Available online at www.sciencedirect.com
ScienceDirect
Expert Systems with Applications 32 (2007) 703–725
Expert Systems with Applications
www.elsevier.com/locate/eswa

Exploring the characteristics of Internet security breaches that impact the market value of breached firms

Francis K. Andoh-Baidoo, Kweku-Muata Osei-Bryson *

Department of Information Systems & The Information Systems Research Institute, Virginia Commonwealth University, Richmond, VA 23284, USA

Abstract

The impact of Internet security breaches on firms has been a concern to both researchers and practitioners. One measure of the damage to the breached firm is the observed cumulative abnormal stock market return (CAR) when there is announcement of the attack in the public media. To develop effective Internet security investment strategies for preventing such damage, firms need to understand the factors that lead to the occurrence of CAR. While previous research have involved the use of regression analysis to explore the relationship between firm and attack characteristics and the occurrence of CAR, in this paper we use decision tree (DT) induction to explore this relationship. The results of our DT-based analysis indicate that both attack and firm characteristics determine CAR. While each of our results is consistent with that of at least one previous study, no previous single study has provided evidence that both firm and attack characteristics are determinants of CAR. Further, the DT-based analysis provides an interpretable model in the form of understandable and actionable rules that may be used by decision makers. The DT-based approach thus provides additional insights beyond what may be provided by the regression approach that has been employed in previous research. The paper makes methodological, theoretical and practical contribution to understanding the predictors of damage when a firm is breached.

Keywords: Internet security breaches; Event study; Market value; Firm characteristics; Attack characteristics; Decision tree induction; Data mining; Regression; Exploratory data analysis

1. Introduction

In the information age, several businesses use the Internet to drive organizational performance and survivability. Amidst its benefits, the Internet opens and exposes organizational networks to security attacks, and in recent times several organizations have been hit with security breaches (i.e. confidentiality, integrity, or availability of a firm's network, computers or information resources is compromised). An Internet security breach can have negative impacts on the firm's performance including lower sales revenues, higher expenses, decrease in future profits and dividends, and a reduction in the market value (Gordon, Loeb, & Lucyshyn, 2003; Power, 2003). The market value of a firm corresponds to the confidence that investors have in that firm. Measuring the market value of a firm that has been compromised is one way of calculating the impact of Internet security breaches. Hence, firm damage can be operationalized as the observed CAR that is attributed to the announcement of Internet security breach. In this paper we use CAR as our measure of firm damage.

Several researchers have used the event study methodology to explore the characteristics of Internet security breaches on the market value of breached firms (e.g., Campbell, Gordon, Loeb, & Zhou, 2003; Cavusoglu, Mishra, & Raghunathan, 2004; Gordon & Loeb, 2002; Hovav & D'Arcy, 2004). The event study methodology typically has two goals: (1) to determine whether or not an event,

* Corresponding author. Tel.: +1 804 827 3632; fax: +1 804 828 3199.
E-mail address: Kweku.Muata@isy.vcu.edu (K.-M. Osei-Bryson).

0957-4174/$ - see front matter © 2006 Published by Elsevier Ltd.
doi:10.1016/j.eswa.2006.01.020

such as the announcement of Internet security breach, leads to CAR, and (2) to examine the factors that influence the observed CAR. While most of the relevant 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 investment strategies to minimize Internet security breaches. In this study we also use the event study methodology to explore the characteristics of Internet security breaches on the market value of breached firms. However, while prior researches used regression, we use decision tree (DT) induction to examine variables that measure the observed negative CAR. Our major motivations for using this approach are that DTs provide an interpretable model in the form of understandable and actionable rules that may be used by decision-makers, and that a DT-based solution may provide additional insights beyond what may be provided by regression.

The rest of the paper is organized as follows. We present an overview of previous relevant research. Following we present an overview of Decision Tree Induction. We then describe our research approach. We discuss our results and highlight the differences in the findings from decision tree and regression. Finally we conclude the paper by mentioning the contributions of the research and suggesting possible future research.

2. Overview of previous research

2.1. Internet security attack characteristics

Cohen and his research partners present an extensive list of sets of attacks, defenses and effects (Cohen, 1997a; Cohen, 1997b; Cohen et al., 1998). One of their models asserts that "*Causes* (also called *threats*) use *Mechanisms* ... to produce *Effects* (also called *consequences*). *Protective Mechanisms* (also called *Defenses*) are used to mitigate harm by acting to limit the causes, mechanisms, or effects" (Cohen et al., 1998, p. 215 emphasis added). Cohen's work complements that of Howard (1997) who presents a theoretical taxonomic framework for classifying Internet security attacks.

Howard (1997) used the CERT/CC database to study the characteristics of the attacks that occurred for the period 1989–1995. He identified different types of attackers each with different objective. Attackers identify vulnerabilities in a firm's IT system and attack the firm's network, data and information. The study showed that a greater portion of security incidents were due to *Unauthorized Use* where individuals or group of individuals such as disgruntled employees abuse their access privileges to corporate networks and perform illegal activities resulting in security breaches. Notwithstanding this, there are other

Table 1
Summary of event studies on Internet security breaches

Author (s)	Period of analysis	Main focus	Variables	Some major findings
Ettredge and Richardson (2001)	February 2000	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
Cavusoglu et al. (2004)	1/1996–12/2001	Internet security breaches in general and economic effect of attack on security developers	Firm size,[a] Firm type, time lag Nature of attack[b]	• Breach firms lost average of 2.1% market value within 2 days of announcement; security developers gained 1.36% within the same period • Firm size, firm type and time lag are determinants of CAR • Nature of attack does not influence CAR
Campbell et al. (2003)[c]	1/1995–12/2000	Confidential Information	Nature of attack(confidential vs. non-confidential)	• Nature of attack influences CAR, i.e., loss of confidential information leads to negative CAR.
Hovav and D'Arcy (2003)	1/1998–6/2002	Denial-of-service attacks	Nature of attack (Denial-of service-attack vs. non-denial-of-service attack)	• Market does not penalize firms that report denial of service attack, i.e. nature of attack is not a determinant of CAR • Net firms have higher negative CAR than non- net firms
Hovav and D'Arcy (2004)	1/1998–12/2002	Virus attacks	Nature of attack (Virus attack vs. non-virus attack)	• Virus attack is not a determinant of CAR, i.e., nature of attack is not a determinant of CAR

[a] In all the studies Firm size was categorized as small or large using financial market data.
[b] Measure of this variable varies across the studies.
[c] In all the studies the hypothesis that Internet security leads to abnormal stock market return was highly significantly confirmed except Campbell et al. where it was marginally significant ($\alpha = 0.051$).