Financial Impact of Information Security Breaches on Breached Firms and their Non-Breached Competitors

Humayun Zafar, Kennesaw State University, USA

Myung S. Ko, The University of Texas at San Antonio, USA

Kweku-Muata Osei-Bryson, Virginia Commonwealth University, USA

ABSTRACT

Information security breaches pose a growing threat to organizations and individuals, particularly those that are heavily involved in e-business/e-commerce. An information security breach can have wide-ranging impacts, including influencing the behaviors of competitors and vice versa within the context of a competitive marketplace. Therefore, there is a need for further exploration of implications of information security breaches beyond the focus of the breached firm. This study investigates the financial impact of publicly announced information security breaches on breached firms and their non-breached competitors. While controlling for size and the industry the firm operates in, the authors focus on specific types of information security breaches (Denial of Service, Website Defacement, Data Theft, and Data Corruption). Unlike previous studies that have used event study methodology, the authors investigate information transfer effects that result from information security breaches using the matched sampling method. The study reveals statistically significant evidence of the presence of intra-industry information transfer for some types of security breaches. The authors also found evidence of contagion effects, but no similar evidence concerning competition effect.

Keywords: *Competition Effect, Contagion Effect, Financial Impact, Information Security Breach, Information Transfer, Organizational Impact*

INTRODUCTION

Over the past decade, more and more organizations and individuals have been using the Internet to conduct business transactions. While this e-business/e-commerce trend has provided important benefits to both organizations and individuals, it has also offered increased opportunities for hackers to breach information systems. So it is not surprising that information security breach incidents have also risen sharply (Bagchi & Udo, 2003; Cavusoglu, Mishra, & Raghunathan, 2004; Claburn, 2009; Gatzlaff & McCullough, 2010; Hovav & D'Arcy, 2004;

DOI: 10.4018/irmj.2012010102

Khansa & Liginlal, 2011) For example, when malware compromised IT systems at Heartland Payment Systems in 2008, over 94 million credit card accounts were compromised (Claburn, 2009). It is estimated that about 85% of all U.S. companies have experienced one or more information security breaches (Riddell, 2011). Costs associated with information security breaches have also increased. The Ponemon Institute in its annual study in 2010 reported that the average cost of a data breach for a firm was $7.2 million, an increase of 7% from the year before (Ponemon Institute, 2010). The report also stated that lost business represented 63% of the total cost in the U.S. A study by McAfee also estimated that global economic losses due to information security breaches in 2008 amounted to over $1 trillion (Mills, 2009).

Given the potentially significant impact that an information security breach may have on individuals and organizations, several researchers have previously investigated implications of this phenomenon on organizational performance (Acquisti, Friedman, & Telang, 2006; Bass, 2000; Cavusoglu et al., 2004; Kim, Lacina, & Park, 2008; Straub & Nance, 1990; Whitworth & Zaic, 2003). For the most part, these studies have focused on the short-term impact of publically announced security breaches on the stock market value of the breached firm (Campbell, Gordon, Loeb, & Zhou, 2003; Ettredge & Richardson, 2003). Some studies have also focused on the medium term impact on the breached firm via accounting performance measures (Ko & Dorantes, 2006; Ko, Osei-Bryson, & Dorantes, 2009).

Events such as information security breaches in firms have a wide-ranging impact. For example, they can influence the behavior of competitors and vice versa within the context of a competitive marketplace. Therefore, there is a need for further exploration of implications of information security breaches beyond the focus of the breached firm. As observed by previous researchers (Kim et al., 2008; Aharony & Swary, 1983; Foster, 1981), information transfer exists between a firm making a public announcement regarding an event, and industry counterparts that are its close competitors. The subject of information transfer effect has been investigated at length in various fields including accounting, economics, and finance (Clinch & Sinclair, 1987; Kim et al., 2008; Szewczyk, 1992), but has been relatively unexplored in information systems (IS) research. Also, past research on the effects of information transfer has shown disparate results (Coroama & Röthenbacher, 2003; Helal, Giraldo, Kaddoura, Lee, El Zabadani, & Mann, 2003), thus suggesting the need for further research on this topic, particularly in regard to IS security.

In this study, we explore the intra-industry information transfer effects of publicly announced information security breaches. An intra-industry information transfer exists when information released by one firm affects the performance of other non-announcing firms in the same industry. For example, in September 2008, when Lehman Brothers announced its bankruptcy, the share prices of Morgan Stanley, Goldman Sachs, and Citigroup also dropped 13.5%, 12.1%, and 15.1%, respectively (Shen, 2008). Such information transfer can occur in two ways: *contagion* and *competition* effects (Floerkemeier & Siegemund, 2003; Szewczyk, 1992). A *Contagion Effect* occurs when a non-announcing firm's financial performance reaction is in the same direction as that of the announcing firm. It also usually arises from industry commonalities. A *Competition Effect* occurs because of shifts in the industry's competitive balance and tends to be in the opposite direction.

In the following section, we review previous studies on information security breaches and intra-industry information transfer effects. After that, we discuss this study's research hypotheses, research method including financial performance indicators, and data collection. Then we report results from our analysis and provide interpretation, implications, and limitations of our results. In the final section, we conclude our study with the inclusion of some suggestions for future studies.