proportion test for all the organizational variables is presented in Table 35.

The results also affirm prior research that has used transformative IT models (e.g., Dehning et al. 2003) to show that *Transformational* investments are rewarded more than *Executional* investments. The claim also agrees with the those that have discussed the intangible assets and complementarity theory (Brynjolfsson et al. 1998) and more recently the theory of primacy of intangible assets (Subramani and Walden 2002) where the investments in complementary assets, here the intangible assets such as business process and new sets of supplier relationships, determine the business value of a firm's IT initiative. All these theories in summary suggest that firms that make *Transformational* IT investments have plans to make complementary investments in intangible assets such as improvement in buyer-supplier relationships, business process enhancements and human resource management improvements that seek to support IT investments. Our results support the view that investors would look at such investments and recognize the future market value that the investments are likely to result and therefore reward such firms.

We are unable to use the resource based view theory to explain the observed CAR and innovativeness variable, because the theory requires that IT be used before we can realize value. Since our period of analysis is for short event window, the theory is not applicable. It must be noted that this should not be regarded as negative. The problems with productivity paradox are minimized with a short event window, and confounding events are minimized. Since the overall CAR for the events was highly significant (at 1% significant level) for the day of the event, our results are very reliable.

Table 29: Strong Individual Rules that include *Innovativeness* as a Predictor

Source	Rules
DT_E	IF **Innovativeness** ='TRANSFORMATIONAL' N = 212 **CAR**: {POSITIVE: 78.8%; NEGATIVE: 21.2%) IF **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'JOINT" N = 97 **CAR**: {POSITIVE: 84.3%; NEGATIVE: 15.7%)

Product Type

Table 30: Strong Individual Rules that include *Product Type* as a Predictor

Source	**Rules**
DT_Gt	IF **Firm Type** = 'NET' & **Customer Type** ='B2B' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 22 **CAR**: {POSITIVE: 0%; NORMAL: 100%)

None of the rules that include *Product Type* as a discriminating variable was statistically significant even at the 10% level. The difference in proportion for the *Product Type* variable was not statistically significant. Hence *Product Type* was not statistically established to be a predictor of CAR in ecommerce initiatives. However, we see in Table 30 that *Product Type* participates in a strong rule where the initiative is *Executional.* Particularly, the *Product Type* serves as conditional variable where *Firm Type* is a discriminating predictor.

We can say from Table 30 therefore that *Product Type* may not be used for testing the relationship with CAR but then it may play a role as a moderating variable where the intermediate variable however impact CAR.

Table 31: Sets of Rules that include *Governance* as a Discriminating Predictor

Source	Rules	**Statistical Testing Results/Comments**
DT_E	IF **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'UNILATERAL' N = 115 **CAR**: {POSITIVE: 74.7%; NORMAL: 25.3%) IF **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'JOINT' N = 97 **CAR**: {POSITIVE: 84.3%; NORMAL: 15.7%)	Statistically Significant **p-value** = 0.04 This pair of rules together suggests that *Governance* is a predictor of CAR if the *Innovativeness* variable is *Transformational*. In this conditional situation, *Joint* initiative is more likely to lead to positive CAR than *Unilateral* initiative.

While the difference in the likelihood of abnormal return for *Unilateral* and *Joint* is relatively small (see Table 31), it is statistically significant at the 5% level. For *Transformational* investments, *Joint* is more likely to have positive CAR than *Unilateral.* The relationship between *Governance* and CAR is conditioned on whether the *Innovativeness* variable is *Transformational. Executional* initiatives are more likely to lead to negative CAR. Firms that undertake *Executional* ecommerce initiatives should not

expect market value increase, because it seems that investors do not recognize the market potential of such moves.

What we observe is that we cannot use the incomplete contract theory alone to explain our findings with *Governance* and CAR. The *Governance* variable has impact on CAR provided the initiative is *Transformational*. Thus we use the *Transformational* IT investments theory and the intangible assets theory to suggest that when firms make strategic investments, it is necessary that they also make complementary investments in intangible assets. Such complementary investment needs to be communicated or implied before the *Governance* variable becomes important. Once these conditions are established by the firm or that the investor gets such an understanding then an initiative through strategic *Joint* alliance has higher likelihood of positive CAR than *Unilateral* ecommerce initiative.

Even with the conditional variables, our finding does not support the incomplete contract theory that suggests that *Unilateral* investments promise higher post ante bargaining power than *Joint* investments. For the incomplete contract theory to be true with our data, CAR for *Unilateral* initiative should be higher than that of *Joint* initiative. We can state that the intangible asset theory and complementarity theory are more effective for explaining the business value of ecommerce initiative with respect to *Governance* than the incomplete contract theory provides.

Table 32: Strong Individual Rules that include *Governance* as a Predictor

Source	Rules
DT_E	IF **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'JOINT' N = 97 **CAR**: {POSITIVE: 84.3%; NORMAL: 15.7%)

In Table 32, *Governance* is part of a strong rule and although *Governance* is not the subject variable, it is likely to be a predictor and the likelihood of this rule leading to positive CAR is about 84.3%. This rule supports the intangible asset theory and the complementarity theory but does not say anything about the incomplete contract theory. Basically, *Joint* initiative requires that firms that form partnership put resources together for an initiative that both believe would generate mutual benefits.

The incomplete contract theory, on the other hand, suggests that with the *Joint* alliance, firms have less post ante bargaining power and are motivated to reduce their initial investments thereby preventing them from providing the necessary infrastructure to support the initiative and the corresponding complementary intangible assets. What the incomplete contract does not address is whether the initiative is *Transformational* or not. Hence we cannot assert that our findings refute or support the incomplete contract theory. What we can say though is that for *Transformational* ecommerce initiatives, the incomplete contract theory is not confirmed by our data. Further, we can state that because of the interaction of the independent variables, the incomplete contract theory is unable to explain the relationship between *Governance* and CAR.

Table 33: Sets of Rules that include *Firm Type* as a Discriminating Predictor

Source	Rules	Statistical Testing Results/Comments
DT_Gt	IF **Firm Type** = 'NON-NET' & **Customer Type** ='B2B' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 22 **CAR**: {POSITIVE: 4.5%; NORMAL: 95.5%) IF **Firm Type** = 'NET' & **Customer Type** ='B2B' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 22 **CAR**: {POSITIVE: 0%; NORMAL: 100%)	Statistical Significant **p-value:** < 0.001 This pair of rules suggests that *Firm Type* is a predictor when innovativeness is *Executional*. *Net* firms are more likely to suffer from value creation when they make *Executional* ecommerce initiatives than *Non-Net* firms.

What Table 33 shows is that *Executional* ecommerce investment is highly likely to result in normal CAR. In particular, when *Governance* is *Joint*, *Product Type* is *Digital*, *Customer Type* is *B2B*, and *Innovativeness* is *Executional*, *Net firms* are more likely to have normal return than *Non-Net firms*. Although the difference in the proportion of cases that fall into the normal class for *Net* and *Non-Net* firms is small (100 vs. 95. 5%) respectively, it is significant at the 5% level. When the conditions upon which *Firm Type* variable has impact on CAR are satisfied, *Net* firms have higher probability of recording normal return than *Non-Net* firms. The incomplete contract theory proposes that ecommerce initiatives by *Net* firms result in positive CAR while those by *Non-Net* firms have normal returns, i.e. have no impact on CAR. *Executional* initiatives made by *Net* firms are more likely to result in negative CAR.

Generally, the strategic intent of *Net* firms and the strategic direction of ecommerce initiatives are in line. Hence, announcing strategic direction that brings minor

changes would not be considered by investors as activity that can create business value. However, *Executional* ecommerce investments may be made by *Non-Net* firms to support traditional operations. While investors could still be skeptical about such moves, they present better opportunities than *Executional* ecommerce investments by *Net* firms.

We can also use the intangible asset theory to explain that minor changes to strategic ecommerce investments do not present the opportunity to make investments in intangible assets to support such direction. Hence, investors would react negatively to investments that do not promise high firm returns. Further, Investors could be less forgiven to *Non-Net* firms because they may create strategic ecommerce initiative to support their brick and mortar operations.

Table 34: Sets of Rules that include *Customer Type* as a Discriminating Predictor

Source	**Rules**	**Statistical Results/Comments**
DT_E	IF **Customer Type** = 'B2B' & **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'UNILATERAL'& **Firm Type** = 'NET' N = 58 **CAR**: {POSITIVE: 81.7%; NORMAL: 19.3%) IF **Customer Type** = 'B2C' & **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'UNILATERAL'& **Firm Type** = 'NET' N = 28 **CAR**: {POSITIVE: 60.9%; NORMAL: 39.1%)	Statistically Significant **p-value:** 0.024 This pair of rules together suggests that customer type is a predictor if the initiative is *Transformational*, *Governance* is *Unilateral* and *Firm Type* is *Net*. *B2B* has high likelihood of positive CAR than *B2C*.

Once a *Transformational* ecommerce investment is made, we observe that initiative that is geared towards *B2B* customers is more likely to generate value. This is in direct contrast to the incomplete contract theory where we expect B2C firms that can enjoy post ante bargaining power to be more likely to receive positive response from investors because they promise future returns.

5.4.3 Summary of DT Induction

Our results reveal that the incomplete contract theory by itself does not offer effective explanation for the relationship between organizational variables and CAR as a result of the announcements of ecommerce initiative. The relationship between the organizational variables and CAR involves conditional interactions between the independent variables. Even when those conditions exist, the incomplete contract theory does not offer explanation for *Governance, Firm Type, Product Type* and *Customer Type* variables. The only variable that the incomplete contract theory is in agreement with is the *Innovativeness*. In particular we find that the predictor variables impact on abnormal return is through interaction of the independent variables.

Our research supports the findings that strategic investment is necessary if the firm expects to create value from that initiative. In particular, within the period of announcement, *Transformational* investments present far higher opportunities for the firm to increase its market value. We show that the *Customer Type* variable and

Governance variable are related to *Transformational* investments while the *Firm Type* and *Product Type* variables influence *Executional* initiatives.

Table 35: Results of the Difference of Proportion Test

Variable	Z	Probability	Significant at 5% level?
Innovativeness	8.926374	<0.001	Yes
Governance	1.750425	0.04	Yes
Firm Type	21.60761	<0.001	Yes
Customer Type	1.975849	0.024	Yes
Product Type	1.103194	0.13	No

Table 35 shows the results of the statistical test of difference of proportions for the organizational variables. Only the *Product Type* variable is not statistically significant at the 5% level and therefore not statistically established to be predictor of CAR for ecommerce initiative announcements.

5.4.4 Summary of Regression Results

Table 36: Regression Models for Ecommerce Initiative

Panel A: Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Firm_Type	946	0	1	.22	.411
Product_Type	946	0	1	.57	.496
Customer_Type	946	0	1	.53	.500
Governance	946	0	1	.63	.484
Innovativeness	946	0	1	.40	.490
CAR	946	-174.00	325.00	1.7359	21.03198
Valid N (listwise)	0				

Panel B: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.216(a)	.047	.042	20.59047

Predictors: (Constant), Innovativeness, Firm_Type, Governance, Product_Type, Customer_Type

Panel C: ANOVA (b)

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	19486.097	5	3897.219	9.192	.000(a)
	Residual	398529.338	940	423.967		
	Total	418015.434	945			

Predictors: (Constant), Innovativeness, Firm_Type, Governance, Product_Type, Customer_Type
Dependent Variable: CAR

Panel D: Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-.894	1.596		-.560	.575
	Firm_Type	-1.550	1.636	-.030	-.947	.344
	Product_Type	-3.143	1.463	-.074	-2.147	.032
	Customer_Type	.264	1.455	.006	.182	.856
	Governance	1.521	1.395	.035	1.090	.276
	Innovativeness	9.117	1.408	.213	6.476	.000

a. Dependent Variable: CAR

The results of the regression analysis show that only two of the predictor variables are significant at the 5% level: *Innovativeness* and *Product Type (*See Table 36 Panels A-D). The *Product Type* variable shows that *Tangible* products have higher CAR than *Digital* products. The *Innovativeness* variable also predicts that *Transformational* initiatives have far higher CAR than *Executional* initiatives. For the *Innovativeness* variable, the incomplete contract theory is supported by our data. What is different is that the regression analysis does not provide any evidence that the impact of the organizational variables on CAR is conditioned on the *Innovativeness* variable.

5.4.5 Comparison of Regression and DT Induction Results

Table 37: Comparative Analysis of Regression and DT Results

Variable	Hypothesis	Variable established as a Predictor?	
		Regression	Decision Tree Induction
Firm Type	H2 H3	Statistically established Not to be a predictor	Statistically established to be a predictor
Customer Type	H4 H5	Statistically established Not to be a predictor	Statistically established to be a predictor
Product Type	H6 H7	Statistically established to be a predictor	Statistically established Not to be a predictor; Evidence, however, suggests that it can be a predictor
Governance	H8 H9	Statistically established Not to be a predictor	Statistically established to be a predictor

Innovativeness	H10 H11	Statistically established to be a predictor	Statistically established to be a predictor

Table 37 depicts how only two of the independent variables: *Product Type* and *Innovativeness* are found to be predictor variables. However, for the decision tree induction all five organizational variables are found to be predictors although the *Product Type* variable is not statistically established to be predictor.

Table 38: Justification of Results of DT Analysis

Variable	**Support for the Incomplete Contract Theory?**	**Justifying Comments**
Firm Type	*No*	The incomplete complete contract theory suggests that *Net* firms will have higher CAR than *Non-Net* firms. Prior research also shows that *Net* firms have high CAR than *Non-Net* firms. However, the incomplete contract theory makes no assumption of strategic *Transformational* investments which our data depicts. Second, *Net* firms are expected, according to the incomplete contract theory, to use the post ante bargaining power to generate more funds and thereby increase market value. However, this is not what was

		observed. The intangible asset theory and complementarity theory can be employed to effectively explain the findings.
Customer Type	*Yes*	The results are in contrast to what the Incomplete contract theory predicts. Even though *B2B* firms had higher CAR than *B2C* firm supporting some of the prior research, the results of this study show that the relationship is dependent on conditional variables which prior research did not show. Perhaps the study whose result is in close proximity to our study in terms of the findings is that by Subramani and Walden (2002) where they develop the theory of primacy in intangible assets.
Product Type	*No*	The difference in proportion for the *Product Type* variable was not statistically significant. Hence *Product Type* was not statistically established to be a predictor of CAR in ecommerce initiatives. However, we note that *Product Type* plays a role in a strong rule where the initiative is *Executional*.
Governance	*No*	The incomplete contract theory suggests that *Unilateral* initiative will have higher CAR than *Joint* but this was not the case with our data.
Innovativeness	*Yes*	Incomplete contract theory suggests that *Transformational* initiative will have

		higher CAR than *Executional*. This was observed in the data set. The result is also in agreement with prior research and ecommerce theories. In fact it is observed that the *Innovativeness* variable is the most important variable as it occurs at the root of the DT.

For the *Product Type* variable the incomplete contract theory is confirmed by the regression results. However, with respect to the DT induction, we see that the *Product Type* variable is only a predictor when the investment is *Executional*. We have discussed how investors do not reward *Executional* investments. What is interesting is that *Digital* products are involved with the strong rule where *Firm Type* is the discriminating variable. What we observe is that when *Net* firms are involved with initiatives that are *Executional* and *Digital*, they do not reap market value. Thus *Net* firms are expected to invest in *Transformational* initiatives.

5.4.6 Comparison with Results of Previous Research

Table 40 compares the results of the current study with those of relevant prior research. Specifically, we show how our study confirms some of the findings of prior research and how our study present new findings that have not been identified by the regression models used in prior research. The short term event window is also found to be

useful for examining abnormal returns resulting from the announcements of novel technologies such as ecommerce.

Table 39: Comparison of Results of This Study vs Previous Studies

Author (s)	Period of Analysis	Variables	Some Major Findings	This Study
Subramani and Walden (1999)	10/1998 – 12/1998	Firm Type, Customer Type[14]	o Firms reported CAR of 3-11 % within event window o Results on difference in CAR between *Net* and *Non-Net* firms did not support hypothesis o CAR for *B2C* was greater than those of *B2B* supporting hypothesis	o CAR of 1.83% was observed over the 3-day window showing that short event window is appropriate for assessing ecommerce investments o Most of the market reaction took place on the announcement day
Subramani and Walden (2000)	10/1998 – 12/1998	*Product Type* (*Digital* v. *Tangible*), *Firm Type*	o CAR for *Net* firms are significant and those of *Non-Net* are not o There is no significant difference	o CAR for *Net* firm is more normal o For *Transformational* investments, there is no significant difference in CAR for *Net* and non *Net* firms

[14] Firms are classified as either B2B or B2C.

			between firms engaged in *Tangible* v. *Digital* goods	
Subramani and Walden (2001)	10/1998 – 12/1998	Firm Type, Customer Type	o CAR for *Tangible* goods are higher than those of *Digital* goods o *Firm Type* results are similar to 1999 study	o *Product Type* is not established statistically as predictor of CAR o *Firm Type* is not predictor for *Transformational* ecommerce but for *Executional*, *Net* firms are more likely to have normal return than *Non-Net* firms
Dehning et al. (2004)	1/1998 – 6/2002	Firm Type, Customer Type, Time lag (2000 v. 1998)	o CAR for *Digital* goods is higher than that of *Tangible* in 2000 but not in 1998 o CAR is not significant in 2000 but in 1998; *B2B* has higher CAR in 1998	o *Product Type* is not established statistically as predictor of CAR o *Product Type* is only a predictor in a strong rule which means that it can be a moderating predictor for executional initiatives
Subramani and Walden (2002)	1/1998-12/2000	Firm Type, Customer Type, Product Type, Governance, Innovativeness	o Results for short event window are not consistent o Results for long event window (1 year) are consistent o CAR for *Net*	o Short time event window provides understanding for ecommerce initiatives (novel technology) o Results on *Transformational* ecommerce is consistent with prior research; however,

			firm is 11.38% o CAR for B2B is 20.55% o CAR for tangible is 13.39% o CAR for transformational is 11.43%	we show that other variables are predictors (*Customer Type, Governance*) only when initiative is *Transformational* o *Product Type* is only a predictor in strong rules which means that they can be moderating predictors for *Executional* initiatives o *Product Type* is not statistically established to be predictor.

5.5 Theoretical Propositions

In this section, we present a theoretical model that represents the relationships between the independent variables and CAR as well as the interaction between the independent variables that result in intermediate variables that ultimately impact CAR.

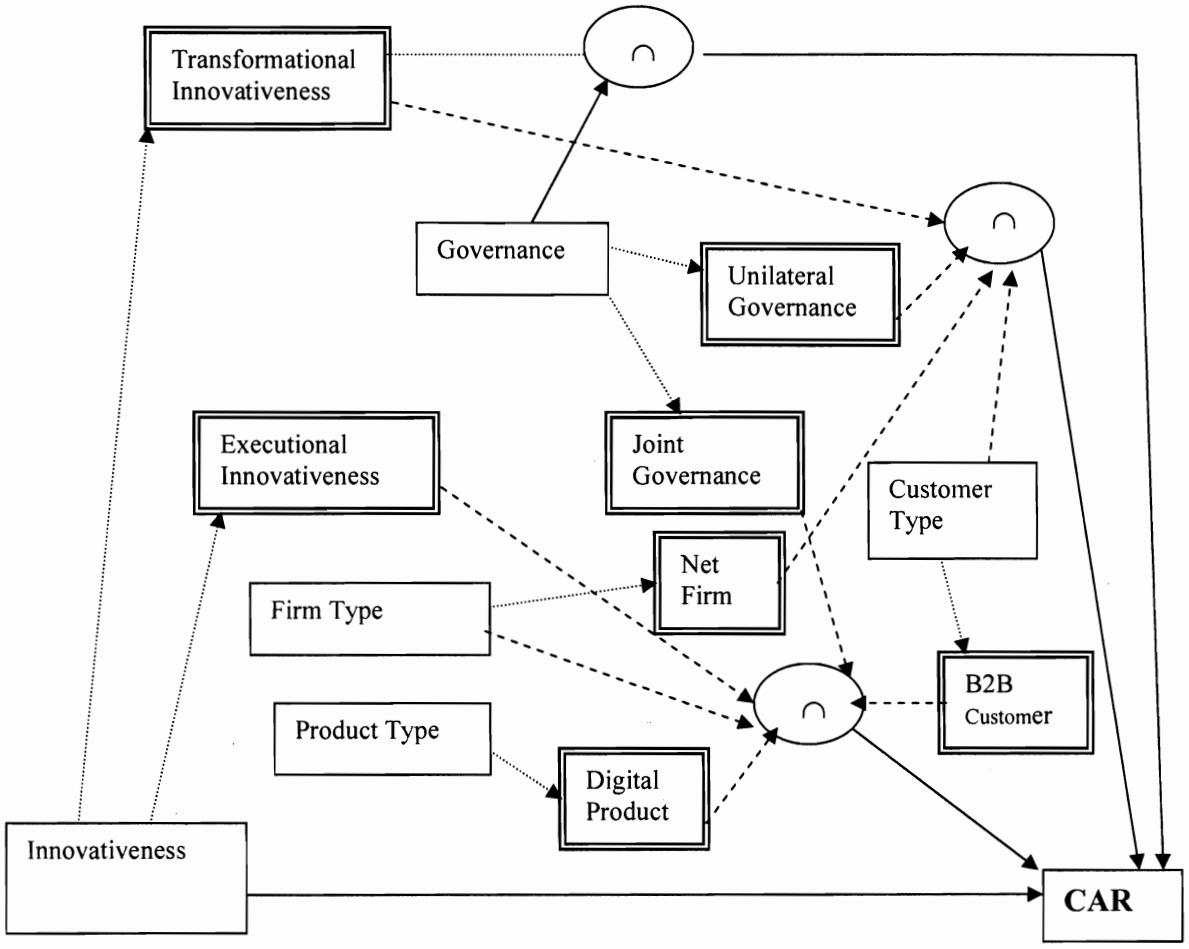

Figure 17: Theoretical Model Representing Relationship between Organizational Variables and CAR for Ecommerce Initiative

Figure 7 is the legend for Figure 17. In the following we describe the relationships for each of the predictor variables. These relationships include the direct relationship with CAR as well as the interaction among the predictor variables.

Innovativeness

Innovativeness is the only organizational variable that has direct impact with other independent variables. In particular, we note that *Transformational* initiatives are more likely to have positive impact on CAR than *Executional* investments.

Governance variable

For *Transformational* initiatives, *Governance* is a predictor variable. Thus the *Transformational* initiative and *Governance* interact to produce an intermediate that impacts CAR. Thus for the interaction, *Governance* is a discriminating predictor when the conditional variable is *Innovativeness* where the specific subtype or subcategory is *Transformational.*

Customer Type

For *Transformational* initiative, *Customer Type* is a discriminating predictor when *Governance* is *Unilateral* and *Firm Type* is *Net.* For these conditions, *B2B* initiatives are more likely to have positive impact on CAR.

Firm Type

For *Executional* initiative, *Firm Type* is a discriminating predictor if *Governance* is *Joint*, the *Product Type* is *Digital* and *Customer Type* is *B2B*. In this case, *Non-Net* firms are more likely to have positive impact than *Net* firms. Conversely and more

correctly, *Net* firm are more likely to have normal return (no impact or more likely to have negative impact) on CAR.

Product Type

Product Type is only a part of *Firm Type* conditions and does not serve a role as a discriminating predictor as it was not established statistically to be a predictor of CAR.

Summary

Recall that when an independent variable plays a discriminating role, then such a variable has direct relationship with the dependent variable which in this case is CAR when there is no conditional variable in the rule. From this we note that only the *Innovativeness* variable has direct relationship with CAR. We can however, develop set of hypothesis from the interaction between the independent variables that may generate intermediate moderating variables and test such interactions on different samples.

Through DT induction, we confirm what existing ecommerce theories say concerning the market value of ecommerce investments. Specifically, we show that *Transformational* ecommerce initiatives are more likely to have positive CAR than *Executional* ecommerce initiatives. We also propose that for *Transformational* initiatives, *Firm Size* and *Governance* are relevant predictors whereas *Product Type* and *Firm Type* are predictors when the initiative is *Executional.* We also propose that there are relationships between the independent variables that can be tested.

CHAPTER 6
CONCLUSION

The event study methodology has been accepted as an appropriate approach in the Information Systems discipline for assessing the market value of business activities. This approach is based on the efficient market hypothesis that asserts that capital markets are efficient mechanism for processing information about firms and that investors use available information about firm's activities to assess the current and future value of firm. Typically, an event study has two main goals, to determine whether an announcement in the public media results in abnormal returns, and to examine the factors that determine the abnormal returns.

Traditionally, regression analysis is used for achieving the second goal. However, in some cases it is difficult to determine all the hypotheses that need to be tested. Prior research indicates that the use of decision tree induction and regression together provides better understanding in data analysis. Motivated by this finding, we propose that an integrative approach be used in examining the determinants of abnormal return in event study. We instantiate this proposal using two business activities that have importance to researchers as well as practitioners: Internet security breach and ecommerce initiative.

For the Internet security breach, we use a set of variables from the literature on firm characteristics and a set of theory-based factors that represent attack characteristics to develop some theoretical propositions on how attack and firm characteristics determine

damage to the breached firm where damage is operationalized as the observed cumulative abnormal return over the event window.

For the ecommerce analysis, we employ organizational variables from the literature to assess the impact of the ecommerce investments on the market value of the firm. We use the incomplete contract theory to develop the hypotheses. Our findings suggest that the incomplete contract theory is unable to effectively explain the findings of our empirical analysis. The combination of several ecommerce theories however, is able to provide better explanation. We also observe that the relationship between the organizational variables and CAR is complex and involves conditional interactions among the independent variables. Our results also show that *Transformational* ecommerce investments are more likely to lead to higher CAR than *Non-Transformational* investments (*Executiona*l).

The interaction between the *Innovativeness* variable, of which *Transformational* and *Executional* are the two categories, is a direct relation. The findings support the incomplete contract theory. The finding is also in line with those of some of the previous event studies on ecommerce and other IT-strategy research that showed that investors reward *Transformational* IT investments more than they do for *Non-Transformational* IT investments. We note that *Product Type* and *Firm Type* variables are predictors only for *Executional* initiatives. While the *Firm Type* variable plays a discriminating role, the *Product Type* variable only participates in a strong rule. Initiatives involving *Net* firms are more likely to lead to normal return when the initiative is *Executional.*

For the Internet security breach, our results show that both attack and firm characteristics influence damage where damage is operationalized as the observed CAR. This is the first time a single study has shown both attack and firm characteristics to be determinants of abnormal return. We present theoretical propositions on the variables that have direct impact on damage and those that interact with each other to possibly create intermediate nodes or intermediate variables that subsequently impact damage. We also show that confidentiality, integrity and availability are all important when considering the impact of security breach on firms. This provides additional insight into prior research that suggested that confidential information is what needs to be protected.

We have shown that the integrative approach provides additional insights than traditional regression model alone provides. The proposed approach is applicable in other business research.

6.1 Answers to the Research Questions

In this section, we present in Table 41 how our research answers the research questions presented in Chapter 1. The details of the results to the research questions have been discussed in the results sections of the paper.

Table 40: Answers to the Research Questions

Question #	Question	Answer	Comments
1	Does the announcement of Internet security breach in the public media lead to negative abnormal return?	Yes	Within 3-day of the announcement firms on the average lost 3.18% of their market share. This was found to be significant at the 1% level
2	Does the announcement of ecommerce initiative in the public media lead to positive abnormal return?	Yes	Within the 3 day event window firms on the average gain 1.83% market value. It is also found that most of the reaction occurred on the actual day of announcements. This is very interesting for several reasons. Some of the prior research had argued that investors may not have all the information necessary to make decisions on the future firm performance within such a short period. Our results state otherwise enhancing the efficacy of the short term event window. It also reflects how the event study method continues to validate the efficient market hypothesis.
3	Using the Internet security	Yes	The regression models

	breach sample data, does the use of Decision Tree Induction provide additional insight that is not presented by regression models?		identified only two of the potential predictor variables as variables that actually influence the observed CAR. Using DT induction, we recognize that three variables have direct relationships with CAR, i.e. damage and that the other variables although do not have direct relationship with damage have interactions with other independent variables by which the impact on CAR can be measured. This also suggests that while some of these independent variables have global impact, others have local impact, i.e., certain conditions have to be favorable for other independent variables to have impact on damage to the firm.
4	Using the ecommerce sample data, does the use of Decision Tree Induction provide additional insight that is not presented by regression models?	Yes	Here the regression models suggest that two variables are predictors of CAR. However, the DT induction shows that all the five organizational variables affect CAR except that they do not directly impact CAR. The only variable that has direct

			impact with CAR is *Innovativeness* and that when the Innovativeness is *Transformational* then the other variables influence CAR. In fact, *Product Type* and *Firm Type* are related to CAR through *Executional* initiatives.
5	Do theory-based factors enhance the understanding of the determinants of CAR for Internet security breach announcements?	Yes	Using Howard Taxonomy as our theoretical model for assessing the impact of Nature of attack on damage, we notice that both attack and firm characteristics are determinants of abnormal returns. We also show that the *Results* variable in Howard's taxonomy is related to Confidentiality, Integrity, and Availability, the three tenets of Information Security. Based on this relationship, we have shown that firms suffer damage if any of the three tenets of Information security are violated. This finding indicates that any violation of the three tenets of information security leads to damage. This is different from what has been

			reported in the literature where it was observed that only confidential information needs to be protected.
6	Does the incomplete contract theory effectively explain the relationship between CAR and organizational variables?	No	The incomplete contract theory is unable to effectively explain the relationship between the organizational variables and CAR, i.e., firm value. We employed additional theories to provide explanation for the behavior of investors to the announcements of ecommerce initiative.

6.2 Limitations of the Study

We examine some of the limitations of our study in this section. One of the problems with performing an event study on Internet security breaches is that of sample size. While firms are eager to make public e-commerce initiatives, the same is not true for Internet security breaches. Although one may consider the sample size of 41 used in the current study to be small, it is greater than the size of events that Campbell et al. (2003) and Hovav and D'Arcy (2003) used. Nevertheless, a large sample size would enhance the validity of the findings. In future research, a larger sample is being sought by looking at other news sources that have not been used in the current and prior studies.

Further, in the future, we would like to enhance Howard's taxonomy to provide better understanding of the impact of the attacker's *Objective* on firm damage. The impact of *Hackers* on firm damage is far more than one would expect requiring that the categorization be reviewed.

Another limitation of both the Internet security and ecommerce studies is with respect to the coding. Only one person read and coded all the events and so it was not possible to compare the coding results. However, the samples were done in batches (100 samples a week) so that the coder was able to revise what was done previously as he gained better understanding through the coding process. We also followed Subramani and Walden's coding scheme.

6.3 Implications for Research and Practice

This research makes theoretical, methodological and practical contribution in several ways. First we have demonstrated how data mining techniques can be used to provide insights that regression models alone may not present. Using Internet security and ecommerce as two case situations, we have shown that data mining techniques can be employed in event studies in general. To the best of our knowledge, this is the first time DT induction approach has been used in studying factors that influence abnormal returns in an event study research. Clearly, there is value in the use of DT induction in the Internet security and ecommerce domains. Thus we have shown that the DT induction employed in this paper has wide applicability in event studies in general.

From a theoretical point of view, we have used the decision tree approach, and theoretical models from the literature, to provide a more comprehensive model of attack and firm characteristics that determine damage to the firm when Internet security breach announcements are made in the public media. This is important because, although research into the technical and organizational aspects of information security breaches have received some attention, economic considerations related to security breaches have been largely overlooked (Gordon and Loeb 2002). There has been a limited emphasis on understanding the relationship between Internet security breaches and market value of the firm.

In summary, we have made the following contributions to research. First, we have extended existing theory on Internet security breaches by introducing new factors that predict abnormal (negative) returns of breached firms, i.e., using the Internet security classification scheme developed by Howard (1997), we establish new factors related to the security incidents that influence the abnormal returns of breached firms. We have shown that confidentiality, integrity and availability are critical in ensuring system security and that comprise of data/information confidentiality, integrity, or availability would lead to damage of the breached firm. Further, we have validated the general findings that announcements of Internet security breaches result in negative CAR on the market value of breached firms. Finally, we have developed a new approach for studying the impact of Internet security breaches on the market value of the breached firms.

The results of regression analysis used in prior event studies for the Internet security breaches domain have the potential to inform organizations on the loss of market

value as a result of the specific factors hypothesized. We argue that other approaches be sought to augment rather than eliminate the use of regression analysis as decision models for Internet security breaches. The approach proposed in this paper has immense implications for practice. It can be used as a decision tool in Internet security investment decisions.

We have presented a model that can be tested. Once that is done, the model can be used for practice. Thus for practice, the proposed models have great potential in providing several guidelines in Internet security investment decisions such as: (1) organizations can predict the likelihood of an Internet security breach leading to abnormal (negative) return based on specific firm and attack characteristics; (2) information providing institutions such as CERT/CC can use our model to predict the likelihood of abnormal (negative) return based on firm and attack characteristics that the institutions that seek the knowledge from CERT/CC provide; and (3) the model presents knowledge for businesses as they make risk management and information security investment decisions. As organizations make conscientious efforts to eliminate or reduce Internet security breaches, it would increase consumer confidence in e-commerce activities and assure investors of firm's commitment to secure their business systems which eventually may enhance business activities and improve the stock market performance.

For ecommerce initiatives, we validate ecommerce theories that show that investors reward *Transformational* investment and not *Executional* investments. We also show the effect of the other independent variables on CAR depending on their

conditional interaction. We show that the organizational variables have positive effect on CAR only when the initiative is *Transformational*. Contrary to what the incomplete contract theory proposes, we find that *Executional* ecommerce investments have negative impact on CAR and also *Tangible* products have negative impact on CAR when the initiative is Executional.

6.3 Future Research

It would be interesting to test our proposed integrative approach over a long event window. In future we seek to test some of the propositions that have been made with respect to Internet security breach and CAR and ecommerce and CAR. Future research direction could also look at using the approach in other domains where there is a lack of theoretical models but where sets of categorical variables are found to be related to the dependent variable. Our results suggest that *Hackers* are more likely to have negative CAR than all the other categories of attackers and that *Challenge/Status* is the most likely category of objective to cause damage. This is very startling knowing that attacks involving this type of *Attacker* and or *Objective* should not have received such attention by investors. It makes it more important for Howard's taxonomy to be reviewed to ensure that what the data revealed at that time is still true as investors have gained more knowledge about Internet security breaches than when Howard presented his work.

REFERENCES

Aktas, Nihat, E. de Bodt, and Jean-Gabriel Cousin (2004), "Event study under noisy estimation period," in Eleventh Annual MFS Conference.

Aktas, Nihat, E. de Bodt, and R. Roll (2003), "Market response to European regulation of business combination." Los Angeles, CA.

Amoroso, Edward G. (1994), Fundamentals of computer security technology. Upper Saddle, NJ: Prentice-Hall.

Ansell, J. and F. Wharton (1992), Risk: analysis, assessment and management. Chichester: John Wiley & Sons Ltd.

Applegate, L.M., C.W. Holsapple, R. Kalakota, F.J. Radermacher, and Andrew B. Whinston (1996), "Electronic Commerce: Building Blocks of New Business Opportunity," Journal of Organizational Computing and Electronic Commerce, 6 (1), 1-10.

Axelsson, S. (2000), "The base-rate fallacy and the difficulty of intrusion detection," ACM transactions on information and system security, 3 (3), 186-205.

Ball, R. and P. Brown (1968), "An empirical evaluation of accounting income numbers," Journal of Accounting Research, 6, 159-78.

Barney, J.B. (1991), "Firm Resources and Sustained Competitive Advantage," Journal of Management, 17 (1), 99-120.

Barua, A. and T. Mukhopadhyay (2000), "Information Technology and Business Performance: Past, Present and Future," in Framing the Domains of IT Management: Projecting the Future through the Past. Cincinnati, OH: Pinnaflex Educational Resources.

Barua, A., C.-H Sophie Lee, and Andrew B. Whinston (1996), "The Calculus of Reengineering," Information Systems Research, 7 (4), 409-28.

Baskerville, Richard (1998), Designing information systems security. New York: John Wiley & Sons.

---- (1993), "Information systems security design methods: implications for information systems development," ACM Computing surveys, 25 (4), 375-414.

---- (1991), "Risk analysis: an interpretive feasibility tool in justifying information systems security," European Journal of Information Systems, 1 (2), 121-30.

Bener, Ayse B. (2000), "Risk perception, trust, and credibility: a case in Internet Banking," London School of Economics and Political Sciences.

Berry, Michael J.A. and Gordon S. Linoff (2004), Data Mining Techniques for Marketing, Sales, and Marketing Relationship Management. Indianapolis, IN: Wiley Publishing, Inc.

Bharadwaj, A. (2000), "A Resource-Based Perspective on IT Capability and Firm Performance: An Empirical Investigation," MIS Quarterly, 24 (1), 169-96.

Bharadwaj, A. and M. Keil (2001), "The effects of information technology failures on the market value of firms: an empirical examination," Emory University.

Binder, John J. (1998), "The Event Study Methodology Since 1969," Review of Quantitative Finance and Accounting, 11 (2), 111-37.

Bishop, M (2003), Computer Security: Art and Science. Boston: Addison Wesley.

Blakley, B., E. McDermott, and D. Geer (2001), "Information security is information risk management," in New Security Paradigm Workshop. Cloudcroft, NM.

Bodie, Zvi, Alex Kane, and Alan K. Marcus (2001), Essentials of Investments (Fourth ed.). Boston: McGraw-Hill.

Bodin, Lawrence D., Lawrence A. Gordon, and Martin P. Loeb (2005), "Evaluating Information Security Investments using the Analytic Hierarchy Process," Communications of the ACM, 48 (2), 79-83.

Breiman, L., J. Friedman, R. Olshen, and C. Stone (1984), Classification and Regression Trees. Belmont, California: Wadsworth.

Brickley, J.A., F.H. Dark, and M.S. Weisbach (1991), "The economic effects of franchise termination laws," Journal of Law and Economics, 34 (1), 101-32.

Brown, D.E., L.E. Gunderson, and M.H. Evans (2000), "Interactive Analysis of Computer Crime," IEEE Computer, 33 (8), 69-77.

Brown, S. and J. Warner (1980), "Measuring security price performance," Journal of Financial Economics, 8, 205-50.

---- (1985), "Using daily stock returns: the case of event studies," Journal of Financial Economics, 14, 3-31.

Brynjolfsson, E. and L.M. Hitt (1996), "Paradox lost? Firm-level evidence on the returns to information systems spending," Management Science, 42 (4), 541-58.

Brynjolfsson, E., L.M. Hitt, and S. Yang (1998), "Intangible Assets: How the Interaction of Computers and Organizational Structure Affects Stock Market Valuations," in International Conference on Information Systems. Helsinki, Finland.

Brynolfsson, E. (1993), "The productivity paradox of information technology," Communications of the ACM, 36 (12), 66-77.

Campbell, Katherine, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou (2003), "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," Journal of Computer Security, 11 (3), 431-48.

Cavusoglu, Huseyin, Birenda Mishra, and Srinivasan Raghunathan (2002), "The effect of Internet security breach announcements on market value of breached firms and Internet security developers," in Workshop on Information Systems and Economics. Barcelona.

---- (2004a), "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.

---- (2004b), "A model for evaluating IT security investments," Communications of the ACM, 47 (7), 87-92.

Cert (2004), "CERT/CC Statistics 1988-2005."

Chang, J.C., G. Torkzadeh, and G. Dhillon (2004), "Re-examining the measurement models of success for Internet Commerce," Information and Management, 41 (5), 577-84.

Chatterjee, D., C. Pacini, and V. Sambamurthy (2002), "The shareholder-wealth and trading-volume effects of information technology infrastructure investments," Journal of Management Information Systems, 19 (2), 7-42.

Chatterjee, D., V.J Richardson, and R.W. Zmud (2001), "Examining the shareholder-wealth effects of announcements of newly created CIO positions," MIS Quarterly, 25 (1), 43-70.

Chen, A.H. and T.F. Siems (2001), "B2B eMarketplace Announcements and shareholder Wealth," Economic and Financial Review, 12-22.

Cohen, Fred (1997a), "Information system defences: a preliminary classification scheme," Computers & Security, 16, 94-114.

---- (1997b), "Information systems attacks: a preliminary classification scheme," Computers & Security, 16, 29-46.

Cohen, Fred, C. Phillips, L.P. Swiler, T. Gaylor, P. Leary, F. Rupley, and R. Isler (1998), "A cause and effect model of attacks on information systems," Computers and Security, 17 (1), 211-21.

Coltman, T., T. M. Devinney, A. Latukefu, and D. F. Midgley (2001), "E-Business: Revolution, Evolution of Hype?," Californian Management Review, 44 (1), 57-85.

Cooper, M.J., O. Dimitrov, and P.R. Rau (2001), "A Rose.com by any other name," The Journal of Finance, 56 (6), 2371-88.

Cooper, R.B. and R. W. Zmud (1990), "Information Technology Implementation Research: A Technological Diffusion Approach," Management Science, 36 (2), 123-39.

Corrado, Charles J. (1989), "A nonparametric test for abnormal security-price performance in event studies," Journal of Financial and Quantitative Analysis, 25, 549-54.

Courtney, R. (1977), "Security risk analysis in electronic data processing," in AFIPS Conference proceedings NCC: AFIPS Press.

Cowan, Arnold R. (1992), "Nonparametric Event study tests," Review of Quantitative Finance and Accounting, 2, 343-58.

Daniels, T.E. and E.H. Spafford (1999), "Identification of host audit data to detect attacks on low-level IP," Journal of Computer Security, 7 (1), 3-35.

Dehning, B., V.J Richardson, and R.W. Zmud (2003), "The Value Relevance of Announcements of Transformational Information Technology Investments," MIS Quarterly, 27 (4), 637-56.

---- (2002), "The Value Relevance of Information Technology Investment Announcements: Incorporating Industry Strategic IT Role," in 35th Annual Hawaii International Conference on Systems Science.

Dehning, Bruce, Vernon J. Richardson, Andrew Urbaczweski, and John D. Wells (2004), "Reexamining the value relevance of e-Commerce initiatives," Journal of Management Information Systems, 21 (1), 55-82.

Denning, D. (1987), "An intrusion-detection model," IEEE Transactions on Software Engineering, 13 (2), 222-26.

Denning, D. and D. Branstad (1996), "A taxonomy of key escrow encryption systems," Communications of the ACM, 39 (3), 34-40.

Dillon, Robin L. (2003), "Including technical and security risks in the development of information systems: a programatic risk management model," in Twenty-Fourth International Conference on Information Systems. Seattle, WA.

Dopuch, N., R.W. Holthausen, and R.W. Leftwich (1986), "Abnormal stock returns associated with media disclosures of 'subject to' qualified audit options," Journal of Accounting and Economics, 8 (2), 93-117.

Dos Santos, B.L., K. Peffers, and D.C. Mauer (1993), "The impact of information technology investment announcement on the market value of the firm," Information Systems Research, 4 (1), 1-23.

Ettredge, M. and V.J. Richardson (2001), "Assessing the risk in e-commerce," in International Conference on Information Systems. New Orleans, LA.

Ewalt, David M (2005), "Are companies liable for ID Data Theft?"

Fama, Eugene F. (1970), "Efficient capital markets A review of theory and empirical work," Journal of Finance, 25, 383-417.

Fama, Eugene F., Lawrence Fisher, Michael C. Jensen, and Richard Roll (1969), "The adjustment of stock prices to new information," International Economic Review, 10 (1), 1-21.

Fitzgerald, J. (1978), "EDP risk analysis for contingency planning," in EDP Audit Control and Security Newsletter Vol. 6.

Frincke, D. (2000), "Balancing cooperation and risk in intrusion detection," ACM transactions on information and system security, 3 (1), 1-29.

Gebauer, J. and M. J. Shaw (2002), "Introduction to the special section: Business-to-business electronic commerce," International Journal of Electronic Commerce, 6 (4), 7-17.

Gordon, L. A., M. P. Loeb, and W. Lucyshyn (2003a), "Information Security Expenditures and Real Options: A Wait-and-See Approach," Computer Security Journal, 19 (2), 1-7.

Gordon, L.A. and M.P. Loeb (2002), "The economics of information security investment," ACM transactions on information and system security, 5 (4), 438-57.

Gordon, Lawrence A. and Martin P Loeb (2001), "Using Information Security as a Response to Competitor Analysis Systems," Communications of the ACM, 44 (9), 71-74.

Gordon, Lawrence A., Martin P. Loeb, and William Lucyshyn (2003b), "Sharing information on computer security: and economic analysis," Journal of Accounting and Public Policy, 22, 461-85.

Gordon, Lawrence A., Martin P. Loeb, and Tashfeen Sohail (2003c), "A framework for using insurance for cyber-risk management," Communications of the ACM, 46 (3), 81-85.

Grossman, S.J. and O.D. Hart (1986), "The costs and benefits of ownership: a theory of vertical and lateral integration," Journal of Political Economy, 94 (4), 691-719.

Gupta, Mukul, Alok R. Chaturvedi, Shailendra Mehta, and Lorenzo Valeri (2000), "The experimental analysis of information security management issues for online financial services," in The Twenty-First International Conference on Information Systems. Brisbane, Australia.

Hart, O.D. and J. Moore (1988), "Incomplete contracts and renegotiation," Econometrica, 56 (4), 755-85.

Hayes, D.C., J.E. Hunton, and J.L. Reck (2000), "Information systems outsourcing announcements:Investigating the impact on the market value of contract-granting firms," Journal of Information Systems, 14 (2), 109-25.

---- (2001), "Market Reaction to ERP Implementation Announcements," Journal of Information Systems, 15 (1), 3-18.

Hitt, L.M. and E. Brynjolfsson (1996), "Productivity, business profitability, and consumer surplus: three different measures of information technology value," MIS Quarterly, 20 (2), 121-42.

Hoffer, J.A. and Detmar W. Struab (1989), "The 9 to 5 Underground: are you policing computer crimes?," Sloan Management Review, 30 (4), 35-44.

Hovav, Anat and John D'Arcy (2003), "The impact of denial-of-service announcements on the market value of firms," Risk Management and Insurance Review, 6 (2), 97-121.

---- (2004), "The impact of virus attack on the market value of firms," Information Systems Security Journal, 13 (3), 32-40.

Howard, J. (1997), "An analysis of Security Incidents on the Internet," PhD Thesis, Carnegie Mellon University.

Iacovou, C.L., I. Benbast, and A.S. Dexter (1995), "Electronic data interchange and small organizations: adoption and impact of the technology," MIS Quarterly, 19 (4), 465-85.

Im, K.S., K.E. Dow, and V. Grover (2001), "Research Report: A Reexamination of IT investment and the market value of the firm - An event study methodology," Information Systems Research, 12 (1), 103-17.

Jensen, Michael C. (1978), "Some anomalous evidence regarding market efficiency," Journal of Financial Economics, 6 (2/3), 95-101.

Jones, Derek C. Ed. (2003), New Economy Handbook. Oxford UK: Academic Press.

Kardaras, D. and E. Papathanassiou (2000), "The Development of B2C E-Commerce in Greece: Current Situation and Future Potential," Internet Research, 10 (4), 284-94.

Kauffman, R.J. and E. A. Walden (2001), "Economics and Electronic Commerce: Survey and Directions for Research," International Journal of Electronic Commerce, 5 (4), 5-116.

Kim, H. and G. Koehler (1995), "Theory and Practice of Decision Tree Induction," Omega, 23 (6), 637-52.

Ko, Myung S. (2003), "An exploration of the impact of information technology investment on organizational performance," Virginia Commonwealth University.

Larsen, K.R.T. and P.A. Bloniarz (2000), "A Cost and Performance Model for Web Service Instrument," Communications of the ACM, 43 (2), 109-16.

Lee, C.M. (2001), "Market efficiency and accounting research: a discussion of capital market research in accounting," Journal of Accounting and Economics (31), 233-53.

Lindquist, Ulf and Erland Jonsson (1997), "How to systematically classify Computer security intrusions," in IEEE Symposium on Security and Privacy. Oakland, CA.

Liu, Peng, Wanyu Zang, and Meng Yu (2005), "Incentive-based modeling and inference of attacker intent, objectives and strategies," ACM Transactions on Information and System Security, 8 (1), 78-118.

Loch, K.D., H.H. Carr, and M.E. Warkentin (1992), "Threats to information systems: Today's reality, yesterday's understanding," MIS Quarterly, 17 (2), 173-86.

Mackinlay, Craig (1997), "Event Studies in Economics and Finance," Journal of Economic Literature, 35, 13-39.

Mahmood, M.A., R. Kohli, and S. Devaraj (2004), "Introduction to the special issue: Measuring the business value of information technology in e-business environments," International Journal of Electronic Commerce, 9 (1), 6-8.

Mercuri, Rebecca T. (2003), "Analyzing Security Costs," Communications of the ACM, 46 (6), 15-18.

Milgrom, Paul and John Roberts (1995), "Complementarities and Fit Strategy, Structure, and Organizational Change in Manufacturing," Journal of Accounting and Economics, 19, 179-208.

Muralidhar, K., D. Batra, and P. Kirs (1995), "Accessibility, security, and accuracy in statistical databases: The case for the multiplicative fixed data pertubation approach," Management Science, 41 (9), 1549-64.

Murphy, Catherine K. (1998), "Induced decision trees for temporal medical data," in Fourth International Conference on Information Systems. Baltimore, MD.

Nance, W.D. and Detmar W. Straub (1988), "An investigation into the usefulness of security software in detecting computer abuse," in Ninth International Conference on Information Systems, J.I. DeGloss and M.H. Olson (Eds.). Minneapolis, MN.

Negroponte, Nicholas (1995), Being Digital. New York.

NIST (1995), "An introduction to Computer security," in Special Publication 800-12: National Institute of Standards and Technology.

Oh, W. and J.W.. Kim (2002), "The effects of firm characteristics on investor reaction to IT investment announcements," in International Conference on Information Systems. New Orleans, LA.

Osborn, S., R. Sandhu, and Q. Munawer (2000), "Configuring role-based access control to enforce mandatory and discretionary access control policies," ACM transactions on information and system security, 3 (2), 85-106.

Osei-Bryson, Kweku-Muata and K. Giles (2002), "Splitting methods for decision tree induction: a comparison of two families," in Eighth Americas Conference on Information Systems. Dallas, TX.

Osei-Bryson, Kweku-Muata and Myung S. Ko (2004), "Exploring the relationship between information technology investments and firm performance using regression splines analysis," Information and Management, 42, 1-13.

Osei-Bryson, Kweku-Muata and Ojelanki K. Ngwenyama (2004), "Peirce, Popper and Data Mining: An Approach to Empirically based Theory Development and Testing."

Peyravian, M., A. Roginsky, and N. Zunic (1996), "Hash-based encryption," Computer Security, 18 (4), 345-50.

Pfleeger, C. (1997), Security in Computing (2nd ed.). Englewood Cliffs, NJ: Prentice-Hall.

Power, R. (2003), "2002 CSI/FBI Computer crime and securuty survey," Computer security issues and trends, 8 (1), 1-21.

Quinlan, J. (1993), C4.5: Programs for Machine Learning. San Mateo, California: Morgan Kaufmann.

---- (1990), "Decision trees and decision making," IEEE Transactions on SMC, 20 (2), 339-46.

Richardson, V.J. and R.W. Zmud (2002), "The effects accompanying appointments of outside directors to the boards of Internet companies," University of Kansas.

Riggins, F.J. and T Mukhopadhyay (1999), "Overcoming adoption and implementation risks of EDI," International Journal of Electronic Commerce, 3 (4), 103-15.

Rosen, K.T. and A.L. Howard (2000), "Gold Rush or Fool's Gold?," California Management Review, 42 (3), 72-100.

Sachs, Goldman, Harris, and Nielsen/NetRatings (December 2003), "E-spending report."

Sandhu, R.S., E.J. Coyne, H.L. Feinstein, and C.E. Youman (1996), "Role-based access control models," IEEE Computer, 29 (2), 38-47.

Schein, E.H. Ed. (1992), The Role of the CEO in the Management of Change: The Case of Information Technology. Oxford: Oxford University Press.

Seidmann, A. and A. Sundararajan (1997), "Building and sustaining interorganizational information sharing relationships: the competitive impact of interfacing supply chain operations with marketing strategy," in Eighteenth International Conference on Information Systems, K. Kumar and J.I. DeGross (Eds.). Atlanta, GA.

Seiler, M.J. (2000), "The efficacy of event-study methodologies: measuring ereit abnormal performance under conditions of induced variance," Journal of Financial and Strategic Decisions, 13 (1), 101-11.

Shapiro, C. and H.R. Varian (1999), Information Rules: A Strategic guide to the Network Economy. Cambridge, MA: Havard Business School Press.

Sharpe, W. (1963), "A simplified model for portfolio analysis," Management Science, 9, 277-93.

Simmons, G. (1994), "Cryptanalysis and protocol failures," Communications of the ACM, 37 (11), 56-64.

Soh, C. and M.L. Markus (1995), "How IT Creates Business Value: A Process Theory Synthesis," in Sixteenth International Conference on Information Systems, J.I. DeGross and G.Ariav and C.Beath and R. Hoyer and C. Kemerer (Eds.). Amsterdam, The Netherlands.

Stillerman, M., C. Marceau, and M Stillman (1999), "Intrusion detection for Distributed applications," Communicatios of the ACM, 1999 (7), 62-69.

Straub, Detmar W. (1990), "Effective IS security," Information Systems Research, 1 (3), 255-76.

Straub, Detmar W., P.J. Carlson, and E.H. Jones (1993), "Cheating by student programmers: a field experiment in computer security," Journal of Management Systems, 5 (1), 33-48.

---- (1992), "Deterring highly motivated computer abusers: a field experiment in computer security: the need for International cooperation," in G.G. Gable and W.J Caelli, Eds. North-Holland, Amsterdam.

Straub, Detmar W. and W.D. Nance (1990), "Discovering and disciplining computer abuse in organizations: a field study," MIS Quarterly, 14 (1), 45-62.

Straub, Detmar W. and Richard J. Welke (1998), "Coping with systems risk: security planning models for management decision making," MIS Quarterly, 23 (4), 441-69.

Subramani, Mani and Eric Walden (1999), "The dot com effect: the impact of e-commerce announcements on the market value of firms," in Twentieth International Conference on Information Systems. Charlotte, NC.

---- (2000), "Economic returns to firms from business-to-business electronic commerce initiatives," in Twenty-first International Conference on Information Systems. Brisbane.

---- (2002), "Employing the event study to assess returns to firms from novel information technologies: an examination of e-commerce initiative announcements," in Management Information Systems Research Center.

---- (2001), "The impact of E-Commerce announcements on the market value of firms," Information Systems Research, 12 (2), 135-54.

Tan, Jennifer (2004), "Firms say 2003 viruses caused $55B damage," in Washington Post.

Torkzadeh, G. and G. Dhillon (2002), "Measuring factors that influence the success of Internet Commerce," Information Systems Research, 13 (2), 187-204.

Truman, G.E. (1998), "An empirical appraisal of EDI implementation strategies," International Journal of Electronic Commerce, 2 (4), 43-70.

Undercoffer, J., J. Pinkston, A. Joshi, and T. Finin (2003), "A target-centric ontology for intrusion detection," in International joint conference on Artificial Intelligence. Acapulco, Mexico.

Wiseman, S. (1986), "A secure capability computer system," in IEEE Symposium on Security and Privacy. Los Alamitos, CA: IEEE Computer Society Press.

Zhu, Kevin and Sean Xu (2004), "The Value of Information Technology in E-business Environments: The Missing Links in the Renewed IT Value Debate," in Twenty-Fifth International Conference on Information Systems. Washington, DC.

APPENDIX 1: EVENT STUDIES IN INFORMATION SYSTEMS

Event	Author (s) and Year
IT Investments	Dos Santos et al.(1993); Im et al.(2001); Oh and Kim (2002); Chatterjee et al. (2002); Dehning et al. (2002)
Newly created CIO positions	Chatterjee et al. (2001)
IT Failures	Bharadwaj and Keil (2001)
Dotcom name change	Cooper et al.(2001)
ERP Implementation	Hayes et al. (2001)
IS outsourcing	Hayes et al. (2000)
Board of Directors nomination for Internet firms	Richardson and Zmud (2002)
ecommerce investments	Subramani and Walden (1999); Subramani and Walden (2000); Subramani and Walden (2001); Dehning et al. (2004)
Internet security breaches	Ettredge et al.(2001); Cavusoglu et al. (2002); Campbell et al. (2003), Hovav and D'Arcy (2003); Hovav and D'Arcy (2004); Cavusoglu et al. (2004a)

APPENDIX 2: SOURCES OF EQUIVALENT COMBINED RULES FOR INTERNET SECURITY BREACH

Table 41: Equivalent Combined Rules used in Table 5

Source	Set of Rules	Equivalent Combined Rule
	IF Firm Size = 'SMALL' & Firm Type = 'NON-NET' & Results ∈ {'THEFT OF SERVICE', 'CORRUPTION OF INFORMATION'} & Attacker ∈ {'CORPORATE RAIDERS', 'VANDALS'} THEN N = 5 CAR: {POSITIVE: 40.0%; NEFATIVE: 60.0%}	IF Firm Type = 'NON-NET' & Results ∈ {'THEFT OF SERVICE', 'CORRUPTION OF INFORMATION'} & Attacker ∈ {'CORPORATE RAIDERS', 'VANDALS'} THEN N = 9 CAR: {POSITIVE:44.4%; NEGATIVE: 55.6%}
	IF **Firm Size** = 'LARGE' & **Firm Type** = 'NON-NET' & **Results** ∈ {'THEFT OF SERVICE', 'CORRUPTION OF INFORMATION'} & **Attacker** ∈ {'CORPORATE RAIDERS', 'VANDALS'} THEN N = 4 **CAR:** {POSITIVE: 50.0%; ABNORMAL: 50.0%}	Abnormal Relative Frequency = (5*40% + 4*50%)/(5+4) = 44.4% Abnormal Relative Frequency = (5*60% + 4*50%)/(5+4) = 55.6%

Table 42: Equivalent Combined Rules used in Table 11

Source	Original Set of Rules	Equivalent Combined Rule
	IF Tools = 'SCRIPTS/PROGRAMS' & Attacker ∈ { 'OTHERS', 'PROFESSIONAL CRIMINALS', 'TERRORISTS'} THEN N = 4 CAR = {POSITIVE: 100.0%; ABNORMAL: 0.0%} IF Tools = 'OTHERS' & Attacker ∈ { 'OTHERS', 'PROFESSIONAL CRIMINALS', 'TERRORISTS'} THEN N = 6 CAR = {POSITIVE: 50.0%; ABNORMAL: 50.0%} IF Tools = 'AUTONOMOUS AGENT' & Attacker ∈ {'OTHERS', 'PROFESSIONAL CRIMINALS', 'TERRORISTS'} THEN N = 6 CAR = {POSITIVE: 33.3%; NEGATIVE: 66.7%}	IF **Attacker** ∈ { 'OTHERS', 'PROFESSIONAL CRIMINALS', 'TERRORISTS'} THEN N = 16 **CAR** = {POSITIVE: 56.2%; NEGATIVE: 43.8%}
	IF Firm Size = 'SMALL' & Attacker = 'HACKERS' THEN N = 3 CAR = {POSITIVE: 33.3%; NEGATIVE: 66.7%} IF Firm Size = 'LARGE' & Attacker = 'HACKERS' THEN N = 6 CAR = {POSITIVE: 0.0%; NEGATIVE: 100.0%}	IF Attacker = 'HACKERS' THEN N = 9 CAR = {POSITIVE: 11.1%; NEGATIVE: 88.9%}
	IF Results ∈ {'DENIAL OF SERVICE', 'DISCLOSURE OF INFORMATION'} & Attacker ∈ {'CORPORATE RAIDERS', 'VANDALS'} THEN N = 4 CAR = {POSITIVE: 0.0%; NEGATIVE: 100.0%} IF Firm Type = 'NET' & Results ∈ {'THEFT OF SERVICE',	IF Attacker ∈ {'CORPORATE RAIDERS', 'VANDALS'} THEN N = 16 CAR = {POSITIVE: 25.0%; NEGATIVE: 75.0%}

	'CORRUPTION OF INFORMATION'} & Attacker ∈ {'CORPORATE RAIDERS', 'VANDALS'} THEN N = 3 CAR = {POSITIVE: 0.0%; NEGATIVE: 100.0%} IF Firm Size = 'SMALL' & Firm Type = 'NON-NET' & Results ∈ {'THEFT OF SERVICE', 'CORRUPTION OF INFORMATION'} & Attacker ∈ {'CORPORATE RAIDERS', 'VANDALS'} THEN N = 5 CAR = { POSITIVE: 40.0%; NEGATIVE: 60.0%} IF Firm Size = 'LARGE' & Firm Type = 'NON-NET' & Results ∈ {'THEFT OF SERVICE', 'CORRUPTION OF INFORMATION'} & Attacker ∈ {'CORPORATE RAIDERS', 'VANDALS'} THEN N = 4 CAR = {POSITIVE: 50.0%; NEGATIVE: 50.0%}	

Table 43: Equivalent Combined Rules used in Table 13

Source	Original Set of Rules	Equivalent Combined Rule

DT_Eb	IF Firm Size = 'SMALL' & Objective = 'CHALLENGE/STATUS' THEN
	N = 3
	CAR = {POSITIVE: 33.3%; NEGATIVE: 66.7%}
	
	IF Firm Size = 'LARGE' & Objective = 'CHALLENGE/STATUS' THEN
	N = 7
	CAR = {POSITIVE: 0.0%; NEGATIVE: 100.0%}
		IF Objective = 'CHALLENGE/STATUS' THEN
		N = 10
		CAR = {POSITIVE: 10.0%; NEGATIVE: 90.0%}

	IF Firm Size = 'SMALL' & Objective = 'DAMAGE' THEN N = 5 CAR = {POSITIVE: 20.0%; NEGATIVE: 80.0%}	IF Objective = 'DAMAGE' THEN N = 11 CAR = {POSITIVE: 27.3%; NEGATIVE: 72.7%}

	IF Firm Size = 'LARGE' & Objective = 'DAMAGE' THEN N = 6 CAR = {POSITIVE: 33.3%; NEGATIVE: 66.7%}	

	IF Tools = 'AUTONOMOUS AGENT' & Objective ∈ {'FINANCIAL GAIN','OTHER','POLITICAL GAIN'} THEN
	N = 6
	CAR = {POSITIVE: 33.3%; NEGATIVE: 66.7%}
	
	IF **Tools** = 'SCRIPTS/PROGRAMS' & **Objective** ∈ {'FINANCIAL GAIN', 'OTHER', 'POLITICAL GAIN'} THEN
	N = 5
	CAR = {POSITIVE: 80.0%; NEGATIVE: 20.0%}
	
	IF Period = 'PRE FEB 2000' & Tools = 'OTHER' & Objective ∈ {'FINANCIAL GAIN', 'OTHER', 'POLITICAL GAIN'} THEN
	N = 4
	CAR = {POSITIVE: 25.0%; NEGATIVE: 75.0%}
	
	IF **Period** = 'POST FEB 2000' & **Tools** = 'OTHER' & **Objective** ∈ {'FINANCIAL GAIN', 'OTHER', 'POLITICAL GAIN'} THEN
	N = 5
	CAR = {POSITIVE: 60.0%; NEGATIVE: 40.0%}
		IF Objective ∈ {'FINANCIAL GAIN','OTHER','POLITICAL GAIN'} THEN
		N = 20
		CAR = {POSITIVE: 50.0%; NEGATIVE: 50.0%}

	IF Firm Size = 'SMALL' & Objective ∈ { 'DAMAGE', 'POLITICAL GAIN'} & Period = 'POST FEB 2000' & Access = 'UNAUTHORIZED ACC' THEN
	N = 5
	CAR = {POSITIVE: 20.0%; NEGATIVE: 80.0%}
	
	IF Firm Size = 'LARGE' & Objective ∈ { 'DAMAGE', 'POLITICAL GAIN'} & Period = 'POST FEB 2000' & Access = 'UNAUTHORIZED ACC' THEN
	N = 7
	CAR = {POSITIVE: 42.9%; NEGATIVE: 57.1%}
		IF Objective ∈ { 'DAMAGE', 'POLITICAL GAIN'} & Period = 'POST FEB 2000' & Access = 'UNAUTHORIZED ACC' THEN
		N = 12
		CAR = {POSITIVE: 33.3%; NEGATIVE: 66.7}

DT_Gb	IF Firm Size = 'SMALL' & Objective ∈ { 'DAMAGE', 'POLITICAL GAIN'} & Period = 'POST FEB 2000' & Access =	IF Objective ∈ { 'DAMAGE', 'POLITICAL GAIN'} & Period = 'POST FEB 2000' &

	'UNAUTHORIZED ACC' THEN N = 5 CAR = {POSITIVE: 20.0%; NEGATIVE: 80.0%} IF Firm Size = 'LARGE' & Objective ∈ { 'DAMAGE', 'POLITICAL GAIN'} & Period = 'POST FEB 2000' & Access = 'UNAUTHORIZED ACC' THEN N = 7 CAR = {POSITIVE: 42.9%; NEGATIVE: 57.1%}	Access = 'UNAUTHORIZED ACC' THEN N = 12 CAR = {POSITIVE: 33.3%; NEGATIVE: 66.7}

Table 44: Equivalent Combined Rules used in Table 17

Source	Original Set of Rules	Equivalent Combined Rule
DT_Eb	IF Period = 'PRE FEB 2000' & Tools = 'OTHER' & Objective ∈ {'FINANCIAL GAIN', 'OTHER', 'POLITICAL GAIN'} THEN N = 4 CAR = {POSITIVE: 25.0%; NEGATIVE: 75.0%} IF Period = 'POST FEB 2000' & Tools = 'OTHER' & Objective ∈ {'FINANCIAL GAIN', 'OTHER', 'POLITICAL GAIN'} THEN N = 5 CAR = {POSITIVE: 60.0%; NEGATIVE: 40.0%}	IF Tools = 'OTHER' & Objective ∈ {'FINANCIAL GAIN', 'OTHER', 'POLITICAL GAIN'} THEN N = 9 CAR = {POSITIVE: 44.6%; NEGATIVE: 55.6%}

Table 45: Equivalent Combined Rules used in Table 19

Source	Original Set of Rules	Equivalent Combined Rule
DT_C	IF **Access** = 'UNAUTHORIZED ACC & **Period** = 'PRE FEB 2000' THEN N= 8 **CAR:** {POSITIVE: 50.0%; NEGATIVE: 50.0%} IF Period = 'POST FEB 2000' & Access = 'UNAUTHORIZED ACC' THEN N= 24 CAR: {POSITIVE: 16.7%; NEGATIVE: 83.3%}	IF **Access** = 'UNAUTHORIZED ACC' THEN N= 32 **CAR:** {POSITIVE: 25.0%; NEGATIVE: 75.0%}

APPENDIX 3: DT GENERATED FROM INTERNET SECURITY BREACH SAMPLE USING THREE SPLITTING METHODS

Table 46: Predicting Abnormal Return; Attacker excluded as Possible Predictor

DT_Eb: Entropy Splitting Method	
IF **Firm Size** = 'SMALL' & **Objective** = 'CHALLENGE/STATUS' N = 3 **Rate Of Return** = {POSITIVE: 33.3%; NEGATIVE: 66.7%}	THEN
IF **Firm Size** = 'LARGE' & **Objective** = 'CHALLENGE/STATUS' N = 7 **Rate Of Return** = {POSITIVE: 0.0%; NEGATIVE: 100.0%}	THEN
IF **Firm Size** = 'SMALL' & **Objective** = 'DAMAGE' N = 5 **Rate Of Return** = {POSITIVE: 20.0%; NEGATIVE: 80.0%}	THEN
IF **Firm Size** = 'LARGE' & **Objective** = 'DAMAGE' N = 6 **Rate Of Return** = {POSITIVE: 33.3%; NEGATIVE: 66.7%}	THEN
IF **Tools** = 'AUTONOMOUS AGENT' & **Objective** ∈ {'FINANCIAL GAIN','OTHER','POLITICAL GAIN'} N = 6 **Rate Of Return** = {POSITIVE: 33.3%; NEGATIVE: 66.7%}	THEN
IF **Tools** = 'SCRIPTS/PROGRAMS' & **Objective** ∈ {'FINANCIAL GAIN', 'OTHER', 'POLITICAL GAIN'} N = 5 **Rate Of Return** = {POSITIVE: 80.0%; NEGATIVE: 20.0%}	THEN
IF **Period** = 'PRE FEB 2000' & **Tools** = 'OTHER' & **Objective** ∈ {'FINANCIAL GAIN', 'OTHER', 'POLITICAL GAIN'} N = 4 **Rate Of Return** = {POSITIVE: 25.0%; NEGATIVE: 75.0%}	THEN
IF **Period** = 'POST FEB 2000' & **Tools** = 'OTHER' & **Objective** ∈ {'FINANCIAL GAIN', 'OTHER', 'POLITICAL GAIN'} N = 5 **Rate Of Return** = {POSITIVE: 60.0%; NEGATIVE: 40.0%}	THEN

Table 47: Predicting Abnormal Return; Attacker excluded as Possible Predictor

DT_Gb: Gini Splitting Method
IF **Firm Type** = 'NON-NET' & **Access** = 'UNAUTHORIZED USE' THEN N = 6 **Rate Of Return =** {POSITIVE: 83.3%; NEGATIVE: 16.7%}
IF **Firm Type** = 'NET' & **Access** = 'UNAUTHORIZED USE' THEN N = 3 **Rate Of Return =** {POSITIVE: 33.3%; NEGATIVE: 66.7%}
IF **Firm Type** = 'NET' & Period = 'PRE FEB 2000' & **Access** = 'UNAUTHORIZED ACC' THEN N = 5 **Rate Of Return =** {POSITIVE: 40.0%; NEGATIVE: 60.0%}
IF **Firm Type** = 'NON-NET' & **Period** = 'PRE FEB 2000' & **Access** = 'UNAUTHORIZED ACC' THEN N = 3 **Rate Of Return =** {POSITIVE: 66.7%; NEGATIVE: 33.3%}
IF **Objective** ∈ { 'CHALLENGE/STATUS', 'FINANCIAL GAIN'} & **Period** = 'POST FEB 2000' & **Access** = 'UNAUTHORIZED ACC' THEN N = 12 **Rate Of Return =** {POSITIVE: 0.0%; NEGATIVE: 100.0%}
IF **Firm Size** = 'SMALL' & **Objective** ∈ { 'DAMAGE', 'POLITICAL GAIN'} & **Period** = 'POST FEB 2000' & **Access** = 'UNAUTHORIZED ACC' THEN N = 5 **Rate Of Return =** {POSITIVE: 20.0%; NEGATIVE: 80.0%}
IF **Firm Size** = 'LARGE' & **Objective** ∈ { 'DAMAGE', 'POLITICAL GAIN'} & **Period** = 'POST FEB 2000' & **Access** = 'UNAUTHORIZED ACC' THEN N = 7 **Rate Of Return =** {POSITIVE: 42.9%; NEGATIVE: 57.1%}

Table 48: Predicting Negative Abnormal Return; Attacker included as Possible Predictor

DT_C: Chi-Square Splitting Method	
IF **Access** = 'UNAUTHORIZED USE' N = 9 **Rate Of Return =** {POSITIVE: 66.7%; NEGATIVE: 33.3%}	THEN
IF **Access** = 'UNAUTHORIZED ACC & **Period** = 'PRE FEB 2000' N = 8 **Rate Of Return =** {POSITIVE: 50.0%; NEGATIVE: 50.0%}	THEN
IF **Period** = 'POST FEB 2000' & **Access** = 'UNAUTHORIZED ACC' N = 24 **Rate Of Return =** {POSITIVE: 16.7%; NEGATIVE: 83.3%}	THEN

APPENDIX 4: DT GENERATED FROM ECOMMERCE INITIATIVE SAMPLE USING THREE SPLITTING METHODS

Table 49: Rules that include *Innovativeness* as a Predictor

Source	Rules
DT_Etv	IF **Innovativeness** ='TRANSFORMATIONAL' N = 212 **CAR**: {POSITIVE: 78.8%; NEGATIVE: 21.2%) IF **Innovativeness** ='EXECUTIONAL' N = 136 **CAR**: {POSITIVE: 34.6%; NEGATIVE: 65.4%) IF **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'UNILATERAL' N = 115 **CAR**: {POSITIVE: 74.7%; NEGATIVE: 25.3%) IF **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'JOINT' N = 97 **CAR**: {POSITIVE: 84.3%; NEGATIVE: 15.7%) IF **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'UNILATERAL'& **Firm Type** = 'NET' N = 29 **CAR**: {POSITIVE: 78.8%; NEGATIVE: 21.2%) IF **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'JOINT'& **Firm Type** = 'NON-NET' N = 86 **CAR**: {POSITIVE: 73.5%; NEGATIVE: 26.5%) IF **Customer Type** = 'B2B' & **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'UNILATERAL'& **Firm Type** = 'NET' N = 58

	CAR: {POSITIVE: 81.7%; NEGATIVE: 19.3%) IF **Customer Type** = 'B2C' & **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'UNILATERAL'& **Firm Type** = 'NET' N = 28 **CAR**: {POSITIVE: 60.9%; NEGATIVE: 39.1%) IF **Product Type** ='DIGITAL' & **Customer Type** = 'B2C' & **Firm Type** = 'NON-NET' & **Governance** = 'UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 16 **CAR**: {POSITIVE: 50.0%; NEGATIVE: 50%) IF **Product Type** ='TANGIBLE' & **Customer Type** = 'B2C' & **Firm Type** = 'NON-NET' & **Governance** = 'UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 16 **CAR**: {POSITIVE: 68.8%; NEGATIVE: 31.3%)
DT_Gt	IF **Firm Type** = 'NET' & **Product Type** = 'TANGIBLE' & **Innovativeness** ='EXECUTIONAL' N = 9 **CAR**: {POSITIVE: 11.1%; NEGATIVE: 88.9%) IF **Customer Type** = 'B2C' & **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'UNILATERAL'& **Firm Type** = 'NET' N = 9 **CAR**: {POSITIVE: 88.9%; NEGATIVE: 11.1%) IF **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'UNILATERAL'& **Firm Type** = 'NET' & **Customer Type** = 'B2B' N = 12 **CAR**: {POSITIVE: 83.3%; NEGATIVE: 16.7%) IF **Customer Type** ='B2B' & **Firm Type** ='NET' & **Governance** ='JOINT' & **Innovativeness** ='TRANSFORMATIONAL' N = 9 **CAR**: {POSITIVE: 55.6%; NEGATIVE: 44.4%) IF **Customer Type** ='B2C' & **Firm Type** ='NET' & **Governance** ='JOINT' & **Innovativeness** ='TRANSFORMATIONAL' N = 8 **CAR**: {POSITIVE: 87.5%; NEGATIVE: 12.5%) IF **Product Type** = 'DIGITAL' & **Firm Type** = 'NON-NET' & **Governance** ='JOINT' & **Innovativeness** = 'TRANSFORMATIONAL'

	N = 29 **CAR**: {POSITIVE: 89.7%; NEGATIVE: 10.3%) IF **Product Type** = 'DIGITAL' & **Customer Type** = 'B2B' & **Firm Type** = 'NON-NET' & **Governance** ='UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 27 **CAR**: {POSITIVE: 74.1%; NEGATIVE: 25.9%) IF **Product Type** = 'TANGIBLE' & **Customer Type** = 'B2B' & **Firm Type** = 'NON-NET' & **Governance** ='UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 9 **CAR**: {POSITIVE: 88.9%; NEGATIVE: 11.1%) IF **Product Type** = 'DIGITAL' & **Customer Type** = 'B2C' & **Firm Type** = 'NON-NET' & **Governance** ='UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 16 **CAR**: {POSITIVE: 50%; NEGATIVE: 50%) IF **Product Type** = 'TANGIBLE' & **Customer Type** = 'B2C' & **Firm Type** = 'NON-NET' & **Governance** ='UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 16 **CAR**: {POSITIVE: 68.8%; NEGATIVE: 31.2%) IF **Customer Type** ='B2B' & **Product Type** ='TANGIBLE' & **Firm Type** ='NON-NET' & **Governance** ='JOINT' & **Innovativeness** = 'TRANSFORMATIONAL' N = 7 **CAR**: {POSITIVE: 71.4%; NEGATIVE: 28.6%) IF **Customer Type** ='B2C' & **Product Type** ='TANGIBLE' & **Firm Type** ='NON-NET' & **Governance** ='JOINT' & **Innovativeness** = 'TRANSFORMATIONAL' N = 5 **CAR**: {POSITIVE: 80%; NEGATIVE: 20%) IF **Governance** ='UNILATERAL' & **Customer Type** ='B2B' & **Firm Type** ='NON-NET' & **Product Type** ='TANGIBLE' & **Innovativeness** ='EXECUTIONAL' N = 20 **CAR**: {POSITIVE: 60%; NEGATIVE: 40%) IF **Governance** ='JOINT' & **Customer Type** ='B2B' & **Firm Type** ='NON-NET' & **Product Type** ='TANGIBLE' & **Innovativeness** ='EXECUTIONAL'

	N = 6 **CAR**: {POSITIVE: 33.3%; NEGATIVE: 66.7%) IF **Governance** ='JOINT' & **Customer Type** ='B2C' & **Firm Type** ='NON-NET' & **Product Type** ='TANGIBLE' & **Innovativeness** ='EXECUTIONAL' N = 26 **CAR**: {POSITIVE: 50%; NEGATIVE: 50%) IF **Governance** ='UNILATERAL' & **Customer Type** ='B2C' & **Firm Type** ='NON-NET' & **Product Type** ='TANGIBLE' & **Innovativeness** ='EXECUTIONAL' N = 58 **CAR**: {POSITIVE: 39.7%; NEGATIVE: 60.3%) IF **Firm Type** = 'NET' & **Customer Type** ='B2C' & **Governance** = 'UNILATERAL' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 5 **CAR**: {POSITIVE: 40%; NEGATIVE: 60%) IF **Firm Type** = 'NON-NET' & **Customer Type** ='B2C' & **Governance** = 'UNILATERAL' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 19 **CAR**: {POSITIVE: 36.8%; NEGATIVE: 63.2%) IF **Firm Type** = 'NON-NET' & **Customer Type** ='B2B' & **Governance** = 'UNILATERAL' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 32 **CAR**: {POSITIVE: 21.9%; NEGATIVE: 78.12%) IF **Firm Type** = 'NET' & **Customer Type** ='B2B' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 7 **CAR**: {POSITIVE: 14.3%; NEGATIVE: 85.7%) IF **Firm Type** = 'NET' & **Customer Type** ='B2C' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 10 **CAR**: {POSITIVE: 30%; NEGATIVE: 70%) IF **Firm Type** = 'NON-NET' & **Customer Type** ='B2C' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL'

	N = 10 **CAR**: {POSITIVE: 10%; NEGATIVE: 90%) IF **Firm Type** = 'NON-NET' & **Customer Type** ='B2B' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 22 **CAR**: {POSITIVE: 4.5%; NEGATIVE: 95.5%) IF **Firm Type** = 'NET' & **Customer Type** ='B2B' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 22 **CAR**: {POSITIVE: 0%; NEGATIVE: 100%)

Table 50: Rules that include *Product Type* as a Predictor

Source	Rules
DT_Etv	IF **Product Type** ='DIGITAL' & **Customer Type** = 'B2C' & **Firm Type** = 'NON-NET' & **Governance** = 'UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 16 **CAR**: {POSITIVE: 50.0%; NEGATIVE: 50%) IF **Product Type** ='TANGIBLE' & **Customer Type** = 'B2C' & **Firm Type** = 'NON-NET' & **Governance** = 'UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 16 **CAR**: {POSITIVE: 68.8%; NEGATIVE: 31.3%)
DT_Gt	IF **Firm Type** = 'NET' & **Product Type** = 'TANGIBLE' & **Innovativeness** ='EXECUTIONAL' N = 9 **CAR**: {POSITIVE: 11.1%; NEGATIVE: 88.9%) IF **Product Type** = 'DIGITAL' & **Firm Type** = 'NON-NET' & **Governance** ='JOINT' & **Innovativeness** = 'TRANSFORMATIONAL' N = 29 **CAR**: {POSITIVE: 89.7%; NEGATIVE: 10.3%)

	IF **Product Type** = 'DIGITAL' & **Customer Type** = 'B2B' & **Firm Type** = 'NON-NET' & **Governance** ='UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 27 **CAR**: {POSITIVE: 74.1%; NEGATIVE: 25.9%) IF **Product Type** = 'TANGIBLE' & **Customer Type** = 'B2B' & **Firm Type** = 'NON-NET' & **Governance** ='UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 9 **CAR**: {POSITIVE: 88.9%; NEGATIVE: 11.1%) IF **Product Type** = 'DIGITAL' & **Customer Type** = 'B2C' & **Firm Type** = 'NON-NET' & **Governance** ='UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 16 **CAR**: {POSITIVE: 50%; NEGATIVE: 50%) IF **Product Type** = 'TANGIBLE' & **Customer Type** = 'B2C' & **Firm Type** = 'NON-NET' & **Governance** ='UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 16 **CAR**: {POSITIVE: 68.8%; NEGATIVE: 31.2%) IF **Governance** ='UNILATERAL' & **Customer Type** ='B2B' & **Firm Type** ='NON-NET' & **Product Type** ='TANGIBLE' & **Innovativeness** ='EXECUTIONAL' N = 20 **CAR**: {POSITIVE: 60%; NEGATIVE: 40%) IF **Governance** ='JOINT' & **Customer Type** ='B2B' & **Firm Type** ='NON-NET' & **Product Type** ='TANGIBLE' & **Innovativeness** ='EXECUTIONAL' N = 6 **CAR**: {POSITIVE: 33.3%; NEGATIVE: 66.7%) IF **Governance** ='JOINT' & **Customer Type** ='B2C' & **Firm Type** ='NON-NET' & **Product Type** ='TANGIBLE' & **Innovativeness** ='EXECUTIONAL' N = 26 **CAR**: {POSITIVE: 50%; NEGATIVE: 50%) IF **Governance** ='UNILATERAL' & **Customer Type** ='B2C' & **Firm Type** ='NON-NET' & **Product Type** ='TANGIBLE' & **Innovativeness** ='EXECUTIONAL' N = 58 **CAR**: {POSITIVE: 39.7%; NEGATIVE: 60.3%)

	IF **Firm Type** = 'NET' & **Customer Type** ='B2C' & **Governance** = 'UNILATERAL' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 5 **CAR**: {POSITIVE: 40%; NEGATIVE: 60%) IF **Firm Type** = 'NON-NET' & **Customer Type** ='B2C' & **Governance** = 'UNILATERAL' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 19 **CAR**: {POSITIVE: 36.8%; NEGATIVE: 63.2%) IF **Firm Type** = 'NON-NET' & **Customer Type** ='B2B' & **Governance** = 'UNILATERAL' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 32 **CAR**: {POSITIVE: 21.9%; NEGATIVE: 78.12%) IF **Firm Type** = 'NET' & **Customer Type** ='B2B' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 7 **CAR**: {POSITIVE: 14.3%; NEGATIVE: 85.7%) IF **Firm Type** = 'NET' & **Customer Type** ='B2C' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 10 **CAR**: {POSITIVE: 30%; NEGATIVE: 70%) IF **Firm Type** = 'NON-NET' & **Customer Type** ='B2C' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 10 **CAR**: {POSITIVE: 10%; NEGATIVE: 90%) IF **Firm Type** = 'NON-NET' & **Customer Type** ='B2B' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 22 **CAR**: {POSITIVE: 4.5%; NEGATIVE: 95.5%) IF **Firm Type** = 'NET' & **Customer Type** ='B2B' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 22 **CAR**: {POSITIVE: 0%; NEGATIVE: 100%)

Table 51: Rules that include *Governance* as a Predictor

Source	Rules
DT_E	IF **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'UNILATERAL' N = 115 **CAR**: {POSITIVE: 74.7%; NEGATIVE: 25.3%) IF **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'JOINT' N = 97 **CAR**: {POSITIVE: 84.3%; NEGATIVE: 15.7%)
DT_Gt	IF **Customer Type** = 'B2C' & **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'UNILATERAL'& **Firm Type** = 'NET' N = 9 **CAR**: {POSITIVE: 88.9%; NEGATIVE: 11.1%) IF **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'UNILATERAL'& **Firm Type** = 'NET' & **Customer Type** = 'B2B' N = 12 **CAR**: {POSITIVE: 83.3%; NEGATIVE: 16.7%) IF **Customer Type** ='B2B' & **Firm Type** ='NET' & **Governance** ='JOINT' & **Innovativeness** ='TRANSFORMATIONAL' N = 9 **CAR**: {POSITIVE: 55.6%; NEGATIVE: 44.4%) IF **Customer Type** ='B2C' & **Firm Type** ='NET' & **Governance** ='JOINT' & **Innovativeness** ='TRANSFORMATIONAL' N = 8 **CAR**: {POSITIVE: 87.5%; NEGATIVE: 12.5%) IF **Product Type** = 'DIGITAL' & **Firm Type** = 'NON-NET' & **Governance** ='JOINT' & **Innovativeness** = 'TRANSFORMATIONAL'

	N = 29 **CAR**: {POSITIVE: 89.7%; NEGATIVE: 10.3%) IF **Product Type** = 'DIGITAL' & **Customer Type** = 'B2B' & **Firm Type** = 'NON-NET' & **Governance** ='UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 27 **CAR**: {POSITIVE: 74.1%; NEGATIVE: 25.9%) IF **Product Type** = 'TANGIBLE' & **Customer Type** = 'B2B' & **Firm Type** = 'NON-NET' & **Governance** ='UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 9 **CAR**: {POSITIVE: 88.9%; NEGATIVE: 11.1%) IF **Product Type** = 'DIGITAL' & **Customer Type** = 'B2C' & **Firm Type** = 'NON-NET' & **Governance** ='UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 16 **CAR**: {POSITIVE: 50%; NEGATIVE: 50%) IF **Product Type** = 'TANGIBLE' & **Customer Type** = 'B2C' & **Firm Type** = 'NON-NET' & **Governance** ='UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 16 **CAR**: {POSITIVE: 68.8%; NEGATIVE: 31.2%) IF **Customer Type** ='B2B' & **Product Type** ='TANGIBLE' & **Firm Type** ='NON-NET' & **Governance** ='JOINT' & **Innovativeness** = 'TRANSFORMATIONAL' N = 7 **CAR**: {POSITIVE: 71.4%; NEGATIVE: 28.6%) IF **Customer Type** ='B2C' & **Product Type** ='TANGIBLE' & **Firm Type** ='NON-NET' & **Governance** ='JOINT' & **Innovativeness** = 'TRANSFORMATIONAL' N = 5 **CAR**: {POSITIVE: 80%; NEGATIVE: 20%) IF **Governance** ='UNILATERAL' & **Customer Type** ='B2B' & **Firm Type** ='NON-NET' & **Product Type** ='TANGIBLE' & **Innovativeness** ='EXECUTIONAL' N = 20 **CAR**: {POSITIVE: 60%; NEGATIVE: 40%) IF **Governance** ='JOINT' & **Customer Type** ='B2B' & **Firm Type** ='NON-NET' & **Product Type** ='TANGIBLE' & **Innovativeness** ='EXECUTIONAL'

	N = 6 **CAR**: {POSITIVE: 33.3%; NEGATIVE: 66.7%) IF **Governance** ='JOINT' & **Customer Type** ='B2C' & **Firm Type** ='NON-NET' & **Product Type** ='TANGIBLE' & **Innovativeness** ='EXECUTIONAL' N = 26 **CAR**: {POSITIVE: 50%; NEGATIVE: 50%) IF **Governance** ='UNILATERAL' & **Customer Type** ='B2C' & **Firm Type** ='NON-NET' & **Product Type** ='TANGIBLE' & **Innovativeness** ='EXECUTIONAL' N = 58 **CAR**: {POSITIVE: 39.7%; NEGATIVE: 60.3%) IF **Firm Type** = 'NET' & **Customer Type** ='B2C' & **Governance** = 'UNILATERAL' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 5 **CAR**: {POSITIVE: 40%; NEGATIVE: 60%) IF **Firm Type** = 'NON-NET' & **Customer Type** ='B2C' & **Governance** = 'UNILATERAL' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 19 **CAR**: {POSITIVE: 36.8%; NEGATIVE: 63.2%) IF **Firm Type** = 'NON-NET' & **Customer Type** ='B2B' & **Governance** = 'UNILATERAL' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 32 **CAR**: {POSITIVE: 21.9%; NEGATIVE: 78.12%) IF **Firm Type** = 'NET' & **Customer Type** ='B2B' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 7 **CAR**: {POSITIVE: 14.3%; NEGATIVE: 85.7%) IF **Firm Type** = 'NET' & **Customer Type** ='B2C' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 10 **CAR**: {POSITIVE: 30%; NEGATIVE: 70%) IF **Firm Type** = 'NON-NET' & **Customer Type** ='B2C' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL'

	N = 10 **CAR**: {POSITIVE: 10%; NEGATIVE: 90%) IF **Firm Type** = 'NON-NET' & **Customer Type** ='B2B' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 22 **CAR**: {POSITIVE: 4.5%; NEGATIVE: 95.5%) IF **Firm Type** = 'NET' & **Customer Type** ='B2B' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 22 **CAR**: {POSITIVE: 0%; NEGATIVE: 100%)

Table 52: Rules that include *Firm Type* as a Predictor

Source	**Rules**
DT_E	IF **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'UNILATERAL'& **Firm Type** = 'NET' N = 29 **CAR**: {POSITIVE: 78.8%; NEGATIVE: 21.2%) IF **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'JOINT'& **Firm Type** = 'NON-NET' N = 86 **CAR**: {POSITIVE: 73.5%; NEGATIVE: 26.5%)
DT_Gt	IF **Firm Type** = 'NET' & **Product Type** = 'TANGIBLE' & **Innovativeness** ='EXECUTIONAL' N = 9 **CAR**: {POSITIVE: 11.1%; NEGATIVE: 88.9%) IF **Customer Type** = 'B2C' & **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'UNILATERAL'& **Firm Type** = 'NET' N = 9 **CAR**: {POSITIVE: 88.9%; NEGATIVE: 11.1%) IF **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'UNILATERAL'& **Firm Type** = 'NET' & **Customer Type** = 'B2B' N = 12

	CAR: {POSITIVE: 83.3%; NEGATIVE: 16.7%) IF **Customer Type** ='B2B' & **Firm Type** ='NET' & **Governance** ='JOINT' & **Innovativeness** ='TRANSFORMATIONAL' N = 9 **CAR**: {POSITIVE: 55.6%; NEGATIVE: 44.4%) IF **Customer Type** ='B2C' & **Firm Type** ='NET' & **Governance** ='JOINT' & **Innovativeness** ='TRANSFORMATIONAL' N = 8 **CAR**: {POSITIVE: 87.5%; NEGATIVE: 12.5%) IF **Product Type** = 'DIGITAL' & **Firm Type** = 'NON-NET' & **Governance** ='JOINT' & **Innovativeness** = 'TRANSFORMATIONAL' N = 29 **CAR**: {POSITIVE: 89.7%; NEGATIVE: 10.3%) IF **Product Type** = 'DIGITAL' & **Customer Type** = 'B2B' & **Firm Type** = 'NON-NET' & **Governance** ='UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 27 **CAR**: {POSITIVE: 74.1%; NEGATIVE: 25.9%) IF **Product Type** = 'TANGIBLE' & **Customer Type** = 'B2B' & **Firm Type** = 'NON-NET' & **Governance** ='UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 9 **CAR**: {POSITIVE: 88.9%; NEGATIVE: 11.1%) IF **Product Type** = 'DIGITAL' & **Customer Type** = 'B2C' & **Firm Type** = 'NON-NET' & **Governance** ='UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 16 **CAR**: {POSITIVE: 50%; NEGATIVE: 50%) IF **Product Type** = 'TANGIBLE' & **Customer Type** = 'B2C' & **Firm Type** = 'NON-NET' & **Governance** ='UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 16 **CAR**: {POSITIVE: 68.8%; NEGATIVE: 31.2%) IF **Customer Type** ='B2B' & **Product Type** ='TANGIBLE' & **Firm Type** ='NON-NET' & **Governance** ='JOINT' & **Innovativeness** = 'TRANSFORMATIONAL' N = 7

	CAR: {POSITIVE: 71.4%; NEGATIVE: 28.6%) IF **Customer Type** ='B2C' & **Product Type** ='TANGIBLE' & **Firm Type** ='NON-NET' & **Governance** ='JOINT' & **Innovativeness** = 'TRANSFORMATIONAL' N = 5 **CAR**: {POSITIVE: 80%; NEGATIVE: 20%) IF **Governance** ='UNILATERAL' & **Customer Type** ='B2B' & **Firm Type** ='NON-NET' & **Product Type** ='TANGIBLE' & **Innovativeness** ='EXECUTIONAL' N = 20 **CAR**: {POSITIVE: 60%; NEGATIVE: 40%) IF **Governance** ='JOINT' & **Customer Type** ='B2B' & **Firm Type** ='NON-NET' & **Product Type** ='TANGIBLE' & **Innovativeness** ='EXECUTIONAL' N = 6 **CAR**: {POSITIVE: 33.3%; NEGATIVE: 66.7%) IF **Governance** ='JOINT' & **Customer Type** ='B2C' & **Firm Type** ='NON-NET' & **Product Type** ='TANGIBLE' & **Innovativeness** ='EXECUTIONAL' N = 26 **CAR**: {POSITIVE: 50%; NEGATIVE: 50%) IF **Governance** ='UNILATERAL' & **Customer Type** ='B2C' & **Firm Type** ='NON-NET' & **Product Type** ='TANGIBLE' & **Innovativeness** ='EXECUTIONAL' N = 58 **CAR**: {POSITIVE: 39.7%; NEGATIVE: 60.3%) IF **Firm Type** = 'NET' & **Customer Type** ='B2C' & **Governance** = 'UNILATERAL' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 5 **CAR**: {POSITIVE: 40%; NEGATIVE: 60%) IF **Firm Type** = 'NON-NET' & **Customer Type** ='B2C' & **Governance** = 'UNILATERAL' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 19 **CAR**: {POSITIVE: 36.8%; NEGATIVE: 63.2%) IF **Firm Type** = 'NON-NET' & **Customer Type** ='B2B' & **Governance** = 'UNILATERAL' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 32

	CAR: {POSITIVE: 21.9%; NEGATIVE: 78.12%) IF **Firm Type** = 'NET' & **Customer Type** ='B2B' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 7 **CAR**: {POSITIVE: 14.3%; NEGATIVE: 85.7%) IF **Firm Type** = 'NET' & **Customer Type** ='B2C' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 10 **CAR**: {POSITIVE: 30%; NEGATIVE: 70%) IF **Firm Type** = 'NON-NET' & **Customer Type** ='B2C' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 10 **CAR**: {POSITIVE: 10%; NEGATIVE: 90%) IF **Firm Type** = 'NON-NET' & **Customer Type** ='B2B' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 22 **CAR**: {POSITIVE: 4.5%; NEGATIVE: 95.5%) IF **Firm Type** = 'NET' & **Customer Type** ='B2B' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 22 **CAR**: {POSITIVE: 0%; NEGATIVE: 100%)

Table 53: Rules that include *Customer Type* as a Predictor

Source	Rules
DT_E	IF **Customer Type** = 'B2B' & **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'UNILATERAL'& **Firm Type** = 'NET' N = 58 **CAR**: {POSITIVE: 81.7%; NEGATIVE: 19.3%) IF **Customer Type** = 'B2C' & **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'UNILATERAL'& **Firm Type** = 'NET'

	N = 28 **CAR**: {POSITIVE: 60.9%; NEGATIVE: 39.1%)
DT_Gt	IF **Customer Type** = 'B2C' & **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'UNILATERAL'& **Firm Type** = 'NET' N = 9 **CAR**: {POSITIVE: 88.9%; NEGATIVE: 11.1%) IF **Innovativeness** ='TRANSFORMATIONAL' & **Governance** = 'UNILATERAL'& **Firm Type** = 'NET' & **Customer Type** = 'B2B' N = 12 **CAR**: {POSITIVE: 83.3%; NEGATIVE: 16.7%) IF **Customer Type** ='B2B' & **Firm Type** ='NET' & **Governance** ='JOINT' & **Innovativeness** ='TRANSFORMATIONAL' N = 9 **CAR**: {POSITIVE: 55.6%; NEGATIVE: 44.4%) IF **Customer Type** ='B2C' & **Firm Type** ='NET' & **Governance** ='JOINT' & **Innovativeness** ='TRANSFORMATIONAL' N = 8 **CAR**: {POSITIVE: 87.5%; NEGATIVE: 12.5%) IF **Product Type** = 'DIGITAL' & **Customer Type** = 'B2B' & **Firm Type** = 'NON-NET' & **Governance** ='UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 27 **CAR**: {POSITIVE: 74.1%; NEGATIVE: 25.9%) IF **Product Type** = 'TANGIBLE' & **Customer Type** = 'B2B' & **Firm Type** = 'NON-NET' & **Governance** ='UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 9 **CAR**: {POSITIVE: 88.9%; NEGATIVE: 11.1%) IF **Product Type** = 'DIGITAL' & **Customer Type** = 'B2C' & **Firm Type** = 'NON-NET' & **Governance** ='UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 16 **CAR**: {POSITIVE: 50%; NEGATIVE: 50%) IF **Product Type** = 'TANGIBLE' & **Customer Type** = 'B2C' & **Firm Type** = 'NON-NET' & **Governance** ='UNILATERAL' & **Innovativeness** = 'TRANSFORMATIONAL' N = 16

	CAR: {POSITIVE: 68.8%; NEGATIVE: 31.2%) IF **Customer Type** ='B2B' & **Product Type** ='TANGIBLE' & **Firm Type** ='NON-NET' & **Governance** ='JOINT' & **Innovativeness** = 'TRANSFORMATIONAL' N = 7 **CAR**: {POSITIVE: 71.4%; NEGATIVE: 28.6%) IF **Customer Type** ='B2C' & **Product Type** ='TANGIBLE' & **Firm Type** ='NON-NET' & **Governance** ='JOINT' & **Innovativeness** = 'TRANSFORMATIONAL' N = 5 **CAR**: {POSITIVE: 80%; NEGATIVE: 20%) IF **Governance** ='UNILATERAL' & **Customer Type** ='B2B' & **Firm Type** ='NON-NET' & **Product Type** ='TANGIBLE' & **Innovativeness** ='EXECUTIONAL' N = 20 **CAR**: {POSITIVE: 60%; NEGATIVE: 40%) IF **Governance** ='JOINT' & **Customer Type** ='B2B' & **Firm Type** ='NON-NET' & **Product Type** ='TANGIBLE' & **Innovativeness** ='EXECUTIONAL' N = 6 **CAR**: {POSITIVE: 33.3%; NEGATIVE: 66.7%) IF **Governance** ='JOINT' & **Customer Type** ='B2C' & **Firm Type** ='NON-NET' & **Product Type** ='TANGIBLE' & **Innovativeness** ='EXECUTIONAL' N = 26 **CAR**: {POSITIVE: 50%; NEGATIVE: 50%) IF **Governance** ='UNILATERAL' & **Customer Type** ='B2C' & **Firm Type** ='NON-NET' & **Product Type** ='TANGIBLE' & **Innovativeness** ='EXECUTIONAL' N = 58 **CAR**: {POSITIVE: 39.7%; NEGATIVE: 60.3%) IF **Firm Type** = 'NET' & **Customer Type** ='B2C' & **Governance** = 'UNILATERAL' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 5 **CAR**: {POSITIVE: 40%; NEGATIVE: 60%) IF **Firm Type** = 'NON-NET' & **Customer Type** ='B2C' & **Governance** = 'UNILATERAL' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 19 **CAR**: {POSITIVE: 36.8%; NEGATIVE: 63.2%) IF **Firm Type** = 'NON-NET' & **Customer Type** ='B2B' & **Governance** = 'UNILATERAL' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL'

	N = 32 **CAR**: {POSITIVE: 21.9%; NEGATIVE: 78.12%) IF **Firm Type** = 'NET' & **Customer Type** ='B2B' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 7 **CAR**: {POSITIVE: 14.3%; NEGATIVE: 85.7%) IF **Firm Type** = 'NET' & **Customer Type** ='B2C' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 10 **CAR**: {POSITIVE: 30%; NEGATIVE: 70%) IF **Firm Type** = 'NON-NET' & **Customer Type** ='B2C' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 10 **CAR**: {POSITIVE: 10%; NEGATIVE: 90%) IF **Firm Type** = 'NON-NET' & **Customer Type** ='B2B' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 22 **CAR**: {POSITIVE: 4.5%; NEGATIVE: 95.5%) IF **Firm Type** = 'NET' & **Customer Type** ='B2B' & **Governance** = 'JOINT' & **Product Type** ='DIGITAL' & **Innovativeness** ='EXECUTIONAL' N = 22 **CAR**: {POSITIVE: 0%; NEGATIVE: 100%)

APPENDIX 5: GLOSSARY OF TERMS

Attack - a single Unauthorized Access attempt, or unauthorized use attempt, regardless of success

Autonomous Agents - a program or program fragment which operates independently from the user to exploit vulnerabilities

CERT®/CC - CERT® Coordination Center, formerly known as the Computer Emergency Response Team Coordination Center

Computer security - preventing attackers from achieving objectives through Unauthorized Access or unauthorized use of computers and networks

Computer virus - see "virus" below

Confidentiality - (secrecy) the principle that keeps information from being disclosed to anyone not authorized to access it

Corporate Raiders - employees of one company who break into computers of competitors for financial gain

Corruption of Information - any unauthorized alteration of files stored on a host computer or data in transit across a network

Data Tap - a device external to a network that can "listen" to the traffic on that network

Denial-of-Service - the intentional degradation or blocking of computer or network resources

Disclosure of Information -the dissemination of information to anyone who is not authorized to access that information

Distributed Tool - tools that are distributed to multiple hosts, which are then coordinated to perform an attack on a target host simultaneously after some delay

Hacker - an individual who breaks into computers primarily for the challenge and status of obtaining access

Incident - a group of attacks that can be distinguished from other incidents because of the distinctiveness of the attackers, and the degree of similarity of sites, techniques, and timing

Rootkit - an Internet toolkit containing a sniffer and Trojan horse programs to hide activity and provide backdoors for later use

Spies - individuals who break into computers primarily for information which can be used for political gain

Taxonomy - agreed upon terminologies and principles of classification in a field of inquiry

Terrorist - an individual who breaks into computers primarily to cause fear which will aid in achieving political gain

Theft of Service - the unauthorized use of computer or network services without degrading the service to other users

Toolkit - a software package contains scripts, programs, or autonomous agents that exploit vulnerabilities

Trap door - see "back doors"

Vandals - individuals who break into computers primarily to cause damage

Virus - a segment of computer code that will copy its code into one or more larger "host" programs when it is activated; it also may perform other unauthorized actions at that time

Vulnerability - a flaw in a computer or network allowing unauthorized use or Unauthorized Access

Web site - a set of files on a host computer that can be linked to over the Internet using special client software known as a Web browser

Worm - an independent program that can travel from host to host across a network

APPENDIX 6: SAMPLE ECOMMERCE ANNOUNCEMENT AND CLASSIFICATION

Copyright 1999 **Business Wire,** Inc.
Business Wire

January 4, 1999, Monday

DISTRIBUTION: Business Editors

LENGTH: 346 words
HEADLINE: Sterling Vision, Inc. to Launch Interactive E-Commerce Website
DATELINE: EAST MEADOW, N.Y.

BODY:
January 4, 1999--Sterling Vision, Inc. (ISEE-NASDAQ), one of the largest retail optical chains in the United States today announced plans to launch a fully interactive, optical goods web-site. The Company has formed a special task force to create what it believes will be the most advanced E-commerce site marketing optical products and services online. Dr. Robert Cohen, Chairman, said "We will use Sterling's 85 years of professionalism, retail experience, product and technical knowledge to enter the 21st century as the country's first true optical E-tailer". The site is currently under construction and is anticipated to be operational by the end of the first quarter of 1999. Cohen added, "The U. S. Optical market is a 15 billion dollar industry, making the potential for optical sales on the Internet virtually unlimited. Sterling is confident that it will be in the forefront of this technology, enabling the Company to increase its existing multi-million customer base of eyeglass and contact lens wearers throughout the country." All statements contained herein (other than historical facts) are based upon current expectations. These statements are forward looking in nature and involve a number of risks and uncertainties. Actual results may differ materially from the anticipated results or other expectations expressed in the Company's forward looking statements. Generally, the words "anticipate", "believe", "estimate", "expects" and similar expressions as they relate to the Company and/or its management, are intended to identify forward looking statements.

CONTACT: Sterling Vision, Inc.
Joseph Silver, Esq.
Executive Vice President &
General Counsel
(516) 390-2144

Today's News On The Net - Business Wire's full file on the Internet

with Hyperlinks to your home page.

URL: http://www.businesswire.com

LOAD-DATE: January 5, 1999

This announcement was coded as *B2C* because the benefits are promised for the end consumer and not the business entity. It was coded *Unilateral* because it was an initiative by a single business entity. This is *Executional* as the firm continues to sell the same products except that they use the Internet to support their operations. The firm is not a *Net* firm because most of the sales are not from the Internet operations but from the traditional markets. Finally the products are *Tangible* and not *Digital*.

VITA

Francis Kofi Andoh-Baidoo, a citizen of Ghana, was born on June 16, 1967 at Sefwi Atronsu, Ghana. He holds an Engineering degree from the Kwame Nkrumah University of Science & Technology, Kumasi, Ghana. He earned a Masters in Business Administration and a Master of Science in Information Technology Management degrees from the University of North Carolina, Greensboro, North Carolina, USA. Kofi is a member of the Phi Kappa Phi and the Beta Gamma Sigma honor societies. He is also a certified Oracle Database Administrator. He received the doctoral level dean's scholar award from the School of Business at the Virginia Commonwealth University for the 2005-2006 academic year.

Prior to his PhD studies, Kofi worked as a Programmer Analyst at the VF Corporation, Greensboro, North Carolina, USA. His research interests are in the areas of Use and Impact of Information and Communication Technologies, Economics of Information Systems, Information Systems Security, Data Mining, and Knowledge Management.

Kofi has published in the *Experts Systems with Applications* and *Electronic Journal on Information Systems for Developing Countries*. His research has also appeared in the proceedings of the *Americas Conference on Information Systems*, the *Hawaii International Conference on System Sciences*, and the *Decision Sciences Institute*. In 2005, a paper he co-authored and submitted to the Americas Conference on

Information Systems was nominated for the best paper award in the Emergency Management Track. One of his papers is to appear as a book chapter in the *Advances in Management Information Systems* published by ME Sharpe Inc. He is a reviewer for the Journal of Information Science and Technology. He also serves as a reviewer for several Conferences including the International Conference on Information Systems, Americas Conferences on Information Systems, and the Hawaii International Conference on System Sciences.