UNIVERSITÄT AUGSBURG
Universitätsbibliothek

OPEN ACCESS
OPUS AUGSBURG

NSA revelations of privacy breaches: do investors care?

Timo Cziesla, Jan Kemper, Jan Muntermann, Griselda Sinanaj

Angaben zur Veröffentlichung / Publication details:

Cziesla, Timo, Jan Kemper, Jan Muntermann, and Griselda Sinanaj. 2015. "NSA revelations of privacy breaches: do investors care?" In *Proceedings of the 21st Americas Conference on Information Systems, AMCIS 2015, Fajardo, Puerto Rico, August 13-15, 2015*, 36. New York, NY: AISeL. https://aisel.aisnet.org/amcis2015/ISSecurity/GeneralPresentations/36/.

Nutzungsbedingungen / Terms of use:

licgercopyright

Dieses Dokument wird unter folgenden Bedingungen zur Verfügung gestellt: / This document is made available under these conditions:
Deutsches Urheberrecht
Weitere Informationen finden Sie unter: / For more information see:
https://www.uni-augsburg.de/de/organisation/bibliothek/publizieren-zitieren-archivieren/publiz/

NSA REVELATIONS OF PRIVACY BREACHES: DO INVESTORS CARE?

Full papers

Griselda Sinanaj
University of Göttingen
griselda.sinanaj@wiwi.uni-goettingen.de

Timo Cziesla
University of Göttingen
timo.cziesla@wiwi.uni-goettingen.de

Jan Kemper
University of Göttingen
jan.kemper@wiwi.uni-goettingen.de

Jan Muntermann
University of Göttingen
muntermann@wiwi.uni-goettingen.de

Abstract

Our study is focused on the financial impact of NSA-security and privacy breach events announced in the news media between June 2013 and March 2014. While prior research has provided empirical evidence on the stock market reaction of security and privacy breaches such as confidentiality, integrity and availability breaches, there is scarce research on the financial impact of NSA-related security and privacy breaches. Based on previous studies, we apply the event study framework to analyze how NSA revelations influence investors' confidence. Results show that NSA-breach announcements have a negative impact on investors' confidence, which is confirmed by the negative cumulated abnormal returns on the event date. Our study contributes hence with insights on a relatively new phenomenon of high relevance concerning the security of information assets.

Keywords

National Security Agency (NSA), security breaches, event study.

Introduction

The National Security Agency (NSA)-scandal started with the revelations of the British newspaper *The Guardian* and the American newspaper *The Washington Post* in June 2013, which brought to the light a list of mass surveillance and data collection programs on citizens' data. News media reports show that intelligence organizations such as the NSA, the British counterpart the Government Communications Headquarters (GCHQ) and other intelligence services of partner countries, are able to access stored data of US technology companies without search warrants. Further revelations include the supervision of telephone data of politicians, monitoring of diplomatic missions, monitoring the World Bank and the International Monetary Fund (The Guardian 2013c). These revelations have triggered strong concerns about the increasing number of domestic surveillance, the scope of global monitoring, but also on the credibility of the technology sector and the safety and privacy of information.

"People will not use technology they do not trust. Governments have put this trust at risk, and Governments need to help restore it. " - Brad Smith, General Counsel, Microsoft (The New Work Times 2013).

The statement above points out the negative effects on companies originating from either the voluntary or forced collaboration with the NSA, which are reflected not only in the short term but might also persist in the long run.

Information security literature distinguishes between two types of costs inflicted by security and privacy breaches: tangible and intangible costs. Tangible costs include lost revenue, lost productivity and

increased hardware and software expenses. Intangible costs are the loss of investors' confidence, loss of competitive advantage and reputational damage (Cavusoglu et al. 2004; Yayla and Hu 2011). The negative effect of security breach events on investors' confidence and the consequent loss of market value has been investigated in several studies (e.g. Garg et al. 2003; Hinz et al. 2015; Hovav and D'Arcy 2003). As the disclosure of NSA-security breaches is a new phenomenon and there is scarce research on this topic, the scope of our study is to investigate the impact of NSA-security breach announcements on the capital market. The research question is: *How does the announcement of NSA-security and privacy breaches reflect into the stock market value of the affected companies*?

To address our research question, we build a representative sample of NSA-security breach events by searching the full text of five major international newspapers: *The Guardian, The Washington Post, The Wall Street Journal, The New York Times and Spiegel Online*. From a methodological perspective, in line with previous literature on the financial impact of security breaches, we perform an event study in order to observe the stock market reaction around the event date. This study provides therefore empirical evidence on a relatively new phenomenon of high relevance concerning the security, safety and privacy of information.

The remainder of the paper is organized in the following parts. The following section provides a summary of the relevant literature dealing with the financial impact of security and privacy breaches. In the sample selection section we describe the data collection process and provide descriptive statistics on the final data sample. Then we describe the event study framework in the methodology section, discuss the results and conclude with the implications, limitations and insights on future research.

Related Work

The scope of information security is to guarantee the confidentiality, availability and integrity of information. The violation of one of these three principles leads to information security breaches (or incidents) (Whitman and Mattord 2011). A confidentiality breach occurs for instance in case of an unauthorized access and appropriation of sensitive information, such as customer or employee data. Integrity breaches are viruses, worms, malware, which compromise the integrity of data. Denial-of-Service (DoS) attacks are availability breaches, since they have the aim to render the use of a website or of a service not available to legitimate users or customers (Kannan et al. 2007).

Studies investigating the impact of security breaches on shareholder wealth from a capital market perspective based on the event study method have generated contradictory results (Yayla and Hu 2011). Focusing on samples of different types of security breaches, some authors find a moderate negative impact due to security breach announcements, yet statistically not significant (Gordon et al. 2011). Campbell et al. (2003) have empirically investigated the impact of information security incidents on a sample of 43 events and do not find evidence of a significant impact. On the contrary, other studies provide evidence of a significant negative market reaction due to security breach events. Yayla and Hu (2011) examined 130 events and found that the decrease in the stock prices is significant at least at the 10% significance level.

Confidentiality breaches result into larger financial losses compared to non-confidentiality breaches. In the study of Campbell et al. (2003), the subsample of 11 confidentiality breaches shows a significant negative market impact, whereas the negative effect of the subsample of 32 non-confidentiality breaches is not significant. In the study of Gordon et al. (2011) the largest financial losses are caused by availability breaches and not from breaches of confidentiality.

The information security literature has also investigated the financial impact of privacy breaches (also known as data breaches) defined as "*instances in which the data of consumers, employers, or third parties associated with a company traded on a public market was exposed through bad security practices, hacker attacks, insider attacks, computer or data thefts, and lost data or equipment* (Acquisti et al. 2006, p. 6). Based on the definition above, privacy breaches can be interpreted as confidentiality breaches that involve the unauthorized appropriation of personally identifiable information that leads to the identification of a person and the consequent identity theft. Some research has focused on the financial impact of privacy breaches, which involve the theft or loss of private information, for instance financial information (e.g. credit card number), medical information (e.g. social security number) etc.

Acquisti et al. (2006) have analyzed the stock market reaction of 79 privacy breaches and have found evidence of negative returns following the disclosure of privacy breach announcements.

Studies focused on breaches of availability by analyzing the capital market reaction of DoS attacks have also generated incongruous results. The study of Ettredge and Richardson (2003) is one of the earliest works that has investigated the negative effects of hacker attacks on e-commerce companies. The authors measure the stock market reaction of four DoS attacks and find significant negative returns due to these breach events. Yayla and Hu (2011) studied 123 cases of IT security incidents in the period from 1994 to 2006 and find that DoS attacks have the greatest impact in comparison to other types of attacks, while Hovav and D'Arcy (2003) do not find any significant negative returns due to DoS attacks. In addition to DoS attacks, Hovav and D'Arcy (2004) have also analyzed the financial effect of virus attacks. Out of more than 186 cases distributed over 15 years, they did not find any evidence of a significant impact on the stock prices of the affected companies.

In sum, security incidents are usually seen as an indicator for poor management of technology and low security standards and have a negative impact on capital markets. However, prior research focused on the economic impact of security and privacy breaches has produced mixed and inconclusive results (Gatzlaff and McCullough 2010; Yayla and Hu 2011). One possible explanation for these findings might be the fact that researchers rely on samples of different characteristics.

Our study differs from previous research in several aspects. First, "classic" security breaches such as viruses, malware, DoS attacks, data theft (clients' names, addresses, email addresses, social security numbers, phone numbers, security positions, cash positions) are inflicted by hackers or third parties whose identity remains unknown to the public. At the center of this study are security breaches inflicted from the government. Furthermore, some of the data collection programs operated by the NSA are court-approved and have been conducted in an unauthorized manner with the knowledge of the cooperating firms, while privacy breaches (or data breaches) indicate an unauthorized action. In addition, NSA has collected in some cases only metadata, which are defined as "data over data" and do not include content of communication (The Guardian 2013a). For instance, based on a legal order, NSA has collected telephone meta data from Verizon Communications Inc., such as "*originating and terminating telephone numbers, time and duration of each call but not the content of telephone conversations*" (The Washington Post 2013). Based on this definition the collection of telephone records at Verizon Communications Inc. cannot be classified as a privacy breach, since metadata do not entail any personal private information but only transactional users' data (The Guardian 2013b). For the scope of this study we assign security breach announcements involving the collection of metadata to the category of privacy breaches. The application of sophisticated computer analysis on this type of data allows analysts to discover patterns which might lead to the identification of a person and is therefore a privacy violation. Although the terms "security" and "privacy" are often used in the literature as synonyms to describe the same phenomenon (Liginlal et al. 2009), in our study we make a distinction between the two terms and classify the identified security breaches into two subcategories: privacy breaches, which involve the unauthorized appropriation of "personally identifiable information" or any kind of private information that might lead to the identification of a person; IT-breaches which concern the IT infrastructure, systems, private networks but not the unauthorized appropriation of sensitive data.

The financial impact of security breach announcements caused by the spying and surveillance programs of the NSA has not been yet investigated in the current literature. The scope of our study is therefore to address this research gap by measuring the capital market reaction of NSA-related security breaches. We test therefore the following research hypothesis:

H1: The revelations of NSA security and privacy breaches have a negative effect on the stock prices of the affected publicly traded companies.

Methodology

We conduct an event study, which is a frequently used methodology to measure the impact of information on stock prices (Fama et al. 1969). Given rational market participants, a stock price adjustment to new information takes places immediately. Therefore, the event study methodology is especially useful for observing the effects of events in a short time period (Campbell et al. 1997). One application for event

studies is e.g., to measure the impact of security breach incidents on stock prices (Campbell et al. 2003; Cavusoglu et al. 2004; Kannan et al. 2007).

For an event study it is essential that the defined event represents new information to the market participants, as an event study aims to measure the impact of an event on the stock price. Hence, the exact date of the event (t_0) needs to be determined. It is also common to examine the period around the event date. By doing so, it may be possible to capture price effects after the announcement or anticipation effects before the announcement. Therefore, an event window (t_{-1} to t_{+1}) is considered to examine the stock price movement during a period of time. However, it is important that during the event window no other stock price relevant events, so called confounding events, take place. Otherwise, the ability to draw inference suffers, because an isolated view on multiple impact factors on the returns is not possible. Logically, observations that contain confounding events during the event window are excluded from the sample. A longer event window leads to a smaller sample size but potentially captures possible price or anticipation effects and vice versa for a shorter event window. An estimation window (t_{-2} to t_{-1}) prior the event window is necessary to model the normal returns for the event window, i.e. the returns that are expected if the event did not take place. The longer the estimation window, the lower is the chance that model parameters are outlier-driven. A longer estimation window reduces the risk of serial correlation of the abnormal returns. In addition, the estimation- and the event window should not overlap. The abnormal return, which can be interpreted as the impact of the event on the stock price, is calculated by subtracting the estimated returns from the observed returns (MacKinlay 1997). Figure 1 visualizes the elements of an event study:

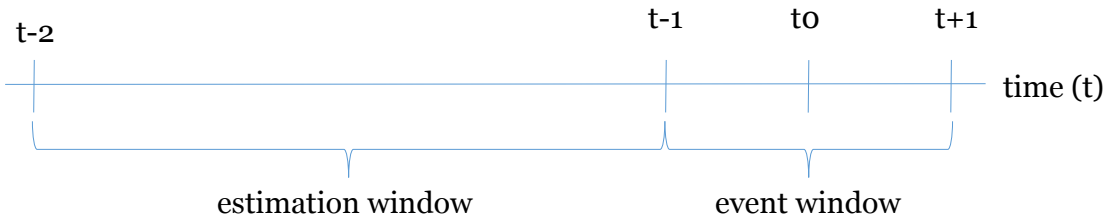

Figure 1. Estimation and Event Window of an Event Study

The approach of our event study is based on MacKinlay (1997). The model for computing the normal stock returns is the market model, which is a well-established model in the literature. The underlying assumption of the market model is the existence of a linear relationship between the stock returns and the market i.e. the matching index for each company:

$$R_{i,t} = \alpha_i + \beta_i R_{m,t} + e_{i,t} \quad (1)$$

Where $R_{i,t}$ is the observed return of stock i at the time t and $R_{m,t}$ the return of the market m at the time t. The coefficients $\hat{\alpha}_i$and $\hat{ß}_i$ are the estimated intercept and slope parameter of stock i which can be obtained by an OLS regression between the stock and its corresponding market index for the estimation window. We set the length of the estimation window to 150 trading days prior the event window, which is a common window that allows for a stable estimation of the parameters. The $e_{i,t}$ represents a zero mean disturbance term. The impact of the event on the stock return can be measured by subtracting the estimated normal returns, i.e. the expected stock returns $E(R_{i,t})$ from the observed returns during the event window. Therefore, to yield the abnormal return $AR_{i,t}$ for stock i at time t, equation (1) can be rewritten as:

$$e_{i,t} = AR_{i,t} = R_{i,t} - \hat{\alpha}_i - \hat{ß}_i R_{m,t} \quad (2)$$

or put differently:

$$AR_{i,t} = R_{i,t} - E(R_{i,t}) \quad (3)$$

In order to draw an overall inference on the capital market reaction on a certain event, the abnormal returns have to be aggregated over all observations *N,* i.e. for the different incidents *n* of our sample. This is done by averaging the abnormal returns AAR_t (average abnormal returns) for each day:

$$AAR_t = \frac{1}{N} \sum_{i=1}^{n} AR_{i,t} \quad (4)$$

Additionally, to capture the entire effects (e.g. anticipation effect or a lag in the stock price movement), it is common to examine the event window as a whole. This can be achieved by cumulating the averaged abnormal returns of the event window $CAAR_{(t-1,tt+1)}$ (cumulative average abnormal returns):

$$CAAR_{(t-1,t+1)} = \sum_{t=1}^{n} AAR_t \quad (5)$$

To test AAR and CAAR for statistical significance, we performed a one-tailed *t*-test. However, the normality tests Shapiro–Wilk and Kolmogorov-Smirnov (Field 2009) show that returns series do not distribute normally. Therefore, we additionally perform the Wilcoxon signed-rank test, which does not require any assumptions on the population distribution. The corresponding null hypothesis is that the AAR and CAAR are zero for every day and event window.

Sample Selection

In this section we provide a detailed explanation of the data collection process, as well as a summary of the sample characteristics. On June 5th 2013 the British daily newspaper *The Guardian* along with *The Washington Post* brought to the light the existence of the data collection program at the Verizon Company conducted by the NSA. Ever since *The Guardian*, as well as other national and international news media sources continue to report on the NSA leaks by revealing information on the programs launched and conducted by the NSA, the names of companies or people involved, the type of data collected etc. Based on news media reports, the programs conducted in the past years from the NSA have not only targeted companies with the scope of collecting large amounts of customer data, but also tapping conversations of persons, such as politicians (The Guardian 2013c). The scope of our study is to identify announcements of security and privacy breaches concerning public companies and related to the NSA-affairs. In order to determine a representative sample of firms involved in the NSA scandal, we electronically searched articles published from the following major news media sources between June 5th 2013 and March 31st 2014: *The Guardian, The Washington Post, The Wall Street Journal, The New York Times and Spiegel Online*. These newspapers are international news media outlets with a very large share of readers and high visibility and might represent therefore a primary source of information also for the investors' community (Campbell et al. 2003).

If the privacy breach event has been announced in different news media outlets, the event date is the date of the earliest news media report. In case the company has been affected by more than one security breach within the data collection interval, we include in our sample only events with at least 150 trading days between then. This step is important in order to avoid overlapping between the estimation windows when applying the event study method (Goel and Shawky 2014). In case we identify an announcement that mentions both the parent company and its subsidiary, we include in our sample only the parent company. For instance, the PRISM surveillance program involved Microsoft Corporation and its subsidiary Skype Technologies SA, as well as Google Inc. and its subsidiary You Tube LLC (The Guardian 2013). Furthermore, if the security breach event was announced during non-trading days (weekend or holidays), the first trading day immediately after the disclosure day is considered as the event date (Goel and Shawky 2014). In addition, we removed companies which were not listed at an exchange during the estimation and the event window. We also identified confounding events within the event window and removed them from the sample. After applying the different selection criteria we are left with a final sample of 27 security breaches[1].

[1] The complete list of the security and privacy breaches can be found in the appendix section (Table 6).

Descriptive Statistics of Security Breaches

This subsection provides a summary on the sample characteristics. As showed in Table 1, out of 27 security breaches, 18 instances (67%) are privacy breaches centered on the appropriation of sensitive data, while the rest of 9 instances are IT-breaches.

Type of security breach	No. of security breaches
I. Privacy breaches	
Metadata	7
Metadata and content	11
II. IT-breaches	
Malware	7
Access to private networks	1
Weak encryption formula	1

Table 1. Types of Security Breaches

Table 2 shows the distribution of security breaches based on company's location. The majority of the security breach announcements are associated to American corporations. With respect to USA, we have fifteen companies and eighteen security breaches, since three companies have experienced two security breaches between June 5th 2013 and March 31st 2014.

Country	No. of firms	No. of security breaches
Belgium	1	1
Brazil	1	1
China	1	1
France	2	2
Ireland[2]	1	1
South Korea	1	1
UK	2	2
USA	15	18

Table 2. Distribution of Security Breaches by Country

The classification of the security breaches depending on sector is displayed in Table 3. As can be seen, the sector of communications is the most affected sector from the NSA-affair, followed by the technology sector.

[2] Seagate Technology plc is currently incorporated in Dublin, Ireland but is part of S&P 500 and is traded at the NASDAQ exchange.

Sector	No. of security breaches
Communications	16
Consumer discretionary	1
Energy	1
Technology	9

Table 3. Distribution of Security Breaches by Sector

Results

The event study results show that NSA-related security and privacy breaches have a negative impact on the affected companies. As displayed in Table 4, AAR values are negative on day -1 and on the event date and become positive on day 1. On day -1 AAR are negative and significant at the 10% significance level, result that can be associated with possible information leakage effects prior to the official event announcement.

Day	AARs(%)	Neg:Pos	*t*-value (*p*-value)	Median (%)	Wilcoxon signed-rank test (*p*-value)
-1	-0.248	17:10	-0.996 (0.164)	-0.437	132 (0.089*)
0	-0.273	15:12	-0.977 (0.169)	-0.060	165 (0.289)
1	0.118	11:16	0.390 (0.650)	0.052	237 (0.876)
$p < .10$* (one-tailed test)					

Table 4. AAR Results on the Full Sample

Another factor that might explain the presence of significant negative returns on day -1 is the different time zone in different countries. Since news reports are published on-line at different hours in different countries, the stock market reaction will not be simultaneous to the announcement date. There might be a delayed or even an anticipated market reaction, based on the effective publishing time of the security breach in the country where the company's stocks are traded.

In an efficient capital market, stock prices constantly incorporate the new information flow conveyed to the market. Rational investors react to the public disclosure of security and privacy breaches by reassessing their expectancies on the future value of companies. However, the negative effect of the breach announcements is a short-term effect, in fact the market starts to recover quickly and returns into positive levels on day +1. Our results are therefore in line with empirical studies investigating the financial impact of "classic" security breaches, whose negative effect persists for a few days after the event announcement (e.g. Acquisti et al. 2006; Campbell et al. 2003). The statements released by the affected companies in the afterwards of the event disclosure could explain the positive abnormal returns on day 1. Immediately after the breach announcement, several companies involved in the surveillance programs fiercely denied any sort of collaboration with intelligence services that might have compromised the privacy and security of customers' data. Such statements could have been perceived as a positive signal from investors, which explains the short term negative returns.

Table 5 summarizes CAAR values over the event window [-1;1]. Mean CAR value on the event date is negative and statistically significant at the 10% significance level (Wilcoxon signed-rank test). Based on these results, we can state that hypothesis 1 is supported.

Day	CAARs(%)	Neg:Pos	*t*-value (*p*-value)	Median (%)	Wilcoxon signed-rank test (*p*-value)
-1	-0.248	17:10	0.996 (0.164)	-0.437	132 (0.089*)
0	-0.521	16:11	-1.864 (0.037**)	-0.253	125(0.064*)
1	-0.403	13:14	-0.971 (0.170)	0.005	173 (0.357)
$p < .10$*; $p < .05$** (one-tailed test)					

Table 5. CAAR Results on the Full Sample

Conclusions

In this paper we investigated the stock market reaction of NSA-related security incidents based on the event study methodology. Overall, the announcement of security and privacy breaches has a negative effect on the stock market value of the affected firms, which is clearly evidenced by the negative cumulated abnormal returns over the event window.

From a theoretical perspective, we contribute to the information security literature as we provide insights on a topic of high actuality centered on the privacy and security of information. Although the context and the dynamic of the NSA-security breaches deviate in different ways from "classic" security breaches so far investigated in the literature, they point to the central issue of information privacy and security, which are both topics of high relevance in the information security literature.

From a practical perspective, the NSA-scandal raises important questions on the security of internet- and phone data stored in enterprises. Companies, in particular those belonging to the internet media industry, should implement rigorous security systems and comply with security standards in order to guarantee the safety of information. In addition, NSA-related security breaches raise ethical issues on how companies handle customers' sensitive information stored on their servers. Although according to the PRISM program NSA has had direct access on companies' servers, these companies strongly denied the existence of the program and any kind of collaboration with the NSA.

One of the limitations of our study is the small sample size, largely due to the fact that the first announcement related to NSA-security breaches dates back to June 2013.

With respect to future research, one interesting research direction would be to analyze the long term-effects of NSA-privacy breaches by performing a long-term event study. Given the seriousness of the NSA-scandal, it is reasonable to expect that the negative effect of the privacy breach announcements persists longer in time. Furthermore, comparing the stock market behavior between firms which suffered security breaches and a control group of firms not affected from such incidents, such as competitors, would offer additional insights on the information transfer- and the contagious effects of NSA-security breaches. In addition, NSA-security breaches continue to receive large media coverage both at a national and international level. It would be therefore helpful to analyze how the information spreads through different social media channels with the aim of observing users' reaction, as new information on the incidents continues to be reported in the news media. Users' interaction and communication through social media outlets generates large amounts of data, which can be analyzed in order to measure the reputational damage or loss of trust in the companies associated to the NSA-security breach announcements.

REFERENCES

Acquisti, A., Friedman, A., and Telang, R. 2006. "Is there a cost to privacy breaches? An event study," Presented at the Proceedings of the 21st International Conference on Information Systems (ICIS), Milwaukee, Wisconsin, pp. 1563–1580.

Campbell, J. Y., Lo, W. A., and MacKinlay, A. 1997. *The Econometrics of Financial Markets*, Princeton University Press.

Campbell, K., Gordon, L. A., Loeb, M. P., and Zhou, L. 2003. "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," *Journal of Computer Security* (11:3), pp. 431–448.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2004. "The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers," *International Journal of Electronic Commerce* (9:1), pp. 70–104.

Ettredge, M. L., and Richardson, V. J. 2003. "Information transfer among internet firms: the case of hacker attacks," Journal of Information Systems (17:2), pp. 71–82.

Fama, E. F., Fisher, L., Jensen, M. C., and Roll, R. 1969. "The Adjustment of Stock Prices to New Information," *International Economic Review* (10:1), p. 1.

Field, A. (2013). *Discovering statistics using IBM SPSS statistics*. Sage.

Garg, A., Curtis, J., and Halper, H. 2003. "Quantifying the financial impact of IT security breaches," *Information Management & Computer Security* (11:2), pp. 74–83.

Gatzlaff, K. M., and McCullough, K. A. 2010. "The Effect of Data Breaches on Shareholder Wealth," *Risk Management and Insurance Review* (13:1), pp. 61–83 (doi: 10.1111/j.1540-6296.2010.01178.x).

Goel, S., and Shawky, H. A. 2014. "The Impact of Federal and State Notification Laws on Security Breach Announcements," *Communications of the Association for Information Systems* (34:1), pp. 37–50.

Gordon, L. A., Loeb, M. P., and Zhou, L. 2011. "The impact of information security breaches: Has there been a downward shift in costs?," *Journal of Computer Security* (19:1), pp. 33–56.

Hinz, O., Nofer, M., Schiereck, D., and Trillig, J. 2015. "The influence of data theft on the share prices and systematic risk of consumer electronics companies," *Information & Management* (52:3), pp. 337–347 (doi: 10.1016/j.im.2014.12.006).

Hovav, A., and D'Arcy, J. 2003. "The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms," *Risk Management and Insurance Review* (6:2), pp. 97–121.

Hovav, A., and D'Arcy, J. 2004. "The Impact of Virus Attack Announcements on the Market Value of Firms.," *Information Systems Security* (13:3), pp. 32–40.

Kannan, K., Rees, J., and Sridhar, S. 2007. "Market Reactions to Information Security Breach Announcements: An Empirical Analysis," *International Journal of Electronic Commerce* (12:1), pp. 69–91.

Liginlal, D., Sim, I., and Khansa, L. 2009. "How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management," *Computers & Security* (28:3-4), pp. 215–228.

MacKinlay, A. C. 1997. "Event studies in economics and finance," *Journal of economic literature*, pp. 13–39.

The Guardian 2013a. http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=0000000 (Accessed: 21.01.2015).

The Guardian 2013b. http://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google (Accessed: 20.01.2015).

The Guardian 2013c. http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-callsbreach/ (Accessed: 20.01.2015).

The New York Times 2013. http://www.nytimes.com/2013/12/09/technology/tech-giants-issue-call-for-limits-on-government-surveillance-of-users.html?pagewanted=all&_r=0 (Accessed: 25.01.2015).

The Washington Post 2013. http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/05/nsa-asked-verizon-for-records-of-all-calls-in-the-u-s/. (Accessed: 20.01.2015).

Whitman, M., and Mattord, H. 2011. *Principles of information security*. Cengage Learning.

Yayla, A. A., and Hu, Q. 2011. "The impact of information security events on the stock value of firms: The effect of contingency factors," *Journal of Information Technology* (26:1), pp. 60–77.

Appendix

EVENT DATE	COMPANY	NEWS MEDIA LINK	COUNTRY
06.06.2013	AOL Inc.	http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/	USA
06.06.2013	Apple Inc.	http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/	USA
06.06.2013	Facebook Inc.	http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/	USA
06.06.2013	Microsoft Corporation	http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/	USA
06.06.2013	Yahoo! Inc.	http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/	USA
07.06.2013	AT&T Inc.	http://www.wsj.com/articles/SB10001424127887324299104578529112289298922	USA
02.08.2013	BT Group plc	http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq	UK

02.08.2013	Level 3 Communications Inc.	http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq	USA
02.08.2013	Verizon Communications Inc.	http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq	USA
02.08.2013	Vodafone Group Plc	http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq	UK
09.09.2013	Petroleo Brasileiro SA	http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras	Brazil
20.09.2013	Belgacom NV	http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html	Belgium
23.09.2013	RSA Security LLC (EMC Corporation)	http://www.theguardian.com/world/2013/sep/21/rsa-emc-warning-encryption-system-nsa	USA
21.10.2013	Alcatel Lucent SA	http://www.theguardian.com/world/2013/oct/21/us-french-surveillance-legitimate-questions	France
21.10.2013	Wanadoo (Orange SA)	http://www.theguardian.com/world/2013/oct/21/us-french-surveillance-legitimate-questions	France
11.11.2013	LinkedIn Corporation	http://www.spiegel.de/international/world/ghcq-targets-engineers-with-fake-linkedin-pages-a-932821.html	USA
09.12.2013	Blizzard Entertainment, Inc. (Activision Blizzard, Inc.)	http://www.theguardian.com/world/2013/dec/09/nsa-spies-online-games-world-warcraft-second-life	USA
30.12.2013	Cisco System, Inc.	http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html	USA

30.12.2013	Hewlett-Packard Company	http://www.spiegel.de/international/world/nsa-secret-toolbox-ant-unit-offers-spy-gadgets-for-every-need-a-941006.html	USA
30.12.2013	Huawei Technology Company Limited	http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html	China
30.12.2013	Samsung Electronics Co.	http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html	South Korea
30.12.2013	Seagate Technology plc	http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.htm	Ireland
30.12.2013	Western Digital Corporation	http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html	USA
27.01.2014	Facebook Inc.	http://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html	USA
27.01.2014	Google Inc.	http://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html	USA
27.01.2014	LinkedIn Corporation	http://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html	USA
27.02.2014	Yahoo! Inc.	http://www.washingtonpost.com/world/national-security/british-spy-agency-kept-images-of-yahoo-webcam-chats/2014/02/27/2d27d5ee-9fee-11e3-a050-dc3322a94fa7_story.html	USA

Table 6. List of NSA-Security Breaches