



Investigating the Impact of Publicly Announced Information Security Breaches on Three Performance Indicators of the Breached Firms

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

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

Carlos Dorantes, The University of Texas at San Antonio, USA

ABSTRACT

This article examines the impact of information security breaches on organizational performance. Until now, there have been only a few empirical academic studies that have investigated this issue and they have investigated information security breaches with the focus on the short-term impact on the market value of the firm. This study offers an alternate approach to investigate this issue as it explores the impact of breaches on financial performance of the firm, one year after the breach. Using a “matched sampling” methodology, we explored the impact of each type of breach (i.e., confidentiality, integrity, and availability) and also by IT intensity and size. Our results suggest that the direction of the impact (i.e., positive, negative) is dependent on the type of security breaches and also the impact of IT intensive firms is different from non-IT intensive firms. Our study also includes some important implications for managers and stock market investors. [Article copies are available for purchase from InfoSci-on-Demand.com]

Keywords: *Availability; Confidentiality; Impact; Information Security; Integrity; Organizational Performance; Security Breach*

INTRODUCTION

Today, as more organizations conduct their businesses over the Internet, exposure to information security attacks is also increasing. The 2004 Global Security Survey of financial institutions by Deloitte and Touche reported that

83% of respondents indicated that their systems had been compromised in 2004, compared to 39% in the previous year, an increase of over 100% in a single year (Anonymous, 2004). The 2004 E-crime Watch survey by Chief Security Officer (CSO) magazine also reported that 43% of respondents noted an increase in information security breaches compared to the previous year

and 70% had experienced at least one breach incident¹. Information security breaches include virus, spyware, unauthorized access to information, theft of proprietary information, denial of service (DOS), system penetration, sabotage, and Web site defacement, and so forth. According to the 2005 Computer Crime and Security Survey by CSI-FBI, the average loss per incident from *unauthorized access to information* has increased to \$300K from \$51K and the loss from *theft of proprietary information* has increased to \$356K from \$169K, indicating a doubling of such losses compared to 2004 (Gordon, Loeb, Lucyshyn, & Richardson, 2004, 2005).

Ponemon Institute reported that total costs for each data breach ranged from less than \$1 million to more than \$22 million in their 2006 annual study, which investigated financial impact of data breaches involving customers' personal information (Ponemon, 2006). In general, costs of a security breach on organization can classify into short-term and long-term costs (Cavusoglu et al., 2004; D'Amico, 2000; Erbschloe, 2005). For example, short-term costs are costs incurred to deal with the breach immediately after or during the period following the breach and thus, are short-term in nature. These costs include costs to repair or replace the systems, loss of business, or decreased productivity due to the disruption of business operations, and any costs related to reporting information to the public, customers, and business partners about the breach, and so forth. Long-term costs are costs that can have a significant impact on the organization's future cash flow and thus they have the long-term economic impact and costs incur over several periods. These costs include revenue lost due to the loss of existing or future customers, a decline in investors' confidence due to a negative reputation of the organization, potential legal liabilities from the breach, and reduced goodwill (Cavusoglu et al., 2004; D'Amico, 2000; Featherman, Valacich, & Wells, 2006; Ponemon, 2006; Tsiakis & Stephanides, 2005). Thus, consequences of a security breach incident could result in tremendous financial losses to the targeted organization (Egan &

Mather, 2005; Garg, Curtis, & Halper, 2003b; Warren & Hutchinson, 2000).

While there are many news and surveys that have reported the magnitude of the monetary losses from the breach incidents, there have been only a few empirical academic studies that have investigated this issue and these previous studies employed an event study methodology with the focus on an impact on the market value of the firm (Campbell, Gordon, Loeb, & Zhou, 2003; Cavusoglu et al., 2004; Garg, Curtis, & Halper, 2003a,b; Hovav & D'Arcy, 2003, 2004). The event study investigates the stock market reaction to the public announcement of a security breach since there is a belief that this unexpected event can have immediate adverse effect on the breached organization's stock price. Accordingly, such unexpected announcement may lower the market value of the breached organization and thus, the organization can incur a loss or experience a negative abnormal return because the actual return of the stock would be lower than the expected return due to the changes in investors' expectations about the company since the organization can suffer from the public relations exposures than the breach itself. However, it is unclear if this loss will affect the organization's ability to generate revenue in the long term.

Our research objective is to assess the relative magnitudes of the impact on organizational performance of different types of security breaches. In this study, we use the three properties of information security—*confidentiality*, *integrity*, and *availability*—to classify the type of security breach. Thus, this study offers an alternate approach to investigate the impact of publicly announced information security breaches on firms.

Previous event studies examined the market value of the breached firm a few days following the announcement of information security breaches and found the significant negative market reaction. If investors' expectations on the breached firms' future cash flows were true, financial performance of the breached firms would be decreased over time. Although organizational performance is a multifaceted aspect

19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/investigating-impact-publicly-announced-information/1357

Related Content

Offshore Software Testing in the Automotive Industry: A Case Study

Tabata Pérez Rentería y Hernándezand Nicola Marsden (2017). *International Journal of Information Technology Project Management* (pp. 1-16).

www.irma-international.org/article/offshore-software-testing-in-the-automotive-industry/187158

Enterprise Information Systems Change, Adaptation and Adoption: A Qualitative Study and Conceptualization Framework

Boris Jukic, Nenad Jukicand Miguel Velasco (2009). *Information Resources Management Journal* (pp. 63-87).

www.irma-international.org/article/enterprise-information-systems-change-adaptation/1356

Neural Networks for Intrusion Detection

Rui Ma (2009). *Encyclopedia of Information Science and Technology, Second Edition* (pp. 2800-2805).

www.irma-international.org/chapter/neural-networks-intrusion-detection/13985

An Empirical Study of the Casual Relationship Between IT Investment and Firm Performance

Qing Huand Robert Plant (2001). *Information Resources Management Journal* (pp. 15-26).

www.irma-international.org/article/empirical-study-casual-relationship-between/1201

Semantic Querying of News Articles With Natural Language Questions

Tuan-Dung Caoand Quang-Minh Nguyen (2021). *Journal of Information Technology Research* (pp. 38-57).

www.irma-international.org/article/semantic-querying-of-news-articles-with-natural-language-questions/279033