Chapter 85
It's Not My Fault: The Transfer of Information Security Breach Information

Tawei Wang
DePaul University, Chicago, USA

Yen-Yao Wang
Auburn University, Auburn, USA

Ju-Chun Yen
National Central University, Taoyuan City, Taiwan

ABSTRACT

This article investigates the transfer of information security breach information between breached firms and their peers. Using a large data set of information security incidents from 2003 to 2013, the results suggest that 1) the effect of information security breach information transfer exists between breached firms and non-breached firms that offer similar products and 2) the effect of information transfer is weaker when the information security breach is due to internal faults or is related to the loss of personally identifiable information. Additional tests demonstrate that the effect of information transfer exhibits consistent patterns across time and with different types of information security breaches. Finally, the effect does not depend on whether the firms are IT intensive. Implications, limitations, and future research are discussed.

INTRODUCTION

In 2013, Target was breached due to the insecure configuration of software and hardware, resulting in over 40 million credit and debit card numbers and 70 million records of personal information stolen from nearly 2,000 Target stores (Radichel, 2014). After news of the breach leaked on December 19, 2013, Target's profit fell nearly 50% in its fourth fiscal quarter of 2013 and its stock dropped by 9%.[1] In today's information-driven marketplace, cyber intrusions have become very common (Malhotra and

DOI: 10.4018/978-1-7998-7705-9.ch085

Kubowicz Malhotra, 2011) and are expected to grow substantially in numbers and complexity (Kwon, Ulmer, & Wang, 2012). Prior research has examined the effect of information security breach information or disclosure in various settings, such as the textual content of risk factor disclosures (e.g., Wang, Kannan, and Ulmer, 2013a), market value (e.g., Gordon, Loeb, and Sohail, 2010), customer satisfaction (e.g., Wang and Huff, 2007), auditor effects (e.g., Yen, Lim, Wang, and Hsu, 2018), board or top management team composition (e.g., Feng and Wang, 2019; Hsu and Wang, 2014a, 2014b, 2015), profitable short-term investment opportunities (e.g., Wang, Ulmer, and Kannan, 2013b), and customer behavior in a multichannel setting (e.g., Janakiraman, Lim, and Rishika, 2018).

Although earlier works provide considerable knowledge on the effects of information security breaches, most of the current literature focuses on the impact of information security breaches on the firms encountering them (i.e., the breached firm). This approach ignores the dynamic effects of information security breaches on other firms in the same industry that are affiliated or compete with the breached firm, which is often referred to as a spillover effect or the transfer of information security breach information. According to Foster (1981), information transfer exists when an economic event of one firm affects another firm's or other firms' stock price(s). In particular, in the context of information security, information transfer refers to the situation where the business value of a firm that is not reported as breached is affected positively or negatively because another firm of similar measure (defined later) has been reported as breached. For instance, information security software or hardware providers can benefit from the proliferation of security incidents, whereas Internet firms can be harmed by other Internet firms' breach announcements (Ettredge and Richardson, 2003; Garg, Curtis, and Halper, 2003). More recently, Kashmiri, Nicol, and Hsu (2017) also find that the Target customer data breach announcement led to a shareholder value loss for other U.S. retailers, suggesting a pressing need to go beyond examining the effects of information security breaches on only the firms encountering them.

Given that information/data security is vital in today's highly dynamic business environment (Wang et al., 2012), understanding the dynamic nature of information security breach information is essential because, in a competitive marketplace, it is less likely that a negative event will affect only the breached firms. Scholars also call for more discussions on the dynamics of information security breach information to better understand the broader implications of information security breaches (e.g., Janakiraman et al., 2018; Kashmiri et al., 2017). Therefore, to gain a more holistic understanding of the impacts of information security incidents, this study attempts to address the following research questions: 1) Does the transfer of information security breach information exist in same-industry groups or among major competitors? 2) How does the transfer of information security breach information vary by cause and type of information compromised?

By using a large data set of information security incidents from 2003 to 2013, we first investigate whether we can detect potential information transfer within an industry or between major competitors. We further examine whether the effect of information transfer can vary by cause or type of information compromised. In addition, several robustness tests by time periods and by information technology (IT) intensive industries are performed to further validate our results and to provide a more holistic view of information transfer associated with the information security incidents.

Our research, different from prior research with a focus on a single industry (e.g., Janakiraman et al., 2018; Kashmiri et al., 2017), suggests that the effect of the transfer of information security breach information does exist between focal breached firms and non-breached firms of high product similarity instead of industry group members. Our study also shows that the effect of information transfer from breached to non-breached firms is short term and is weaker when the breach is caused by internal faults