International Review of Financial Analysis xxx (2017) xxx–xxx

Contents lists available at ScienceDirect

International Review of Financial Analysis

The effect of data breach announcements beyond the stock price: Empirical evidence on market activity

Pierangelo Rosati [a], Mark Cummins [b,*], Peter Deeney [b], Fabian Gogolin [b], Lisa van der Werff [b], Theo Lynn [a]

[a] Irish Centre for Cloud Computing and Commerce, Dublin City University, Dublin 9, Ireland
[b] DCU Business School, Dublin City University, Dublin 9, Ireland

ARTICLE INFO

Article history:
Received 9 August 2016
Received in revised form 14 December 2016
Accepted 12 January 2017
Available online xxxx

JEL codes:
G12
G14
O30

Keywords:
Data breach
Stock market
Bid-ask spread
Trading volume
Event study

ABSTRACT

Extending the literature that has focused thus far on stock price impact, this study investigates the effect of data breach announcements on market activity, specifically through the response of the bid-ask spread and trading volume. We investigate data breach announcements as a potential source of asymmetric information and provide a new dimension to the ongoing debate on market efficiency. Adopting an event study methodology on a sample of 74 data breaches from 2005 to 2014, we find that data breach announcements have a positive short-term effect on both bid-ask spread and trading volume. The effect is only evidenced however on the day of the event, with market efficiency ensuring a quick return to normal market activity. No abnormal trading activity emerges before announcements, so there is no evidence in our study that these types of events are being exploited by informed market participants. The magnitude of event day effects is found to be more pronounced for large breaches, and when the breach involves lost devices.

1. Introduction

In the last decade the amount of data collected, processed and stored by firms has grown exponentially and this tendency will probably continue in the next years (LaValle, Lesser, Shockley, Hopkins, & Kruschwitz, 2011). Data analytics has been, and still is, reshaping many industries (Minelli, Chambers, & Dhiraj, 2012) e.g. healthcare, banking, finance and media and communications, but it also raises a firms' activity risk (Chen, Chiang, & Storey, 2012). Stored data are usually highly sensitive and extremely valuable thus they attract the attention of cyber criminals; as a result, the number and the cost of incidents have grown significantly in the last decade (Ponemon, 2015; Verizon, 2015) and cyber security has become a key issue for both managers and regulators (Deloitte, 2016; George, 2016; Hulme, 2015; SEC, 2014, 2016).

Within this context, we analyse the impact of data breach announcements on market activity, in order to investigate the presence of informed trading and test for market efficiency around this new corporate event type. We extend the existing literature that to date has focused on stock price impact and the effect on corporates. We move attention to the broader issue of market activity and address concerns of relevance to the wider investment community. A number of contributions are made.

First, we analyse bid-ask spread determination through analysing data breach announcements as a potential source of asymmetric information between market dealers and uninformed liquidity traders, and informed traders. A myriad of corporate events have been studied to date including earnings announcements (Affleck-Graves, Callahan, & Chipalkatti, 2002; Krinsky & Lee, 1996; Lee, Mucklow, & Ready, 1993; Venkatesh & Chiang, 1986); auditor change (Hagigi, Kluger, & Shields, 1993); stock repurchases (Franz, Rao, & Tripathy, 1995); management earnings forecasts (Coller & Yohn, 1997); bankruptcy (Frino, Jones, & Wong, 2007) and merger and acquisition (Chan, Ge, & Lin, 2015). Heretofore however, market activity around data breach announcements has not been studied. Furthermore, data breaches have particular characteristics compared to other corporate events. Data breach events are truly unexpected, both in terms of timing and frequency of occurrence (Ko, Osei-Bryson, & Dorantes, 2009), which is an advantage in a study like this. Many of the corporate events studied to date are expected, to varying degrees, and primary interest lies in deviations from market expectations. Mergers and acquisitions come closest to unexpected events (Augustin, Brenner, & Subrahmanyam, 2015), but are not truly unexpected given the protracted nature of the associated negotiations and strategic manoeuvrings by the players involved. Data breaches therefore present a fresh testing ground to analyse market behaviour.

* Corresponding author.
E-mail address: mark.cummins@dcu.ie (M. Cummins).

http://dx.doi.org/10.1016/j.irfa.2017.01.001
1057-5219/

Second, we conduct a round of testing on trading volume as an alternative measure of market activity, to investigate whether there is consistency with our findings on the bid-ask spread. While the effect of (expected or unexpected) corporate events on pricing is unambiguous, namely the widening of the bid-ask spread to protect market dealers from uninformed traders, the effect on trading volume is, to the contrary, ambiguous and more nuanced. One school of thought suggests that trading volume may increase in the presence of asymmetric information, resulting from the exogeneity and inelasticity of uninformed liquidity trading (Chae, 2005; Kyle, 1985), while another suggests that trading volume may decrease in the presence of asymmetric information, where it is assumed in this case that liquidity traders have timing discretion (Admati & Pfleiderer, 1988; Chae, 2005; Foster & Viswanathan, 1990). Either way, the suggested abnormal volume effects correspond to informed traders optimizing their advantage over market dealers and uninformed liquidity traders.

Third, we examine the duration of abnormal trading activity, if it exists, post data breach announcements. How fast the market absorbs new information is at the core of the Efficient Market Hypothesis (Fama, 1970). Other corporate events that have been analysed in the past show mixed evidence as to whether markets are efficient or not. Our analysis sheds new light on this topic of market efficiency, showing to what extent the market monitors and responds to emerging news on the modern corporate phenomenon of data breaches.

Finally, we examine the factors that may determine the magnitude and direction of impacts on market activity from data breach events. Informed by the literature, we consider the size of the breach as a possible factor, positing that impacts are more pronounced for larger breaches relative to smaller breaches. We also examine whether the type of breach that has occurred is a factor, and whether the consequences of a data breach depend on the industry in which a breached firm operates. Analysing the impact of data breach announcements on market activity across these dimensions adds additional insight to the existing evidence on stock price response.

Using a dataset of 74 data breaches, involving US publicly traded firms over the period 2005 to 2014, we assess the impact of the associated announcements on market activity. We find evidence of a positive short-term impact of data breach announcement on bid-ask spread and trading volume. The effect is only evidenced however on the day of the event, with market efficiency ensuring a quick return to normal market activity. No abnormal trading activity emerges before announcements, providing evidence that these types of events are not being exploited by informed market participants. The effect on bid-ask spread is evidenced to be more pronounced for events that involve a large number of records or that involve lost devices; the effect on trading volume is evidenced to be more pronounced for larger firms and for events that involve lost devices.

The rest of the paper is organised as follows. Section 2 provides a review of the relevant literature and formally states the research hypotheses. Section 3 presents the data. Section 4 discusses the research design. Section 5 presents the results of the empirical analysis. Section 6 reports some important concluding remarks.

2. Literature review and hypotheses development

The number of incidents affecting information systems is growing every year and actual and emerging trends such as social media, cloud computing, mobile devices and big data exacerbate this issue (Abbasi, Sarker, & Chiang, 2016; Romanosky, Hoffman, & Acquisti, 2014). Goldstein, Chernobai, and Benaroch (2011) classify such events into two main categories, namely data-related and function-related events. A data-related event is any threat to the confidentiality of data assets that can result in the disclosure, misuse, or destruction of these assets. A function-related event, instead, is any threat to the availability or to the integrity of functional information systems (that may eventually affect data assets). Although both event types impose significant costs to the affected companies, such costs are due to different causes and are spread differently over time. Short-term costs of data events are mainly related to investigation and remediation activities, legal advisory and fines, while long-term costs are related to loss of present and future revenues and deterioration of customers' or partners' trust (Cavusoglu, Mishra, & Raghunathan, 2004). Short-term costs of function events include losses in terms of lost productivity and lost transactions (Paquette, Jaeger, & Wilson, 2010), as well as remediation costs that can vary depending on the type of incident (Charette, Adams, & White, 1997; Dennis, Wixom, & Tegarden, 2015), while long-term costs are related to loss of growth opportunities (Bharadwaj, Bharadwaj, & Konsynski, 1999) and inefficiencies (Arend, 2004). Regardless of the event type, a breach imposes significant costs on the affected firm.

Famous cases of data and function events are ChoicePoint and Nasdaq. In early 2006, ChoicePoint paid a $10 million fine as a result of its breach and another $5 million to a fund to compensate affected individuals (FTC, 2009). In 2012, the websites of exchanges Nasdaq and BATS suffered a 24-hour attack that led to intermittent service disruptions (Krudy, 2012) and to a 12% decrease in daily US stock trading activity (Savitz, 2012).

Given that the overall cost of a breach includes many different components, and that such components span over different periods of time, the quantification of such a cost is extremely complex. The change in stock price following the data breach announcement is often adopted as a proxy. This assumption is based on the semi-strong Efficient Market Hypothesis as stated by Fama (1970). Following this hypothesis, a stock price incorporates all public information and all future expected firm cash flows. The majority of existing empirical studies focus on the wider category of security breaches and they analyse typically small samples. Campbell, Gordon, Loeb, and Zhou (2003) analyse 43 events from 1995 to 2000 and they find no statistically significant abnormal returns except for 11 events, which involve confidential data, where stock prices drop by 5.5% over a three-day period around the announcement. Garg, Curtis, and Halper (2003) examine 22 information security incidents from 1996 to 2002 and they find an average share price decline of −5.3% over a three-day period following the announcement. Hovav and D'Arcy (2003) examine 23 denial-of-service (DOS) attacks between 1998 and 2002, and they show no statistically significant stock price response. Cavusoglu et al. (2004) analyse 66 events from 1996 to 2001 and they provide evidence of an average abnormal return of −2.1% over a two-day window following the event. They also demonstrate that the breach cost is higher for those firms that rely only on the Internet for doing business, and that this cost is not significantly different across breach types.

The conflicting results of these studies may be due to event choice since they typically analyse security breach events or a mixture of security and data breaches. Such events are different from each other and some of them may have non-significant economic impact. To the extent of our knowledge, only Gatzlaff and McCullough (2010) examine data breach events as defined above. Their sample includes only events that involve employees' or customers' personal information. Their analysis of 77 events from 2004 to 2006 shows a decline in share price of 0.84% over a two-day time window starting from the announcement day and that the breach effect is more significant in the most recent period of the analysis.

While the impact of breach announcements on financial markets is garnering greater attention, existing studies focus solely on price reaction (i.e. abnormal returns). None have investigated other important aspects of trading activity, such as the bid-ask spread and trading volume. Bid-ask spread and trading volume are well-established proxies to detect informed trading and allow for an examination of the effect of temporary information advantages that informed investors might hold (Chae, 2005; Pinder, 2003). We are motivated to take the dual approach of analysing bid-ask spread and trading volume together in our study given that data breach events have not been considered to date in this

Please cite this article as: Rosati, P., et al., The effect of data breach announcements beyond the stock price: Empirical evidence on market activity, *International Review of Financial Analysis* (2017), http://dx.doi.org/10.1016/j.irfa.2017.01.001