Intangible Costs of Data Breach Events

Dissertation

zur Erlangung des wirtschaftswissenschaftlichen Doktorgrades
der Wirtschaftswissenschaftlichen Fakultät der Georg-August-Universität Göttingen

vorgelegt von
Griselda Sinanaj, M.Sc.
geboren in Orikum, Vlore

Göttingen, 2017

Betreuungsausschuss

Erstbetreuer:	Prof. Dr. Jan Muntermann
Zweitbetreuer:	Prof. Dr. Olaf Korn
Drittbetreuer:	Prof. Dr. Lutz M. Kolbe
Tag der mündlichen Prüfung:	17.10.2017

Table of Contents

List of Tables

List of Figures

Acronyms

AAR	Average Abnormal Returns
AAS	Average Abnormal Sentiment
AMAC	America's Most Admired Companies
AMCIS	Americas Conference on Information Systems
AR	Abnormal Returns
AS	Abnormal Sentiment
BYOD	Bring Your Own Device
CAAR	Cumulative Average Abnormal Returns
CAS	Cumulative Abnormal Sentiment
CBR	Customer-based Corporate Reputation
CIA	Confidentiality Integrity Availability
CSR	Corporate Social Responsibility
DOS/DoS	Denial of Service
ECIS	European Conference on Information Systems
EMH	Efficient Market Hypothesis
GCHQ	Government Communications Headquarters
GDT	General Deterrence Theory
GI	General Inquirer
GO	Governmental Organization
HBR	Harvard Business Review
IBM	International Business Machines
ICIS	International Conference on Information Systems
ID	Identifier
IS	Information Systems
IT	Information Technology
JISSec	Journal of Information System Security
MIS	Management Information Systems

NSA	National Security Agency
NYSE	New York Stock Exchange
OLS	Ordinary Least Regression
PACIS	Pacific Asia Conference on Information Systems
PC	Personal Computer
PMT	Protection Motivation Theory
PRC	Privacy Rights Clearinghouse
PT	Prospect Theory
RBV	Resource-based View
RITE	Responsibility Integrity Trust Ethicality
RQ	Research Question
SCCT	Situational Crisis Communication Theory
TPB	Theory of Planned Behavior
TSME	Theory of Stock Market Efficiency
US	United States
USA	United States of America
VIF	Variance Inflation Factor
WI	Wirtschaftsinformatik

A Foundations

This chapter consists of three sections: introduction, theoretical background, methodologies and data. The introductory section presents the motivation for research, it frames the research questions and the structure of this cumulative thesis. In addition, it depicts the research framework, which provides a schematic representation of the studies, and it highlights the relationships between each study and the overarching research goal of the thesis. The second section reviews theoretical concepts related to the research field of information security and the scope of this thesis. It examines the various definitions of information security, followed by the illustration of the main information security goals and the costs of data breach events. In addition, an overview on information security literature is provided. The last section provides a detailed analysis of the methodological approaches and the data used in each study of the thesis.

I Introduction

1 Motivation and Problem Statement

The arrival of the internet era and the power of digital innovations have profoundly influenced the philosophy of conducting business and radically transformed business models and processes at the organizational level (Chae et al., 2014; Sabherwal and Jeyaraj, 2015). Despite the overall benefits of information technology on organizational performance (Chae et al., 2014; Mithas and Rust, 2016; Mithas et al., 2012), information technology exposes companies to various threats and risks, such as security failures and breaches (D'Arcy et al., 2014; Liang and Xue, 2009). Information security breaches originate from the failure of security systems and standards to protect the confidentiality, integrity and availability of information resources (Campbell et al., 2003; Kannan et al., 2007). In particular, data breaches, also referred to as breaches of confidentiality in technical terms (Campbell et al., 2003; Kannan et al., 2007), are defined as the "compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored, or otherwise processed" (International Standards Organization, 2016, ISO/IEC 27050, 3.3). The compromised information in data breach events is strictly confidential and if this information is misused by unauthorized parties, it can result in the identity theft of individuals, such as firm employees and customers. The targeted information in such incidents, in technical terms known as "personally identifiable information" (Romanosky et al., 2011, p. 256), consists in credit and debit card numbers, driving licenses, birthdates, social security numbers, E-mail addresses, usernames and passwords etc. (Romanosky et al., 2011).

At the beginning of the digital era, data breaches were considered sporadic crisis events resulting from companies' inability to protect the confidentiality of information resources through state of the art security measures. Nowadays data breach events have become a global and enduring threat for every company relying upon technology and digital information (Experian, 2017; Symantec, 2016). Various reports show that both the frequency and the magnitude of data breach events in terms of number of data records exposed have constantly increased over the past decade. According to the statistics provided by the Identity Theft Research Center, from 2006 to 2016 the number of data breach events announced in the U.S. has grown from 321 to 1093, leading to an increase of 340% (Identity Theft Resource Center, 2016). The overall number of data records compromised in data breach events also shows an increasing trend. While in 2005 the number of records exposed amounted to over 48 million, the latest figure provided from Privacy Rights Clearinghouse shows a cumulated value of over 900 million data records (Privacy Rights Clearinghouse, 2017). Mega-breaches, consisting of at least ten million records, represent the largest portion of the cumulated size of data breach events in the past decade. The number of large-scale data breach incidents rose steeply by 125% from 2014 to 2015, resulting in over 90 million data records compromised (Symantec, 2016).

The data collection scandal of the National Security Agency (NSA), the U.S. governmental institution responsible for the collection and the assessment of electronic data, is one of the most striking events in the history of data breaches. While prior to this event a typical data breach incident affected only a single company, the NSA data collection programs involved the simultaneous extraction of large data volumes from a preselected pool of large corporations (Landau, 2013, 2014, 2016; Toxen, 2014). The substantial difference between data breaches prior to this event and the NSA revelations is the breach source. In contrast to previous intentional data breach events where the breach originates from the ambition of malicious actors to illegally obtain corporate confidential information, the source responsible for the confidentiality violations in the NSA revelations was a governmental institution. This has lead scholars, as well as practitioners, to question existing security concepts and to rethink information security objectives (Landau, 2014; Toxen, 2014).

Data breach events have a significant negative impact on the affected companies (Campbell et al., 2003; Hovav et al., 2017; Martin et al., 2017; Schatz and Bashroush, 2016). The overall cost of a data breach incident is decomposed in a tangible and intangible component (Yayla and Hu, 2011). Tangible costs of data breach events are typically short-term costs including the loss of revenues and sales, hardware and software costs, reduced employee productivity (Yayla and Hu, 2011) and litigation costs (Campbell et al., 2003; Gatzlaff and McCullough, 2010). In general tangible costs are derived from companies' financials. For instance, the negative impact of a data breach on firm sales is assessed by analyzing firms' income statements and earnings announcements (e.g. Xu et al., 2008). Intangible costs are immaterial and elusive costs such as reputational damage (Acquisti et al., 2006; Campbell et al., 2003; Romanosky et al., 2011), loss of investor confidence, loss of customer trust and reduced competitive advantage towards industry competitors (Yayla and Hu, 2011). In contrast to tangible costs, there are no established approaches for the measurement of the previously outlined intangible costs. The estimation of intangible costs is however a key factor for the prevention and the management of data breach events. Intangible costs represent a substantial portion of the global cost of data breach incidents and therefore play an essential role in IT security investment decisions (Cavusoglu et al., 2004a). The accurate estimation of intangible costs is crucial for the determination of the optimal amount of IT security expenditure (Cavusoglu et al., 2004a). Furthermore, from the perspective of crisis and risk managers, the estimation of intangible costs is an essential input for the implementation of tailored response strategies in the wake of data breach events (Coombs, 2007; Coombs and Holladay, 2006; PwC, 2014).

The intangible impact of data breach incidents at the organizational level has increasingly become one of the most relevant topics in information security literature. Although the body of research investigating this research problem has provided initial insights and empirical evidence, various aspects and facets of this complex topic still remain unexplored. To contribute to this knowledge gap, this thesis investigates the intangible costs of data breach incidents,

particularly the loss of investor confidence and the loss of corporate reputation. Thus, this cumulative dissertation advances information security research by providing theoretical insights and empirical evidence on a topic which has been explored only to a limited extent. In addition, it provides relevant insights for practitioners and managers to effectively respond to and manage data breach incidents.

2 Research Questions

As already explicated in the previous section, optimal security investments and the selection of appropriate management strategies depend to a great extent on the estimation of the intangible costs of data breach incidents (Cavusoglu et al., 2004a; Coombs, 2007; Coombs and Holladay, 2006). Since intangible costs, such as loss of investor confidence and loss of corporate reputation, are immaterial and not directly observable, a deep understanding of the underlying theoretical concepts is essential for the assessment of such costs (Cavusoglu et al., 2004b; Yayla and Hu, 2011). In spite of the recognized relevance of the assessment of the intangible costs of data breach announcements in research and practice, it is unclear to what extent this topic has been examined in literature. The scientific instrument at researchers' disposal to establish whether a research problem has been explored in depth within a particular research stream is the structured literature review. This approach of systematically examining literature allows researchers to structure extant research through conceptual frameworks, uncover significant theoretical gaps and provide guidelines for future research (Rowe, 2014; Schryen, 2015; vom Brocke et al., 2015; Webster and Watson, 2002).

Information security research taken as a whole has been examined in several academic articles. Such studies are however characterized by a wide focus and do not provide insights specific to the research area investigating the intangible costs of data breach incidents (e.g. Silic and Back, 2014; Siponen et al., 2008; Zafar and Clark, 2009). Hence, this thesis covers an important knowledge gap by reviewing this research stream, paying particular attention to the theories and methodological approaches applied to explore the intangible impact of data breaches. Through the close examination of the different methods and theoretical underpinnings, this thesis aims to achieve a deeper understanding of the concept of intangible costs, as well as to identify major theoretical deficits and methodological flaws in the current literature. The aforementioned aspects are addressed from the first research question of this thesis, formulated as follows:

Research question 1 (RQ 1): To what extent have the intangible costs of data breach events been addressed in the literature?

Prior research has shown that data breach incidents have a negative impact on investor confidence (Acquisti et al., 2006; Martin et al., 2017; Song et al., 2017; Spanos and Angelis, 2016; Yayla and Hu, 2011). In a business context, the concept of investor confidence synthesizes investors' beliefs, expectations and assessments of a company's financial soundness and future economic

performance. Negative changes in the level of investor confidence due to the announcement of negative business events have an adverse impact on stock purchase behavior, firm market value and the cost of raising capital (Hoffmann and Post, 2016). Because investor confidence directly affects stock market activity, the loss of firm market value is used in research to gauge the loss of investor confidence (Yayla and Hu, 2011).

The investigation of the impact of NSA data and privacy breach events on investor confidence and firm market value represents a relevant research gap in the existent literature. Because of the massive amount of extracted data and the immense violations of information confidentiality, the NSA revelations of data breaches represent one of the darkest chapters in the history of information security (Landau, 2013, 2016). Within the context of the NSA scandal, the boundaries between confidentiality and the violation of confidentiality became blurred. With this regard, the question whether such large-scale data collection programs constitute a violation of information confidentiality has been much debated both in traditional media and security research (Landau, 2013, 2016; Schneier, 2014; Toxen, 2014). A vast majority of the data collected though the enactment of massive data collection programs belong to the category of metadata, in technical terms known as transactional information (Gray and Watson, 1998). Metadata are "data about the data", consisting of brief descriptive information on a particular information set without affecting the specific content (Gray and Watson, 1998, p. 86). Although the collection of metadata has been often described not as critical as a breach of confidentiality, through the application of sophisticated processing techniques metadata can provide exact information on a person's identity. Thus, security scholars agree that metadata, although per definition not implying a breach of confidentiality, represent effectively a form of confidentiality breach and should be therefore handled as such (Landau, 2014).

This thesis picks up on the previously stated research gap and examines the intangible cost in the context of a unique data breach event, which differs in many aspects from the classic data breach incidents investigated in literature. The second research question is therefore formulated as follows:

Research question 2 (RQ 2): How do data breach events associated with the NSA revelations affect investor confidence?

Data breach incidents are negative crisis events which represent a constant threat to the intangible asset of corporate reputation (Forbes Insights, 2014; Ponemon Institute, 2011; Syed and Dhillon, 2015). The study of corporate reputation, both in conceptual and methodological terms, has led to a vast body of research in various scientific disciplines including management, marketing, economics and information systems research (Love et al., 2016; Rindova et al., 2005; Seebach et al., 2013; Zavyalova et al., 2016). Corporate reputation is defined as "the overall opinion about a firm by customers, investors, employees and the general public" (Colleoni et al., 2011, p. 4). A favorable corporate reputation is rewarding in terms of long-term competitive advantage

(Brønn and Brønn, 2015), superior financial performance (Roberts and Dowling, 2002; Sabate and Puente, 2003) and acts as a buffering factor in times of organizational crisis (Coombs and Holladay, 2006; Jones et al., 2000). Conversely, a damaged reputation impairs consumer trust, diminishes firm value and can be a hazard factor to future business continuity and to a firm's existence (Rhee and Valdez, 2009).

Various technical reports conducted on executives of large companies provide insights regarding the adverse impact of data breaches on corporate reputation. According to the 2014 Forbes Insights study, reputation damage caused by data breach events is accountable for the sharp decline of sales, revenues and the loss of customer trust (Forbes Insights, 2014). A much more critical problem for companies involved in data breach incidents is rebuilding corporate reputation. With this regard, according to the survey study of the Ponemon Institute conducted on over 800 corporate executives from a wide range of industries, the recovery time of damaged corporate reputation is estimated between eight and twelve months (Ponemon Institute, 2011). The speed of the recovery process of corporate reputation depends on a variety of factors. In particular, the exposure of the breach event, both in traditional media and social media channels, has the potential to devastate corporate reputation and decelerate the reputation recovery process (Syed and Dhillon, 2015). Companies' prompt reaction and the response strategy in the wake of a data breach incident play a crucial role in mitigating reputational costs and restoring corporate reputation (Forbes Insights, 2014; Huq, 2015; Ponemon Institute, 2011). The crisis response plan is the most critical phase of the crisis management lifecycle and encompasses a range of actions and defensive measures designated to fully restore corporate reputation (Deloitte, 2016). Ill-timed and strategically unfitting response plans may however generate a counterproductive effect by intensifying reputational losses. Effective response plans require therefore a deep understanding of the magnitude of reputational losses (Coombs, 2007) and of the drivers of reputation damage (Deloitte, 2016).

There is however a paucity of research examining the reputational cost of data breach incidents, primarily due to the operationalization of the concept of reputation (Syed and Dhillon, 2015). The third research question picks up on this research gap and addresses the question of assessing the reputational impact of data breach incidents as well as the drivers of corporate reputation:

Research question 3 (RQ 3): How to assess the impact of data breach events on corporate reputation and what are the influencing factors of the reputational impact of data breaches?

Research question 3a (RQ 3a): How to assess the impact of data breach events on corporate reputation?

Research question 3b (RQ 3b): What are the influencing factors of the reputational impact of data breaches?

The extent of reputational losses and the loss of investor confidence are determined by stakehold-

ers' perceptions of the severity of the data breach event and contextual factors, such as breach and firm characteristics (Gatzlaff and McCullough, 2010). While investors evaluate the breach incident in terms of how it affects firms' future performance (Zafar et al., 2012), reputational damage is driven by the loss of trust (Syed and Dhillon, 2015). As data breach incidents affect different categories of stakeholders who assess the event impact from different viewpoints, the impact on investor confidence and on firm market value may differ significantly from the impact on reputation. The efficient allocation of resources and timely actions are the building blocks of successful management strategies and effective crisis response frameworks of data breach events (Deloitte, 2016; PwC, 2014; Rasoulian et al., 2017). In order to efficiently respond to a data breach event with regard to available resources, companies have to identify the most severe consequences with regard to both previously mentioned types of intangible costs. In addition, the lack of a timely response following the breach announcement increases the reputational losses as well as the loss of investor confidence and severely damages firms' future financial performance (Deloitte, 2016; Rasoulian et al., 2017). The simultaneous examination of intangible costs can be an expedient for the detection of major differences in the size, the longevity and the persistence of the different intangible effects of data breach events. The scope of the comparative view of intangible costs is to provide constructive insights in order to establish priority actions in crisis management plans and efficiently allocate the available resources (Deloitte, 2016; PwC, 2014; Rasoulian et al., 2017). Against this background, the fourth guiding research question of this thesis examines the differences between the impact on investor confidence and the impact on corporate reputation:

Research question 4 (RQ 4): What is the difference between the impact of data breach events on investor confidence and the impact on corporate reputation?

3 Research Framework

This thesis investigates the intangible costs of data breach events at the organizational level, in particular the impact of such events on investor confidence and on corporate reputation. An overview of the studies included in this thesis is provided in Table A-1.

Table A-1: Summary of studies included in the thesis

Study	Title	Research question	Outlet	Section
Study 1	The Intangible Cost of Information Security Breaches: A State of the Art Analysis	(RQ 1): To what extent have the intangible costs of data breach events been addressed in the literature?	JISSec 2015	B.I.1
Study 2	NSA Revelations of Privacy Breaches: Do Investors Care?	(RQ 2): How do data breach events associated with the NSA revelations affect investor confidence?	AMCIS 2015	B.II.1
Study 3	How Data Breaches Ruin Firm Reputation on Social Media! – Insights from a Sentiment-based Event Study	(RQ 3a): How to assess the impact of data breach events on corporate reputation?	WI 2015	B.III.1
Study 4	Do Data Breaches Affect our Beliefs? - Investigating Reputation Risk in Social Media	(RQ 3b): What are the influencing factors of the reputational impact of data breaches?	JISSec 2017	B.III.2
Study 5	Who Wins in a Data Breach? - A Comparative Study on the Intangible Costs of Data Breach Incidents	(RQ 4): What is the difference between the impact of data breach events on investor confidence and the impact on corporate reputation?	PACIS 2016	B.IV.1

The research framework depicted in Figure A-1 provides an overview of the studies constituting the pillars of this thesis. The framework organizes the studies in four parts and highlights the investigated type of intangible cost, the scope of research and the applied methodological approach. **Study 1** presents the results of a concept-based literature review, whereas **Study 2** investigates the impact of data breach events on investor confidence. The effect of data breach events on corporate reputation is addressed in **Study 3** and **Study 4**. Finally, **Study 5** identifies the differences between the impact on investor confidence and the impact on corporate reputation in a comparative analysis of intangible costs.

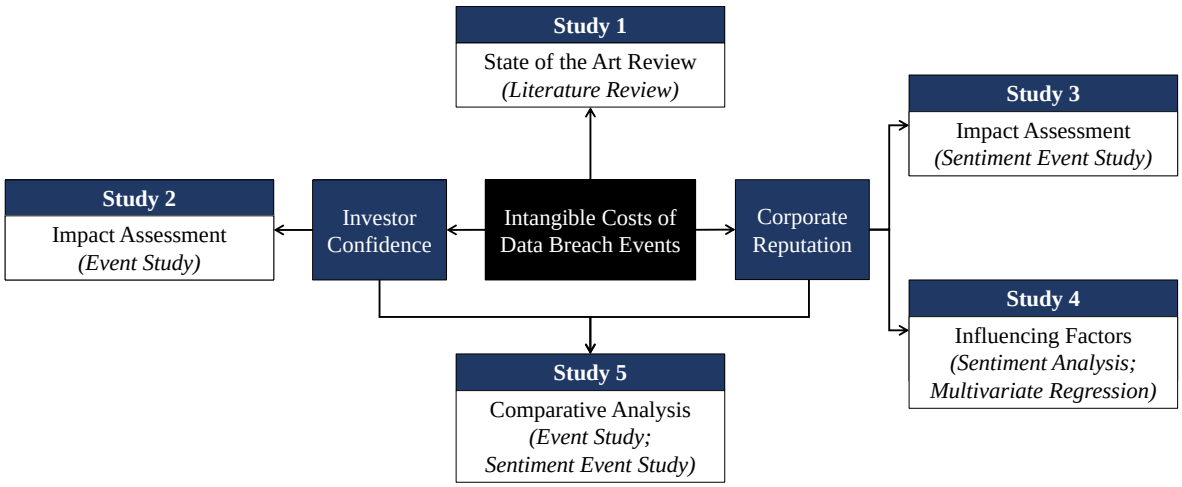

Figure A-1: Research framework

(I) State of the Art Literature Review

Study 1 addresses research question one (RQ 1: To what extent have the intangible costs of data breach events been addressed in the literature?) through a state of the art review of the extant body of research dealing with the intangible costs of information security breaches. As previously mentioned, previous literature review studies on information security are comprehensive and provide a global review of various information security research streams (Willison and Siponen, 2007; Zafar and Clark, 2009). **Study 1** takes a selective approach and focuses on a narrow topic to gain deep insights into intangible costs and establish the relevance of this research topic in literature. To overcome methodological constraints, theoretical deficits and identify new paths of research, the review process aims to critically analyze the theoretical lenses and methodological approaches employed to investigate the intangible costs of data breach events.

(II) Impact on Investor Confidence

Study 2 provides insights on the market value impact of the NSA revelations of data and privacy breaches and is guided by research question two (RQ 2: How do data breach events associated with the NSA revelations affect investor confidence?). The impact of data breaches on investor confidence and shareholder wealth has received attention in the last decade of security research (e.g. Hovav et al., 2017; Kannan et al., 2007; Song et al., 2017; Yayla and Hu, 2011). Based on the event study method, several studies provide empirical evidence of the strong negative stock market reaction following the announcements of confidentiality breach events (Campbell et al., 2003; Kannan et al., 2007). Despite the privacy violation due to the collection of massive amounts of confidential information and the adverse exposure in traditional media (Landau, 2014), the empirical evidence regarding the effect of NSA data and privacy breaches on investor confidence and firm market value is lacking. Accordingly, **Study 2** picks up on this knowledge gap and tests the hypothesis of whether NSA data and privacy breaches have an adverse impact

on investor confidence and on the stock market value of the companies involved in the NSA data collection programs.

(III) Impact on Corporate Reputation

Study 3 and **Study 4** address research question three (RQ 3: How to assess the impact of data breach events on corporate reputation and what are the influencing factors of the reputational impact of data breaches?). The common denominator of **Study 3** and **Study 4** is the investigation of the impact of data breach events on corporate reputation. Although security scholars agree that data breach events do represent a serious threat to the intangible asset of corporate reputation (Acquisti et al., 2006; Campbell et al., 2003; Garg et al., 2003a,b; Ko and Dorantes, 2006; Tsiakis and Stephanides, 2005), empirical research exploring the reputational impact of data breach events is lacking. **Study 3** and **Study 4** aim to fill this knowledge gap and deliver significant insights both to research and practice. **Study 3** addresses RQ 3a (How to assess the impact of data breach events on corporate reputation?) and investigates the reputational cost of data breach incidents. It proposes a new approach for the measurement of reputation losses, the sentiment based-event study approach. While **Study 3** has a methodological focus, **Study 4** is guided by RQ 3b (What are the influencing factors of the reputational impact of data breaches?) and takes an explorative approach by examining the antecedents of corporate reputation. **Study 3** and **Study 4** contribute therefore to information security research with new empirical evidence on the magnitude, the longevity and the influencing factors of corporate reputation. In addition, the novel reputation measurement approach and the identification of reputation risk factors are intended to support security practitioners in the reputation risk management process.

(IV) Comparative Analysis between the Impact on Investor Confidence and on Corporate Reputation

While **Study 2**, **Study 3** and **Study 4** examine the isolated effect of data breach incidents on investor confidence (**Study 2**) and corporate reputation (**Study 3**, **Study 4**), **Study 5** takes a different approach by concurrently analyzing two categories of intangible costs: (i) investor confidence and (ii) corporate reputation and is guided by research question four (RQ 4: What is the difference between the impact of data breach events on investor confidence and the impact on corporate reputation?). As in **Study 2**, the impact on firm market value is measured with the event study approach (Campbell et al., 2003), whereas the impact on corporate reputation relies upon the sentiment-based event study approach as in **Study 3**. By confronting two categories of intangible costs on the basis of a similar approach, **Study 5** aims to uncover differences and similarities in the severity and the longevity of the intangible costs of data breach incidents. The empirical observation of the behavior of stock prices and social media sentiment during security crisis events generates useful insights for the existing literature and future research. In addition, the insights of this study are beneficial to security practitioners for the management of crisis situations.

4 Structure of Thesis

This thesis has a cumulative structure and is composed of three chapters: chapter A, foundations; chapter B, which encompasses five studies on the intangible costs of data breach incidents and chapter C, contributions. The introductory section (chapter A) highlights the practical and theoretical relevance of this thesis and specifies the guiding research questions. Theoretical background discusses key information security concepts and examines information security research. The third section explicates the research methods and the datasets used in each study.

Chapter B entails five studies on the intangible costs of data breach incidents, **Study 1**, **Study 2**, **Study 3**, **Study 4** and **Study 5**. **Study 1** is guided by research question one (RQ 1) and presents the results of a structured literature review on the intangible costs of data and security breach events. **Study 2** investigates the impact of the NSA data breaches on investor confidence and contributes with original insights on an underexplored topic. **Study 3** and **Study 4** address research question three (RQ 3) and focus on the concept of corporate reputation. While **Study 3** proposes a novel approach for the measurement of reputational damage, **Study 4** investigates the drivers of corporate reputation in the aftermath of data breach incidents. Through a comparative analysis, **Study 5** uncovers the differences between two categories of intangible costs: impact on investor confidence and impact on corporate reputation.

The third chapter (chapter C) recapitulates the findings of each study and discusses the theoretical, practical and policy implications of this thesis as well as the limitations and suggestions for future research opportunities. A schematic representation of the thesis structure is given in Figure A-2.

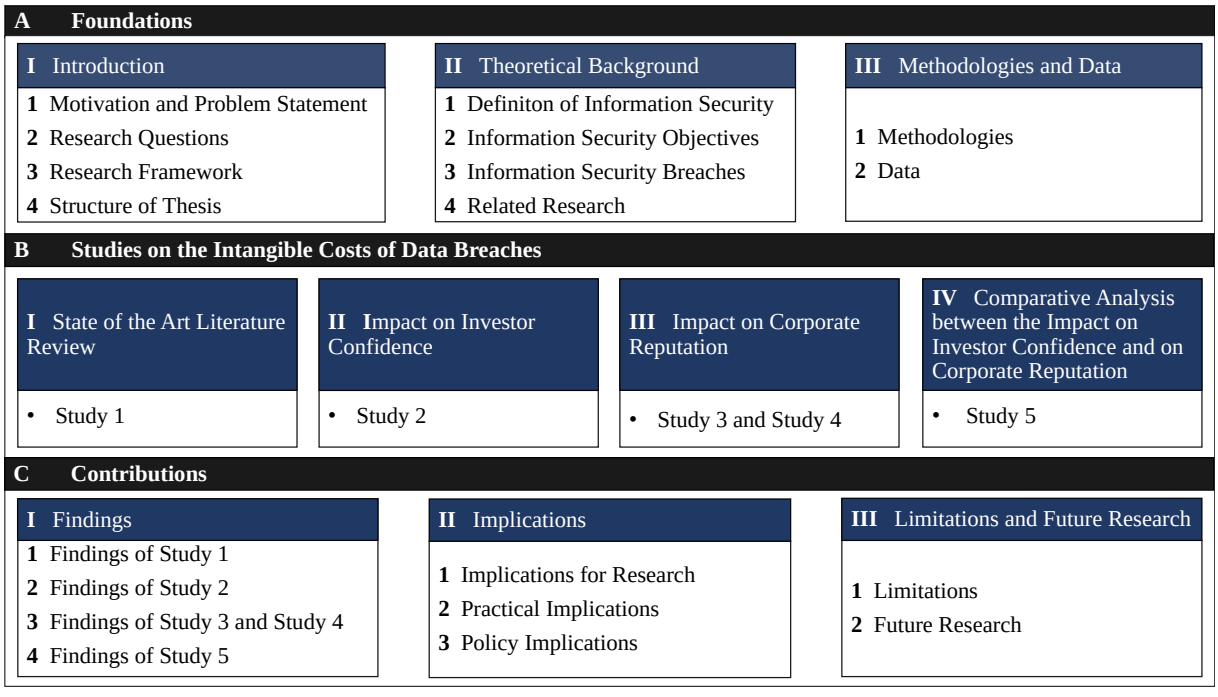

Figure A-2: Structure of thesis

II Theoretical Background

1 Definition of Information Security

The notion of information security is an evolving concept associated with various interpretations (Anderson, 2003; Cherdantseva and Hilton, 2013b; Silic and Back, 2014; Torres et al., 2006). The absence of a standard and consensual definition of information security from the plethora of existing definitions represents a critical issue in information security research (Von Solms, 2000; Zafar and Clark, 2009). Information security literature has been dominated for many decades by a technical point of view, which confines information security to a set of technical principles and standards (Dhillon and Backhouse, 2000, 2001; Samonas and Coss, 2014; Siponen, 2000; Von Solms, 2000). This period of time is known as the "technical wave" and is characterized by a technical approach of information security (Von Solms, 2000). The study of Anderson (2003) is one of the first to scrutinize the variety of technical definitions of information security by identifying and analyzing their limitations and flaws. A summary of the most representative definitions of information security and their respective limitations is presented in Table A-2.

Table A-2: Definitions of information security based on the study of Anderson (2003)

Definition	**Limitation (s)**
"Rests on confidentiality, integrity and availability" (Bishop, 2003, p. 3)	Lack of completeness
"Encompasses the use of physical and logical data access controls to ensure the proper use of data and to prohibit unauthorized or accidental modification, destruction, disclosure, loss or access to automated or manual records and files as well as loss, damage or misuse of information assets" (Peltier, 2001, p. 266)	Operational description
"Attempts to ensure the confidentiality, integrity, and availability of computing systems' components" (Pleeger and Pfleeger, 2003, p. 29)	Lack of precision and accuracy

As depicted in Table A-2, the current definitions of information security either lack precision and accuracy, or provide a partial explication of the concept and thus, lack completeness, or outline information security activities and tasks (Anderson, 2003, p. 309, 310). Bishop (2003) identifies information security with the pillars of the CIA security model, *confidentiality*, *integrity* and *availability*. The interpretation of information security as a direct function of the CIA security model has been embraced for several decades both from information security scholars and industry practitioners (Choobineh et al., 2007; Dhillon and Backhouse, 2001; Kolkowska et al.,

2009; Mishra and Dhillon, 2006; Von Solms and Van Niekerk, 2013). To overcome the limitations of the existing definitions of information security regarding the "technical view", Anderson (2003) proposes a new definition of information security that is grounded on the concept of assurance: "*information security is a well-informed sense of assurance that information risks and controls are in balance*" (Anderson, 2003, p. 310). The ultimate scope of information security is therefore achieving the optimal balance between the maximization of information controls and the minimization of information risks. In this regard, technical expertise and security controls are necessary requisites but not sufficient to mitigate security risks and to assure the safety of information resources (Anderson, 2003). In addition to technical knowledge and skills, information security practitioners should be aware of the interplay between information security and the organizational environment as well as of the business implications of information security (Anderson, 2003; Cherdantseva and Hilton, 2013a).

The socio-technical school of thought in information security literature extends the technical view of information security and depicts information security as a socio-technical phenomenon (Dhillon and Backhouse, 2001; Kayworth and Whitten, 2010; Mishra and Dhillon, 2006). Because "organizations are no longer characterized by physical assets but by a network of individuals who create, process, hold, and distribute information" (Dhillon and Backhouse, 2000, p. 125), individuals are a vital component of information security and a key factor in achieving safe security environments and fulfilling security goals (Dhillon and Backhouse, 2001). In a business environment constantly influenced by the pace of technological innovations, security standards, protocols and internal security policies do not suffice to guarantee the safety of corporate information resources. Another crucial factor contributing to information safety is the establishment of a corporate security culture, which refers to a set of moral and ethical values, being aware of the occupied role within the company and of the consequences deriving from irresponsible actions (Chowdhuri and Dhillon, 2012; Dhillon and Backhouse, 2000; Thomson et al., 2006).

The review of the current definitions of information security reveals that information security is not a steady concept but rather evolves with the pace of technology and organizational developments. Thus, the concept of information security should be constantly revised to reflect the latest technological and organizational developments as well as to highlight the most relevant security goals (Cherdantseva and Hilton, 2013a).

2 Information Security Objectives

Accurate and updated definitions of information security are crucial as they point to major information security goals and serve as a roadmap for the management of security threats and risks. Information security goals bear a strategic role in the implementation of security programs and policies to protect the vulnerable asset of information in an incessantly growing ecology of

IT security risks and threats (Cherdantseva and Hilton, 2013a).

The security principles of *confidentiality*, *availability* and *integrity* are the components of the CIA security model, developed in the 1970s during the period known as the "technical wave" of information security. The CIA triad (also known as the CIA triangle) is deemed the flagship model of security objectives and has been for many decades the gold standard for information security managers (Dhillon and Backhouse, 2000; Samonas and Coss, 2014; Von Solms and Van Niekerk, 2013). To avoid an erroneous association with the Central Intelligence Agency, the CIA triad is known alternatively as the AIC triad (Susan Hansche et al., 2003). The model has been conceptualized and developed by security experts and has had a significant impact in information security research as well as in practice (Samonas and Coss, 2014). Figure A-3 depicts the CIA triad and the interdependence between the three main attributes of information security.

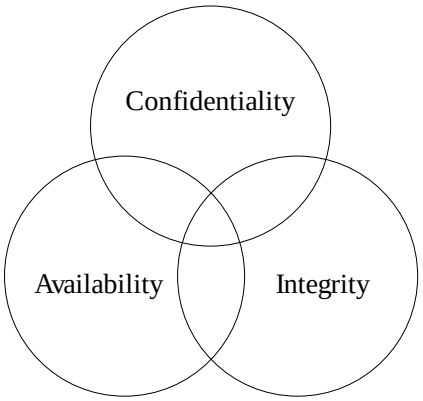

Figure A-3: CIA triad of information security objectives (Andress, 2014, p. 5)

Confidentiality of information is preserved under the condition that access to the content of confidential information is reserved exclusively to authorized individuals. To guarantee information *integrity*, modifications and amendments of data should be performed with authorization and be transparently documented. *Availability* establishes that authorized individuals are allowed to access and exploit the content of information (Dhillon and Backhouse, 2000; Von Solms and Van Niekerk, 2013; Whitman et al., 2012).

For more than two decades the role of the CIA triad as the reference framework for the successful management of information security remained uncontested. Despite the wide acceptance and the vast applications both in research (Hedström et al., 2011; Kolkowska and Dhillon, 2013; Kolkowska et al., 2009) and at the organizational level, the validity of the CIA triplet has been subject to large criticism due to the provision of a partial explanation of information security goals. Donn B. Parker, a renowned scholar and specialist in the field of information security, proposed amendments to the triplet *confidentiality-integrity-availability* and designed the Parkerian Hexad model of security goals (Parker, 1994, 1997). The framework preserves the technical focus and consists of six pillars, the CIA principles and three supplementary security

principles: *authenticity*, *possession* and *utility* (Parker, 1994, 1997). In contrast to the CIA security model, the Parkerian Hexad covers the full spectrum of security goals and provides a consolidated framework for the management of security threats and information loss scenarios. *Authenticity* depicts an additional attribution of the Parkerian Hexad model, which concerns the provenience of information and ensures that information derives from a legitimate source. Losing the *possession* of confidential information does not necessarily imply a breach of confidentiality. The violation of confidentiality results solely from the divulgation of confidential information content. The element of *utility* regards the usability of information resources. The lack of access to encoded information due to technical reasons indicates a typical scenario of information utility loss (Parker, 1994, 1997).

At the beginning of 2000s, the classical traditional technical view of information security was gradually abandoned as the emerging socio-technical perspective and the RITE (*responsibility*, *integrity*, *trust* and *ethicality*) security principles became established (Dhillon and Backhouse, 2000; Dhillon, 2001). The RITE principles emphasize the human, social and organizational facets of information security. Rather than contradicting the CIA technical security goals, these principles provide a supplementary perspective of contemplating information security by emphasizing the necessity of establishing a solid organizational security culture. *Responsibility* refers to how individuals and firm employees perceive their role and are aware of the consequences of irresponsible security behavior. In the era of digital information, personal *integrity* as a moral value plays a major role in preserving the security of information assets and resources. The concept of *trust* has gained an increasing role as organizational controls to monitor security behavior have become less stringent. *Trust* at any hierarchy level is the building block of security culture which fosters a wealthy and balanced security environment. While employees are obliged to comply with regulations and internal information security policies, *ethicality* depicts the willingness to behave professionally in accordance with ethical principles and behavioral norms (Dhillon and Backhouse, 2000; Thomas and Dhillon, 2006).

3 Information Security Breaches

Despite the applied measures to constantly ensure a balanced security environment, often companies fail in their endeavor to protect their information assets and are involved in security breach incidents. The most common framework applied in literature for the classification of information security breaches is the DAD triangle (*disclosure*, *alteration*, *denial*), which depicts the opposite action of preserving the CIA triplet of security goals (Solomon and Chapple, 2009). The unified graphical representation of the CIA model of security goals and the DAD framework of information security breaches is given in Figure A-4.

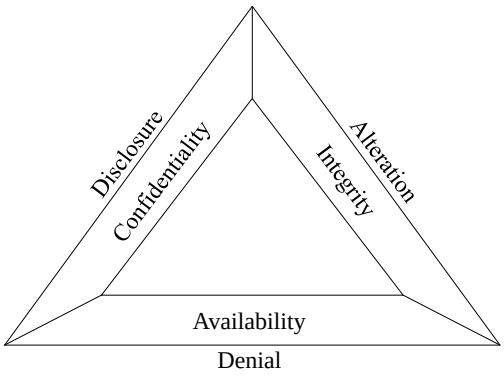

Figure A-4: DAD model of information security breaches (Solomon and Chapple, 2009, p. 5)

Malware, such as computer viruses and trojans, are instruments employed by malicious individuals to infect corporate networks with the scope of gaining access to sensitive information. The successful infiltration of malwares in corporate security networks denotes a typical scenario of an integrity breach. Availability breaches result from the violation of the *availability* security principle. Denial-of-service attacks are availability breaches resulting in the temporary inaccessibility to a determinate service or information (Yayla and Hu, 2011). Data breach incidents represent a potential risk for all companies in possession of digitally stored information and result from the divulgation of classified information. Based upon the taxonomy developed by Curtin and Ayres (2008), there are three major classes of data breach events: logical, procedural and physical. While procedural and physical data breach events are due to unintentional actions of disclosing the content of reserved information, logical data breaches originate from deliberate and conscious actions of breaching information confidentiality (Curtin and Ayres, 2008). Major risk factors for intentional logical breach incidents are insiders (e.g. firm employees), third parties with direct access to corporate confidential information, and external malicious individuals (e.g. hackers) (Privacy Rights Clearinghouse, 2017).

4 Related Research

In literature information security is investigated at three different levels: technical, behavioral and economical (Herath and Rao, 2009; Hua and Bapna, 2013). Technical information security denotes the subfield of information security research dealing with the development and the implementation of security techniques and procedures, such as technical security protocols, antivirus softwares, digital signatures, digital certificates and access control systems. Technical security measures are implemented to continuously safeguard organizational information resources and to prevent the occurrence of data breach incidents (Jain et al., 1997; Venter and Eloff, 2003).

Using different theoretical lenses behavioral security research explores the relationship between information security and human behavior, in particular employees' behavior and misbehavior toward regulations and information security policies (Anderson and Agarwal, 2010; D'Arcy and Devaraj, 2012; D'Arcy et al., 2014; Foth, 2016; Ng et al., 2009). Behavioral security literature is

characterized by a rich theoretical basis and draws upon well-established theories, such as general deterrence theory (GDT), protection motivation theory (PMT) and theory of planned behavior (TPB), adopted from the research fields of social psychology, sociology and criminology (Hua and Bapna, 2013; Lebek et al., 2014; Mishra and Dhillon, 2006).

Economics of information security was initiated almost a decade ago as a distinct research area from the technical and the behavioral security research streams (Anderson and Schneier, 2005; Mai et al., 2016). Within this research stream security scholars address two major research problems. The first research problem deals with the question of how to determine the optimal level of investment in information security from a methodological perspective (Gordon et al., 2014; Mai et al., 2016; Shinoda and Matsuura, 2016; Wang, 2017). Among the various mathematical and economic models proposed with the scope of addressing the problematic of under- or over-investment of information security resources (Gordon and Loeb, 2002; Hausken, 2014; Wang et al., 2008; Willemson, 2010), Gordon-Loeb's 2002 model remains the most significant security investment model (Farrow and Szanton, 2016; Gordon and Loeb, 2002). A major implication of Gordon-Loeb's security model is the beneficial impact of proactive security investments in terms of prevention from future data breach events. Companies willing to invest in information security are less likely to be affected by data breach events, in contrast to companies with low security investment budgets. The model also highlights the importance of the estimate of the overall cost of data breach incidents as a crucial variable for the determination of the optimal level of security expenditure (Gordon and Loeb, 2002).

The second major research topic in the body of research dealing with economic aspects of information security is the estimation of the cost of data breach incidents (Hua and Bapna, 2012), defined as the sum of tangible and intangible costs (Acquisti et al., 2013; Layton and Watters, 2014; Yayla and Hu, 2011). As previously discussed, a critical variable of Gordon-Loeb's model is the estimate of the overall cost of data breach events, which has a direct impact on security investment decisions and on the probability of occurrence of data breach events (Gordon and Loeb, 2002). Given the methodological limitations regarding the estimation of the intangible costs of data breaches, the determination of the optimal amount of security expenditure depends to a large extent from the accuracy of the estimation of the intangible costs of data breach incidents (Cavusoglu et al., 2004a). Table A-3 identifies the main categories of tangible and intangible costs of data breach incidents.

Table A-3: Tangible and intangible costs of data breach events based upon the classification schema of Yayla and Hu (2011)

Cost	Type of Cost	Source
Loss of revenue	Tangible	Xu et al. (2008)
Reputational damage	Intangible	Campbell et al. (2003); Goel and Shawky (2009); Goldstein et al. (2011)
Loss of investor confidence	Intangible	Yayla and Hu (2011)
Loss of consumer trust	Intangible	Cavusoglu et al. (2004a); Goldstein et al. (2011); Zafar et al. (2012)
Loss of competitive advantage	Intangible	Yayla and Hu (2011); Zafar et al. (2012)

Data breach events have an adverse impact on firm sales, revenues and the overall financial performance of the affected firms. The study of Xu et al. (2008) analyzes the impact of a massive confidentiality breach incident at TJX Companies Inc. on revenues and earnings. This major security breach event was publicly announced on January 2007 and involved the theft of credit card information of circa 45 million customers due to a massive hacker attack (Xu et al., 2008). The figures of the quarterly income statements of TJX Companies published in the second quarter of 2007 reveal the extent of the suffered financial loss. Because of the loss of revenues, firm profits decreased from $162 million in the first quarter of 2007 to $59 million in the second quarter of 2007, leading to a total loss of $100 million (Xu et al., 2008).

While the tangible impact of data breaches on revenues and earnings is directly measured based on corporate financial statements, the estimation of intangible costs requires indirect measurement approaches (Campbell et al., 2003; Layton and Watters, 2014; Yayla and Hu, 2011). Due to methodological reasons security scholars have primarily analyzed the effect of data and security breaches on investor confidence. Since the announcement of data breach incidents is reflected on stock market value and thus affects the decision-making of investors, the loss of market value of publicly traded companies is used as a proxy to estimate the loss of investor confidence (Campbell et al., 2003; Yayla and Hu, 2011). In this regard, the event study methodology, which is the standard approach to measure the impact of business and financial events on firm market value (Malkiel and Fama, 1970), represents the indirect approach employed to estimate the impact of data and security breach incidents on investor confidence (Campbell et al., 2003; Kashmiri et al., 2017; Martin et al., 2017). Based on the market value approach, prior research has shown that information security breaches have a negative impact on investor confidence and firm market value. In addition, it has been shown that the magnitude of the impact on investor confidence depends on the breach type. Data breaches resulting from the violation of the confidentiality are penalized to a greater extent from investors than integrity or availability breaches (Campbell et al., 2003).

Although the investigation of the intangible consequences of data breach incidents is relevant both in research and practice, it still remains underexplored due to methodological constraints. To fill this knowledge gap, this thesis investigates the intangible costs of data breach events, and in particular the impact on investor confidence and on corporate reputation.

III Methodologies and Data

1 Methodologies

Systematic Literature Review

A literature review indicates the scientific approach of identifying and scrutinizing targeted literature systematically (Boell and Cecez-Kecmanovic, 2015; Webster and Watson, 2002; Wolfswinkel et al., 2013). Literature reviews focalize on research problems relevant to research and practice and contribute to knowledge in a variety of ways. They provide a summary of high quality research published on a particular research topic; provide new perspectives to mitigate major conceptual, theoretical and methodological gaps emerged through the review process; encourage the development of new theories and improve the theoretical foundations of a specific research stream (Schryen et al., 2015, 2016). A systematic literature review consists of two major phases: (i) the identification of the most influential studies published on the topic of interest through a sequence of predefined steps; (ii) the analysis and the synthesis of selected literature grounded in conceptual frameworks and theoretical models (Bandara et al., 2011; Levy and Ellis, 2006; vom Brocke et al., 2015; Wagner et al., 2016).

Study 1 synthesizes the body of research investigating the intangible costs of data and information security breaches and has the character of a descriptive literature review. Based on the guidelines of Webster and Watson (2002) for systematic literature review studies, the selection process is guided by a conceptual framework and the findings are organized in a concept-based matrix encompassing the following concepts: *intangible cost*, which refers to the type of intangible cost investigated in the respective study, *breach type*, meaning the type of security breach included in the sample, *theory*, the theoretical foundation, and *method* refers to the methodological approach used to quantify the intangible costs. The concepts of *theory* and *method* are constituting elements of Laudan' theory or "reticulated model of scientific rationality" (Laudan, 1984; Hunt, 1990; Freedman, 1999; Patterson and Williams, 1998). Laudan's model, which delineates the relationship between the foundation pillars of scientific research, sustains that theories and methods are indicators of the scientific progress of a research discipline. Focusing on theories and methods as key aspects of a literature review enables researchers to identify theoretical deficits, methodological limitations and to promote the progress of future research (Dibbern et al., 2004).

Sentiment Analysis

Sentiment analysis (or sentiment mining) comprises a series of steps applied to detect and analyze individuals' attitude, judgements and opinions referred to a specific situation and context (Feldman, 2013; Liu, 2012; Wang and Zhai, 2017). Sentiment mining techniques are amply applied on unstructured social media data to extract social media users' sentiment from text units regarding product reviews (Tripathy et al., 2016), movie reviews (Zhuang et al., 2006), stocks (Feldman et al., 2011) etc. Techniques in existing literature for the detection and classification of sentiment are broadly classified in two major categories: supervised and non-supervised machine learning algorithms and lexicon-based techniques. While machine learning approaches enable an automated sentiment analysis through different algorithms, lexical approaches rely upon predefined word lists of dictionaries to measure the subjectivity and sentiment polarity of text documents (Taboada et al., 2011).

In this thesis sentiment analysis is applied to recognize and measure social media users' reaction and the average sentiment in the wake of data breach incidents. Sentiment polarity, which indicates whether a word has a positive, negative or neutral semantic orientation, is gauged in **Study 3** and **Study 5** with the General Inquirer content analysis software (Stone et al., 1966). Based upon the Harvard IV-4 psychosocial dictionary, General Inquirer determines the text's valence in terms of the frequency of words with positive and negative connotation. The SentiStrength software, developed with the scope of detecting sentiment in short informal online texts (Thelwall et al., 2010), is applied in **Study 4**. The software assesses the sentiment strength by providing a range of scores for both the positive and negative connotation of words.

Event Study

Event study is a quantitative statistical approach (Henderson Jr, 1990) designed to quantify the impact of business events on market value and shareholder wealth under the assumption of efficient behavior of capital markets (Boehmer et al., 1991; Brown and Warner, 1985; Dyckman et al., 1984). While there are three different scales of market efficiency, the underpinning theoretical foundation of the event study methodology is the semi-strong form. The semi-strong form of market efficiency presupposes an immediate incorporation of newly released public information in firm share prices. Accordingly, publicly available information already merged in the stock prices cannot be exploited to achieve higher returns, neither with the use of fundamental analysis or technical analysis (Fama, 1991, 1998; Malkiel and Fama, 1970). Originally developed with the scope of detecting abnormal price reactions related to corporate events in the field of financial economics (Wright et al., 1995), the method has been largely employed in various business research fields such as accounting (Olibe, 2016), marketing (Sorescu et al., 2017), management (McWilliams and Siegel, 1997), information systems research (Konchitchki and O'Leary, 2011) and information security research (Spanos and Angelis, 2016). In information security research event studies have been mainly employed to investigate the intangible cost of

data and information security breaches. In particular, it has been utilized in the research stream dealing with the intangible costs of information security breach events to measure the impact of data breach events on investor confidence and firm market value (Spanos and Angelis, 2016).

Two key variables define the event study approach: abnormal returns and cumulative abnormal returns. Triggered by the announcement of business-relevant events, abnormal returns reflect the discrepancy of stock price performance between the event window and the estimation window. The event window is positioned around the event date in order to capture the immediate stock price reaction resulting from the event disclosure. The event date denotes the public disclosure of the event and the reference point for the specification of the estimation window. The estimation window on the other hand depicts a time interval positioned before the event announcement in order to measure the average normal stock price performance (Binder, 1998; MacKinlay, 1997; McWilliams and Siegel, 1997). Abnormal returns measure the change of stock price performance on a specific day of the event window. Cumulative abnormal returns synthesize the cumulative impact of the announced event on stock price returns and are measured as the sum of abnormal returns over the event window (Binder, 1998; Konchitchki and O'Leary, 2011; McWilliams et al., 1999).

Event study is not delimited to the measurement of daily cumulative abnormal stock price returns. Other empirical applications of the event study methodology include the measurement of the impact of financial events on trading volume (Im et al., 2001), as well as the intraday analysis of capital market liquidity (Boudt and Petitjean, 2014). Given the versatile character of the event study methodology (Im et al., 2001), the event study is applied in two different forms within this thesis. The standard event study method is employed in **Study 2** and **Study 5** to measure the impact of data breach announcements on stock price returns. In **Study 2** the event study approach measures the impact of NSA-related data breaches on market value and shareholder wealth over a three-day event window. While **Study 2** deals with a specific type of data breach events, in **Study 5** the event study method assesses the effect of classic data breach events on investor confidence. Because **Study 5** draws a comparison between two categories of intangible costs, investor confidence and corporate reputation, abnormal returns are measured over a longer event window spanning over a period of twelve days. Sentiment-based event study, which uses social media content as input, is the approach employed in **Study 3** and **Study 5** to measure the impact of data breach events on social media sentiment and corporate reputation. Sentiment-based event study results from the combination of sentiment analysis techniques with the framework of the event study method and provides a solid basis for the measurement of corporate reputation.

Abnormal sentiment and cumulative abnormal sentiment are the central variables of the sentiment event study approach that quantify the size of the reputational impact of data breaches. Abnormal sentiment indicates the difference between two entities: the sentiment polarity values over the event window and the normal sentiment polarity values over the estimation window. Cumulative abnormal sentiment aggregates sentiment polarity scores over the event window and measures

the cumulative impact of data breach events on corporate reputation.

Multivariate Regression

A cross-sectional multivariate regression analysis is performed in **Study 4** to explore the influencing factors of corporate reputation in the presence of a data breach crisis event. The regression model aims to uncover statistically significant relationships between corporate reputation and four predictors: *news media exposure*, *prior reputation*, *breach history* and *firm size*.

2 Data

The systematic state of the art review of the literature dealing with the intangible costs of data breach announcements in **Study 1** is performed on the basis of a step-by-step-procedure. The various steps consist of criteria for the identification, retrieval, selection and analysis of pertinent literature in line with the study's research scope.

Data breach samples analyzed in this thesis are obtained from different sources. The sample of NSA data breach events explored in **Study 2** results from the manual search of news articles and reports published in international traditional media outlets. Data breaches investigated in **Study 3**, **Study 4** and **Study 5** are retrieved from two major data breach electronic databases: DataLossDB (Datalossdb, 2017) in **Study 3**, **Study 5** and Privacy Rights Clearinghouse (Privacy Rights Clearinghouse, 2017) in **Study 4**. Both databases provide an extensive chronology of data breaches occurred in the past fifteen years and specify company and incident characteristics, such as organization type, breach type, breach source and loss size (Sen and Borle, 2015).

Thomson Reuters Datastream is the source of structured financial data (stock prices and market capitalization) used in **Study 2**, **Study 4** and **Study 5**. Time series of stock prices were used to measure the impact of data breach announcements on investor confidence and firm market value with the event study approach (MacKinlay, 1997) in **Study 2** and **Study 5**. Market capitalization is the proxy for the variable *firm size* in the multivariate regression model performed in **Study 4**.

Social media data used in **Study 3** and **Study 5** to measure sentiment fluctuations and the reputational impact of data breach incidents originate from the social media intelligence tool SDL SM2 (SDL SM2, 2017). The raw data, which consist of social media postings published before and after the data breach announcement in a wide range of social media platforms, are processed with sentiment analysis techniques to derive sentiment polarity and assess the impact on corporate reputation. **Study 4** uses Twitter data to explore the influencing factors of corporate reputation.

B Studies on the Intangible Costs of Data Breaches

This chapter incorporates five studies part of this thesis dealing with the intangible costs of data breach announcements. Following the depiction of the research framework in section A.I.3, the chapter is partitioned in four sections. The first section comprises **Study 1**, which presents the results of a state of the art literature review, followed by **Study 2** dealing with the impact of data breaches on investor confidence and firm market value. The third section focuses on the impact of data breach events on corporate reputation and comprises **Study 3** and **Study 4**. The last section of chapter B includes **Study 5**, which examines simultaneously the impact on investor confidence and on corporate reputation.

I State of the Art Literature Review

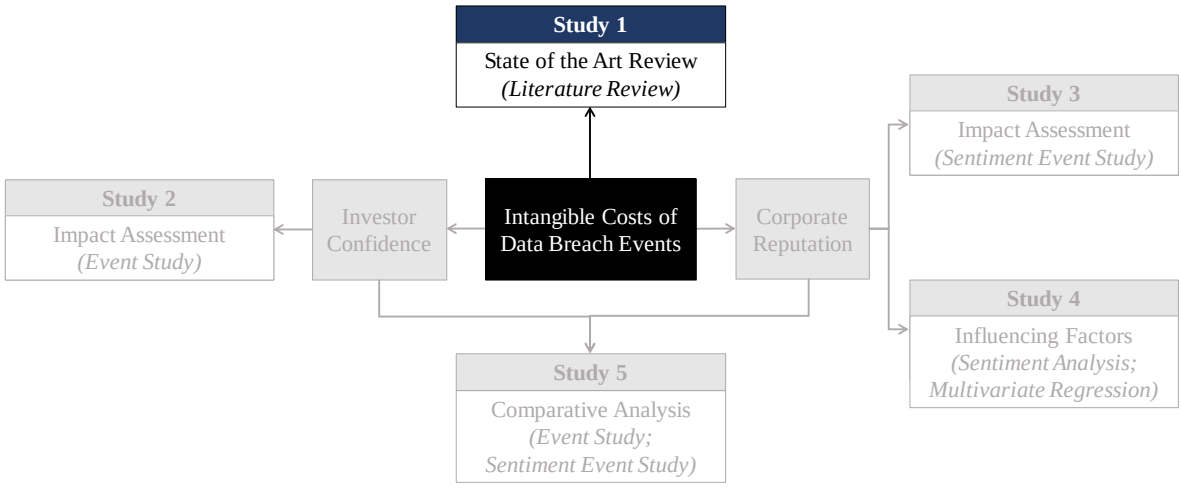

Figure B-1: Part of the research framework addressed by Study 1

1 The Intangible Cost of Information Security Breaches: A State of the Art Analysis

(The full-text of this study has been omitted due to copyright)

Table B-1: Fact sheet of Study 1

Title	The Intangible Cost of Information Security Breaches: A State of the Art Analysis
Authors	Griselda Sinanaj, griselda.sinanaj@wiwi.uni-goettingen.de* *University of Göttingen
Outlet	Journal of Information System Security (JISSec 2015), Volume 11, Issue 2, 111-130, Completed Research Paper
Abstract	Information security breaches constitute a major concern for businesses in today's interconnected digital economy. Practice and previous research mention that security breaches have various tangible and intangible consequences on organizations. Decreased sales and lost revenue are tangible effects, while loss of investors' confidence, reputation damage, loss of competitiveness and loss of consumer trust are intangible costs. In contrast to the tangible costs of security breaches, the quantification of the intangible costs is not straightforward, therefore this literature review study focuses on the intangible costs of security breaches. The analysis reveals that while certain costs, such as loss of investors' confidence, have received considerable attention in research, others, such as reputation damage or loss of consumer trust remain barely explored and require further inquiry. In addition, several studies show a lack of theory, as they do not build upon specific reference theories to address their research objectives.
Keywords	Information security breaches, tangible costs, intangible costs, investors' confidence, reputation damage, loss of consumer trust

II Impact on Investor Confidence

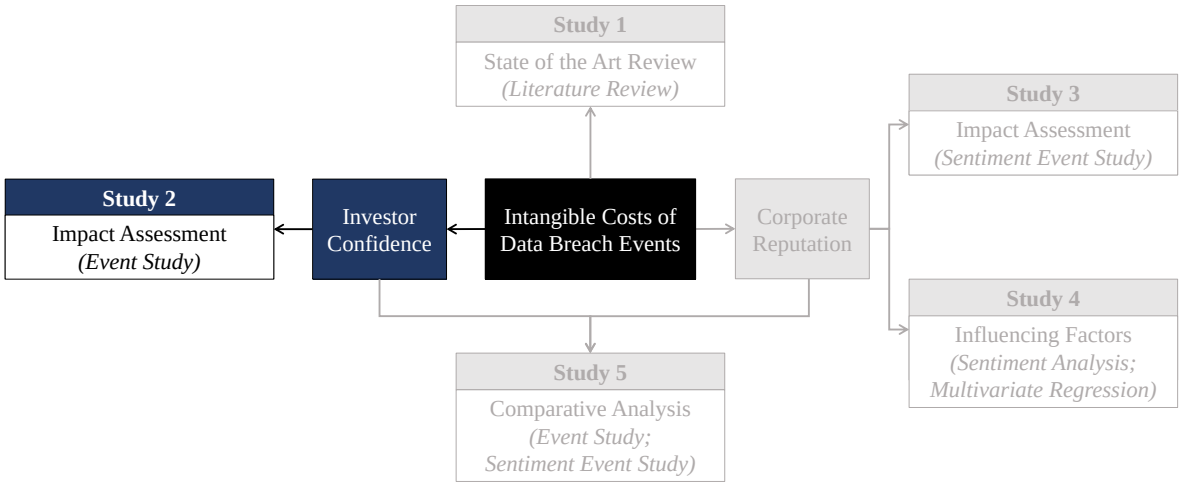

Figure B-2: Part of the research framework addressed by Study 2

1 NSA Revelations of Privacy Breaches: Do Investors Care?

Table B-2: Fact sheet of Study 2

Title	NSA Revelations of Privacy Breaches: Do Investors Care?
Authors	Griselda Sinanaj, griselda.sinanaj@wiwi.uni-goettingen.de* (Corresponding author) Timo Cziesla, timo.cziesla@wiwi.uni-goettingen.de* Jan Kemper, jan.kemper@wiwi.uni-goettingen.de Jan Muntermann, muntermann@wiwi.uni-goettingen.de* *University of Göttingen, Göttingen, Germany
Outlet	Proceedings of the 21st Americas Conference on Information Systems (AMCIS 2015), Completed Research Paper
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

1.1 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, 2013a). 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 York 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., 2004b; 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., 2003b; 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.

1.2 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 consumer or other parties' data was exposed through bad security practices, hacker attacks, insider attacks, computer or data thefts, and lost data or equipment"* (Acquisti et al., 2006, p. 1567-1568). 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, 2013b). 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, 2013c). 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.

1.3 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 place 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., 2004b; 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 B-3 visualizes the elements of an event study:

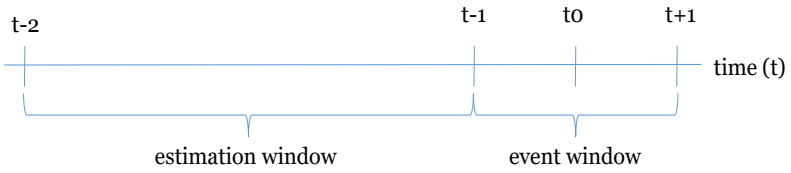

Figure B-3: Estimation and event window of an event study

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:

$$R_{i,t} = \alpha_i + \beta_i R_{m,t} + e_{i,t} \tag{1}$$

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 $\widehat{\alpha_i}$ and $\widehat{\beta_i}$ 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:

$$e_{i,t} = AR_{i,t} = R_{i,t} - \widehat{\alpha_i} - \widehat{\beta_i} R_{m,t} \tag{2}$$

or put differently:

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

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:

$$AAR_t = \frac{1}{N}\sum_{i=1}^{N} AR_{i,t} \tag{4}$$

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 $CAAR_{(t-1,t+1)}$ (cumulative average abnormal returns):

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

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.

1.4 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 5^{th} 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, 2013a). 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 5^{th} 2013 and March 31^{st} 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, 2013c). 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].

1.4.1 Descriptive Statistics of Security Breaches

This subsection provides a summary on the sample characteristics. As showed in Table B-3, 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.

Table B-3: Types of security 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 B-4 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 5^{th} 2013 and March 31^{st} 2014.

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

Table B-4: Distribution of security breaches by country

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

The classification of the security breaches depending on sector is displayed in Table B-5. As can be seen, the sector of communications is the most affected sector from the NSA-affair, followed by the technology sector.

Table B-5: Distribution of security breaches by sector

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

1.5 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 B-6, 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.

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

Table B-6: AAR results on the full sample

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

$^{*}p < .10$ (one-tailed test)

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 B-7 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.

Table B-7: CAAR results on the full sample

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)

1.6 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.

III Impact on Corporate Reputation

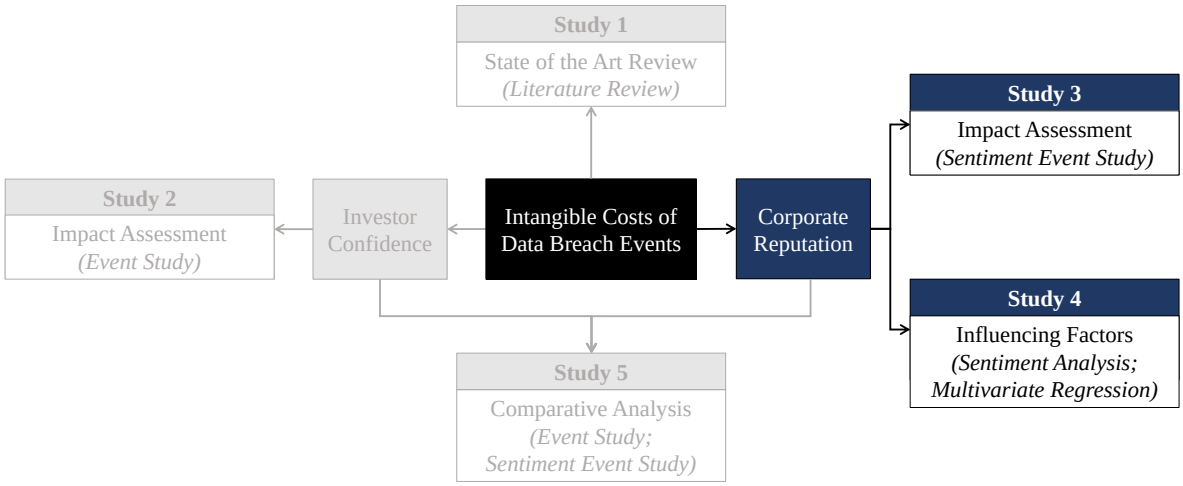

Figure B-4: Part of the research framework addressed by Study 3 and Study 4

1 How Data Breaches Ruin Firm Reputation on Social Media! – Insights from a Sentiment-based Event Study

Table B-8: Fact sheet of Study 3

Title	How Data Breaches Ruin Firm Reputation on Social Media! – Insights from a Sentiment-based Event Study
Authors	Griselda Sinanaj, griselda.sinanaj@wiwi.uni-goettingen.de* (Corresponding author) Jan Muntermann, muntermann@wiwi.uni-goettingen.de* Timo Cziesla, timo.cziesla@wiwi.uni-goettingen.de* *University of Göttingen, Göttingen, Germany
Outlet	Proceedings of the 12th International Conference Wirtschaftsinformatik (WI 2015), Completed Research Paper
Abstract	Data breach events are heavily discussed in social media. Data breaches, which imply the loss of personal sensitive data, have negative consequences on the affected firms such as loss of market value, loss of customers and reputational damage. In the digital era, wherein ensuring information security is extremely demanding and the dissemination of information occurs at a very high speed, protecting corporate reputation has become a challenging task. While several studies have provided empirical evidence of the financial consequences of data breaches, little attention has been dedicated to the link between data breaches and reputational risk. To address this research gap, we have measured the reputational effect of data breaches based on social media content by applying a novel approach, the sentiment-based event study. The empirical results provide strong evidence that data breach events deteriorate the reputation of companies involved in such incidents.
Keywords	Data breaches, social media, reputational risk, sentiment analysis, sentiment-based event study

1.1 Introduction

In August 2014, the largest U.S bank J.P Morgan announced being victim of a data breach incident involving the theft of 76 million households data, including names, addresses, phone numbers and e-mail addresses, and 7 million data of small businesses (Forbes, 2014). Data breach incidents, which have become a common phenomenon businesses have to cope with, generate on average a unitary cost of $145 to the affected companies (Ponemon Institute, 2014) and additional significant loss of market value to publicly listed firms (Yayla and Hu, 2011).

Data breaches are negative events and as such, are also heavily discussed in social media. With this regard, survey studies reveal that data breach incidents have a negative influence on corporate reputation, due to the presence of social media venues acting as amplifiers through the rapid dissemination of information (Economic Intelligence Unit, 2012). While research has primarily focused and provided empirical evidence of the financial implications of security incidents (Yayla and Hu, 2011), apart from survey studies emphasizing the risk of reputational harm of data breaches, little attention has been devoted to the empirical investigation of the link between data breaches and corporate reputation.

To tackle the lack of research on this issue, we empirically investigate the reputation effect of data breach incidents by analyzing users' reaction on social media platforms. For this purpose, we measure the change in the social media sentiment before and after the disclosure of data breaches by applying a sentiment-based event study.

This study contributes primarily with new theoretical insights on the link between IT security incidents and corporate reputation and proposes a novel approach, which can be extended to other contexts. To the best of our knowledge, there have been no previous attempts of adapting the classical event study method to analyze event-related opinion formation utilizing unstructured data from social media.

The remainder of the paper is structured as follows. The following section focuses on the critical analysis of the current literature, establishes the research gaps and formulates the research questions. Further on, we proceed with the sample selection process and with a detailed description of the applied research methodology. We conclude with the interpretation of results and provide a summary of limitations and potential directions for future research.

1.2 Related Work

1.2.1 Economic Impact of Data Breaches

In spite of the substantial benefits to companies such as lower operating costs, increase of productivity and efficiency (Mithas et al., 2012), technological advances have additionally increased the vulnerability of information systems. These systems are often target of skilled intruders who attack them and come into possession of large amounts of sensitive data (Andoh-

Baidoo et al., 2010; Whitman, 2004). Data breaches belong to the broad category of information security incidents and imply the loss or theft of personal data records in electronic form, such as social security numbers, credit card numbers, user names and addresses (Romanosky et al., 2011). The occurrence of such events can turn into large costs for the affected organizations. Tangible costs are immediately covered in the aftermath of the public dissemination of the incidents and include for instance, notification of customers through hotline customer support, forensic expertise (Romanosky et al., 2011), software and hardware costs, while intangible costs are not easily quantifiable and entail the loss of investor confidence, competitive advantage, trust and also reputational damage (Yayla and Hu, 2011).

Several studies have attempted to quantify the intangible costs of information security breaches by measuring the financial impact of security breach announcements on listed companies (Cavusoglu et al., 2004a, p. 68). These studies adapt the event study method from the financial domain to measure the capital market reaction of the involved firms. This is the main aspect related to the economic impact of security breach events being actually addressed in the literature. There is yet no clear understanding of what are the dynamics of the other potential intangible costs, other than the loss of investor confidence and the financial impact. Hence, there are evident research gaps in the current literature that call for future contributions.

We claim that special attention should be especially devoted to the potential reputational losses originating from security breaches. Corporate reputation is commonly considered as one of the most valuable intangible assets that can help an organization gain competitive advantage over its rivals. Although literature offers a wide range of definitions on corporate reputation (Fombrun, 1996), in this study reputation is defined as "the overall opinion about a firm by customers, investors, employees and the general public" (Colleoni et al., 2011, p. 4).

1.2.2 Social Media and Corporate Reputation

With the advance of Web 2.0 technologies, social media has become an additional driver of reputation risk (Aula, 2010). Content generated through communication in social media can become viral as it reaches and involves a large number of users worldwide (Colleoni et al., 2011). While on the one hand, stakeholders such as consumers, investors and customers are free to post and exchange their personal thoughts and ideas on brands and products, on the other hand organizations do have little influence in terms of controlling or altering user generated content in social media (Kaplan and Haenlein, 2010). As a consequence, companies do not have any more a full control on their reputation; in contrast, reputation in the social web environment is dictated primarily by the voice of users expressed in on line conversations (Jones et al., 2009).

Several cases show that social media can act as a reputational risk factor. For example, when an airline accidentally damaged a musician's guitar and refused to replace it, the musician published a music video about the incident on a social video platform. Millions of people watched the

video and as the newspaper and television started to report on the story, the airline gave in, trying to prevent further reputational damage (Aula, 2010).

To measure corporate reputation on social media data, we make use of the sentiment analysis, whose widespread application in academia has coincided with the rise of the social media phenomenon and the consequent generation of large amounts of unstructured data. At the center of sentiment analysis or opinion mining is the study and analysis of humans' emotions, opinions and evaluations. Sentiment analysis has been applied in diverse research domains including finance and management (Liu, 2012), as well as for the measurement of corporate reputation based on social media content.

Seebach et al. (2013) used sentiment analysis to analyze the way social media content can be exploited for corporate reputation management. The study provides empirical evidence of the beneficial impact of social media on corporate reputation from a business agility perspective. Benthaus et al. (2013) applied sentiment analysis to quantify reputation of ten large corporations based on historical social media data extracted from the microblogging platform Twitter. Sentiment analysis has been utilized to measure the daily sentiment values for each firm, while, in a second step, an estimating technique provides a linear representation of the sentiment values. Furthermore, the presented approach is validated by comparing the study results with the reputation ranking provided by the Reputation Institute, which is a survey-based and hence a classical measure of reputation. Colleoni et al. (2011) developed instead an open source platform to measure online corporate reputation on the basis of real time Twitter stream data. Based on a predefined word lexicon, an algorithm generates a sentiment score for each incoming tweet based on the number of affective words. The open platform provides also a graphical representation of such sentiment values, which serve as a proxy for corporate reputation and offer hence the temporal evolution of the reputation values.

With respect to the measurement methods of corporate reputation, a very common approach used so far in academia relies on survey studies, e.g. the popular Fortune's survey of America's Most Admired Corporations. The participation on these surveys is usually reserved to a limited category of stakeholders such as the board of management and business analysts. Hence, such reputation measures do not encompass the evaluations and assessments of another category of important stakeholders, such as potential customers, consumers and employees (Deephouse, 2000). Reputation measures anchored on social media data represent an alternative approach to survey-based measures which are obtained from the exploitation of unstructured data that differ substantially from the data at the basis of survey measures (Benthaus et al., 2013). Corporate reputation measures based on social media content incorporate thus the opinions and assessments of a wider range of stakeholders.

In sum, prior research has already analyzed on the one side, the relationship between social media and corporate reputation and on the other side the financial consequences of information

security incidents, while the interrelation of the triad data breach-social media-reputation has received little consideration. Hence, we aim at addressing this research gap by analyzing the reputational impact of data breach incidents on the basis of social media contents. In line with previous research, we apply the sentiment analysis method to analyze social media datasets in order to quantify corporate reputation (Benthaus et al., 2013; Colleoni et al., 2011). We separate ourselves from previous studies since we develop a new approach to investigate how corporate reputation is affected by critical discussions in social media following the public dissemination of data breaches. Based on this theoretical background we derive the following research questions that we aim to address in this study:

Research question 1 (RQ1): How to measure reputational effects of data breaches utilizing social media content?

Research question 2 (RQ2): Does social media promptly reflect newly available negative information on data breach incidents and how long does this effect persist?

1.3 Data Sources and Sample Selection

We exploited two distinct databases for the data collection process. The primary data set utilized for the sample selection comprises data breach incidents extracted from DataLossdb.org. This data source is an open-source relational database developed by the Open Security Foundation providing access to information on security vulnerabilities or data breaches. DataLossdb.org provides descriptive metadata about each single security incident recorded. Relevant to our study is the following information: incident ID, name of organization involved, date of occurrence and number of lost/stolen ID's (Open Security Foundation, 2014). Date of occurrence corresponds to the incident date as publicly (firstly) reported on primary news media sources, hereafter denoted as event date $[t_0]$.

The selection criteria applied to identify the final data sample are ranked as follows: a) Data breach incidents occurred worldwide between 1^{st} January, 2010 and 16^{th} November, 2012. At this point, the dataset has been controlled for the presence of incident duplicates, which have been accordingly excluded. Multiple data breaches associated to the same firm were treated as separate events (Acquisti et al., 2006). b) Since we seek to measure the reputational impact of data breaches on global firms, the sample has been restricted to publicly traded companies at the event date. Incidents that affected privately held companies, governmental organizations, hospitals and universities have been accordingly removed. c) Finally, to ensure a significantly broad social media coverage for each security incident, we selected only those incidents with more than 30,000 lost or stolen records. Setting up this restriction on the original dataset increases the likelihood of extracting a high number of postings related to the specific firm involved in the data breach event.

Next we collected social media data on the sample of breach incidents through the social media

monitoring tool SDL SM2. Social media data has been crawled from the following social media platforms: "blogs", "microblogs" (e.g. Twitter), "social networks"(e.g. Facebook), "online message boards", "wikis", "video- and photo-sharing" and "classified/review sites" (SDL SM2, 2014). To ensure the extraction of all postings referred to the company affected by the respective data breach, we set up the search query based on the company name e.g. "Citibank" and additionally refined the search by setting two parameters: English language and date range $[t_{-45}; t_5]$. Social media data has been collected for a total of 51 days, starting 45 days before the event date and 5 days afterwards, including the event date $[t_0]$ and entails only postings in English language. We provide further clarification on the date range parameter in the following methodological section. Searching through social media outlets based on the same search query along the entire time interval $[t_{-45}; t_5]$, aims at assuring consistency in the empirical analysis and avoiding biased results. The final output resulting from the search query contains the following relevant fields: result ID; media type (e.g. blog); author name; content of posting and timestamp (date of publication).

Further on, we screened thoroughly the data sample for the presence of confounding events (e.g. earning announcements or important managerial decisions) (McWilliams and Siegel, 1997), whose disclosure overlaps with our predefined event window (-3;+5). This procedure although demanding, assures us that the effect on the reputation of the affected firms we are measuring is triggered from data breach announcements and not from such exogenous factors. Therefore, from the sample of breach incidents, two instances of data breaches have been discarded, leading to 40 data breach events.

Finally, we included only data breach events with postings on each single day within the time interval $[t_{-45}; t_5]$. This criteria (i.e. daily data) it is a necessary requisite to apply the sentiment-based event study approach. If the estimation or the event window contains any missing values, it would be necessary to apply interpolation techniques, which, in consequence, would counteract our objective to appropriately measure the changes in the sentiment values.

After applying the selection criteria we obtain a final sample of 30 data breach incidents. Table B-9 provides a summary of our sample selection process.

Table B-9: Sample selection criteria

Selection criteria	**Number of observations left**
Step 1: Data breach sample identification based on Datalossdb.org	
Time span: 1.1.2010 to 16.11.2012	1736
Public firms	282
Loss size: No. of ID's lost/stolen greater than 30,000	42
Confounding events during the event window	40
Step 2: Social media data collection based on SDL SM2	
Postings on each day within $[t_{-45}; t_5]$	30

1.4 Research Design

This section addresses our first stated research question RQ1 and contains a detailed explanation of the methodological approach applied in order to measure reputational consequences of data breaches based on social media content.

1.4.1 Sentiment Analysis

Three different methodologies can be utilized to perform sentiment analysis: linguistic, machine learning, and dictionary-based (Colleoni et al., 2011). To analyze the content of texts extracted from social media platforms we apply the dictionary-based approach, which relies on predefined word lexicons for the text classification (Feldman, 2013). Social media data have been processed with the General Inquirer (GI) content analysis software based on the Harvard IV-4 psychosocial dictionary and is characterized by pre-labeled word lists with a particular semantic orientation such as positive, negative, strong, happy, sad. GI counts the word occurrences for the respective word category and provides a final output with the text classification (Stone et al., 1966). Relevant to our context are the word categories labeled as "positive" and "negative". We use the sentiment polarity measure as a proxy for the overall users' opinion on social media (Tetlock et al., 2008, p. 1442):

$$\textit{sentiment polarity} = \frac{\#Words_{POS} - \#Words_{NEG}}{\#Words_{POS} + \#Words_{NEG}} \tag{1}$$

Sentiment polarity values are comprised in the interval [-1;+1], with the highest value of (+1) and the lowest value of (-1). In case the number of positive words equals the number of negative words, the text has a neutral sentiment and polarity is zero. The sentiment polarity variable will then be integrated into the sentiment-based event study approach in order to measure the reputational effects of data breaches.

1.4.2 Sentiment-based Event Study

To measure the impact of data breach announcements on corporate reputation, we combined the classic event study method (MacKinlay, 1997) with the sentiment analysis. The theoretical fundament of the classical event study is the Efficient Market Hypothesis, which claims that any information newly available to the market will be instantly reflected by the asset prices (Fama et al., 1969). Implementing an event study requires the specification of both an event window and an estimation window. While the estimation window is used for assessing price movements that can be expected when no significant event has happened, the event window covers an interval around the event date (MacKinlay, 1997).

Miyajima and Yafeh (2007) have applied the event study method to analyze the effect of the Japanese banking crisis in non-financial companies considering a short estimation window of 40 days, between -60 and -20 days prior to the event under investigation. In line with previous research (e.g. Miyajima and Yafeh (2007)), we opted for a short estimation window comprising only 36 days starting at day -45 and ending at day -10. Communication through social media platforms generates large amounts of unstructured data whose extraction and processing for empirical research is time consuming (Benthaus et al., 2013). Therefore, unlike many other classical event studies being based on long estimation windows (e.g. 250 trading days) we chose a relatively short one.

Next, we defined an event window of nine days covering the period from day -3 to day 5 including the event date t_0. The choice of this event window has two main purposes. First, the three days prior to the event date account for any leakage of information related to data breaches prior to its public disclosure through traditional media channels. In addition, it is common practice in classic event studies to consider event windows comprising several days following the event date, in order to observe the gradual recovery of stock prices after the information has been incorporated into the prices (Goldstein et al., 2011). In doing so, we can observe at which point of time the effect of data breach disclosure will be entirely absorbed by the opinion formation observed in social media.

One disadvantage of a long event window, in particular if the analysis sample contains large corporations, is the high presence of other firm-related events or confounding events, whose effects blur the event study results (McWilliams et al., 1999). If we opt for a longer window, it is very likely that we obtain a final sample of less than 30 data breaches, which in turn would reduce drastically the power of statistical tests (Brown and Warner, 1980). In addition, previous studies using the classic event study method typically detect significant price effects only a few days prior and subsequent to the event dates (Goldstein et al., 2011).

In classical event studies, abnormal returns (AR_{it}) measure the deviation of the actual stock returns (R_{it}) from the ex-ante normal returns expected if the event did not occur $[E(R_{it}|X_{it})]$ and are calculated as follows (MacKinlay, 1997, p. 15):

$$AR_{it} = R_{it} - E(R_{it}|X_{it}) \tag{2}$$

Cumulative abnormal returns (CAR_{it}) are obtained from the sum of AR_{it} for each day of the event window (MacKinlay, 1997, p. 21):

$$CAR_{it} = \sum_{t=1}^{N} AR_{it} \tag{3}$$

Following the above procedure, we define abnormal sentiment (AS_{it}) as the central variable of our sentiment-based event study in order to quantify the reputational effect of data breaches, formally specified as follows:

$$AS_{it} = S_{it} - E(S|X_{it}) \tag{4}$$

Since sentiment polarity S_{it} and $E(S|X_{it})$ assume values in the range [-1;1], AS_{it} values will be comprised in the interval [-2;2]. Similarly to the classical event study, cumulated abnormal sentiment (CAS_{it}) on each day of the event window is calculated with the expression:

$$CAS_{it} = \sum_{t=1}^{N} AS_{it} \tag{5}$$

There are basically three main statistical models used to evaluate the normal performance $E(R_{it}|X_{it})$ of stock prices in the context of event studies: (1) constant-mean return model which generates mean-adjusted returns; (2) market-adjusted return model and (3) the market model. We adopt the constant-mean return model based on the assumption that the ex-ante expected return $E(R|X_{it})$ of each security i is constant during the estimation window, i.e. $E(R|X_{it}) = \mu$ (MacKinlay, 1997):

$$AR_{it} = R_{it} - \mu \tag{6}$$

The sentiment-based event study builds upon social media sentiment values and not on stock price returns unlike the classical event study. Adapting the market-adjusted return model would require the estimation of an overall market sentiment, which does not appear feasible. Furthermore, the market model is also not appropriate to our approach, as it requires the estimation of the market sentiment and of the model parameters. Hence, we measure abnormal sentiment AS_{it} values as follows:

$$AS_{it} = S_{it} - \mu \tag{7}$$

The constant-mean return model, although not being the most popular approach applied in practice, yields similar results as the other two models and does not influence the quality and the reliability of our empirical results. This is due to the low sensitiveness of the variance of abnormal returns against the normal returns model (Brown and Warner, 1980).

1.5 Empirical Analysis

1.5.1 Descriptive Statistics

Our final dataset comprises a sample of 30 data breach incidents and a total number of 388,635 postings obtained from social media platforms through the business intelligence software SDL SM2. The average number of records compromised by the breach incidents equals 4,350,237. The number of data records as well as the large number of postings illustrate respectively the relevance of our data breach sample and the richness of our social media dataset. With respect to breach source, for 70% of the incidents the source of the breach is outside of the involved firms, for 23% of the breaches inside of the firms and for the remaining 7% such information is not available. Considering the type of breach, 57% of the incidents were caused by hackers, 7% by fraud, followed by other types of breaches such as lost tapes, stolen drives and snail mails.

In terms of the distribution of data breaches over the time, recent years were characterized by a higher number of reported data breaches. The highest number of incidents were observed in 2012 (40%) and 2011 (40%), compared to 20% in 2010.

1.5.2 Results

To address our second research question RQ2, we computed over a nine-day long event window [-3;+5] the metrics average abnormal sentiment (AAS) and its cumulated effect over the event window, cumulated average abnormal sentiment (CAAS). To test the statistical significance of AAS and CAAS, we adopted and carried out the classic parametric *t*-test on the full sample. Formally, the validity of the null hypothesis $H_0 : \mu_{\text{AS}}(\mu_{\text{CAS}}) \geq 0$ has been tested against the alternative hypothesis $H_1 : \mu_{AS}(\mu_{\text{CAS}}) < 0$. Since the sample size equals 30 observations, the parametric approach is in this case applicable since the sampling distribution tends to be normally distributed (Field, 2009, p. 134). To test the robustness and the validity of results, we additionally report nonparametric test statistics based on the Wilcoxon signed-rank test. Mean and median values of AS and CAS are displayed for the event window along with the parametric- and nonparametric test results in Table B-10 and Table B-11 respectively. Mean AS (mean CAS) is equivalent to AAS (CAAS) respectively.

Table B-10: Statistical test results on AAS between day (-3) and day (+5)

	Parametric test		**Nonparametric test**	
Day	Mean AS (% neg. AS)	*t*-statistic (*p*-value)	Median AS	*W*-statistic (*p*-value)
-3	0.029 (43)	1.184 (0.877)	0.019	278 (0.825)
-2	0.018 (43)	0.696 (0.754)	0.019	263 (0.735)
-1	-0.004 (53)	-0.163 (0.436)	-0.004	223 (0.428)
0	-0.178 (67)	-3.383 (0.001***)	-0.108	98 (0.002***)
+1	-0.152 (67)	-3.503 (0.001***)	-0.109	91 (0.001***)
+2	-0.095 (60)	-2.411 (0.011**)	-0.050	149 (0.044**)
+3	-0.123 (70)	-3.373 (0.001***)	-0.088	95 (0.002***)
+4	-0.083 (67)	-2.771 (0.005***)	-0.076	110 (0.005***)
+5	-0.067 (67)	-1.536 (0.068*)	-0.020	146 (0.038**)

$^{*}p < 10\%$, $^{**}p < 5\%$, $^{***}p < 1\%$ (one-tailed test)

Table B-10 shows that both test procedures lead to similar results in terms of statistical significance, with exception of output values referred to day 5 (p-value=0.038 and p-value=0.068). Changes in sentiment polarity are detected from the day prior to the breach announcement (mean AS=-0.004, median=-0.004), supported also from the increase of 10% in the number of negative AS values (from day -2 to day -1). Substantial abnormal deviations of sentiment values from the normal performance are observed from the event day 0 until 5 days afterwards. The most negative value of AS is observed on the event day at which the incident became public. Additionally, from day -1 to day 0 we observe an increase of 14% of negative AS values, which provides further evidence of the sensitiveness of social media users against data breach disclosures. *t*-test results on mean AS and Wilcoxon test results on median AS computed from day 0 to day 4, indicate strong statistical significance of the results at least at the 95% confidence level. On the last day of the event window, the results still remain significant despite the recovery of the downward trend of mean AS (median AS) values. In summary, we accept the validity of the alternative

hypothesis H_1 and reject the null hypothesis H_0.

Table B-11 summarizes CAAS values computed for each day of the event window. We observe that there is no negative sign of CAS in day -1, opposite to mean AS. The highest statistical significance at the 99% confidence level is achieved on days 1, 2, 3, 4, 5. Mean (median) CAS on the event date exhibit a lower significance of 90% (95%). These outcomes provide further evidence for the disapproval of the null hypothesis in favor of the alternative hypothesis. Hence, the abnormal sentiment is triggered by the security breach disclosure and is not simply attributable to pure chance.

Table B-11: Statistical test results on CAAS between day (-3) and day (+5)

	Parametric test		**Nonparametric test**	
Day	Mean CAS (% neg. CAS)	*t*-statistic (*p*-value)	Median CAS	*W*-statistic (*p*-value)
-3	0.029 (43)	1.184 (0.877)	0.019	278 (0.825)
-2	0.046 (43)	1.151 (0.870)	0.008	268 (0.768)
-1	0.042 (50)	0.865 (0.803)	0.004	261 (0.722)
0	-0.136 (63)	-1.824 (0.039**)	-0.170	147 (0.040**)
+1	-0.288 (67)	-2.654 (0.006***)	-0.306	118 (0.009***)
+2	-0.384 (63)	-2.736 (0.005***)	-0.281	122 (0.011**)
+3	-0.507 (67)	-3.002 (0.003***)	-0.511	110 (0.005***)
+4	-0.590 (63)	-3.092 (0.002***)	-0.592	107 (0.004***)
+5	-0.656 (67)	-2.984 (0.003***)	-0.544	105 (0.004***)

$^{*}p < 10\%$, $^{**}p < 5\%$, $^{***}p < 1\%$ (one-tailed test)

Figure B-5 depicts the behavior of the two variables, mean AS and mean CAS on each day of the event window. Data breaches reflect negatively on the reputational status of the involved firms, as evidenced by the sharp drop at the event date exhibited from both AAS (light-coloured line) and CAAS values (dark-coloured line).

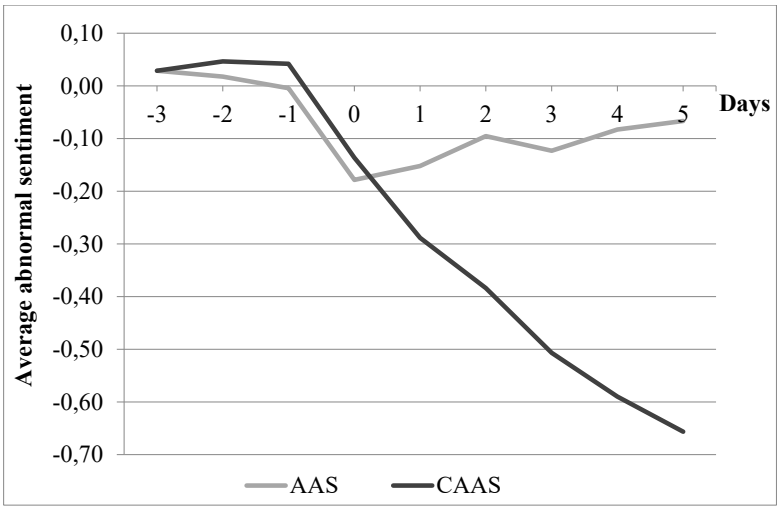

Figure B-5: AAS and CAAS values three days prior to the data breach disclosure and five days afterwards, including the event date [event window (-3;5)]

1.6 Discussion and Contributions

We observe statistically significant negative average abnormal sentiment (AAS) and cumulative abnormal sentiment (CAAS) following the public disclosure of data breaches until five days afterwards, which clearly show that such events effectively damage corporate reputation. The results do not reveal evidence of significant negative abnormal sentiment (cumulative abnormal sentiment) during the pre-event days, which indicates the absence of information leakage related to the breach incidents.

One major finding our study reveals is that the most negative values of AAS are observed immediately on the date of public disclosure of data breaches, meaning that the highest reputational losses occur when such events become of public domain. The figures evidence clearly how quickly the perception and the trust of individuals towards a company changes when their privacy sphere has been compromised. Such prompt reaction of the online community when data breaches are rendered public is however expectable due to the sensitive nature of the data type involved in data breaches. It is reasonable that people will lose trust and confidence on the involved firms as they blame them for such incidents and for not investing enough in information security (Andoh-Baidoo et al., 2010). On the one hand, the results implicate that privacy still remains a great concern for individuals, in spite of the frequent occurrence and coverage of data breaches in news media. On the other hand, organizations should adapt and apply appropriate security policies in order to prevent the future occurrence of such events.

Taking into account the processing of new information and the duration of the effect of data breaches in social media venues, the following observations can be made. With respect to users' behavior, similarly to the investors' reaction in the capital market scenario, stakeholders revise instantly the state of their beliefs, opinions, and evaluations based on the new flow of conveyed

information, as evidenced by the abnormal change in the sentiment polarity. Hence, social media seem to process information "efficiently", just as financial markets do under the condition of the efficient market hypothesis (EMH). In addition, reputational damage immediately observable from the public disclosure of data breaches indicates the vulnerability of this intangible asset under the influencing power of social media in the presence of negative events.

With focus on the duration of the data breach impact, the figures of AAS demonstrate significance from day 0 to day 5, implying that reputational damage caused by data breaches persists longer and is hence not entirely captured from the selected event window. This is a surprising finding since classic event studies have shown that asset prices typically reflect new information related to data breach announcements within a few days around the event date (Acquisti et al., 2006; Goel and Shawky, 2009). Therefore, the results signalize that differences exist between investors' and social media users' behavior when considering the persistence of such reactions in time. Capital market reaction due to data breach announcements is observable in the short term within few days after the incident. Reputational harm is immediately observable in the aftermath of the event but unlike financial market reaction, lasts for a longer period of time. Hence, it would be interesting to observe and analyze the trend of reputational effects for a longer event window in order to obtain deeper insights on reputational effects in the long-term. This is of critical relevance to businesses, which have to respond to reputational damage with appropriate strategies in the long run.

With the findings of this study we contribute to the existent literature on the impact of information security incidents and raise new theoretical issues not tackled from previous research. Over the last decade, a body of IS literature has supplied empirical evidence of the financial implications of data breach incidents. Financial losses cover though one single aspect of the repercussions of such occurrences, which further encompass loss of trust and reputational tarnish. We contribute to this lack of knowledge with empirical results related to the intangible effects of data breaches and demonstrate thereby how data breach announcements damage firm reputation based on social media content and provide additional insights on the economic aspects of such incidents.

From a methodological perspective we provide a new approach stemming from the integration of sentiment analysis in the classical event study methodology. With the classical event study approach it is possible to quantify the change in the market value of firms involved in data breach incidents and measure therefore the financial impact triggered by such events on listed companies. With the sentiment-based event study, we provide instead a robust approach to measure the intangible effect of data breaches, such as reputational damage, and consequently contribute to the literature stream of corporate reputation. In addition, measurement approaches for the construct of corporate reputation proposed in the literature are mainly of qualitative nature and build upon large-scale survey studies, which are costly and require a long preparation time (Benthaus et al., 2013). A clear advantage of our approach derives from the adoption of social media data to quantify corporate reputation, which entails valuable information that differs

substantially from survey-based reputation measures.

The results emerged from this study have practical relevance for practitioners and businesses as well. As corporate reputation in the social web era is a primary concern for every operating business, we provide evidence of the devastating effect of social media on corporate reputation when data breach incidents become known to the public. Hence, the insights of our study can help businesses to increase awareness on the risks social media can pose to corporate reputation in case of a negative scenario, and also, to promptly respond with the necessary strategic measures in order to protect their intangible assets. More generally, measuring social media sentiment on a continuous basis is a helpful instrument for businesses to monitor fluctuations of corporate reputation on real time. Hence, firms can exploit the variety of social media outlets to gain competitive advantage and online visibility in order to positively influence the overall online users' opinion and corporate reputation, too.

1.7 Limitations and Future Research

In spite of the theoretical and practical contributions, this study it is not exonerated from shortcomings and limitations. One limitation is the relative small sample size, mainly due to the fact that we are analyzing massive amounts of social media data, whose collection and preparation requires considerable efforts and a long processing time. Nevertheless, several studies on information security breaches are based on small samples too (e.g. Hovav and D'Arcy (2003) used 23 events while Ko and Dorantes (2006) used in their study 19 events).

Furthermore, the choice of a short event window comprising three days before the event date and only five days afterwards, hinders the observation and interpretation of reputational effects in the long term. A longer event window would contain a higher number of confounding events, whose esclusion would lead to a sample size of less than thirty data breaches, which would strongly influence the reliability of the statistical test results (Brown and Warner, 1980). We aim though to address this limitation in our future research.

Collecting social media data based on a keyword search leads to the entity recognition problem, in the sense that we cannot control if the posting content is effectively directed to the specific firm or it has been simply mentioned by users in relation to another context. In addition, with regard to sentiment analysis the sentiment of words or sentences could be erronously classified as positive or negative, although the overall tone might be sarcastic, ironic or even without sentiment. These are some of the general problems when dealing with sentiment analysis techniques (Liu, 2012), which represent also a limitation of this study.

The findings of this study, although encouraging, constitute only the first step towards the investigation of the reputational impact and in general of the intangible effects of information security incidents, where further research is needed. Our goal is to extend this study by conducting a joint analysis of the classic- and sentiment event study with a larger data set and a longer event

window. The contemporaneous analysis of the stock market, as well as of the social media reaction of data breaches, will provide a deeper understanding of the dynamics and the rationale behind opinion formation and investor behavior from a theoretical standpoint.

2 Do Data Breaches Affect our Beliefs? - Investigating Reputation Risk in Social Media

(The full-text of this study has been omitted due to copyright)

Table B-12: Fact sheet of Study 4

Title	Do Data Breaches Affect our Beliefs? - Investigating Reputation Risk in Social Media
Authors	Griselda Sinanaj, griselda.sinanaj@wiwi.uni-goettingen.de* (Corresponding author) Frederick Beyer *University of Göttingen, Göttingen, Germany
Outlet	Journal of Information System Security (JISSec 2017), Volume 13, Issue 2, 97–116, Completed Research Paper
Abstract	Data and privacy breaches have turned into a constant threat for every organization and continue to increase from year to year. In research and practice, one of the fundamental problems regarding data breach incidents is the limited knowledge on their economic and organizational consequences. Several studies have shown that firms having experienced data breach events suffer substantial losses in their market value. Data breaches can also damage corporate reputation, yet this aspect is still understudied and the empirical evidence not sufficient. To fill this knowledge gap, this study investigates the impact of data breaches on social media with the scope of measuring the repercussion on reputation. As hypothesized, data breaches have an adverse impact on corporate reputation. Furthermore, we found that the impact of data breaches on reputation depends on the news media exposure of the breach incident and on the breach history of each firm. Specifically, data breach events announced through news media cause a stronger negative impact on reputation than data breach incidents not publicized in news media. In addition, companies which have already experienced in the past data breach events suffer greater reputational losses than firms who experience for the first time a data breach incident.
Keywords	Data breaches, corporate reputation, social media, drivers, sentiment analysis

IV Comparative Analysis between the Impact on Investor Confidence and on Corporate Reputation

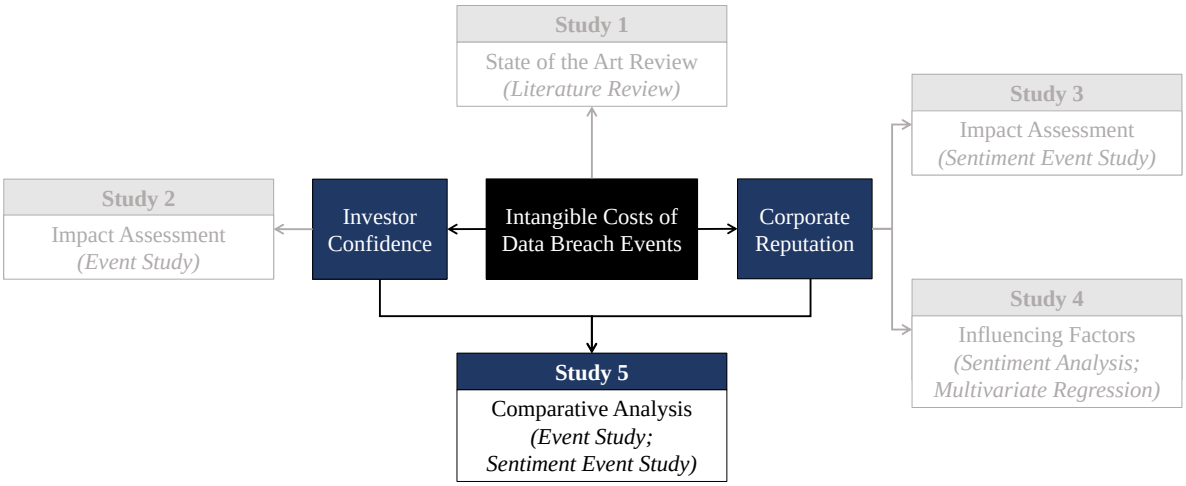

Figure B-6: Part of the research framework addressed by Study 5

1 Who Wins in a Data Breach? - A Comparative Study on the Intangible Costs of Data Breach Incidents

Table B-13: Fact sheet of Study 5

Title	Who Wins in a Data Breach? - A Comparative Study on the Intangible Costs of Data Breach Incidents
Authors	Griselda Sinanaj, griselda.sinanaj@wiwi.uni-goettingen.de* (Corresponding author) Humayun Zafar, hzafar@kennesaw.edu** *University of Göttingen, Göttingen, Germany **Kennesaw State University, Kennesaw, USA
Outlet	Proceedings of the 20th Pacific Asia Conference on Information Systems (PACIS 2016), Completed Research Paper
Abstract	Over the years data breaches have become a status quo due to an attacker's repeated ability to successfully infiltrate networks. 2015 was no stranger to these cases. Victims included millions of customers of Anthem, BlueCross BlueShield, Experian/T-Mobile, and Office of Personnel Management, all of whom lost confidential data. Needless to say, data breaches have a significant impact on the financial performance and reputation of firms. Collectively, the majority of the previous security studies on breach announcements have used event study methodology. These studies have focused on the change in market value of the company within a few days of the security breach announcements and concluded that there is a negative impact. But what is the impact of negative publicity due to a data breach on an organization's reputation? How should that be gauged? In this study we compare the financial impact with the reputational damage of data breaches. We performed two event studies: an event study on stock prices and additionally a sentiment event study applied on social media data. In contrast to previous research, shareholders do not react negatively to data breach announcements, whereas the impact on reputation is statistically significant as negative.
Keywords	Data breaches, corporate reputation, event study, sentiment analysis

1.1 Introduction

Data breaches, which involve the loss or theft of personally identifiable information (Romanosky et al., 2011, p. 256), are crisis events that interrupt the normal progress of daily business activities (Gupta and Ranganathan, 2007) and might be very costly for the affected organizations (Ko and Dorantes, 2006). Companies having experienced data breach incidents may incur in either tangible costs, such as decreased earnings (Xu et al., 2008) or intangible costs, such as loss of consumer trust (Nofer et al., 2014), loss of productivity and reputation damage (Yayla and Hu, 2011). In the last decade, a large body of research in the information security literature has investigated the intangible impact of security breaches, in particular the impact of data breach events on investors' confidence and shareholder wealth (e.g. Acquisti et al., 2006; Campbell et al., 2003; Gatzlaff and McCullough, 2010; Hinz et al., 2015; Morse et al., 2011). Despite the economic and strategic relevance of corporate reputation (Fombrun and Van Riel, 1997) and the reputational risks which arise in crisis situations (Dean, 2004), scholars have devoted little attention to the investigation of the impact that data breaches have on reputation.

For the scope of this research, reputation is defined as "the overall opinion about a firm by customers, investors, employees and the general public" (Colleoni et al., 2011, p. 4). A favourable reputation is a valuable economic asset that generates positive outcomes in terms of competitive advantage and business continuity (Fombrun and Van Riel, 1997). Data breaches might have an adverse impact on corporate reputation because of the negative publicity in the news media (Dean, 2004) and the transfer of negative information from traditional news media to social media, contributing to the creation of negative word-of-mouth (Coombs, 2007). Crisis events draw the attention of a large number of users on social media platforms, who actively engage in online communities to discuss and express their own opinion on the event (Jin et al., 2011). Information related to crisis events posted in the social media has the power to negatively influence perceptions and judgements on a company and thus on its reputation because it is considered by users as a trustworthy information source (Colleoni et al., 2011). As little efforts have been devoted to the reputational impact of data breaches, we argue that more research is needed to better understand the longevity and severity of reputational effects, which is necessary to develop effective crisis management strategies.

In this study we performed a comparative analysis between the reputational effect of data breaches and the impact on shareholder value. First, we measured the impact of data breach events on shareholder value by using the event study approach. In a further step, to quantify the effect of data breach events on corporate reputation we applied the event study approach on social media data. To measure overall user mood, we calculated daily average sentiment in regard to the companies in the sample and then similarly to the classic event study approach, we calculated abnormal sentiment values (and cumulative abnormal sentiment) to measure the impact on reputation. The results were surprising. Cumulative abnormal returns are not statistically

significant over the entire event window. The opposite holds for cumulative abnormal sentiment values, which are statistically significant, meaning that data breach events have a negative impact on corporate reputation. Contrary to what previous empirical studies have reported, in actuality shareholders do not react to the announcement of data breach events and completely ignore them. While the judgements and the evaluations of investors on the future economic performance of the companies seem not to be affected from data breach incidents, the overall judgement of users seems to suffer from data breach announcements. From a theoretical perspective, our results contradict previous literature, which has consistently reported a significant negative impact of data breach incidents on the stock market. Since the literature is overwhelmed with studies measuring the impact of data and security breach events on the capital market, research efforts should be focused on other important intangible effects, such as corporate reputation. Only through a deep understanding of the effects and consequences of data breach events, companies can develop optimal crisis response strategies with the scope of mitigating reputational losses.

The remainder of the paper is organized as follows. In section 2 we describe the efficient market hypothesis theory and develop the research hypotheses, after having described the relevant literature. In section 3 we describe the sample selection process for both event studies. Section 4 presents the methodological approach. Hereby we used the event study method to measure the effect of data breaches on stock prices and the event study combined with the sentiment analysis to measure corporate reputation. The results are presented and discussed in section 5. The study concludes with a summary of the findings and offers suggestions and recommendations for future research opportunities.

1.2 Theoretical Background

In this section we describe the relevant literature pertaining to the research objectives and develop the research hypotheses. We first describe the efficient market hypothesis, the theoretical fundament of the event study methodology. In addition, we analyse the body of research investigating the relation between security breach incidents and capital market reaction and derive the first hypothesis. Finally, we describe the theoretical link between the concept of reputation, social media and security breaches, in this study and generally named as crisis events, and derive the second hypothesis.

1.2.1 Efficient Market Hypothesis (EMH)

This study investigates the impact of data breaches on corporate reputation and on market value. Hereinto we performed two event studies: a classical event study on stock prices and additionally, a sentiment event study applied on social media data. The theoretical basis of the event study method is EMH, considered to be one of the most influential financial theories in modern finance. The theory, developed by Fama in 1969, is built upon the assumption of investor's rationality and postulates that markets are efficient when they fully and quickly reflect

all the available information. Market efficiency assumes three different forms, depending on the type of information incorporated in the stock prices: (i) markets are efficient in the weak-form if stock prices reflect only the information concerning past historical returns; (ii) in the semi-strong form, prices reflect not only information on past returns but also publicly available information to all market participants. Public information is defined as relevant information for stock prices movements, such as dividend announcements, stock splits, earnings announcements, mergers and acquisitions etc.; (iii) strong-form, i.e. stock prices fully incorporate three sets of information: information on past prices, public information and private information. EMH goes hand in hand with the Random Theory, which states that future prices follow a random walk and are therefore not predictable (Malkiel and Fama, 1970, p. 383).

EMH, which has been embraced for several decades by economists to explain the behaviour of financial markets, has been heavily criticized in the last decades by behavioural economists. Behavioural finance, which focuses on the psychological and sociological aspects of finance, challenges the theoretical foundations of the EMH and provides empirical evidence that markets are inefficient (Shleifer, 2000). Anomalies and deviations from the EMH and market efficiency have been documented in several studies (e.g. Bondt and Thaler, 1985). In an attempt to overcome the limitations of the EMH, Lo developed the "Adapted Market Hypothesis", a concept which binds together the classical form of the EMH with concepts of behavioural finance and psychology (Lo, 2004). Financial markets are not static environments, but they are rather described as dynamic ecological systems subject to continuous changes in the course of time. The author applies concepts borrowed from the discipline of evolutionary biology to explain market efficiency: competition, adaptation and natural selection. As markets evolve, the combination and the interaction of the aforementioned forces dictate the degree of efficiency the market can achieve (Lo, 2005). This framework offers thus a common solution for both opponents and supporters of the EMH.

1.2.2 Intangible Costs of Security Breaches

1.2.2.a Impact of Data Breach Announcements on Shareholder Value

Security breach incidents are problematic because they might expose the affected organizations to a long list of added costs. These costs might be tangible or intangible (reputational damage, loss of consumer trust, loss of market value) and might arise either short after the event announcement or months later (Ko and Dorantes, 2006). Economics of information security is the research stream within the information security literature investigating the economic consequences of security breach incidents at the organizational level (Camp and Lewis, 2006). In particular, the quantification of the intangible costs represents the biggest challenge for researchers as these costs are difficult to quantify (Cavusoglu et al., 2004b). Most of the existing research on information security breaches has focused on the empirical investigation of the financial impact of these events. Hereby scholars applied the event study method to determine if these events will

be negatively perceived by investors and will cause negative abnormal returns. This body of research has delivered mixed results. Table B-14 offers a summary of the most relevant studies, which we classified in two groups, based on the significance of the empirical results. As can be seen from Table B-14, the majority of the studies have shown that security breaches are perceived negatively by investors and have an adverse effect on firms' stock prices. Additionally, while security breaches, which entail the whole spectrum of security incidents and not solely data breaches are not always associated with a pronounced negative reaction on the capital market, the effect of data breaches on stock prices is systematically negative and strongly significant. With regard to the type of breach, one part of the studies focuses on all types of security breaches, while others deal with one particular type of security breach. The studies of Acquisti et al. (2006); Gatzlaff and McCullough (2010); Hinz et al. (2015) measure the financial impact of data breach events, which imply the loss or theft of private sensitive information, whose improper use might lead to identity theft (Romanosky et al., 2011). All the studies report statistically significant negative cumulative abnormal returns around the event date.

Table B-14: Overview of studies investigating the impact of security breaches on stock prices

Author(s)	**Breach type**	**Event window**
Negative and statistically significant cumulative abnormal returns (CAR)		
(Acquisti et al., 2006)	Data breaches	(-1;+1)
(Campbell et al., 2003)	Confidential data	(-1;+1)
(Cavusoglu et al., 2004b)	Security breaches	(0;+1)
(Hinz et al., 2015)	Data theft	(0;+3)
(Gordon et al., 2011)	Security breaches	(-1;+1)
(Gatzlaff and McCullough, 2010)	Data breaches	(-1;0) (0;+39)
(Pirounias et al., 2014)	Data breaches	(0;0)
(Yayla and Hu, 2011)	Security breaches	(-1;+1) (-1;+10)
Cumulative abnormal returns (CAR) not significant		
(Hovav and D'Arcy, 2003)	Denial-of-Service attacks	
(Hovav and D'Arcy, 2004)	Computer virus	
(Kannan et al., 2007)	Security breaches	

The second part of the table presents the studies that do not report a significant effect of security breach incidents on shareholder value. Hovav and D'Arcy (2003) and Hovav and D'Arcy (2004), who investigated the financial impact of computer viruses and DOS attacks, found that these events have a light negative effect on stock prices which isn't statistically significant. Unlike data breaches, computer viruses and DOS attacks do not involve the breach of personal private information, such as customer or employee data. While computer viruses might damage either

information integrity or information availability, DOS attacks, e.g. shutdown of a website, are described as availability breaches, as they impede users to access the desired information (Gordon et al., 2011).

In line with previous research (Acquisti et al., 2006; Gatzlaff and McCullough, 2010; Hinz et al., 2015), this study also investigates the impact of data breach incidents on shareholder value. While the majority of the studies described above, with few exceptions, focus exclusively on companies traded at a U.S. stock exchange, we in our sample also included companies from different countries. Based on these theoretical considerations, we formulate the first research hypothesis as follows:

Hypothesis 1: The announcement of data breach events will be negatively reflected into the stock market and will cause negative abnormal returns.

1.2.2.b Impact of Data Breach Announcements on Corporate Reputation

A crisis "is a major occurrence with a potentially negative outcome affecting an organization, company, or industry, as well as publics, products, services or good name. A crisis interrupts normal business transactions and can sometimes threaten the existence of the organization" (Fearn-Banks, 2010, p. 2). Therefore crisis events indicate unexpected and sudden negative events, such as an earthquake, fire, explosion, security breach, natural disaster, which create an emergency situation that necessitates quick responses (Gupta and Ranganathan, 2007). Organizations fear crisis events because they might have an adverse impact both at the stakeholder and at the organizational level (Coombs, 2007). Crisis events might produce a wide range of negative economic consequences on the affected organizations: loss of sales, damage of corporate reputation and brand image and even threaten the existence of the company (Coombs, 2014). Once the data breach incident has been discovered, the affected companies take several actions to repair the compromised infrastructure, investigate the incident causes and identify the authors. These expenses imply tangible costs, whereas reputation damage, loss of consumer trust and loss of shareholder wealth are known as intangible costs (Cavusoglu, 2002; Kannan et al., 2007).

Because crisis events have the potential to damage the asset of reputation (Coombs, 2007), the study of the impact of crisis events on organizational reputation has received significant attention among communication research scholars (Cooley and Cooley, 2011). The amount of reputational damage caused by crisis situations depends to a large extent on the post-crisis response strategy that the affected companies take. As there is no general consensus or a specific guideline to define the optimal response strategy, scholars develop new theories to cover this theoretical gap (Coombs and Holladay, 2002). With this regard, Situational Crisis Communication Theory (SCCT) was developed to contribute to this knowledge gap and represents one of the leading theories in crisis communication research. Attribution of responsibility, i.e. the level of responsibility the public appoints to the organization for the crisis event is the key variable of SCCT and is directly related to reputational threat. According to SCCT, intentional crisis events are associated with higher

levels of responsibility and lead to a stronger negative impact on reputation. Unintentional crisis events are in contrast due to external factors and are characterized by a lower level of crisis responsibility and thus have a milder impact on reputation. SCCT posits that crisis response plans should take into account three factors: type of crisis event, level of crisis responsibility and reputational damage (Coombs, 2007; Coombs and Holladay, 2002).

The measurement of corporate reputation has for many years been object of study among reputation scholars (Rindova et al., 2005; Wartick, 2002). Different reputation measurement approaches are available in the literature, such as reputation surveys, the Reputation Quotient (Fombrun et al., 2000), RepTrak™ Pulse (Ponzi et al., 2011) etc. America's Most Admired Companies index (AMAC), for the first time released in 1984 by *Fortune*, is the first and at the same time the most popular reputation measure in research (Sarstedt et al., 2013). With the advent and rapid diffusion of social media, more research efforts have been invested on corporate reputation measurement. The goal is to develop novel measurement approaches that overcome the drawbacks of the traditional existent approaches (Colleoni et al., 2011).

In recent years researchers have proposed new reputation measures derived from social media content. The study of Benthaus et al. (2013) is one of the first to propose a novel reputation measure which resumes the opinions and judgements of social media users. Reputation measures developed from social media content have several advantages over traditional survey-based approaches. Surveys built upon the opinions and knowledge of managers and financial analysts, whereas social media sentiment reflects public's opinion. In addition, social media-based reputation measures can be calculated within a short time, in contrast to reputation surveys (Benthaus et al., 2013).

The investigation of the reputational effect of data breach incidents has received little attention in research. In the context of data breach incidents, the study of Sinanaj et al. (2015b) applies a sentiment based event study to measure the reputational impact of data breaches. The metric used to quantify reputation is abnormal sentiment, i.e. the difference between actual sentiment and expected sentiment. In line with the study of Sinanaj et al. (2015b), we also applied a sentiment based event study.

To summarize, given the variety of reputation measures the biggest challenge for reputation scholars in the future will be the development of a widely accepted reputation measure that best captures the multidimensional character of reputation and overcomes the limitations of the traditional measurement approaches. Based on this theoretical background, we derive the second research hypothesis:

Hypothesis 2: Data breach events are perceived negatively by social media users and have a negative impact on corporate reputation.

1.3 Sample Selection and Data

In this paper we performed two analyses: first, we analysed the impact of data breaches on capital market based on the event study method. Furthermore, we conducted a sentiment event study on social media data. To determine the final samples for both analyses we applied several selection criteria: common selection criteria and specific criteria to each approach. We collected data breach incidents through the global database datalossdb.org, which offers a chronological history of data breach events occurred worldwide. The website of datalossdb.org is curated by volunteers, who constantly enlarge the database by inserting the latest data breach events announced through traditional media outlets. For each data breach listed in the database, the following information is given: date of event, name of organization(s), location, source of breach (inside accidental, inside malicious, outside, unknown), breach type (hack, stolen laptop, fraud-se, lost tape, missing media and unknown) as well as news media reports. Several information security studies have used datalossdb.org to investigate the economic impact of security breach incidents (Hinz et al., 2015; Morse et al., 2011; Pirounias et al., 2014).

The initial sample of data breaches comprised events occurred between 1.11.2011 and 31.12.2013. Because of the classical event study method, we selected only publicly traded companies and accordingly removed GOs, education institutions and non-profit organizations. The next criteria regards loss size. We focused on breaches having affected a large number of customers (number of ID's lost/stolen at least 10.000) as for these events it is reasonable to expect a relevant economic impact, in contrast to less relevant incidents. When performing the event study it is essential to remove from the sample the events having experienced other business events i.e. confounding events (e.g. departure of directors, dividend announcements etc.) over the event window (-1;+10). By doing so, we are able to isolate the net effect of the breach events both on capital market and social media. Next we apply specific criteria for the classical event study and the social media event study. The requisite for the adapted event study is social media data availability for all the companies in the sample over the estimation- and event window, i.e. over the window (-44;+10). The source of social media data is SDL-SM2, a proprietary social media monitoring software, which provides historical social media data for businesses from different social media platforms such as microblogs, social networks and blogs. For the classical event study approach we considered only listed firms during the estimation- and the event window. Table B-15 reports the selection criteria for both cases.

At this point it is important to highlight and explain the differences in the sample sizes between the sentiment event study on social media data and the classic event study. As can be seen from Table B-15, the number of confounding events in the two samples is different, despite identical event windows. This effect is due to the different data type and data availability at the basis of each approach. Stock prices are structured data available on working days only, while social media data are unstructured data available on a daily basis, including official holidays and

weekends. This leads to a shift effect within the event window, which at the same time affects the number of confounding events to be eliminated and the sample size too. In sum, the classical event study method was applied on a sample of 28 data breach events, while social media based - event study was applied on a sample of 31 events.

Table B-15: Sample selection criteria

Criteria	**Event study # events left**	**Sentiment event study # events left**
Initial sample	2266	2266
Listed firms	285	285
Loss size	56	56
Social media data	-	46
Stock prices data	50	-
Confounding events	28	31

1.4 Methodology

Event studies allow researchers to investigate the impact of corporate announcements on stock prices. The metric that quantifies the event impact on stock prices is the abnormal return, calculated as the difference between actual returns and normal returns (Binder, 1998). Event studies have been applied not only to investigate the impact of business events on stock prices but also on trading volume. In this paper we conducted two event studies: first, a classic event study on stock returns data to analyse the financial impact of data breaches; second, an event study on social media sentiment data to measure data breaches impact on corporate reputation. In the classic event study we used daily stock returns, while in the adapted event study approach the variable of interest is daily sentiment, which resumes the overall users' opinions and evaluations on a particular company.

The event study requires the specification of the following criteria: (i) length of estimation window, (ii) length of event window and (iii) model choice for normal returns (Campbell et al., 1997). We chose a 43 day-long estimation window, starting 44 days prior to the event until two days before the event date. Studies on the cost of data breaches typically use longer estimation windows comprising at least 100 trading days (Yayla and Hu, 2011). The relatively short estimation window is due to reasons related to the collection and preparation of social media data for the sentiment event study. The event study has been conducted both on daily stock prices and daily sentiment data. While financial data are structured and easily retrievable, the process of collection and analysis of social media data presents a higher degree of difficulty. The event window comprises 12 days, starting one day before the event date until day 10 afterwards, while t_0 indicates the event date.

We used sentiment analysis to determine daily sentiment polarity values over the estimation and event window. Sentiment analysis or *opinion mining* implies procedures and approaches to analyse and quantify opinions, judgements, evaluations and emotions of people (Pang and Lee, 2008). In this paper we applied a dictionary-based approach to determine the sentiment for each social media posting by using the General Inquirer software (Stone et al., 1966). To measure the polarity of each document, we used two word lists from General Inquirer, positive and negative. The polarity is calculated with the following formula as in the study of Sinanaj et al. (2015b),

$$\text{sentiment polarity} = \frac{\text{n}_{\text{pos}} - \text{n}_{\text{neg}}}{\text{n}_{\text{pos}} + \text{n}_{\text{neg}}}$$

where n_{pos} indicates the number of positive words and n_{neg} the number of negative words. In contrast to the study of Sinanaj et al. (2015b) that uses absolute sentiment values, we calculated the daily change of sentiment values. To ensure consistency between the two event studies, we calculated daily polarity changes (%) for each event, between two consecutive days, in a similar way as the calculation of stock price returns:

$$\text{sentiment polarity } (\%) = \frac{\text{polarity}_{\text{t}} - \text{polarity}_{\text{t-1}}}{\text{polarity}_{\text{t-1}}} * 100\%$$

In both event studies, expected returns and expected sentiment are calculated with the constant-mean return model, which assumes a constant average return (average sentiment) over the estimation window. Abnormal returns measure the effect of data breaches on stock prices and are calculated as the difference between actual returns and expected returns (Campbell et al., 1997):

$$\text{ar}_{\text{it}} = \text{r}_{\text{it}} - \text{E}(\text{r}_{\text{it}})$$

Abnormal sentiment expresses the difference between actual sentiment and expected sentiment and is calculated in the following way (Sinanaj et al., 2015b):

$$\text{as}_{\text{it}} = \text{s}_{\text{it}} - \text{E}(\text{s}_{\text{it}})$$

Since we are using the constant-mean return model to calculate expected returns, the expected returns for a company i are constant (Campbell et al., 1997):

$$\text{ar}_{\text{it}} = \text{r}_{\text{it}} - \mu$$

Similarly, the average sentiment is calculated as follows (Sinanaj et al., 2015b):

$$\text{as}_{\text{it}} = \text{s}_{\text{it}} - \mu$$

To aggregate abnormal returns for a company i over t days of the event window, the following formula is used (Campbell et al., 1997):

$$\text{car}_{\text{it}} = \sum_{\text{t=1}}^{\text{N}} \text{ar}_{\text{it}}$$

Similarly, cumulative abnormal sentiment is obtained by aggregating sentiment values over the event window (Sinanaj et al., 2015b):

$$\text{cas}_{\text{it}} = \sum_{\text{t=1}}^{\text{N}} \text{as}_{\text{it}}$$

The statistical significance of cumulative abnormal sentiment values (CAS) was tested with both parametric and non-parametric tests. Parametric procedures can be applied on large sample sizes (> 30) without a prior testing of the normality assumption, since the sampling distribution tends to be normal. Both tests generated similar results in terms of statistical significance. With respect to CAR values, the normality assumption does not hold due to the small sample size (< 30) and the normality of the data should be tested before applying the tests. Both normality tests applied on CAR, Shapiro-Wilk and Kolmogorov-Smirnov show that the data does not follow a normal distribution. Wilcoxon signed-rank test was used to test the statistical significance of CAR values.

1.5 Results and Discussion

In this section we present the empirical results and discuss the theoretical and practical implications.

Impact of Data Breaches on Shareholder Value

The results of the event study on stock prices are presented in Table B-16. Due to the small sample size (< 30), we tested the statistical significance of CAR with a non-parametric test, the Wilcoxon signed-rank test. Abnormal returns assume negative values only on day -1 and day 0, yet not statistically significant. Overall data breaches do not have a significant impact on shareholder value.

Table B-16: Cumulative abnormal returns over the event window (-1;+10)

Day	**Median CAR (%)**	***W*-statistic (p-value)**
-1	-0.06	218 (0.636)
0	-0.30	196 (0.442)
+1	0.22	233 (0.753)
+2	0.82	247 (0.842)
+3	0.82	258 (0.895)
+4	0.30	249 (0.853)
+5	0.88	258 (0.895)
+6	1.31	276 (0.953)
+7	2.25	281 (0.963)
+8	1.46	278 (0.957)
+9	2.21	264 (0.918)
+10	1.70	258 (0.895)

Impact of Data Breaches on Corporate Reputation

To quantify the impact of the security breach events on social media and corporate reputation, we calculated cumulative abnormal sentiment values over the event window (-1;+10), which are summarized in Table B-17. Negative values of CAS denote the reputational damage of the data breach events on the affected organizations. As shown in Table B-17, CAS assume negative and statistically significant values over the event window (-1;+3), clearly showing the negative effect of such events on social media and corporate reputation. According to our definition, corporate reputation is represented by the way a specific company is perceived by the on-line community, engaged in the creation and exchange of content with regard to a specific company. The day prior to the event has been included in the event window in order to capture a possible anticipated effect of the data breaches on social media, typically due to a leak of information prior to the official announcement. Mean and median CAS on the days preceding the event announcement are negative and statistically significant at the 5% significance level. According to these results, there is an information leakage effect of data breaches on social media. On the event date, both mean CAS and median CAS are statistically significant at the 5% significance level, clearly showing that data breaches are negatively perceived by users and heavily discussed on social media, leading to a negative impact on corporate reputation. This effect persists until day +3 of the event window. Both parametric and non-parametric tests report consistent results in terms of statistical significance with exception of day +3. Based on the results displayed in Table B-17, we can reject $H2_0 : \mu_{CAS} \geq 0$ in favour of $H2_1 : \mu_{CAS} < 0$, which asserts that data breaches tarnish corporate reputation.

Table B-17: Cumulative abnormal sentiment values over the event window (-1;+10)

	Parametric test		**Nonparametric test**	
Day/Window	**Mean CAS (%)**	**t-statistic (p-value)**	**Median CAS** (%)	**W-statistic (p-value)**
-1	-12.86	-1.713 (0.048**)	-10.34	149 (0.026**)
0	-57.14	-2.203 (0.018**)	-16.92	133 (0.012**)
+1	-93.77	-2.271 (0.015**)	-34.05	118 (0.005***)
+2	-75.37	-1.434 (0.081*)	-4.56	174 (0.076*)
+3	-106.92	-1.012 (0.160)	-11.99	162 (0.047**)
+4	-82.93	-0.743 (0.232)	-1.49	229 (0.360)
+5	-113.63	-0.980 (0.167)	-7.41	198 (0.168)
+6	-111.23	-0.874 (0.194)	3.65	232 (0.382)
+7	-106.03	-0.853 (0.200)	8.12	229 (0.360)
+8	-107.11	-0.835 (0.205)	-6.11	219 (0.291)
+9	-77.83	-0.641 (0.263)	-12.18	205 (0.205)
+10	-84.50	-0.680 (0.251)	-3.87	222 (0.311)
(0;+1)	-80.91	-2.226 (0.017**)	-27.90	121 (0.006***)
(0;+3)	-94.06	-0.900 (0.188)	-11.83	163 (0.049**)
(0;+5)	-100.78	-0.881 (0.193)	-16.09	199 (0.173)
(0;+10)	-71.64	-0.585 (0.282)	-17.26	213 (0.252)

$^{*}p < 10\%$, $^{**}p < 5\%$, $^{***}p < 1\%$ (one-tailed test)

While the impact on social media and corporate reputation is immediate, and statistically significant over the event window (-1;+3), quite the opposite holds for the impact on capital markets. Despite the fact that in this sample we included relevant data breaches with a number of records greater than 10.000, the breach size criteria does not correlate with the reaction on the capital market. In contrast to social media users, who are very sensitive to the disclosure of data breach incidents, investors on the other hand seem to ignore them. The lack of a significant impact of data breach announcements on the stock market has been also reported in the news media. Two massive data breach incidents which affected Ebay Inc. in 2014 and Target Corporation in 2013 and having affected 145 million and 40 million customers respectively, despite the huge breach size and the intense media exposure, did not affect the stock prices during the trading day (Bloomberg, 2014).

The lack of a significant impact of data breach incidents on the stock market signals that data breach events are not perceived by the investors' community as crisis events. Particularly relevant data breaches having affected large companies, have been very often publicized in national and international news media and investors might have developed a certain grade of "*immunity*" towards data breach events over time. A plausible explanation for the investors' reaction towards data breach announcements might be the fact that these events nowadays do not represent a new phenomenon for companies to face. The more firms assemble and store large amounts of customer data to increase the number of customers and profits, the more increases the risk of data breach incidents and privacy violations (Institute for Information Security and Privacy (IISP), 2016). Companies are therefore aware of security risks and expect to experience data and security breach incidents in the future (PwC, 2015). The stock market does not penalize data breach events because investors consider them part of daily business activities (Manworren et al., 2016).

In contrast to investors' behaviour, data breach announcements are perceived by social media users as crisis events and generate negative sentiment, which in turn damages corporate reputation. While the stock market reaction is the result of the behaviour of a single category of stakeholders, social media sentiment reflects the average mood of different stakeholders, such as investors, consumers, potential customers and actual customers. Cyber-attacks and data breaches could be interpreted by the public as a sign of the inability of the companies to guarantee the safety and confidentiality of customer data. Data breach announcements damage corporate reputation because of the *negativity bias* effect (Ito et al., 1998, p. 887), implying the predominance of negative information over favourable information in terms of perceived relevance. Unconsciously, people discriminate between positive and negative information and sense non favourable information as more relevant than favourable information. Negative information has therefore a great influential power on shaping the perceptions, opinions and ideas of people (Ito et al., 1998). Data breach announcements create negative sentiment in the public which is also reflected on reputation.

From a research perspective, prior studies that have analysed the financial impact of data breach events report statistically significant negative cumulative abnormal returns around the event date, contrary to our results. With regard to the type of breach, investors and the stock market penalized in the past data breaches at a great extent and ignored other types of security breaches, such as DOS attacks (Hovav and D'Arcy, 2003) or availability breaches (Campbell et al., 2003). In addition, prior research provides evidence of a positive correlation between breach size and abnormal returns (Gatzlaff and McCullough, 2010). Other intangible costs caused by data breach incidents, such as damage of corporate reputation, have received little attention by researchers, despite of all the evident risks social media creates around reputation in crisis situations. Our study offers interesting insights on the intangible cost of data breaches and contributes to the information security literature. In summary, our findings should be understood by scholars as an opportunity to explore other facets related to the economic and financial impact of data breaches which have received little attention, despite their high relevance both in research and practise.

From a practical point of view, our results regarding corporate reputation point to the necessity of crisis management strategies in organizations. Data breach events have an adverse effect on corporate reputation and companies can leverage social media communication platforms to monitor the longevity and degree of reputation damage in the aftermath of crisis events. Companies do not have control on the information released in the news media and social media and cannot predict how the public and the stakeholders will react to such information. Furthermore, users' reaction in social media depends on if and to which extent consumers blame the company for the crisis event. It is essential to communicate and deliver a message to the customers affected by breach incidents and social media can be a very useful tool to achieve this goal.

1.6 Conclusions

In this paper we investigated the effect of data breach incidents on corporate reputation and on shareholder value based on the event study approach. The event study was applied on two types of data: on stock prices to measure abnormal returns and on social media data to quantify reputational changes. We found that data breach incidents do not have a significant effect on investors' community in contrast to prior research, which consistently reports negative and significant cumulative abnormal returns. Additionally, we found that data breaches are discussed with negative tones on social media and cause therefore reputation damage. Our results indicate that firms affected by data breach incidents should focus on the asset of reputation and design response plans with the goal of limiting reputational losses.

Our findings offer several directions for future research opportunities. Future research could explore the relationship between the reputation status prior to the crisis event and the impact on reputation post event based on the "*reservoir hypothesis*". According to this hypothesis, reputation, described as a "*reservoir of goodwill*" is a valuable resource during periods of crisis

because it has a protective function (Jones et al., 2000). Prior research provides evidence of the protective power of reputation in presence of crisis situations. Jones et al. (2000) show that the market crash in 1987 had a milder negative impact on the market value of firms with good reputation. Companies with a strong reputation before crisis events have a higher degree of immunity, thus suffer less reputational losses than companies with a less good reputation (Coombs, 2007).

In future research we aim to extend this study and additionally investigate the reputational impact of data breaches based on news media content. While traditional media and social media are both important information sources for a firm's stakeholders, there are substantial differences between the professional content of news media and user generated content in social media. Our objective is to measure the reputational effect of data breaches with two different media sources and uncover the differences between the two approaches.

C Contributions

This chapter illustrates the findings and the contributions of this dissertation thesis. The first section of the chapter C.I presents in detail the findings of each study in accordance with the research framework and the respective research questions. The theoretical, practical and policy implications inferred from the findings of each study are presented in section C.II. Finally, section C.III discusses the research limitations and concludes with insights and suggestions for future research avenues.

I Findings

1 Findings Regarding the State of the Art Literature Review

The research objective of **Study 1** is to identify the categories of intangible costs investigated in security research with particular focus on the theoretical foundations and methodological approaches. Following the recommendations of Webster and Watson (2002) for literature review studies, the selected research articles were synthesized on the basis of a concept-matrix comprising the following components: *intangible cost*, *breach type*, *theory* and *method*. Table C-1 provides basic information on **Study 1** including the title, the addressed research question and the applied research method.

Table C-1: Outline of Study 1

Title	The Intangible Cost of Information Security Breaches: A State of the Art Analysis
Research question	RQ 1: To what extent have the intangible costs of data breach events been addressed in the literature?
Research method	Structured literature review

With regard to the first element of the concept-matrix, *intangible cost*, three categories of intangible costs were identified through the review process: loss of investor confidence, loss of corporate reputation and loss of consumer trust. **Study 1** reveals that while certain types of intangible costs have received considerable attention in research, empirical evidence on the impact of other costs is still very limited. The loss of investor confidence, which refers to the consequences of data breach events on firm market value and shareholder wealth (Yayla and Hu, 2011, p. 62), is explored in the majority of the examined studies, thus evidencing a high concentration of research on this cost category. The low concentration of research on other categories of intangible costs, such as corporate reputation and consumer trust, signalizes a distinct research gap urging for more attention in future research. Methodological constraints are the rationale behind the uneven distribution of research efforts between the impact on investor confidence and the loss of corporate reputation. The effect of data breach announcements on investor confidence is gauged with the event study methodology approach (Spanos and Angelis, 2016), which captures abnormal changes in stock price behavior. The limited empirical evidence on other categories of intangible costs, such as corporate reputaton, is due to the lack of appropriate methodologies to quantify intangible concepts that are not directly observable.

Study 1 additionally reviews the theoretical lenses and the methodologies employed to explore the intangible costs of data breach events. The theory of stock market efficiency (Ball, 1995) (or the Efficient Market Hypothesis (Malkiel and Fama, 1970)), which is used to examine the impact on investor confidence and firm market value, is the most frequently cited theory and represents

the theoretical foundation of the majority of the examined studies. With regard to methods, the stream of research on the intangible costs of data breaches is dominated by the event study approach (MacKinlay, 1997), which is underpinned by the theory of stock market efficiency (Malkiel and Fama, 1970) and is used to measure the impact of data breaches on firm market value. The other four identified theories, theory of corporate social responsibility (McWilliams and Siegel, 2001), theory of planned behavior (Ajzen, 1985), prospect theory (Kahneman and Tversky, 1979) and the resource-based view (Wernerfelt, 1995), have been applied to a limited extent in the context of data breach events. The limited number of theories identified in **Study 1** points to a theoretical paucity in the line of research dealing with the intangible costs of data breach events. In this regard, the extension of the theoretical basis by adopting existing theories from various research disciplines may help scholars to better comprehend and explore the theoretical underpinnings of the intangible costs of data breach incidents.

2 Findings Regarding the Impact on Investor Confidence

Study 2 tackles the question of how the National Intelligence Agency (NSA)-related data breach events brought to the public's attention in 2013 affect investor confidence and firm market value. The empirical analysis builds upon a sample of data breaches collected through a careful analysis of media reports appeared in international news media sources such as *The Guardian*, *The Washington Post*, *The Wall Street Journal*, *The New York Times* and *Spiegel Online*. A succinct summary of **Study 2** including the title, the research question and the methodological approach is presented in Table C-2.

Table C-2: Outline of Study 2

Title	NSA Revelations of Privacy Breaches: Do Investors Care?
Research question	RQ 2: How do data breach events associated with the NSA revelations affect investor confidence?
Research method	Event study

In line with previous studies (Acquisti et al., 2006; Cavusoglu et al., 2004b; Pirounias et al., 2014), **Study 2** explores the impact of NSA data and privacy breaches on investor confidence and firm market value by applying the event study method under the assumption of efficient capital markets (Malkiel and Fama, 1970). While the short-term impact of data breach events on firm market value has been reported in various studies (Acquisti et al., 2006; Hinz et al., 2015; Kashmiri et al., 2017; Martin et al., 2017), the investigation of the impact of NSA data breach incidents has received little attention in literature. Prior security literature has predominantly focused on the technical, legal and ethical facets of such events (Landau, 2016), paying less attention to the financial and economic impact. By investigating the effect of NSA data breaches on investor confidence and firm market value, this study addresses a research gap and delivers

original insights on a unique data breach event not investigated in prior research.

Through the analysis of the cumulated average abnormal returns it is shown that the effect on the stock market is negative and statistically significant. This confirms the research hypothesis postulating a negative effect of the NSA data breach incidents on investor confidence and shareholder wealth. The negative effect of NSA data breach events is incorporated in the stock prices prior to the announcement in conventional news media channels, implying information leakage effects. Similar to other studies investigating the effect of data breach events on firm market value (Campbell et al., 2003; Hovav et al., 2017), the negative stock price reaction of NSA data breaches is a short-term effect as stock prices return to their previous level within a few days. The adverse reaction of investors to the announcement of NSA data breach events is quickly reflected in the stock prices and is visible over a period of two trading days.

3 Findings Regarding the Impact on Corporate Reputation

Study 1 contributes with a state of the art literature review on the intangible costs of data breach events and reveals a substantial lack of empirical evidence regarding the impact of data breach events on corporate reputation. The progress of information security research regarding the investigation of the intangible costs of data breach events is related to the researchers' ability to design cutting-edge methodological approaches for the challenging task of measuring the intangible concept of corporate reputation. **Study 3** tackles the issue of how data breach events affect corporate reputation and provides empirical evidence of the reputational impact of data breaches. An outline of **Study 3** is provided in Table C-3.

Table C-3: Outline of Study 3

Title	How Data Breaches Ruin Firm Reputation on Social Media! – Insights from a Sentiment-based Event Study
Research question	RQ 3a: How to assess the impact of data breach events on corporate reputation?
Research method	Sentiment-based event study

Study 3 makes two major contributions. First, it introduces the sentiment–based event study approach for the measurement of corporate reputation, making a methodological contribution relevant not solely for information security research but also for corporate reputation literature. While the main variable in the event study is represented by abnormal stock price returns (MacKinlay, 1997), the measure of reputation in the sentiment-based event study is the abnormal sentiment derived from social media data by means of sentiment analysis. Abnormal sentiment captures unusual deviations of current social media sentiment from the average normal sentiment calculated over a time period prior to the event announcement. Positive abnormal sentiment values indicate a positive effect of the event announcement on reputation, whereas negative

sentiment scores point to a damage of corporate reputation.

Negative abnormal sentiment values on the event date measured with the sentiment-based event study approach indicate a negative impact of data breaches on corporate reputation. This finding confirms the suppositions of information security scholars asserting an adverse impact of data breach announcements on corporate reputation (Goel and Shawky, 2009; Goldstein et al., 2011; Hovav and Gray, 2014). The empirical results suggest that a constant monitoring of social media sentiment and corporate reputation should be a major priority in companies involved in data breach incidents, especially in the wake of the incident disclosure. As reputational losses can undermine customers' trust and impair sales, revenues and future financial performance (Rindova et al., 2005), companies should be aware of the damaging effect of social media exposure on corporate reputation and should be constantly prepared to mitigate the resulting intangible costs. The impact of data breach events on reputation is negative and strongly significant not only on the event date but also in the following days, indicating an enduring effect. One plausible explanation for the persistence of negative sentiment over the event window is the publication of data breach related news in the days following the event date. Since data breach events affect individuals' sensitive information and compromise customers' identity (Romanosky et al., 2011), concerns of stakeholders and social media users are reflected in social media sentiment and corporate reputation scores.

Study 3 and **Study 4** focus both on the intangible cost of corporate reputation. **Study 3** contributes to the advancement of reputation measurement approaches and offers first insights on the extent of data breaches' impact on corporate reputation. **Study 4** takes a step further by examining the factors influencing the extent of reputation damage of data breach incidents through a multivariate regression model. The study examines the predicting power of four variables on corporate reputation: *news media exposure*, *breach history*, which is a theory-based variable derived from the Situational Crisis Communication Theory (Coombs, 2004), *prior reputation* which builds upon the "reservoir hypothesis" (Sánchez et al., 2012) and *firm size*, which is derived from the reputation literature (Fombrun and Shanley, 1990) and information security literature (Gatzlaff and McCullough, 2010). Table C-4 offers a brief summary of **Study 4**.

Table C-4: Outline of Study 4

Title	Do Data Breaches Affect our beliefs?- Investigating Reputation Risk in Social Media
Research question	RQ 3b: What are the influencing factors of the reputational impact of data breaches?
Research method	Sentiment analysis; multivariate regression

Two variables included in the cross-sectional regression model were found to be significant

predictors of corporate reputation: *news media exposure* and *breach history*. With regard to *news media exposure*, the study reveals that the extent of reputation damage is determined from the publicity of the breach event in conventional news media channels. Data breaches covered in traditional news media lead therefore to greater reputational losses than non-exposed breach incidents. Due to the role of traditional news media as a primary information source (Einwiller et al., 2010), the incident's exposure in social media is influenced from the news media coverage. Data breach information regarding the incident size, incident causes and the time gap between the incident discovery and customers' notification (Fowler, 2016) receives particular attention in traditional media and is highly discussed in social media. News media coverage of the breach event influences the building process of the opinions and evaluations of social media users and stakeholders and is reflected in corporate reputation values.

4 Findings Regarding the Comparison between the Impact on Investor Confidence and on Corporate Reputation

Study 5 adopts a comparative approach in order to detect differences in the extent of two categories of intangible costs: investor confidence and corporate reputation. The simultaneous assessment of the intangible effects of data breaches in **Study 5** identifies the most severe intangible costs and supports decision-making process of managers in response to data breach events. The data breach impact on investor confidence is assessed with the classic event study approach similarly to **Study 2**, whereas the reputational impact is measured with the sentiment-based event study approach similarly to **Study 3**. Table C-5 offers an overview of **Study 5**.

Table C-5: Outline of Study 5

Title	Who Wins in a Data Breach? - A Comparative Study on the Intangible Costs of Data Breach Incidents
Research question	RQ 4: What is the difference between the impact of data breach events on investor confidence and the impact on corporate reputation?
Research method	Event study; sentiment event study

The empirical results regarding the effect of data breach events on investor confidence reject the hypothesis of a negative effect. Contrary to what is hypothesized, data breach announcements do not provoke an adverse effect on investors' behavior and stock market value. Cumulative average abnormal returns, which gauge the overall effect on investor confidence and stock market activity, are statistically insignificant. The lack of a significant negative impact in the level of investor confidence indicates a change in investors' awareness of the impact of data breach incidents in future firm profitability. Although this result is counterintuitive at first sight, the absence of a significant effect on investors' behavior may be related to the characteristics and the

size of the disclosed event. As the frequency of data breach announcements increases with the pace of digital innovations, investors may differentiate between events of small and moderate impact and large-scale incidents with the potential of compromising future sales and company's profitability (Kvochko and Pant, 2015). The opposite effect is observed regarding social media sentiment and corporate reputation. Abnormal sentiment values, which measure the deviation of actual sentiment from average normal sentiment, are negative and statistically significant. The simultaneous analysis of intangible costs reveals useful insights for the management of data breach events and the implementation of appropriate crisis response plans.

II Implications

1 Implications for Research

This thesis makes several contributions to information security literature and other related research areas, which are recapitulated in Table C-6.

Table C-6: Contributions to research

Study	Contribution
Study 1	• Recognizes major research gaps, theoretical deficits and methodological limitations in the area of research investigating the intangible costs of data breach events
Study 2	• Provides novel insights regarding the impact of NSA data breach events on investor confidence and firm market value
Study 3	• Suggests a novel approach for the operationalization and measurement of the concept of corporate reputation in a data breach scenario • Provides empirical evidence on the extent of the reputational impact of data breach incidents
Study 4	• Investigates and identifies the influencing factors of reputation damage during a data breach event
Study 5	• Identifies major differences regarding the impact of data breach events on investor confidence and on corporate reputation

Overall this thesis emphasizes the importance of exploring and assessing the intangible costs of data breach events, especially in the light of their practical relevance in terms of prevention and management of data breach incidents. In this regard, the literature review performed in **Study 1** brings the intangible costs of data breach incidents to the attention of security scholars and overcomes gaps of prior literature review studies in security research. Prior systematic literature reviews of security research adopt a comprehensive perspective by considering the full spectrum

of information security literature (Silic and Back, 2014; Willison and Siponen, 2007; Zafar and Clark, 2009). **Study 1** focalizes instead on a narrow topic of information security research and provides a concept-based overview of the extant research on the intangible costs of data and security breach incidents. **Study 1** reveals a strong concentration of research on one category of intangible costs, given by the loss of investor confidence (Acquisti et al., 2006; Hinz et al., 2015; Kannan et al., 2007, e.g.), and an evident knowledge gap regarding the reputational impact of data breaches. **Study 1** identifies research gaps, theoretical deficits, methodological limitations and therefore serves as a reference point for scholars aiming to contribute to this line of research.

Regarding the impact of data breaches on market value, **Study 2** contributes to information security research with new insights on the impact of NSA data breach events on investor confidence and firm market value. The NSA data breaches depict a special category of confidentiality breach events and differ in several aspects from classic data breach incidents investigated in literature. NSA data breach events represent an atypical data breach event based on the current definitions of confidentiality breaches and have raised serious concerns at the ethical, legal and economic level. While legal and ethical aspects related to the NSA events have been often addressed in the literature, little evidence exists on the economic outreach of such incidents (Landau, 2014). Bearing this in mind, **Study 2** tests the hypothesis of an adverse effect of NSA data breaches on investor confidence and provides evidence of a negative impact of the NSA security scandal on investor confidence. Therefore, this study closes a relevant research gap and extends the knowledge on the intangible costs of data breach incidents.

With regard to the impact of data breaches on corporate reputation, **Study 3** and **Study 4** provide several contributions to research. **Study 3** addresses the question of how data breach events affect corporate reputation and makes a two-fold contribution to research. First, **Study 3** tackles the methodological facet of corporate reputation by proposing a novel approach to assess the effect of data breach events on reputation. The sentiment-based event study integrates social media sentiment values (Liu, 2012) in the methodological framework of the conventional event study method (MacKinlay, 1997). **Study 3** offers a new approach for the operationalization and the assessment of the concept of reputation, making a contribution at the methodological level. This approach enables a prompt measurement of reputation scores and depicts an improvement to traditional reputation measures derived from long-term survey studies (Benthaus et al., 2013). The application of the sentiment-based event study approach is not context-specific and can be extended to other areas of research to measure the impact of other types of business-related events on corporate reputation. Accordingly, **Study 3** contributes not only to the information security research, but also to information systems literature and the general reputation management literature. **Study 3** lays a methodological basis for the measurement of the reputational effect of data breach events, thus providing a starting point for the further exploration of intangible costs in future research. Given the knowledge gap on the relationship between data breaches and corporate reputation, the second contribution of **Study 3** regards the extent of the reputational

effect of data breach incidents. The study addresses the previously mentioned research gaps regarding the reputational impact of data breaches, revealing that data breach incidents have a strong negative effect on reputation that is persistent for several days after the event disclosure.

Study 4 contributes to information security literature by providing insights on the antecedents of reputational damage in the context of data breach events. As in **Study 3**, **Study 4** extends the body of knowledge on the reputational impact of data breaches by exploring the impact of data breaches on reputation. **Study 4** provides evidence of a significant negative effect and corroborates the results of **Study 3**. A major contribution of **Study 4** is the examination of the drivers of reputation damage following the announcement of data breach events. In this regard, through a multivariate regression analysis **Study 4** identifies two influencing factors of reputation damage: *news media coverage* and *breach history*. Data breach announcements discussed in conventional news media channels induce a larger negative impact on corporate reputation compared to breach events not exposed by the media. In addition, *breach history*, which refers to the recurrence of data breach events over time, represents a penalizing factor for corporate reputation. The findings of **Study 4** add to the growing body of literature on the intangible costs of data breach incidents and encourage future research.

The findings of **Study 5**, which examines the impact of data breach events on investor confidence and on corporate reputation with a comparative approach, add to the body of research investigating the impact of data breaches on investor confidence and corporate reputation. As in **Study 3**, the sentiment-based event study approach shows a negative and significant effect on corporate reputation. In addition, contrary to **Study 2** which shows a significant negative effect on stock market value, **Study 5** reveals that data breach announcements do not have a significant negative effect on investor confidence. The significant change in the level of investors' awareness towards the phenomenon of data breach events is due to the increasing trend of data breaches in the past decade. Since the threat of data breaches constantly rises with the technological trends, investors evaluate a breach incident in terms of how it might affect the profitability and the future financial performance of the affected companies. Investors penalize to a greater extent data breach incidents that might have a significant adverse effect on future sales and profits, thus leading to greater losses of market value (Kvochko and Pant, 2015).

2 Practical Implications

The addressed aspects and the findings of this thesis have managerial implications and are particularly relevant to security investment managers, cyber security risk managers and crisis response teams. A summary of the practical and managerial implications of the studies included in this thesis is provided by Table C-7.

Table C-7: Practical implications

Study	Contribution
Study 1	• Highlights the strong link between data breach intangible costs and security managerial decisions
Study 2	• Signalizes the necessity of implementing crisis response frameworks to mitigate the loss of market value resulting from data breach events
Study 3	• Suggests a novel approach based on social media sentiment to measure and monitor the impact of data breach incidents on corporate reputation • The novel approach can enhance the accuracy level of IT security expenditures and investments as well as the effectiveness of crisis management programs
Study 4	• Identifies the influencing factors of the reputational impact of data breaches to be integrated in crisis response plans
Study 5	• Provides directions on how to increase the effectiveness of crisis response plans in order to mitigate the intangible costs of data breaches

Study 1 suggests that a deep understanding of reputation risk factors and the development of methodological approaches for the assessment of intangible costs can positively influence IT security decisions and the management process of data breach incidents. Given the strong link between data breach intangible costs and IT security decisions, **Study 1** emphasizes the necessity of developing new assessment approaches in order to provide companies with novel reputation monitoring tools. Due to the methodological constraints regarding the assessment of data breach intangible losses, intangible costs are not taken into account in security investment decisions, often leading to a condition of sub-optimal security expenditure (Cavusoglu et al., 2004a).

Study 2 indicates that massive data breach events have an adverse effect on investor confidence and firm market value. Therefore, crisis response programs and strategic countermeasures should be promptly enacted in order to contain the loss of market value and the future impact on business performance. Complex data breach events, such as the NSA confidentiality breach scandal, might raise serious concerns in investors regarding the long-term financial impact of such critical events (Landau, 2016). Communications to investors should therefore take into account the contextual characteristics of the breach incident and provide transparency on the security measures undertaken to contrast the consequences of such events in the future (Fowler, 2016).

By proposing the sentiment-based event study approach, **Study 3** offers a novel perspective of measuring corporate reputation, which can be employed by companies to measure the reputational losses caused by data breach events. The methodological contribution of **Study 3** benefits the decision-making process regarding IT security investments by increasing the effectiveness of information security expenditures. Better security investments in terms of improved technical

infrastructure and the enactment of training security programs reduce the risk of data breach incidents and contribute to a safer security environment (Huang et al., 2014). The sentiment-based event study approach can be also employed to constantly monitor the corporate reputation trend after a breach announcement in order to adapt crisis response programs in accordance with the severity of the reputational losses. Finally, the sentiment-based event study is a flexible approach that can be adapted to other business contexts to examine the impact of other relevant business events on corporate reputation.

As the risk of data breaches increases with the pace of technological advances and innovations, companies should be constantly prepared to manage an increasing number of data breach crisis situations. Well-studied crisis response frameworks require a deep understanding of the risk factors bearing the potential of intensifying intangible losses and a coordination of roles and responsibilities in crisis respons teams (Deloitte, 2016). In this respect, **Study 4** identifies two influencing factors of corporate reputation: *news media exposure* and *breach history*. Both factors should be taken into account from crisis response teams in order to be integrated in the implementation of crisis response programs. Since companies cannot anticipate the news media coverage of the breach incident, communications to firm stakeholders should be a priority of crisis response programs in order to avert a reputational crisis. Companies' immediate reaction in the wake of a data breach event can contribute to a higher transparency of the breach incident and to a reassuring effect on firm's stakeholders (Fowler, 2016). Companies' reaction and response in the onset of a crisis event is particularly critical for companies which have been affected by multiple data breach events in the past. Repeated breach incidents imply a vulnerable security environment and a substantial lack of efficacious prevention measures and management strategies (Kashmiri et al., 2017). Communications to stakeholders, customers and other affected parties should thus focus on company's strategy to prevent persistent security issues in the future.

The comparative analysis between the impact on investor confidence and on corporate reputation in **Study 5** offers directions on how to enhance the effectiveness of crisis response programs. **Study 5** reveals an insignificant effect of data breach announcements on investor confidence and a significant negative effect on corporate reputation. In such crisis situations characterized by a different extent of intangible costs, companies should be able to quickly detect the most critical intangible costs in order to effectively deploy available crisis management resources. In this scenario characterized by significant reputational losses, communication strategies should play a crucial role in the onset of the incident announcement. To avert further reputational losses, companies should provide transparency on the incident causes and clearly delineate the steps undertaken to contrast the consequences of the breach incident (Fowler, 2016). **Study 5** also shows that the extent of the intangible losses resulting from data breach incidents can vary between different incidents. Depending upon the extent of the intangible costs, **Study 5** suggests that the management strategy of data breach incidents should be adapted to the specific data breach context.

3 Policy Implications

Besides the theoretical and practical contributions, this thesis provides recommendations for policy makers, legal scholars and regulatory authorities. The recent developments regarding the NSA revelations of data breaches show that the collection of massive amounts of data by governmental institutions has a harmful effect on shareholder wealth and firm market value. In such a data breach scenario, where the violation of confidentiality results from the actions of governmental institutions, the boundary between the legal process of collecting data and the violation of the confidentiality security principle is puzzling. Therefore, the data breach event related with the NSA revelations represents an unprecedented event and should encourage policy makers to improve the regulatory landscape by addressing critical issues such as reshaping the current definitions of data breaches, rethinking information security principles and reinforcing the application of sanctions and punishments (Landau, 2016).

The introduction and the enactment of data breach notification laws, such as in Europe, U.S., Australia etc., have the scope to assure transparency for the affected individuals and incentivize companies to develop effective data breach management solutions (Buckman et al., 2017; Karyda and Mitrou, 2016; Maurushat, 2009). Other countries, such as Japan and Canada, on the other hand have not established mandatory data breach notification requirements for companies involved in data breach incidents (Maurushat, 2009). It is however acknowledged that data breaches represent a serious threat to corporate reputation (Syed and Dhillon, 2015), shareholder wealth (Hovav et al., 2017; Kashmiri et al., 2017) and future business performance (Zafar et al., 2012). In order to enhance companies' awareness regarding the risk of data breach incidents and to promote the design and implementation of robust prevention and management strategies, policy makers and legislative bodies should promote the institution of data breach notification laws. The introduction and enactment of specific data breach notification requirements as well as the application of penalties for non-compliant behavior can increase in companies the level of security awareness in order to guarantee the safety of data in a constantly evolving security environment (Bisogni, 2016; Karyda and Mitrou, 2016).

Current legal frameworks effective in countries which have promulgated data breach notification laws are characterized by several flaws (Maurushat, 2009; Bisogni, 2016). In the U.S. for instance, the legal requirements regarding mandatory data breach notifications as well as the penalties and sanctions applied in cases of non-complying behavior, vary to a large extent among the different states. The main differences regard principally the categories of subjects that must be notified, the type of information involved in the breach incident and covered by the respective state law, and the severity of sanctions and punishment for non-compliant behavior (Bisogni, 2016). The reinforcement of current legal frameworks and the improvement of flaws and gaps characterizing the regulatory landscape should represent a priority for policy makers and legal scholars. The lack of harmonization in the application of data breach notification frameworks can

hinder the development of a robust organizational security culture and the uniform application of mandatory legal requirements and sanctions (Bisogni, 2016; Maurushat, 2009).

III Limitations and Future Research

1 Limitations

The studies conducted to investigate the intangible impact of data breach events are characterized by several research limitations, primarily regarding the size of the analyzed samples, the data collection process and the applied methodology.

The rationale of the moderate sample size in **Study 3**, **Study 4** and **Study 5**, which primarily focus on the reputational impact of data breach events, lies in the collection and the processing of unstructured social media data. Due to the lack of a clear structure, the process of collecting, structuring and analyzing unstructured data presents a higher degree of complexity and is highly demanding in terms of time and resources in contrast to the structured counterpart (Baars and Kemper, 2008).

A further limitation of **Study 3**, **Study 4** and **Study 5** regards the procedure of identifying social media postings referred to data breach events by using the name of the respective firm in the search string. In doing so, the final search output encompasses postings whose content is effectively not pertinent to the investigated context, affecting thus the overall accuracy of historical sentiment scores.

With regard to methodology, the main methodological limitation concerns the dictionary-based sentiment analysis approach employed in **Study 3**, **Study 4** and **Study 5** to measure the reputational impact of data and security breach events. The calculation of sentiment values relies upon the matching process between the words extracted from social media postings and predefined word lists of the Harvard IV-4 dictionary without taking into account the potential ironic or sarcastic tone of content (Stone et al., 1966).

2 Future Research

This thesis identifies relevant aspects of the intangible costs of data breach incidents necessitating further exploration in future research. Although **Study 2** addresses a relevant research gap by offering insights on the impact of NSA data breach events on investor confidence and firm market value, the study does not examine the factors driving the loss of investor confidence. Scholars should examine the drivers of the market value reaction and provide insights on unexplored facets of NSA data breach events.

A major shortcoming of the dictionaries applied in **Study 3**, **Study 4** and **Study 5** to assess social media sentiment values is that they do not recognize sarcasm or irony at the sentence

and document level (Liu, 2012). Thus, scholars could focus on the methodological aspects of the reputational effect of data breach incidents by applying alternative sentiment detection techniques. The overcoming of methodological limitations enhances the accuracy of sentiment measures and the validity of the empirical results regarding the reputational effect of data breach incidents.

Building upon the theoretical assumptions of the Situational Crisis Communication Theory (SCCT) (Coombs, 2004), **Study 4** shows that the prior history of data breaches as well as exposure in news media have a negative impact on corporate reputation. In particular, this study could be extended in future research by exploring the predictive power of *crisis responsibility*, which depicts a fundamental component of SCCT not included in the analysis of **Study 4**, on corporate reputation. In a data breach scenario, crisis responsibility indicates to what extent the company is liable for the data breach incident and has a direct impact on corporate reputation (Syed and Dhillon, 2015). An additional research path for future studies could be the investigation of the predictive power of additional variables on firm reputation such as firm characteristics (e.g. industry type) and breach characteristics (e.g. loss size, accidental events vs. intentional events). The investigation of the antecedents of corporate reputation in data breach situations can generate insights that are necessary for the implementation of suitable crisis management strategies.

References

Acquisti, A., Friedman, A., and Telang, R. (2006). Is there a cost to privacy breaches? An event study. In *Proceedings of the 27th International Conference on Information Systems (ICIS),* Milwaukee, Wisconsin, USA, pages 1563–1580.

Acquisti, A., John, L. K., and Loewenstein, G. (2013). What is privacy worth? *The Journal of Legal Studies*, 42(2):249–274.

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In *Action-control: From Cognition to Behavior*, SSSP Springer Series in Social Psychology, pages 11–39. Springer, Heidelberg.

Anderson, C. L. and Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3):613–643.

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security*, 22(4):308–313.

Anderson, R. and Schneier, B. (2005). Guest editors' introduction: Economics of information security. *IEEE Security & Privacy*, 3(1):12–13.

Andoh-Baidoo, F. K., Amoako-Gyampah, K., and Osei-Bryson, K.-M. (2010). How internet security breaches harm market value. *IEEE Security & Privacy*, 8(1):36–42.

Andress, J. (2014). *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice*. Syngress.

Aula, P. (2010). Social media, reputation risk and ambient publicity management. *Strategy & Leadership*, 38(6):43–49.

Baars, H. and Kemper, H.-G. (2008). Management support with structured and unstructured data—An integrated business intelligence framework. *Information Systems Management*, 25(2):132–148.

Ball, R. (1995). The theory of stock market efficiency: Accomplishments and limitations. *Journal of Applied Corporate Finance*, 8(1):4–18.

Bandara, W., Miskon, S., and Fielt, E. (2011). A systematic, tool-supported method for conducting literature reviews in information systems. In *Proceedings of the 19th European Conference on Information Systems (ECIS 2011),* Helsinki, Finland.

Benthaus, J., Pahlke, I., Beck, R., and Seebach, C. (2013). Improving sensing and seizing capabilities of a firm by measuring corporate reputation based on social media data. In *Proceedings*

of the 21st European Conference on Information Systems (ECIS), Utrecht, Netherlands, pages 1–12.

Bharadwaj, A., Keil, M., and Mähring, M. (2009). Effects of information technology failures on the market value of firms. *The Journal of Strategic Information Systems*, 18(2):66–79.

Binder, J. (1998). The event study methodology since 1969. *Review of Quantitative Finance and Accounting*, 11(2):111–137.

Bishop, M. A. (2003). *Computer security: Art and science*. Addison-Wesley.

Bisogni, F. (2016). Proving limits of state data breach notification laws: Is a federal law the most adequate solution? *Journal of Information Policy*, 6(1):154–205.

Bloomberg (2014). `http://www.bloomberg.com/news/articles/2014-05-23/investors-couldnt-care-lessabout-data-breaches`, [Accessed: April 1st, 2016].

Boehmer, E., Masumeci, J., and Poulsen, A. B. (1991). Event-study methodology under conditions of event-induced variance. *Journal of Financial Economics*, 30(2):253–272.

Boell, S. K. and Cecez-Kecmanovic, D. (2015). On being 'systematic' in literature reviews in IS. *Journal of Information Technology*, 30(2):161–173.

Bolster, P., Pantalone, C. H., and Trahan, E. A. (2010). Security breaches and firm value. *Journal of Business Valuation and Economic Loss Analysis*, 5(1).

Bondt, W. F. and Thaler, R. (1985). Does the stock market overreact? *The Journal of Finance*, 40(3):793–805.

Boudt, K. and Petitjean, M. (2014). Intraday liquidity dynamics and news releases around price jumps: Evidence from the DJIA stocks. *Journal of Financial Markets*, 17:121–149.

Brønn, C. and Brønn, P. S. (2015). A systems approach to understanding how reputation contributes to competitive advantage. *Corporate Reputation Review*, 18(2):69–86.

Brown, S. J. and Warner, J. B. (1980). Measuring security price performance. *Journal of Financial Economics*, 8(3):205–258.

Brown, S. J. and Warner, J. B. (1985). Using daily stock returns: The case of event studies. *Journal of Financial Economics*, 14(1):3–31.

Buckman, J., Bockstedt, J. C., Hashim, M. J., and Woutersen, T. (2017). Do organizations learn from a data breach? In *16th Annual Workshop on the Economics of Information Security (WEIS),* San Diego, California, USA.

Camp, L. J. and Lewis, S. (2006). *Economics of information security*. Springer Science & Business Media.

Campbell, J. Y., Lo, A. W.-C., MacKinlay, A. C., et al. (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):431–448.

Cavusoglu, H. (2002). The economics of information technology (IT) security. In *Proceedings of the 8th Americas Conference on Information Systems (AMCIS),* Dallas, Texas, USA, pages 2481–2485.

Cavusoglu, H., Cavusoglu, H., and Raghunathan, S. (2004a). Economics of IT security management: Four improvements to current security practices. *Communications of the Association for Information Systems*, 14:65–75.

Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004b). 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):70–104.

Chae, H.-C., Koh, C. E., and Prybutok, V. R. (2014). Information technology capability and firm performance: Contradictory findings and their possible causes. *MIS Quarterly*, 38(1):305–326.

Cherdantseva, Y. and Hilton, J. (2013a). Information security and information assurance: Discussion about the meaning, scope and goals. In *F. Almeida, and I. Portela (eds.), Organizational, Legal, and Technological Dimensions of Information System Administration*. IGI Global.

Cherdantseva, Y. and Hilton, J. (2013b). A reference model of information assurance & security. In *Proceedings of the Eighth International Conference on Availability, Reliability and Security (ARES),* Regensburg, Germany, pages 546–555.

Choobineh, J., Dhillon, G., Grimaila, M. R., and Rees, J. (2007). Management of information security: Challenges and research directions. *Communications of the Association for Information Systems*, 20:958–971.

Chowdhuri, R. and Dhillon, G. (2012). Understanding information security. *Journal of Information System Security*, 8(2):3–18.

Colleoni, E., Arvidsson, A., Hansen, L. K., and Marchesini, A. (2011). Measuring corporate reputation using sentiment analysis. In *Proceedings of the 15th International Conference on Corporate Reputation: Navigating the Reputation Economy,* New Orleans, Louisiana, USA.

Cooley, S. C. and Cooley, A. B. (2011). An examination of the Situational Crisis Communication Theory through the General Motors bankruptcy. *Journal of Media and Communication Studies*, 3(6):203–211.

Coombs, W. T. (2004). Impact of past crises on current crisis communication: Insights from

Situational Crisis Communication Theory. *Journal of Business Communication*, 41(3):265–289.

Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of Situational Crisis Communication Theory. *Corporate Reputation Review*, 10(3):163–176.

Coombs, W. T. (2014). *Ongoing crisis communication: Planning, managing, and responding*. Sage Publications.

Coombs, W. T. and Holladay, S. J. (2002). Helping crisis managers protect reputational assets: Initial tests of the Situational Crisis Communication Theory. *Management Communication Quarterly*, 16(2):165–186.

Coombs, W. T. and Holladay, S. J. (2006). Unpacking the halo effect: Reputation and crisis management. *Journal of Communication Management*, 10(2):123–137.

Curtin, M. and Ayres, L. T. (2008). Using science to combat data loss: Analyzing breaches by type and industry. *I/S: A Journal of Law and Policy for the Information Society*, 4:569–601.

D'Arcy, J. and Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences*, 43(6):1091–1124.

D'Arcy, J., Gupta, A., Tarafdar, M., and Turel, O. (2014). Reflecting on the "dark side" of information technology use. *Communications of the Association for Information Systems*, 35:109–118.

D'Arcy, J., Herath, T., and Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, 31(2):285–318.

Datalossdb (2017). `https://blog.datalossdb.org/about/` [Accessed: January 24th, 2017].

Dean, D. H. (2004). Consumer reaction to negative publicity: Effects of corporate reputation, response, and responsibility for a crisis event. *Journal of Business Communication*, 41(2):192–211.

Deephouse, D. L. (2000). Media reputation as a strategic resource: An integration of mass communication and resource-based theories. *Journal of Management*, 26(6):1091–1112.

Deloitte (2016). Cyber crisis management: Readiness, response, and recovery. , Deloitte Touche Tohmatsu Limited. `https://www2.deloitte.com/global/en/pages/risk/articles/cyber-crisis-management.html` [Accessed: March 14th, 2017].

Dhillon, G. (2001). Principles for managing information security in the new millennium. In

Information Security Management: Global Challenges in the New Millennium, pages 173–177. IGI Global.

Dhillon, G. and Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, 43(7):125–128.

Dhillon, G. and Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal*, 11(2):127–153.

Dibbern, J., Goles, T., Hirschheim, R., and Jayatilaka, B. (2004). Information systems outsourcing: A survey and analysis of the literature. *ACM Sigmis Database*, 35(4):6–102.

Dyckman, T., Philbrick, D., and Stephan, J. (1984). A comparison of event study methodologies using daily stock returns: A simulation approach. *Journal of Accounting Research*, 22:1–30.

Economic Intelligence Unit (2012). IBM global reputational risk and IT study: How security and business continuity can shape the reputation and value of your company. Research report, Conducted by the Economist Intelligence Unit on behalf of IBM. `https://www-935.ibm.com/services/us/gbs/bus/html/risk_study-2012-infographic.html` [Accessed: May 10th, 2014].

Einwiller, S. A., Carroll, C. E., and Korn, K. (2010). Under what conditions do the news media influence corporate reputation? The roles of media dependency and need for orientation. *Corporate Reputation Review*, 12(4):299–315.

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

Experian (2017). Fourth annual 2017 data breach industry forecast. Data breach industry forecast report, Experian ® Data Breach Resolution. `http://www.experian.com/data-breach/2017-data-breach-industry-forecast.html` [Accessed: January 11th, 2017].

Fama, E. F. (1991). Efficient capital markets: II. *The Journal of Finance*, 46(5):1575–1617.

Fama, E. F. (1998). Market efficiency, long-term returns, and behavioral finance. *Journal of Financial Economics*, 49(3):283–306.

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):1–21.

Farrow, S. and Szanton, J. (2016). Cybersecurity investment guidance: Extensions of the Gordon and Loeb model. *Journal of Information Security*, 7:15–28.

Fearn-Banks, K. (2010). *Crisis communications: A casebook approach*. Routledge.

Feldman, R. (2013). Techniques and applications for sentiment analysis. *Communications of the ACM*, 56(4):82–89.

Feldman, R., Rosenfeld, B., Bar-Haim, R., and Fresko, M. (2011). The stock sonar—Sentiment analysis of stocks based on a hybrid approach. In *Proceedings of the Twenty-Third Innovative Applications of Artificial Intelligence Conference (IAAI),* San Francisco, California, USA, pages 1642–1647.

Field, A. (2009). *Discovering statistics using SPSS*. Sage publications.

Fombrun, C. (1996). *Reputation: Realizing value from the corporate image*. Harvard Business School Press.

Fombrun, C. and Shanley, M. (1990). What's in a name? Reputation building and corporate strategy. *Academy of Management Journal*, 33(2):233–258.

Fombrun, C. and Van Riel, C. (1997). The reputational landscape. *Corporate Reputation Review*, 1(1-2):5–13.

Fombrun, C. J., Gardberg, N. A., and Sever, J. M. (2000). The Reputation QuotientSM: A multi-stakeholder measure of corporate reputation. *Journal of Brand Management*, 7(4):241–255.

Forbes (2014). `http://www.forbes.com/sites/maggiemcgrath/2014/10/02/jp-morgan-says-76-million-households-affected-by-data-breach/` [Accessed: October 27th, 2014].

Forbes Insights (2014). The reputational impact of IT risk. , Forbes Insights in association with IBM. `https://www-935.ibm.com/services/multimedia/RLL12363USEN_2014_Forbes_Insights.pdf` [Accessed: June 3rd, 2017].

Foth, M. (2016). Factors influencing the intention to comply with data protection regulations in hospitals: Based on gender differences in behaviour and deterrence. *European Journal of Information Systems*, 25(2):91–109.

Fowler, K. (2016). *Data breach preparation and response: Breaches are certain, impact is not*. Syngress.

Freedman, K. (1999). Laudan's naturalistic axiology. *Philosophy of Science*, 66:526–537.

Garg, A., Curtis, J., and Halper, H. (2003a). The financial impact of IT security breaches: What do investors think? *Information Systems Security*, 12(1):22–33.

Garg, A., Curtis, J., and Halper, H. (2003b). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, 11(2):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):61–83.

Goel, S. and Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*, 46(7):404–410.

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*, 34:37–50.

Goldstein, J., Chernobai, A., and Benaroch, M. (2011). An event study analysis of the economic impact of IT operational risk and its subcategories. *Journal of the Association for Information Systems*, 12(9):606–631.

Gordon, L. A. and Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4):438–457.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., Zhou, L., et al. (2014). Externalities and the magnitude of cyber security underinvestment by private sector firms: A modification of the Gordon-Loeb model. *Journal of Information Security*, 6:24–30.

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):33–56.

Gray, P. and Watson, H. J. (1998). Present and future directions in data warehousing. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 29(3):83–90.

Gupta, U. and Ranganathan, N. (2007). Multievent crisis management using noncooperative multistep games. *IEEE Transactions on Computers*, 56(5):577–589.

Hausken, K. (2014). Returns to information security investment: Endogenizing the expected loss. *Information Systems Frontiers*, 16(2):329–336.

Hedström, K., Kolkowska, E., Karlsson, F., and Allen, J. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems*, 20(4):373–384.

Henderson Jr, G. V. (1990). Problems and solutions in conducting event studies. *Journal of Risk and Insurance*, 57(2):282–306.

Herath, T. and Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2):154–165.

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):337–347.

Hoffmann, A. O. and Post, T. (2016). How does investor confidence lead to trading? Linking investor return experiences, confidence, and investment beliefs. *Journal of Behavioral and Experimental Finance*, 12:65–78.

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):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):32–40.

Hovav, A. and Gray, P. (2014). The ripple effect of an information security breach event: A stakeholder analysis. *Communications of the Association for Information Systems*, 34:893–912.

Hovav, A., Han, J., and Kim, J. (2017). Market reaction to security breach announcements: evidence from South Korea. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 48(1):11–52.

Hua, J. and Bapna, S. (2012). How can we deter cyber terrorism? *Information Security Journal: A Global Perspective*, 21(2):102–114.

Hua, J. and Bapna, S. (2013). The economic impact of cyber terrorism. *The Journal of Strategic Information Systems*, 22(2):175–186.

Huang, C. D., Behara, R. S., and Goo, J. (2014). Optimal information security investment in a Healthcare Information Exchange: An economic analysis. *Decision Support Systems*, 61:1–11.

Hunt, S. D. (1990). Truth in marketing theory and research. *The Journal of Marketing*, 54(3):1–15.

Huq, N. (2015). Follow the data: Dissecting data breaches and debunking myths. Trend Micro analysis of Privacy Rights Clearinghouse 2005–2015 data breach records. Research paper, Trend Micro. `https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/follow-the-data` [Accessed: December 2nd, 2016].

Identity Theft Resource Center (2016). Data breach reports. 2016 End of year report. Breach report, Identity Theft Resource Center (ITRC) and CyberScout. `http://www.idtheftcenter.org/2016databreaches.html` [Accessed: April 1st, 2017].

Im, K. S., Dow, K. E., and Grover, V. (2001). Research report: A reexamination of IT investment and the market value of the firm—An event study methodology. *Information Systems Research*, 12(1):103–117.

Institute for Information Security and Privacy (IISP) (2016). Emerging cyber threats report. , Giorgia Institute for Technology. `http://www.iisp.gatech.edu/2016-emerging-cyber-threats-report` [Accessed: February 20th, 2016].

International Standards Organization (2016). ISO/IEC 27050. `https://www.iso.org/`

obp/ui/#iso:std:iso-iec:27050:-1:ed-1:v1:en [Accessed: December 10th, 2016].

Ito, T. A., Larsen, J. T., Smith, N. K., and Cacioppo, J. T. (1998). Negative information weighs more heavily on the brain: The negativity bias in evaluative categorizations. *Journal of Personality and Social Psychology*, 75(4):887–900.

Jain, A. K., Hong, L., Pankanti, S., and Bolle, R. (1997). An identity-authentication system using fingerprints. *Proceedings of the IEEE*, 85(9):1365–1388.

Jin, Y., Liu, B. F., and Austin, L. L. (2011). Examining the role of social media in effective crisis management: The effects of crisis origin, information form, and source on publics' crisis responses. *Communication Research*, 41(1):74–94.

Jones, B., Temperley, J., and Lima, A. (2009). Corporate reputation in the era of Web 2.0: The case of Primark. *Journal of Marketing Management*, 25(9-10):927–939.

Jones, G. H., Jones, B. H., and Little, P. (2000). Reputation as reservoir: Buffering against loss in times of economic crisis. *Corporate Reputation Review*, 3(1):21–29.

Kahneman, D. and Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica: Journal of the Econometric Society*, 47(2):263–292.

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):69–91.

Kaplan, A. M. and Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. *Business Horizons*, 53(1):59–68.

Karyda, M. and Mitrou, L. (2016). Data breach notification: Issues and challenges for security management. In *Proceedings of the 10th Mediterranean Conference on Information Systems (MCIS),* Paphos, Cyprus, pages 1–12.

Kashmiri, S., Nicol, C. D., and Hsu, L. (2017). Birds of a feather: Intra-industry spillover of the Target customer data breach and the shielding role of IT, marketing, and CSR. *Journal of the Academy of Marketing Science*, 2(45):208–228.

Kayworth, T. and Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive*, 9(3):163–175.

Kim, S., Koh, S., and Son, S. (2014). The impact of personal information breaches on the firm's value in the South Korean stock market – A comparative study of IT and non-IT industries. *International Journal of Applied Mathematics and Informatics*, 8:42–49.

Ko, M. and Dorantes, C. (2006). The impact of information security breaches on financial

performance of the breached firms: An empirical investigation. *Journal of Information Technology Management*, 17(2):13–22.

Kolkowska, E. and Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security*, 33:3–11.

Kolkowska, E., Hedström, K., and Karlsson, F. (2009). Information security goals in a Swedish hospital. In *Proceedings of the 8th Annual Security Conference,* Las Vegas, Nevada, USA.

Konchitchki, Y. and O'Leary, D. E. (2011). Event study methodologies in information systems research. *International Journal of Accounting Information Systems*, 12(2):99–115.

Kvochko, E. and Pant, R. (2015). Why data breaches don't hurt stock prices. *Harvard Business Review*.

Landau, S. (2013). Making sense from snowden: What's significant in the NSA surveillance revelations. *IEEE Security & Privacy*, 11(4):54–63.

Landau, S. (2014). Highlights from making sense of Snowden, part II: What's significant in the NSA revelations. *IEEE Security & Privacy*, 12(1):62–64.

Landau, S. (2016). Is it legal? Is it right? The can and should of use. *IEEE Security & Privacy*, 14(5):3–5.

Laudan, L. (1984). *Science and values: An essay on the aims of science and their role in scientific debate*. University of California Press.

Layton, R. and Watters, P. A. (2014). A methodology for estimating the tangible cost of data breaches. *Journal of Information Security and Applications*, 19(6):321–330.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., and H. Breitner, M. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review*, 37(12):1049–1092.

Leung, A. and Bose, I. (2008). Indirect financial loss of phishing to global market. In *Proceedings of the 29th International Conference on Information Systems (ICIS),* Paris, France, pages 1–14.

Levy, Y. and Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science*, 9:181–212.

Liang, H. and Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, 33(1):71–90.

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):215–228.

Liu, B. (2012). Sentiment analysis and opinion mining. *Synthesis lectures on human language technologies*, 5(1):1–167.

Lo, A. W. (2004). The adaptive markets hypothesis: Market efficiency from an evolutionary perspective. *Journal of Portfolio Management*.

Lo, A. W. (2005). Reconciling efficient markets with behavioral finance: The adaptive markets hypothesis. *Journal of Investment Consulting*, 7(2):21–44.

Love, E. G., Lim, J., and Bednar, M. (2016). The face of the firm: The influence of CEOs on corporate reputation. *Academy of Management Journal*.

MacKinlay, A. C. (1997). Event studies in economics and finance. *Journal of Economic Literature*, 35(1):13–39.

Mai, B., Kulkarni, S., and Salehan, M. (2016). Vulnerability enhancement vs. loss mitigation: Optimal information security investment. *Journal of Information System Security*, 12(2):77–92.

Malhotra, A. and Kubowicz Malhotra, C. (2011). Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research*, 14(1):44–59.

Malkiel, B. G. and Fama, E. F. (1970). Efficient capital markets: A review of theory and empirical work. *The Journal of Finance*, 25(2):383–417.

Manworren, N., Letwat, J., and Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons*, 59(3):257–266.

Martin, K. D., Borah, A., and Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1):36–58.

Maurushat, A. (2009). Data breach notification law across the world from California to Australia. Research paper, University of New South Wales. `https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1412063` [Accessed: April 21st, 2017].

McWilliams, A. and Siegel, D. (1997). Event studies in management research: Theoretical and empirical issues. *Academy of Management Journal*, 40(3):626–657.

McWilliams, A. and Siegel, D. (2001). Corporate social responsibility: A theory of the firm perspective. *Academy of Management Review*, 26(1):117–127.

McWilliams, A., Siegel, D., and Teoh, S. H. (1999). Issues in the use of the event study methodology: A critical analysis of corporate social responsibility studies. *Organizational Research Methods*, 2(4):340–365.

Mishra, S. and Dhillon, G. (2006). Information systems security governance research: A

behavioral perspective. In *Proceedings of the 1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference,* New York, USA, pages 18–26.

Mithas, S. and Rust, R. T. (2016). How information technology strategy and investments influence firm performance: Conjectures and empirical evidence. *MIS Quarterly*, 40(1):223–245.

Mithas, S., Tafti, A. R., Bardhan, I., and Goh, J. M. (2012). Information technology and firm profitability: Mechanisms and empirical evidence. *MIS Quarterly*, 36(1):205–224.

Miyajima, H. and Yafeh, Y. (2007). Japan's banking crisis: An event-study perspective. *Journal of Banking & Finance*, 31(9):2866–2885.

Modi, S. B., Wiles, M. A., and Mishra, S. (2015). Shareholder value implications of service failures in triads: The case of customer information security breaches. *Journal of Operations Management*, 35:21–39.

Morse, E. A., Raval, V., and Wingender Jr, J. R. (2011). Market price effects of data security breaches. *Information Security Journal: A Global Perspective*, 20(6):263–273.

Ng, B.-Y., Kankanhalli, A., and Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46(4):815–825.

Nofer, D.-K. M., Hinz, O., Muntermann, J., and Roßnagel, H. (2014). The economic impact of privacy violations and security breaches. *Business & Information Systems Engineering*, 6(6):339–348.

Olibe, K. O. (2016). Response to discussion of "security returns and volume responses around International Financial Reporting Standards (IFRS) earnings announcements". *The International Journal of Accounting*, 51(2):271–274.

Open Security Foundation (2014). `http://datalossdb.org/` [Accessed: June 20th, 2014].

Pang, B. and Lee, L. (2008). Opinion mining and sentiment analysis. *Foundations and Trends® in Information Retrieval*, 2(1–2):1–135.

Parker, D. B. (1994). Demonstrating the elements of information security with loss scenarios. *Information Systems Security*, 3(1):17–22.

Parker, D. B. (1997). Information security in a nutshell. *Information Systems Security*, 6(1):14–19.

Patterson, M. E. and Williams, D. R. (1998). Paradigms and problems: The practice of social science in natural resource management. *Society and Natural Resources*, 11(3):279–295.

Peltier, T. R. (2001). *Information security risk analysis*. Auerbach Publications, div. of CRC Press LLC.

Pirounias, S., Mermigas, D., and Patsakis, C. (2014). The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study. *Journal of Information Security and Applications*, 19(4–5):257–271.

Pleeger, C. and Pfleeger, S. L. (2003). *Security in computing*. Prentice Hall, New Jersey.

Ponemon Institute (2011). Reputation impact of a data breach. U.S. study of executives & managers. Research report, Conducted by Ponemon Institute LLC, sponsored by Experian ® Data Breach Resolution. https://www.experian.com/assets/data-breach/white-papers/reputation-study.pdf [Accessed: November 18th, 2014].

Ponemon Institute (2014). 2014 Cost of data breach study: Global analysis. Research report, Conducted by Ponemon Institute LLC, sponsored by IBM. http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis [Accessed: April 15th, 2014].

Ponzi, L. J., Fombrun, C. J., and Gardberg, N. A. (2011). Reptrak™ pulse: Conceptualizing and validating a short-form measure of corporate reputation. *Corporate Reputation Review*, 14(1):15–35.

Privacy Rights Clearinghouse (2017). https://www.privacyrights.org/ [Accessed: March 24th, 2017].

PwC (2014). Cyber security crisis management: A bold approach to a shadowy analysis. , PricewaterhouseCoopers LLP. http://www.pwc.com/ca/en/technology-consulting/security/publications/pwc-cyber-security-crisis-management-2013-05-en.pdf, [Accessed: November 6th, 2016].

PwC (2015). 2015 Information security breaches survey. Technical report, Conducted by PwC in association with Infosecurity Europe. https://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html, [Accessed: February 12th, 2015].

Rao, A., Warsame, M., and Williams, J. L. (2011). Intraday study of the market reaction to distributed denial of service (Dos) attacks on internet firms. *Academy of Accounting and Financial Studies Journal*, 15(2):59.

Rasoulian, S., Grégoire, Y., Legoux, R., and Sénécal, S. (2017). Service crisis recovery and firm performance: Insights from information breach announcements. *Journal of the Academy of Marketing Science*, pages 1–18.

Rhee, M. and Valdez, M. E. (2009). Contextual factors surrounding reputation damage with potential implications for reputation repair. *Academy of Management Review*, 34(1):146–168.

Rindova, V. P., Williamson, I. O., Petkova, A. P., and Sever, J. M. (2005). Being good or

being known: An empirical examination of the dimensions, antecedents, and consequences of organizational reputation. *Academy of Management Journal*, 48(6):1033–1049.

Roberts, P. W. and Dowling, G. R. (2002). Corporate reputation and sustained superior financial performance. *Strategic management journal*, 23(12):1077–1093.

Romanosky, S., Telang, R., and Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management*, 30(2):256–286.

Rowe, F. (2014). What literature review is not: Diversity, boundaries and recommendations. *European Journal of Information Systems*, 23(3):241–255.

Sabate, J. M. d. l. F. and Puente, E. d. Q. (2003). Empirical analysis of the relationship between corporate reputation and financial performance: A survey of the literature. *Corporate Reputation Review*, 6(2):161–177.

Sabherwal, R. and Jeyaraj, A. (2015). Information technology impacts on firm performance: An extension of Kohli and Devaraj (2003). *MIS Quarterly*, 39(4):809–836.

Samonas, S. and Coss, D. (2014). The cia strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, 10(3):21–45.

Sánchez, J. L. F., Sotorrío, L. L., and Díez, E. B. (2012). Can corporate reputation protect companies' value? Spanish evidence of the 2007 financial crash. *Corporate Reputation Review*, 15(4):228–239.

Sarstedt, M., Wilczynski, P., and Melewar, T. (2013). Measuring reputation in global markets—A comparison of reputation measures' convergent and criterion validities. *Journal of World Business*, 48(3):329–339.

Schatz, D. and Bashroush, R. (2016). The impact of repeated data breach events on organisations' market value. *Information & Computer Security*, 24(1):73–92.

Schneier, B. (2014). Metadata= surveillance. *IEEE Security & Privacy*, 12(2):84.

Schryen, G. (2015). Writing qualitative IS literature reviews-Guidelines for synthesis, interpretation and guidance of research. *Communications of the Association for Information Systems*, 37:286–325.

Schryen, G., Benlian, A., Rowe, F., Pare, G., Larsen, K., and Gregor, S. (2016). Standalone literature reviews in IS research: What can be learnt from the past and other fields? In *Proceedings of the 37th International Conference on Information Systems (ICIS),* Dublin, Ireland.

Schryen, G., Wagner, G., and Benlian, A. (2015). Theory of knowledge for literature reviews: An epistemological model, taxonomy and empirical analysis of IS literature. In *Proceedings of the 36th International Conference on Information Systems (ICIS),* Fort Worth, USA.

SDL SM2 (2014). http://www.sdl.com/products/SM2/ [Accessed: July 20th, 2014].

SDL SM2 (2017). http://www.sdl.com/de/industries/government/Social-media-monitoring.html [Accessed: February 18th, 2017].

Seebach, C., Beck, R., and Denisova, O. (2013). Analyzing social media for corporate reputation management: How firms can improve business agility. *International Journal of Business Intelligence Research*, 4(3):50–66.

Sen, R. and Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, 32(2):314–341.

Shinoda, S. and Matsuura, K. (2016). Empirical investigation of threats to loyalty programs by using models inspired by the Gordon-Loeb's formulation of security investment. *Journal of Information Security*, 7:29–48.

Shleifer, A. (2000). *Inefficient markets: An introduction to behavioural finance*. Oxford University Press.

Silic, M. and Back, A. (2014). Information security: Critical review and future directions for research. *Information Management & Computer Security*, 22(3):279–308.

Sinanaj, G. (2015). The intangible cost of information security breaches: A state of the art analysis. *Journal of Information System Security*, 11(2):111–130.

Sinanaj, G. and Beyer, F. (2017). Do data breaches affect our beliefs? - Investigating reputation risk in social media. *Journal of Information System Security*, 13(2):97–116.

Sinanaj, G., Cziesla, T., Kemper, J., and Muntermann, J. (2015a). NSA revelations of privacy breaches: Do investors care? In *Proceedings of the 21st Americas Conference on Information Systems (AMCIS),* Puerto Rico, USA.

Sinanaj, G., Muntermann, J., and Cziesla, T. (2015b). How data breaches ruin firm reputation on social media!-Insights from a sentiment-based event study. In *Proceedings of the 12th International Conference on Wirtschaftsinformatik,* Osnabrück, Germany, pages 902–916.

Sinanaj, G. and Zafar, H. (2016). Who wins in a data breach?-A comparative study on the intangible costs of data breach incidents. In *Proceedings of the 20th Pacific Asia Conference on Information Systems (PACIS),* Chiayi, Taiwan.

Siponen, M., Willison, R., and Baskerville, R. (2008). Power and practice in information systems security research. In *Proceedings of the 29th International Conference on Information Systems (ICIS),* Paris, France, pages 14–17.

Siponen, M. T. (2000). Critical analysis of different approaches to minimizing user-related faults in information systems security: Implications for research and practice. *Information Management & Computer Security*, 8(5):197–209.

Solomon, M. G. and Chapple, M. (2009). *Information security illuminated*. Jones & Bartlett Publishers.

Song, Z., Wang, G. A., and Fan, W. (2017). Firm actions toward data breach incidents and firm equity value: An empirical study. In *Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS),* Hawaii, USA, pages 4957–4966.

Sorescu, A., Warren, N. L., and Ertekin, L. (2017). Event study methodology in the marketing literature: An overview. *Journal of the Academy of Marketing Science*, 45(2):186–207.

Spanos, G. and Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, 58:216–229.

Stone, P. J., Dunphy, D. C., and Smith, M. S. (1966). The General Inquirer: A computer approach to content analysis.

Susan Hansche, C., John Berti, C., and Hare, C. (2003). *Official (ISC) 2 guide to the CISSP exam*. CRC Press.

Syed, R. and Dhillon, G. (2015). Dynamics of data breaches in online social networks: Understanding threats to organizational information security reputation. In *Proceedings of the 36th International Conference on Information Systems (ICIS),* Fort Worth, Texas, USA.

Symantec (2016). Internet security threat report. , Symantec Corporation. `https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf` [Accessed: October 20th, 2016].

Taboada, M., Brooke, J., Tofiloski, M., Voll, K., and Stede, M. (2011). Lexicon-based methods for sentiment analysis. *Computational linguistics*, 37(2):267–307.

Telang, R. and Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software Engineering*, 33(8):544–557.

Tetlock, P. C., Saar-Tsechansky, M., and Macskassy, S. (2008). More than words: Quantifying language to measure firms' fundamentals. *The Journal of Finance*, 63(3):1437–1467.

The Guardian (2013a). `http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-callsbreach/` [Accessed: January 20th, 2015].

The Guardian (2013b). `http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=0000000` [Accessed: January 21st, 2015].

The Guardian (2013c). `http://www.theguardian.com/world/2013/jun/08/`

nsa-prism-server-collection-facebook-google [Accessed: January 20th, 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: January 25th, 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: January 20th, 2015].

Thelwall, M., Buckley, K., Paltoglou, G., Cai, D., and Kappas, A. (2010). Sentiment strength detection in short informal text. *Journal of the American Society for Information Science and Technology*, 61(12):2544–2558.

Thomas, M. and Dhillon, G. (2006). Deep structures of information systems security. In *Proceedings of the 12th Americas Conference on Information Systems (AMCIS),* Acapulco, Mexico, pages 3473–3480.

Thomson, K.-L., von Solms, R., and Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, 2006(10):7–11.

Torres, J. M., Sarriegi, J. M., Santos, J., and Serrano, N. (2006). Managing information systems security: Critical success factors and indicators to measure effectiveness. In *Proceedings of the 9th International Conference on Information Security (ISC),* Samos, Greece, pages 530–545.

Toxen, B. (2014). The NSA and Snowden: Securing the all-seeing eye. *Communications of the ACM*, 57(5):44–51.

Tripathy, A., Agrawal, A., and Rath, S. K. (2016). Classification of sentiment reviews using n-gram machine learning approach. *Expert Systems with Applications*, 57:117–126.

Tsiakis, T. and Stephanides, G. (2005). The economic approach of information security. *Computers & Security*, 24(2):105–108.

Venter, H. and Eloff, J. H. (2003). A taxonomy for information security technologies. *Computers & Security*, 22(4):299–307.

vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., and Cleven, A. (2015). Standing on the shoulders of giants: Challenges and recommendations of literature search in information systems research. *Communications of the Association for Information Systems*, 37:205–224.

Von Solms, B. (2000). Information security—the third wave? *Computers & Security*, 19(7):615–620.

Von Solms, R. and Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38:97–102.

Wagner, G., Prester, J., Roche, M. P., Benlian, A., and Schryen, G. (2016). Factors affecting the scientific impact of literature reviews: A scientometric study. In *Proceedings of the 37th International Conference on Information Systems (ICIS),* Dublin, Ireland.

Wang, H. and Zhai, C. (2017). Generative models for sentiment analysis and opinion mining. In *A Practical Guide to Sentiment Analysis*, pages 107–134. Springer.

Wang, J., Chaudhury, A., and Rao, H. R. (2008). Research note-A value-at-risk approach to information security investment. *Information Systems Research*, 19(1):106–120.

Wang, S. (2017). Integrated framework for information security investment and cyber insurance. Research paper, Nanyang Technological University. `https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2918674` [Accessed: December 20th, 2016].

Wartick, S. L. (2002). Measuring corporate reputation definition and data. *Business & Society*, 41(4):371–392.

Webster, J. and Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, 26(2):xiii–xxiii.

Wernerfelt, B. (1995). The resource-based view of the firm: Ten years after. *Strategic Management Journal*, 16(3):171–174.

Whitman, M. E. (2004). In defense of the realm: Understanding the threats to information security. *International Journal of Information Management*, 24(1):43–57.

Whitman, M. E. and Mattord, H. J. (2011). *Principles of information security*. Cengage Learning.

Whitman, M. E., Mattord, H. J., Mackey, D., and Green, A. (2012). *Guide to network security*. Cengage Learning.

Willemson, J. (2010). Extending the Gordon and Loeb model for information security investment. In *Proceedings of the Fifth International Conference on Availability, Reliability and Security (ARES), Krakow, Poland*, pages 258–261.

Willison, R. and Siponen, M. (2007). A critical assessment of IS security research between 1990-2004. In *Proceedings of the 15th European Conference on Information Systems (ECIS),* St. Gallen, Switzerland, pages 1551–1559.

Wolfswinkel, J. F., Furtmueller, E., and Wilderom, C. P. (2013). Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems*, 22(1):45–55.

Wright, P., Ferris, S. P., Hiller, J. S., and Kroll, M. (1995). Competitiveness through management

of diversity: Effects on stock price valuation. *Academy of Management Journal*, 38(1):272–287.

Xu, W., Grant, G., Nguyen, H., and Dai, X. (2008). Security breach: The case of TJX companies, inc. *Communications of the Association for Information Systems*, 23:575–590.

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):60–77.

Zafar, H. and Clark, J. G. (2009). Current state of information security research in IS. *Communications of the Association for Information Systems*, 24:557–596.

Zafar, H., Ko, M., and Osei-Bryson, K.-M. (2012). Financial impact of information security breaches on breached firms and their non-breached competitors. *Information Resources Management Journal*, 25(1):21–37.

Zavyalova, A., Pfarrer, M. D., Reger, R. K., and Hubbard, T. D. (2016). Reputation as a benefit and a burden? How stakeholders' organizational identification affects the role of reputation following a negative event. *Academy of Management Journal*, 59(1):253–276.

Zhuang, L., Jing, F., and Zhu, X.-Y. (2006). Movie review mining and summarization. In *Proceedings of the 15th ACM international conference on Information and knowledge management*, pages 43–50.

Appendix

Appendix 1: List of NSA-security breaches

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

Continued

Appendix 1: List of NSA-security breaches

Event date	Company	News media link	Country
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

Continued

Appendix 1: List of NSA-security breaches

Event date	Company	News media link	Country
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&SouthKorea	
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

Continued

Appendix 1: List of NSA-security breaches

Event date	Company	News media link	Country
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