Dynamics of Data Breaches in Online Social Networks: Understanding Threats to Organizational Information Security Reputation

Completed Research Paper

Romilla Syed
University of Massachusetts Boston
100 Morrissey Blvd., Boston, MA 02125, USA
romilla.syed@umb.edu

Gurpreet Dhillon
Virginia Commonwealth University
301 W. Main Street, Richmond, VA 23284, USA
gdhillon@vcu.edu

Abstract

The consequences of data breaches can be severe for the Information Security Reputation (ISR) of organizations. Using social media analytical techniques, this study examines Twitter postings to identify (1) ISR dimensions attributed as being responsible for data breaches and (2) social media sentiments in the aftermath of data breaches. By analyzing tweets related to the data breaches at Home Depot and JPMorgan Chase in 2014, the results suggest that five dimensions of organizational ISR are put into question: Risk and Resilience Structure; Security Ethics and Practices; Structures of Governance and Responsibility; Response Readiness; Social and Moral Benevolence. The attributions and sentiments vary for the five ISR dimensions. Moreover, tweets that attribute data breach responsibility carry more negative sentiments. This study makes an important theoretical contribution by identifying threats to ISR of organizations in social networks. The findings could benefit organizational strategies for social media reputation management and post-data breach intervention.

Keywords: Information Security Reputation; Reputation Threat; Data Breaches; Online Social Networks; Social Media Analytics

Introduction

Reputation in its ubiquitous usage has a very intuitive appeal to organizations. Management scholars recognize the potential of Online Social Networks (OSNs) to reflect and affect organization reputation and thereby influence perceptions and opinions of observers about the organization (Bampo et al. 2008; Rindova et al. 2007). The interpersonal exchanges in OSNs hold "informational value" over and above the messages communicated by organizations about themselves (Brown et al. 2007). Consequently, organizations are becoming increasingly concerned about their reputation in OSNs of how well the organizations meet stakeholder expectations (Jansen et al. 2009; Coombs 2007). Particularly, in times of crisis, OSNs increase the reputational threats for organizations substantially (Coombs 2007; Coombs and Holladay 2005; Deephouse 2000). For example, a recent survey by Freshfields Bruckhaus Deringer (2013), a law firm, shows that 28% of crises information spreads internationally within an hour and that failure to respond within 21 hours leaves an organization open to "trial on Twitter." Crisis leads jarring stakeholders attribute the responsibility to organization and thereby create negative Word of Mouth

(WOM) (Coombs 2007). A higher level of attribution of crisis responsibility decreases the reputation score of the organizations that face crisis.

There is potentially an endless list of reputation threats to organizations. In this study we are concerned about the threats to the *Information Security Reputation (ISR)* of organizations in the aftermath of a data breach. Research shows that a data breach represents the single biggest security risk to an organization's reputation (Merritt 2014). A data breach not only puts customer information at risk but also shakes the customer confidence in the organization's capability to protect information. Additionally, the recent surge of data breaches indicate that breach related news trends instantly in OSNs, providing an opportunity for individuals to share comments and opinions about the information security health of an organization. For example, after the big data breach at Target Corporation, which exposed records of millions of customers, the company faced huge public wrath, which resulted in a significant amount of negative WOM (Pinsker 2014). Currently, organizations lack mechanisms for managing online reputation in the event of data breaches. An organization could lose reputation abruptly if data breach is perceived as jarring by its stakeholders. Informed by Situational Crisis Communication Theory (SCCT) (Coombs 2007), we argue that, in order to contain threats to ISR, it is important to understand the emotional and behavioral responses of OSN users following a data breach. Consequently, this study answers the following two research questions:

RQ1: What dimensions of organizational Information Security Reputation (ISR) are discussed in Twitter postings following a data breach?

RQ2: What are the characteristics of responsibility-attributions and user-sentiments expressed in Twitter Postings related to ISR dimensions?

Using 16,200 tweets related to the data breaches at the Home Depot (Banjo and Yadron 2014) and JPMorgan Chase,(Glazer 2014) this study: (1) performs text analysis to identify the dimensions of an organization's Information Security Reputation (ISR), (2) statistically assesses the extent of attribution of data breach responsibility with respect to the identified ISR dimensions, and (3) summarizes the user-sentiments for the ISR dimensions and statistically tests the association between sentiments and attributions.

The remainder of this paper is organized as follows. Following this brief introduction, we present a review of the theory and literature that informs this research. Next, we discuss our research methodology – *social media data analytics*. The procedure for data collection and analysis of Twitter data set are presented. We present the findings corresponding to the different methods employed for identifying ISR dimensions, attributions, and sentiments. Next, we discuss the implications of the findings on theory and practice. The limitations of the study are also noted. Finally, the paper concludes by identifying future avenues for research.

Background Literature

In this section we present a review of the informing theory and literature.

Theory: Situational Crisis Communication Theory

A growing body of literature on crisis communication aims to understand the interrelationship between the crisis situation, stakeholder perception, and response strategies. Scholars argue that crisis impacts organizational reputation and post-crisis communication provides an opportunity to repair damaged reputation (Coombs and Holladay 2005; Coombs 2007). Coombs notes that crisis management requires evidence-based guidance to facilitate post-crisis communication and decision-making. To this effect, Situational Crisis Communication Theory (SCCT) provides a framework to help organizations strategize about crisis response and minimize reputation damage (Coombs 2007). The main tenets of SCCT are discussed in the following paragraphs.

Grounded in Attribution Theory (Weiner 1986), SCCT provides a rationale for stakeholder behavioral responses in the event of a crisis, which threatens organizations' reputation, and then prescribes strategies to prevent reputational damage. Stakeholders could become angry and an organization's reputation could suffer if they attribute the crisis responsibility to the organization. This attribution deters

stakeholder relationship with the organization and generates negative word of mouth. By understanding the crisis situation, crisis manager can assess the level of reputation threat i.e. the potential damage an organization's reputation could suffer in case no action is taken.

SCCT posits that one of the important factors that shapes reputational threat is initial crisis responsibility Crisis responsibility is defined as the extent to which stakeholders attribute damage caused by a crisis to the organization. Typically, stakeholders attribute different degrees of responsibility depending on the type and severity of the crisis (Coombs 2006; 2007). An increased level of attribution decreases the reputation score of organizations. Based on stakeholder attribution, SCCT identifies three crisis clusters: victim cluster, accidental cluster, and intentional cluster. In the case of victim cluster the organization is viewed as being a victim of the crisis and stakeholders thus attribute low responsibility to the organization. This includes mostly natural events such as natural disasters, violence or rumor. In the case of accidental cluster, the event is being viewed as uncontrollable or unintentional, and thus stakeholders attribute minimum responsibility of the crisis to the organization e.g., technical breakdowns. In the intentional cluster, the organization is viewed as having knowingly exposed people to risk, and thus stakeholders attribute a strong crisis responsibility to the organization e.g. misdeeds, human error.

Organization Reputation

Reputation is defined as the aggregate stakeholders' evaluation of how well an organization meets their expectations (Wartick 1992). Reputation is a valuable intangible asset of an organization (Hall 1993). Several factors shape organizational reputation such as: stakeholder interaction, information disseminated about the organization, and its actions (Fombrun 1996; Caudron 1997; Fombrun and Shanley 1990). Lange et al. (2011) argue that, "reputation is rooted in the organization's historical behavior and associations but can be abruptly changed if new information about the organization's past behavior comes to light or if the organization's latest behaviors or associations are jarring to observers" (pg. 154). Organizations build a positive reputation by demonstrating superior competence year after year (Hall 1993). Research shows that positive reputation attracts customers, retains top employee talent, earns the organization a competitive advantage, improves financial performance, and earns positive comments from analysts (see, Lange et al. 2011).

The most commonly used indicator for measuring organizations' reputation is the Fortune's "America's Most Admired Companies" rating. Since 1982, these ratings are published early every year based on the survey results of the previous year. Respondents, who include executives, directors, and analysts, rate the organizations on multiple attributes using a 10-point scale. A higher Fortune rating is desirable as research shows that it has a positive relation to stock market and accounting performance (McMillan and Joshi 1997; Roberts and Dowling 1997; Love and Kraatz 2009; Pfarrrer et al. 2010). However, as Deephouse (2000) reasons, Fortune ratings have three major weaknesses: 1) the ratings are highly correlated with the financial performance; 2), the respondents represent a limited set of stakeholders. Customers, employees, suppliers, and government agencies are not representative of the respondent sample; 3), Fortune ratings are only available for large U.S. based companies. Smaller companies and non-U.S. based companies are not rated. These weaknesses imply the need for an alternate mechanism to better understand organization reputation. Specifically, in times of crisis, such as data breaches that put customer information at risk, understanding an organization's reputation from a customer or a public perspective is important for ensuring business continuity and credibility.

Organizational crisis is defined as any unusual event that evokes a sense of threat to its high priority goals, image, legitimacy, profitability, or survival (Seeger et al. 2003). Crisis situations can potentially have many negative consequences, ranging from losing customers, profitability, and market share to declining stock prices and job losses. A much less explored, but very important factor, is the impact of crisis on organizational reputation. As crisis impacts stakeholders emotionally, physically, and financially, stakeholders think negatively of organization (Coombs 2007). Such negative thoughts about an organization inflict a possibility of reputation damage (Dowling 2002). Stakeholders assess organizational reputation based on the information that they learn about the crisis. The media and Internet play a critical role in reducing this information asymmetry. Stakeholders largely depend on news agencies and other intermediaries for the dissemination of information to stakeholders, and these thus play a "reputation-signaling role" (Deephouse 2000). If the perceptual reputation shifts to an unfavorable state, then

stakeholders exhibit a change in their behavioral responses to the organization and they spread a negative word of mouth about the organization (Coombs 2006).

Online Social Networks (OSN) and Word of Mouth (WOM)

Online Social Networking is a pervasive mechanism, which uses Web 2.0 technology to distill interactions among people (Asur and Huberman 2010). According to a report published by Pew Internet Project (2014), by Jan 2014, 74% of all Internet users used social networking sites, which represented a 32% increase since Sept 2013. Research shows that the diffusion of information in Online Social Networks (OSN), which is also referred as electronic Word of Mouth (eWOM), plays a central role from influencing product purchasing decision (Brown et al. 2007) to shaping nations (Howard et al. 2011). Traditional communication theorists consider informal WOM to exhibit powerful influence on individual behavior with regard to information searching, evaluating, and subsequent decision-making (Brown and Reingen 1987; Silverman 2001). Through multiple exchanges, particularly in online social networks, eWOM can reach and shape behaviors of individuals at a much larger magnitude than by offline WOM. From an economic perspective, WOM involves sharing information, opinions and reactions about products and services with network associates (Jansen et al. 2009). Brown et al. (2007) argue that such interpersonal exchanges hold "informational value" over and above the messages communicated by the organizations about themselves, and thus exert a powerful influence in shaping recipient opinions and subsequent decision-making. Moreover, research indicates that people trust the disinterested opinions of individuals beyond their immediate social networks (Duana et al. 2008).

Although a number of social networking sites have emerged overtime, we are particularly interested in the most popular microblogging site -Twitter- for its efficacy in generating large-scale eWOM (Jansen et al. 2009). Twitter allows users to post short messages up to 140 characters, which are referred to as tweets. Twitter deserves serious research attention on account of its usefulness during crisis situations (see, Vieweg et al. 2010; Acar and Muraki 2011). The efficacy of Twitter in disseminating information in times of disasters has led to its ubiquitous use in crisis management. It is increasingly being used both as a communication tool during emergency situations and also as a medium to collect information about the crisis situation- situational awareness (Vieweg et al. 2010). In times of organizational crisis, the diffusion or propagation of crisis information has unique implications for an organization's reputation. Twitter has several features, which makes it indispensable for eWOM communication (Jansen et al. 2009). Users create a social network by "following" other users, or by allowing other users to "follow" them. It is by the virtue of "follower-followee" network that information in online social networks spread beyond geographic borders. Moreover, unlike online reviews and similar to news headlines, the short length of tweets make them easier to consume and re(produce). Furthermore, messages can be asynchronously noninvasive as individuals can decide whom to receive tweets from and when to check their tweets. Finally, tweets are archived and are searchable by web engines.

Social Media Data Analysis and Findings

This study theorizes about the ISR threats perceived in the content generated in OSNs in the aftermath of a data breach. Therefore, we are interested in Twitter postings that are posted after the announcement of data breaches. We deployed R-Hadoop integrated environment to collect, cleanse, transform, and analyse the data (Das et al. 2010). We collected the tweets published on Twitter's public message board using twitteR package available in the R library. The twitteR package provides an interface to connect to the Twitter's Search API (Gentry 2013). We searched for relevant tweets using hashtags. Twitter uses the # character appended to a word or phrase to relate the tweets by a common theme or topic e.g. #HDBreach #ChaseHack.

We collected the tweets immediately after the data breach had been announced. The first data set is related to the Home Depot breach, covering a period from Sept 8, 2014 to Oct 30, 2014. The second data set is related to the JPMorgan Chase breach, spanning the four weeks from Oct 3, 2014 to Oct 31, 2014. We collected a total of 39,416 tweets related to the Home Depot and the JP Morgan data breaches. We used Hive queries to remove redundant tweets i.e. tweets with identical Twitter ID, Text, and Tweet Create timestamp. This reduced the number of tweets to 29, 247. The data set is further pruned by deleting irrelevant tweets i.e. tweets that do not discuss anything related to data breaches. We identified such tweets by first listing the most frequent words in the tweet corpus. We used the text mining package

tm to identify words that occur at least 50 times. A quick glance at words allowed us to identify irrelevant words, examples being: #sweepstakes, #letsgogameday, etc. This allowed us to rule out the all tweets corresponding to these keywords, which further reduced the final number of tweets to 16,200.

To answer the two research questions, multiple methods were employed for the analysis of tweets. A brief description of the methods and the corresponding findings follows.

Topic Modeling

Given the large size and unstructured form of tweet postings, the manual annotation of tweet corpus is impossible due to the limited human cognition and time. Twitter postings are unstructured natural language text. Natural language is considered unstructured information, as humans bend the linguistic utterances for communicative and creative needs (Manning and Schütze 1999). Moreover, as the size of text grows, it becomes increasingly difficult to identify the structure or pattern of the content (Blei 2012). To overcome the difficulty of analyzing large text corpuses, machine-learning researchers developed a suite of algorithms known as probabilistic topic modeling (Blei et al. 2003). Probabilistic modeling techniques are statistical approaches for analyzing the text documents to discover and annotate words around the thematic pattern. The advantage of topic modeling is that users are not required to pre-annotate the documents, as the technique is able to identify the themes – referred to as topics – that emerge from the text. Topic modeling techniques generate semantically coherent and interpretable topics by enumerating most probable words corresponding to each topic Furthermore, topic modeling techniques are well designed to account for synonymy (words with a similar meaning) and polysemy (words with multiple meanings) (Mimno and McCallum 2007; Mimno et al. 2007).

Although several topic-modeling approaches are available, this study employed the Latent Dirichlet Allocation (LDA) (Blei et al. 2003; Blei 2012) technique to identify the dimensions of ISR discussed in eWOM. LDA has many advantages over other topic modeling techniques (see, Uys et al. 2008) and it is widely used to leverage the value from unstructured information. Moreover, LDA is known to information systems researchers (e.g. Alfaro et al. 2013; Blei 2012) and has also been applied in the context of Twitter (e.g. Zhao et al. 2011). LDA treats each document as a "bag of words" without considering the order of occurrence. It then identifies a set of words -"stop words"- which have no significance in identifying topics such as a, an, the, etc. Next, it creates a corpus by extracting a set of meaningful words and eliminating stop words. In doing so, the model maintains a reference directory of each word with respect to its document and also the frequency of word occurrence. Based on the number of topics specified by the user, the LDA model generates the number of topics by associating words with one or more topics with a certain probability. The model then returns a topic-word matrix, which presents the topics with the associated words. The user inspects each topic and then provides a descriptive label by evaluating the words associated to each topic.

The R package *topicmodels*, which is available in R library, is used for fitting topics (Hornik and Grun 2011). With respect to our data set, LDA treated each tweet as a single document. LDA was run multiple times by varying the number of topics to be generated. The algorithm was run for 15, 25, 50, 75, and 100 topics. However, given that tweets are short in length, the model with 15 topics was chosen. Other researchers have acknowledged such difficulties with Twitter data set as well (e.g. Uys et al. 2008). Furthermore, the 15 topics were highly discriminant and were easy to interpret. Next, the words under each topic were systematically analyzed and the topics were labeled. The topics were grouped by common higher-level theme, referred to as topic category.

Findings

The topic model discriminates among 15 different topics. As part of our analysis, 15 topics were collapsed into seven categories. Table 1 lists the topics, corresponding top 8 words that describe each topic, and the resultant seven topic categories.

Latent Dirichlet Allocation (LDA) Results		
Topic Words	Topic	Topic Category
cyberattack, hacker, new, hit, attack, data, card,	Announce Data	Situational

cripple	Breach	Awareness
hit, million, infiltrate, steps, security, malware, password, vulnerable	Security Failure Reasons	
million, data, expose, need, know, people, hack, system	Loss of Customer Data	Catastrophic Implications
breach, confirm, affect, household, biggest, among, historic, data	Magnitude of Breach	
mandiant, attack, fireeye, data, companies, new, report, say	Prospective Measures	Preventive Means
card, take, today, cybertatack, charges, protect, thank, replace	Post Breach Measures	
help, hacker, free, stop, look, plan, new, world	Seeking Attention	Future Assurance
encourage, shoplocal, never, scary, help, safeguard, BeResponsible, cost	Recommending Alternatives	
spied, china, alleged, behind, cyberattack, hacker, unit, official	Accusations	Negative Word-of-Mouth
protect, fraud, worse, breach jpmorganchase, upset, decline, notify	Abysmal comments	
hack, indict, official, data, custom, report, hacker, make	Demanding Indictment	Social Justice
life, sentence, serious, proposed, speech, cyberattack, year, hacker	Suitable Punishment	
protect, members, heck, statements, aware, attention, account, scams	Raising Attention	Moral Responsibility
Priority, free, monitor, cover, prevent, fraud, not, jpmorganchase	Empathizing Victims	
cyberattack, hacker, new, hit, attack, data, card, cripple	Announce Data Breach	

Table 1. Topics and Categories

The first category, *Situational Awareness*, provides general information about the data breaches. The corresponding topics announce the breach (e.g. new, hit, cripple) and inform users about the potential causes of the data breach (e.g. malware, weak password). The second category, *Catastrophic Implications,* discusses the repercussions of the data breaches in terms of loss of customer data (hack, exposed, millions) and magnitude of breach (e.g. biggest, affect, household, historic). The third category, *Preventive Means,* provides information about the proactive and reactive measures which are employed to prevent the data breach. The topics include prospective measures that could potentially prevent future data breaches (e.g. mandiant, fireeye) and post breach measures that would minimize the data breach affect (e.g. card replace, today). The fourth topic category, *Future Assurance,* includes the topics that seek attention for the need to implement robust information security measures (e.g. help, hackerfree, world) and recommend alternatives for information assurance (encourage, shoplocal, safeguard). The fifth category, *Negative Word-of-Mouth,* involves topics that express anger and frustration. Topics include accusations for being responsible for the data breach (e.g. China, spied, behind) and abysmal and derogatory tweets about the organizations (JPMorgan, fraud, worse, headline). The sixth category demands *Social Justice*. Topics discuss the need for indictment (e.g. indict, hacker) and punishment (e.g. life, sentence, hacker). Finally, the seventh category, *Moral Responsibility,* includes topics that raise a voice against the event, thus demanding the organization's attention to the situation (protect, members, heck) and that offer information to victims (e.g. free, monitor, prevent). To validate the topic model, we conducted a content analysis of a random sub-sample of tweets. The approach to content analysis is discussed in the following subsection.

Content Analysis: Grounded Theory Approach

To complement the results of LDA, a content analysis of tweet postings was performed using grounded theory methodology (Strauss and Corbin 1988). Urquhart et al. (2010) provide guidelines for conducting and evaluating grounded theory-based research in information systems. The process starts with the researcher's initial hunches, which informs the area of inquiry or the substantive area. Following this, the researcher extracts initial slices of data and then defines conceptual categories as the first elements of grounded theory. The properties for initial categories are defined as well. Next, the researcher makes use of additional data slices and further conceptualizes the categories and constructs by establishing relationships between them. This process of constant comparison with previous data continues until no new categories, constructs or relationships are identified. The saturated concepts are then reduced to the relationship between core categories, which leads to the formulation of grounded theory.

We selected a random 20% sub-sample of tweets (3,240 tweets) that were analyzed previously by the topic modeling technique. Following the Grounded Theory's inductive approach to category and thematic development, the tweet posting were read several times, while being informed by the research question: *What dimensions of organizational information security reputation are discussed in Twitter postings following a data breach?* The categories and themes emerged through constant comparison and iterative conceptualization.

Findings

The summary of the content analysis is presented in Table 2. The five higher-level Information Security Reputation (ISR) dimensions that emerged from the data analysis are: *Risk and Resilience Structure; Security Ethics and Practices; Structures of Governance and Responsibility; Response Readiness;* and *Social and Moral Benevolence.* In the following paragraphs, the five dimensions are discussed. The existing literature complementing the findings along with the exemplar tweets are also discussed. Finally, for each ISR dimension, the topic categories identified by LDA algorithm are related.

Content Analysis Results		
First-Order Codes	Second-Order Themes	Aggregate ISR Dimension
Inadequate Protective Controls; Security Measures shortfall; Lack of Adopting Resilient Means to Safeguard Customers; Lack of Focus on Protecting Customer Data	Lack of Robust Security Controls to Safeguard Customer Data	Risk and Resilience Structure
High Magnitude of Impact; Too Big to Fail; Large Scale Vulnerability	Capability of Causing Catastrophic Damage	
Concern for Victimization of Customers; Expressing Discontent Through Angry Messages; Expressing Worry About Implications; Disappointed Customers about Organizations doing	Concerns about Organization's Role in Victimizing Customers	
Suspecting Engagement in Unethical Business Practices; Suspecting Company's Intentions	Suspicions About Company's Ethics and Intentions	Security Ethics and Practices
Speculating Recovery to Pre-Crisis Stage; Distrust in improvisation Strategies; Negative Perceptions about Future Credibility of the organization	Lack of Trust in Company's credibility	
Poor Post-Crisis Response; Distorted Information About the Event; Discontented With Post Crisis Response; Delayed Acknowledgement of being Responsible for Crisis	Discontentment about Post-Crisis Response Strategy	
Legal intervention into Crisis; Agencies Warning Customer of implications; Regulatory Litigations	Seeking Corporate	Structures of

	Regulation Through Litigation	Governance and Responsibility
Competitors Assuring Better Services; Competitor Targeting	Competitors Leverage the Crisis Situation	
Adverse Self-Protection Measures; Secondary Identity Monitoring Services; Customers Applauding Secondary Responders; Calling for Action Against Organization	Resort to Alternate Means of Safeguarding	Response Readiness
Seeking Attribution Information; Instructing Information About the Crisis; Seeking Assurance for Recovery	Instructing Attribution Information for Assurance	
Negative Future Benchmarking; Derogatory Comparisons; Associating Market Trends to the Crisis	Social Irresponsibility of Company	Social and Moral Benevolence
Spreading Unsubstantiated Information; Mocking Behavior Towards the Crisis Situation	Posting Unsubstantial Negative Remarks	

Table 2. Dimensions of Information Security Reputation (ISR)

Risk and Resilience Structure

Corporate risk and resiliency planning is important for organizations to be able to bounce back from disruptions and thus retain stakeholder confidence. Research suggests that a resilient and secure business environment is a key in neo-liberal economy (e.g. Greenburg et al. 2007) and that it earns a competitive advantage (Sheffi 2005). Understanding and identifying potential adverse events in computerized networks is important for planning and implementing resilient mechanisms to defend, detect, and remediate from such threats (Sterbenz et al. 2010). Past research suggests that an exclusive focus on technological solutions doesn't provide secure information security, however (Dhillon and Backhouse 2001; Siponen 2005). The risk reduces when organizations implement both resilient technical and socio-organizational mechanisms. The need to integrate risk and resilience mechanisms into the organizational culture to prevent security breaches is well echoed in Twitter postings. Our findings indicate that there is a concern about the absence of resilient security controls in organizations to protect customer data. The lack of implementation of adequate measures by organizations increases the risk of the victimization of customers. The topic mining results describe this dimension with the following two categories: Situational Awareness and Catastrophic Implications. Some example tweets which describe this dimension include:

> *Ex-Employees Say Home Depot Left Data Vulnerable; Lets face it: most banks have IT systems from XIX century. I'm sure we'll hear about more stories; JPMorganChase #hackers got into system through 1 weak password. Stole info on 76million US customers millions of data stolen from #target; #homedepot Even the pentagon's info isn't safe.*

Security Ethics and Practices

The ethical conundrum about the use of computers and information technology has long been a subject of research. To minimize the liability in the modern litigious society, organizations must thoroughly understand the legal and ethical obligations. The significance of ethical security practices has been repeatedly emphasized in research. For example, Dhillon and Backhouse (2001) aspire that organization's members would behave ethically in both foreseen and unforeseen situations. A large body of research acknowledges a "knowing-doing" gap in human behavior as a cause of information security contraventions (e.g. see Workman et al. 2008). Amongst others, situational ethics is proposed as a behavioral intervention technique for addressing the "knowing-doing" gap (Hsu and Kuo 2003; Kurland 1995). However, in times of data breach, the relationship between ethics and breach management gets complicated. Data breaches might generate a wrongdoing especially if the organizations want to be quiet about the event. For example, a Google Apps bug leaked data of 280,000 users in 2013, and yet the leak was first revealed in a blog post by researchers from Cisco (Lumb 2015). One could perceive Google's behavior in this instance as being ethically poor whereas Cisco's whistleblowing behavior could be regarded as ethically laudable behavior. Along similar lines, the findings highlight suspicions about the

ethical practices of the organizations that face security breaches. Tweets indicate a "knowing-doing" gap in organization's practices, as users express suspicions and a lack of trust about the actions and credibility of the organizations in question. The topic modeling results describe this dimension with the Negative Word-of-Mouth topic category. Tweets that question security ethics and practices of the organizations include:

> *Something's Wrong With Home Depot's Explanation of the Hack; A better statement from Home Depot would've been "We can't confirm PINs were compromised," not "there is no evidence."; The attack was under way for a month before it was discovered in July. Concerning but not surprising.. home depot knew of its security flaws 6 years ago*

Structures of Governance and Responsibility

Successful information security governance requires the consideration of several aspects. Amongst many, information security governance requires the consideration of dimensions that involve the organization, policy, best practices, ethics, legality, personnel, technical, compliance, auditing, and awareness (Solms and Solms 2004). The evolving legal systems around the world have increased the responsibility of corporate managers to ensure the governance of information security assets. Moreover, heavy corporate and personal liabilities have made corporate governance responsibility absolutely essential. In the existing literature, weak governance has been cited as a cause for organizational crisis e.g., the impact of corporate governance on the financial crisis (Mitton 2002), whereas strong governance during crisis can earn rewards, e.g. it impacts firm profitability in time of economic crisis (Joh 2003). Our findings emphasize the need for accountability and governance structure to ensure security of data. With respect to the topic modeling results, the following topic categories describe this dimension: Social Justice and Future Assurance. Tweets indicate that, on the one hand, customers voice the need for regulating data protection mechanisms and competitors, yet on the other hand, they exploit the weak governance structure of the breached organization to their advantage. Some of the exemplary tweets that reflect ineffective information security governance and responsibility mention the following:

> *the security breach at #jpmorgan shows why #bitcoin is preferred; its security model is decentralized; community banks absorb #databreach costs upfront primary concern is to protect their custmrs from fraud; databreach costs should ultimately be borne by the party that experiences the breach; most security software companies focus on worms, mandiant focuses on detecting chinese espionage.*

Response Readiness

With the increasing sophistication of information security attacks, organizations feel pressurized to mitigate and plan for future threats. Given the sophistication of intrusions, forensic investigations are usually reactive and the organizations have to develop custom solutions for each case (Casey 2006). Forensic investigators have to be equipped with the right tools and skills to be able to analyze the information for finding the potential evidence and the cause and effect. Despite these difficulties, Casey (2006) argues for the integration of forensic principles into security tools, training, and techniques for intelligence gathering to determine when and how the intruders breached the computer system, to appraise what sensitive information was exposed, the intruder's intent, and then possibly being able to apprehend or mitigate future intrusions. The data analysis suggests that social media users are concerned about the effectiveness of organizations in terms of its post breach response capabilities, processes, and tools. Crisis creates a need for information, therefore it is in the interest of organization's reputation to initiate the communication and address the physical and psychological concerns of the stakeholders (Coombs 2007). The data suggests that the organizations with a passive response strategy cause panic as victims try to seek resources and information to protect themselves after the crisis announcement. Moreover, dissatisfaction about post breach response from the organization is common. The corresponding topic-modeling category that complements this dimension is Preventive Means. A few of the tweets that infer ineffective response strategy are:

> *I was about to be the first card printed on a new machine ... But it jammed; How Home Depot breach could have been avoided: hear from the experts!; should banks reissue your card or just closely monitor it after a breach?*

Social and Moral Benevolence

Unlike security ethics and practices, this dimension demeans the moral traits of the breached organization. In the literature, social and moral benevolence is equated with philanthropic responsibilities. For example, Carroll (1991) differentiates philanthropic responsibility from ethical responsibility, in that the former is a discretionary or voluntary act, such as donating resources for humanitarian reasons or being a good corporate citizen. Benevolent behavior is highly prized and rewarded; however, organizations will not be regarded unethical if they do not commit the necessary resources for benevolence. In normative language, beneficence refers to the moral obligation of acting in favor of others for the advancement of their legitimate and important interests, usually by preventing possible harm. While beneficence refers to action, benevolence refers to the moral trait of acting in favor of others. Crisis changes the perceptions of stakeholders towards the benevolent or philanthropic responsibilities of the organization. The distortion of corporate image by questioning the benevolent trait of organizations to protect customer data and to prevent the harm is a threat to ISR. Our topic modeling results describe this dimension with the Moral Responsibility category. A few of the Tweets in this category that criticize company's capability and social responsibility are:

> *anyone still banking with #jpmorgan #chase deserves no protection. #stop #banking with a #criminal; why ever pay for credit monitoring? just wait for the next place you shop at to have to give it to you free; Thanks #HomeDepot for the #homedepotbreach. You owe me a weekend's worth of lost frequent flier miles! And the hour spent reporting fraud!; are we becoming numb to data breaches? #homedepot*

Tweet Annotation Methodology

The growing popularity of social media content has triggered a flurry of research in social media linguistic analysis. However, the majority of standard linguistic tools perform poorly, as tools have to be trained for a particular data set and context (Finin et al. 2010). Specifically, the conversational nature of tweets coupled with the lack of orthography and character limitation, poses additional challenges to utilize the traditional Treebank approach, such as Wall street journal corpus to tag Twitter data (Gimpel et al. 2011; Owoputi et al. 2013). For these reasons, NLP researchers recommend tagging the data manually which could be later used to train the models. Given that the data breaches represent a unique context and that no automated tagger is suitable to annotate such tweets, a semi-automated linguistic analysis of the Twitter data set was conducted. The approach is described as follows.

Firstly, the tweet text was analyzed to classify corresponding tweets into five ISR dimensions. A database column 'ISR' was created and populated using Hive queries. The Hive queries searched for tweets by topic words using the findings from topic modeling and content analysis phases. Tweets that do not fall into any of the categories were then labeled as 'NA.' To validate the results of automated annotation, 1% of random sub-sample of tweets was manually coded. We had 94% agreement for ISR dimensions.

Secondly, the annotation identifies the tweets that indicate the attribution of data breach responsibility and correspondingly we updated the 'attribution' column to 'True' or 'False'. To accomplish this, the tweet corpus was generated i.e. the collection of tweet text. The *tm* package available in the R library was used to transform and analyze the tweet corpus (Hornik 2014). The transformation involves converting tweet text to lower case, removing numbers, punctuations, stop words, and URLs, stripping whitespaces, and stemming and identifying synonyms. The *tm* package provides a set of functions to perform these transformations. Next the Document-Term Matrix (DTM) was created i.e. a matrix with documents as rows, terms as columns, and the frequency of terms as the value of each cell of the matrix. In the case of a Twitter dataset, each tweet was treated as a document and the words in each tweet were treated as terms. The DTM had 16,200 documents with 8,821 terms. Finally, an ordered list of terms by frequency was obtained to identify the most frequent and least frequent terms. The threshold for least frequent terms was set as 50, i.e. a word occurs at least 50 times in the tweet corpus. Using the set threshold, we found 465 terms that occur less than 50 times. Upon close examinations, 13 terms indicating the attribution of breach responsibility were annotated and the rest of the "infrequent" terms are then ignored from further analysis.

Following the Part-Of-Speech (POS) tagging approach proposed by Gimpel et al. (2011), the remaining frequent terms were manually analyzed to identify words that indicate the attribution of data breach responsibility. A total of 308 such attribution terms were found. The attribution column is populated using Hive queries to 'True' or 'False' depending on the presence of these terms. To test for the accuracy of

the approach, 25% of random tweets from the corpus were manually annotated. The accuracy of attribution responsibility for the complete data set is 98.7%.

Findings

The five ISR dimensions trigger a varying amount of tweets (see Table 3). A significantly higher proportion of tweets (62%) discuss the Security Ethics and Practices of the organizations, followed by the Risk and Resilience Structure (23%) and Social and Moral Benevolence (13%). In comparison a lower proportion of tweets are related to Structures of Governance and Responsibility (2%) and Response Readiness (1%).

Table 3 describes the frequencies of the tweets for five ISR dimensions and the corresponding proportion of attributions. Data breach attribution responsibility classifies a tweet into True/False, depending on whether the author attributes data breach responsibility to the organization. Overall, 48% (7,778) tweets attribute the data breach responsibility to the organizations. The highest number of attributions is for Risk and Resilience Structure (63%), whereas the lowest attributions are for Social and Moral Benevolence (37%). Furthermore, a Chi-square test of independence determines whether the proportion of attribution is different for the five ISR dimensions. The results suggest that the attribution proportion significantly varies with respect to ISR dimensions. The overall sample has a chi-square value of 448.602 with four 4 degrees of freedom giving a p-value < 2.2e-16.

Furthermore, post-hoc analysis using a Chi-square test of each pairwise comparison of ISR dimension tests for the exact difference among ISR dimensions. Table 4 summarizes the results. As there are ten comparisons, the Bonferroni-adjusted p-value needed for significance is 0.05/10, or 0.005. Only six of the ten comparisons are significant. The p-value for Risk and Resilience Structure vs. all other dimensions is significant, which indicates that there are significantly more cases of attribution for Risk and Resilience than any other dimension. Also, the p-values for Security Ethics and Practices and Structures of Governance and Responsibility are significant, which indicates that there are more attribution cases for these categories in comparison to Social and Moral Benevolence.

ISR Dimensions	**Attributions**		
	True (%)	False (%)	Total (%)
Risk and Resilience Structure	2291 (63)	1364 (37)	3,655(23)
Security Ethics and Practices	4508 (45)	5512 (55)	10,020(62)
Structures of Governance and Responsibility	164 (47)	187 (53)	351(2)
Response Readiness	57 (39)	89 (61)	146(1)
Social and Moral Benevolence	758 (37)	1270 (63)	2,028(13)
Total	7778 (48)	8422(52)	16,200(100)
Pearson's Chi-squared = 448.602, df =4, p-value < 0.000			

Table 3. Frequency of attributions for ISR dimensions

ISR Dimensions	**Chi-square**	**P value**
Risk & Resilience Structure vs. Security Ethics and Practices	334.581	0.000*
Risk & Resilience Structure vs. Structures of Governance & Responsibility	33.701	0.000*
Risk & Resilience Structure vs. Response Readiness	32.232	0.000*
Risk & Resilience Structure vs. Social & Moral Benevolence	334.842	0.000*
Security Ethics & Practices vs. Structures of Governance & Responsibility	0.345	0.557
Security Ethics & Practices vs. Response Readiness	1.825	0.177
Security Ethics & Practices vs. Social & Moral Benevolence	39.425	0.000*
Structures of Governance & Responsibility vs. Response Readiness	2.163	0.141
Structures of Governance & Responsibility vs. Social & Moral Benevolence	10.623	0.001*
Response Readiness vs. Social & Moral Benevolence	0.098	0.755
**Significant at 0.05 level*		

Table 4. Post-hoc Analysis for ISR dimensions

Besides attributing breach responsibility, an organization perceives reputation threat if a tweet expresses negative sentiment. Our approach to conduct sentiment analysis of the tweets is described in the following sub-section.

Sentiment Analysis

Sentiment analysis also known as opinion mining represents a systematic approach to analyze the author's opinions, emotions, evaluations, attitudes, and behavior towards a particular subject or its characteristics (Liu 2012). Although several general-purpose sentiment analysis algorithms have been constructed, understanding the context and domain specific sentiments remains a big challenge (Liu 2012). Since reputation threat in the event of a data breach represents a unique context, we decided to use Jeffrey Breen's approach for sentiment analysis (Breen 2012). Breen's logic has been used successfully in few recent studies (e.g. Chung and Liu 2011; Ramagopalan et al. 2014). Breen approach requires a list of positive and negative words to calculate sentiment valence and to classify tweets as being positive, negative or neutral. We used the opinion lexicon in English with 2,006 positive words and 4,783 negative (Hu and Liu 2014). Furthermore, following Breen, the lexicon was enhanced with the domain specific words. The words analyzed using *tm* package previously were added to positive or negative word lists.

The sentiment valence was calculated by first subtracting the number of positive words from the number of negative words and then determining tweet valence based on score. If the sentiment score is > 0, then the tweet expresses an overall 'positive opinion; if the sentiment score is < 0, then the tweet expresses an overall 'negative opinion', if the sentiment score=0, then the tweet is considered to be a 'neutral opinion'. To ensure that the algorithm returned correct results, 250 tweets were manually coded using Breen's approach. The results of this manual coding were compared with those of the automated approach. The intercoder agreement between the manual and algorithmic coding is quite high (93.04%).

Findings

Results show that 32% of tweets (5,138) have neutral sentiment or mixed sentiment (see, Table 5). This indicates that people use Twitter to seek or share situational awareness during data breach incidents (e.g. Vieweg et al. 2010). 56% of tweets (9,007) express negative sentiment. This is inline with the previous argument that crisis situation generate large scale negative WOM (Coombs and Holladay 2007). In addition to overall sentiment, a detailed analysis of sentiments with respect to five ISR dimensions is presented in Table 5. Overall there is more negative sentiment followed by neutral sentiment for all the five ISR dimensions. Out of 3,655 tweets discussing Risk and Resilience Structure 77% of tweets (2,803) exhibit negative sentiment. This is followed by Response Readiness and Structures of Governance and Responsibility, where 60% and 53% of tweets express negative sentiment respectively. Finally, 50% tweets related to Security Ethics and Practices, and 47% tweets related to Social and Moral Benevolence have negative sentiment.

Finally, we analyzed the sentiments for the tweets that attribute breach responsibility. As shown in Table 6, tweets that attribute organizational responsibility have more negative sentiment (54%), whereas tweets that do not attribute responsibility to organizations have more positive sentiment (62%). At both levels of attribution, neutral sentiment is comparatively greater than negative sentiment (attribution is true) and positive sentiment (attribution is false). Furthermore, to statistically test the association between the attribution of data breach responsibility and negative sentiments, a Chi-square test of independence is performed. At the significance level of 0.05, the Pearson Chi-square is 344.45 with 2 degrees of freedom and a p-value of 2.2e-16. The p-value is highly significant, and therefore the null hypothesis is rejected. This is followed up with post-hoc analysis to determine the comparative differences of sentiments. Because there are three comparisons, the Bonferroni-adjusted p-value needed for significance is 0.05/3 or 0.016. Results show that there are significantly more cases of attribution in those tweets that express negative sentiment than those tweets that express positive sentiment or neutral (see, Table 7).

ISR Dimensions	Tweets (%)	Positive (%)	Negative (%)	Neutral (%)
Risk and Resilience Structure	3,655(23)	289(8)	2,803(77)	563(15)
Security Ethics and Practices	10,020(62)	1,293(13)	4,984(50)	3,743(37)
Structures of Governance & Responsibility	351(2)	59(17)	185(53)	107(30)
Response Readiness	146(1)	17(12)	87(60)	42(29)
Social and Moral Benevolence	2,028(13)	397(20)	948(47)	683(34)
Total	16,200(100)	2,055(13)	9,007(56)	5,138(32)

Table 5. Sentiment Analysis of ISR dimensions

Attribution	Positive (%)	Negative (%)	Neutral (%)
True	785 (38)	4908 (54)	2085 (41)
False	1270 (62)	4099 (46)	3053 (59)
Total	2055 (13)	9077 (56)	5138 (32)
Chi-square=344.443, df=2, P <0.000			

Table 6. Sentiment Analysis for Attribution Tweets

	Chi-square	p-value
Negative vs. Positive	177.1394	<0.000*
Negative vs. Neutral	252.7235	<0.000*
Positive vs. Neutral	3.3702	0.06638

Table 7. Post-hoc Analysis for Sentiments and Attributions

Discussion

Using the exploratory analysis of Twitter postings, this study identifies five major dimensions of Information Security Reputation (ISR). To the best of our knowledge, this is the first study of its kind to examine Twitter postings for threats to information security reputation of organizations. The findings suggest that the relative number of tweets vary in an orderly manner, with most of the tweets resonating with Security Ethics and Practices, followed by Risk and Resilience Structure, Social and Moral Benevolence, Structures of Governance and Responsibility, and Response Readiness. The results show that there are more negative sentiments in the tweets. This is consistent with the literature, which argues that important events are associated with negative sentiments (Thelwall et al. 2011). Furthermore, the higher percentage of neutral sentiments is consistent with the previous literature, which argues that a large number of tweets in time of crisis situations are related to situational awareness (Vieweg et al. 2010). The attribution of data breach responsibility is considerable, although not shocking; however, the varying amount of attributions for the five ISR dimensions indicates the varying importance of the dimensions. Finally, there are significantly more cases of data breach responsibility attribution in tweets that express negative sentiment, than in the tweets that express positive or neutral sentiments.

This study makes an important theoretical contribution to the understanding of reputational threats to the perceptions of organizational effectiveness in the social media discourse. The perceptions of stakeholders about an organization are an important aspect of organizational identity (Brown et al. 2007). A positive external identity, i.e. reputation possesses institutionalization qualities, which keeps stakeholder groups believing that an organization is risk-averse, trustworthy, and safe. The findings from this study suggest that the secure management of information systems is crucially important for maintaining the reputation of a secure organization. One of the main contributions of this research is the identification of the constructs for the secure organizational reputation and also the mechanisms that could threaten such a reputation. Furthermore, the attribution of breach responsibility coupled with emotional arousal in social media intensify the reputation threats Overall, the findings indicate that information security reputation management involves three aspects: 1) the five dimensions of ISR define the measures for safeguarding consumer data. The findings corroborate the calls made by researchers and practitioners that security cannot be achieved just by technological controls and that it should encompass people, processes and technology (see, Hamill et al. 2005; Dhillon and Backhouse 2001); 2) the

humiliations in the social media chat presents a new threat to the information security reputation of organizations. The attribution of breach responsibility and the diffusion of those attributions in social networks define an additional dimension of information security management; 3) in light of the above findings, information security reputation management requires pre-breach and post-breach planning. Much of the literature to date focuses on proactive planning as a means for preventing security incidents. However, a robust organization requires a plan for post data breach as well. For example, the data analysis shows that while risk and resilience has to be established to prevent data breaches, response readiness determines the preparedness of an organization to respond to customer concerns and to take preventive measures. Finally, this study shows that information security planning requires an outward focus. Furthermore, the negative sentiments and attributions prevalent in OSN chat present a new challenge for information security planning.

This study provides practical insights about the aspects of ISR to be managed in OSNs. As the content of the Twitter postings convey information about whether the breach responsibility is attributed to the organizations, the crisis manger can summarize the Twitter postings with respect to ISR dimensions and quantify the levels of attributions. Moreover, the crisis manager can quantify the associated sentiments of reputation threatening tweets. Having such information will allow a crisis manager to assess the reputation threat and adequately prepare and communicate post breach response for managing reputation of a secure and trustworthy organization.

The Twitter postings allow researchers to observe and analyze the real behavior in response to data breach events. The data collected for the Home Depot and JPMorgan Chase account for a certain degree of replication. The theoretical saturation achieved in the process of iterations between data and concepts generalized the pattern across the organizations being studied. Moreover, the generalizability of the emergent theory increases by linking the resultant grounded theory with the existing theories from literature. However, as Lee (1989, p. 41) mentions that, "…theory concerning MIS would be generalizable to other settings only on the basis of actually being confirmed by additional case studies that test it against the empirical circumstances of other settings." Thus the empirical validation and elaboration of the findings of this study in other settings is needed. Specifically, the reputation dimensions and their characteristics in other OSNs and crisis instances need to be tested and elaborated. Another limitation of this study is that the Twitter data set represents a snapshot of the public's opinion and behavioral responses. Although data collection was stopped once the new codes did not reveal any new information, the full range of tweets could serve to increase the rigor. However as a word of caution, increasing the number of predictions, propositions, consequents, competing theories and/or environmental settings can make the research unnecessarily rigorous. As Lee (1989) argues conformance to scientific methods ensures the adequate rigor, beyond which further rigor if pursued can be called into question.

Conclusion

In this research we examined threats to the reputation of organizations that face data breaches. Using multiple data analytical approaches this study sheds light on the threats resulting from the negative WOM characteristically generated in the event of a data breach. This negative communication is detrimental for organizations, as it influences the opinions and behavior of people. Consequently, a response strategy to counteract negative communication about the organizations is an interesting opportunity that needs to be explored.

The essence of online reputation management is to know what is being said about the organization in electronic WOM communications. The availability of online social networks, coupled with the innovations in data analytical technology, provides a great opportunity for organizations to assess their reputation as perceived by stakeholders outside the organization. Whilst this study provides initial insights about threats to the reputation of an organization, a logical question, which arises, is how to manage online reputation. Among many possibilities for future research, it will be interesting to prescribe the strategy to managing the reputation of organizations that face data breaches. More specifically, we plan to apply decision analysis techniques to assess the significance of various alternatives for managing reputation risks in online social networks.

References

Acar, A., and Muraki, Y. 2011. "Twitter for crisis communication: lessons learned from Japan's tsunami disaster," *International Journal of Web Based Communities* (7:3), pp. 392-402.

Alfaro, I., Bhattacharyya, S., and Watson-Manheim, M. B. 2013. "Organizational Adoption Of Social Media In The Usa: A Mixed Method Approach," in *Proceedings of the 21st European Conference of Information Systems*.

Asur, S., and Huberman, B. A. 2010. "Predicting the future with social media," in *Web Intelligence and Intelligent Agent Technology (WI-IAT),* International Conference on IEEE/WIC/ACM, pp. 492-499. IEEE.

Bampo, M., Ewing, M. T., Mather, D. R., Stewart, D., and Wallace, M. 2008. "The effects of the social structure of digital networks on viral marketing performance," *Information Systems Research* (*19*:3), pp. 273-290.

Banjo, S. and Yadron, D. 2014. "Home Depot Confirms Data Breach," *The Wall Street Journal* (available at http://www.wsj.com/articles/home-depot-confirms-data-breach-1410209720).

Blei, D. M., Ng, A. Y., and Jordan, M. I. 2003. "Latent dirichlet allocation," *the Journal of machine Learning research* (*3)*, pp. 993-1022.

Blei, D. M. 2012. "Probabilistic topic models," *Communications of the ACM* (55:4), pp. 77-84.

Breen, J. O. 2012. "Mining twitter for airline consumer sentiment," in *Practical Text Mining and Statistical Analysis for Non-structured Text Data Applications*, pp. 133.

Brown, J., Broderick, A. J., and Lee, N. 2007. "Word of mouth communication within online communities: Conceptualizing the online social network," *Journal of interactive marketing* (21:3), pp. 2-20.

Brown, J. J., and Reingen, P. H. 1987. "Social ties and word-of-mouth referral behavior," *Journal of Consumer research*, pp. 350-362.

Casey, E. 2006. "Investigating sophisticated security breaches," *Communications of the ACM* (49:2), pp. 48-55.

Carroll, A. B. 1991. "The pyramid of corporate social responsibility: Toward the moral management of organizational stakeholders," *Business horizons* (34:4), pp. 39-48.

Caudron, S. (1997). Forget image: It's your reputation that matters. *Industry Week*, February, 3: 13–16.

Chung, S. and Liu, S. 2011. *Predicting Stock Market Fluctuations from Twitter*, Berkeley, California.

Coombs, W.T. 2006. "The protective powers of crisis response strategies: Managing reputational assets during a crisis," *Journal of Promotion Management* (12), pp. 241–259.

Coombs, W.T. and Holladay, S.J. 2005. "Exploratory study of stakeholder emotions: Affect and crisis," in *Research on Emotion in Organizations: Volume 1: The Effect of Affect in Organizational Settings,* N.M. Ashkanasy, W.J. Zerbe and C.E.J. Hartel (eds.), Elsevier: New York, pp. 271–288.

Coombs, W. T. 2007. "Protecting organization reputations during a crisis: The development and application of situational crisis communication theory," *Corporate Reputation Review*, (10:3), pp. 163-176.

Das, S., Sismanis, Y., Beyer, K. S., Gemulla, R., Haas, P. J., and McPherson, J. 2010. "Ricardo: integrating R and Hadoop," in *Proceedings of the 2010 ACM SIGMOD International Conference on Management of data*, ACM , pp. 987-998.

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

Dhillon, G., and Backhouse, J. 2001. "Current Directions in Information Security Research: Toward Socio-Organizational Perspectives," Information Systems Journal (11:2), pp. 127-153.

Dowling, G. 2002. Creating Corporate Reputations: Identity, Image, and Performance, Oxford University Press: New York.

Duana, W., Gub, B., and Whinston, A.B. 2008. "Do online reviews matter?— An empirical investigation of panel data," *Decision Support Systems* (45:3), pp. 1007–1016.

Finin, T., Murnane, W., Karandikar, A., Keller, N., Martineau, J., and Dredze, M. 2010. "Annotating named entities in Twitter data with crowdsourcing," In *Proceedings of the NAACL HLT 2010 Workshop on Creating Speech and Language Data with Amazon's Mechanical Turk,* Association for Computational Linguistics, pp. 80-88.

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

Fombrun, C. 1996. *Reputation: Realizing value from the corporate image*, Boston: Harvard Business SchoolPress.

Freshfields Bruckhaus Deringer 2013. "Half of businesses unprepared to handle 'digital age' crises," (available at http://www.freshfields.com/en/news/Half_of_businesses_unprepared_to_handle_'digital_age'_crises/).

Gentry, J. 2013. "twitteR: R based Twitter Client. R package version 1.1.7," Available at http://CRAN.R-project.org/package=twitteR.

Gimpel, K., Schneider, N., O'Connor, B., Das, D., Mills, D., Eisenstein, J., ... and Smith, N. A. 2011. "Part-of-speech tagging for twitter: Annotation, features, and experiments," In *Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies: short papers*, Association for Computational Linguistics, pp. 42-47.

Glazer, E. 2014. "J.P. Morgan Says About 76 Million Households Affected By Cyber Breach," *The Wall Street Journal* (available at http://www.marketwatch.com/story/jp-morgan-says-about-76-million-households-affected-by-cyber-breach-2014-10-02-17103316).

Greenburg, M., Mantell, N., Lahr, M., Felder, F. and Zimmerman, R. 2007. "Short and intermediate economic impacts of terrorist-initiated loss of electric power: Case study of New Jersey," *Energy Policy* (35:) pp. 722–733.

Hall, R. 1993. "A framework linking intangible resources and capabilities to sustainable competitive advantage," *Strategic Management Journal* (14:), pp. 607–618.

Hamill, J. T., Deckro, R. F., and Kloeber, J. M. 2005. "Evaluating information assurance strategies," *Decision Support Systems* (39:3), pp. 463-484.

Hornik, K., and Grün, B. 2011. "topicmodels: An R package for fitting topic models," *Journal of Statistical Software* (40:13), pp. 1-30.

Howard, P. N. and Duffy, A. 2011 "Opening closed regimes: what was the role of social media during the Arab Spring?," *Project on Information Technology and Political Islam*, pp. 1–30.

(2011).

Hsu, M-H. and Kuo, F-Y. 2003. "An investigation of volitional control in information ethics," *Behavior and Information Technology* (22:), pp. 53–62.

Hu, M. and Liu, B. 2014 "A list of positive and negative opinion words or sentiment words for English," Available at http://www.cs.uic.edu/~liub/FBS/sentiment-analysis.html.

Jansen, B. J., Zhang, M., Sobel, K., and Chowdury, A. 2009. "Twitter power: Tweets as electronic word of mouth," *Journal of the American society for information science and technology* (60:11), pp. 2169-2188.

Joh, S. W. 2003. "Corporate governance and firm profitability: evidence from Korea before the economic crisis," *Journal of Financial Economics* (68:2), pp. 287-322.

Kurland, N. B. 1995. "Ethical intentions and the theories of reasoned action and planned behavior," *Journal of Applied Social Psychology* (25:), pp. 297–313.

Lange, D., Lee, P. M., and Dai, Y. 2011. "Organizational reputation: A review," *Journal of Management* (37:1), pp. 153-184.

Lee, A. S. 1989. "A scientific methodology for MIS case studies," *MIS Quarterly*, pp. 33-50.

Liu, B. 2012. "Sentiment analysis and opinion mining," *Synthesis Lectures on Human Language Technologies* (5:1), pp. 1-167.

Love, E. G., and Kraatz, M. S. 2009. "Character, conformity, or the bottom line? How and why downsizing affected corporate reputation," *Academy of Management Journal* (52:), pp. 314-335.

Lumb, D. 2015. "Google Apps Bug Leaks 280000 Users' Domain Data," Available at http://www.fastcompany.com/3043667/fast-feed/google-apps-bug-leaks-280000-users-domain-data.

Manning, C. D. 1999. Foundations of statistical natural language processing, H. Schütze (Ed.), MIT press.

McMillan, G. S. and Joshi, M. P. 1997. "Sustainable competitive advantage and firm performance: The role of intangible resources," *Corporate Reputation Review* (1:), pp. 81–85.

Merritt, J. 2014. "What Experts Say is the Single Largest Security Threat to Your Company's Reputation," Available at https://www.reputationmanagement.com/blog/experts-say-single-largest-security-threat-companys-reputation, Accessed on March 2015.

Mimno, D. and McCallum, A. 2007. "Mining a digital library for influential authors," in *Proceedings of the 7th ACM/IEEE-CS joint conference on Digital libraries,* ACM, pp. 105-106.

Mimno, D., Li, W., and McCallum, A. 2007. "Mixtures of hierarchical topics with pachinko allocation," in *Proceedings of the 24th international conference on Machine learning,* ACM, pp. 633-640.
Mitton, T. (2002). A cross-firm analysis of the impact of corporate governance on the East Asian financial crisis. *Journal of financial economics*, *64*(2), 215-241.
Owoputi, O., O'Connor, B., Dyer, C., Gimpel, K., Schneider, N., and Smith, N. A. 2013. "Improved Part-of-Speech Tagging for Online Conversational Text with Word Clusters," in *HLT-NAACL*, pp. 380-390.
Pew Internet Project. 2014. "Social Networking Fact Sheet," Available at http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/, Accessed on April 2015.
Pfarrer, M. D., Pollock, T. G., and Rindova, V. P. 2010. "A tale of two assets: The effects of firm reputation and celebrity on earnings surprises and investors' reactions," *Academy of Management Journal* (53:5), pp. 1131-1152.
Ramagopalan, S., Wasiak, R., and Cox, A. P. 2014. "Using Twitter to investigate opinions about multiple sclerosis treatments: a descriptive, exploratory study," *F1000Research*, *3*.
Rindova, V. P., Petkova, A. P., and Kotha, S. 2007. "Standing out: how new firms in emerging markets build reputation," *Strategic Organization* (5:1), pp. 31-70.
Roberts, P. W. and Dowling, G. R. 1997. "The value of a firm's corporate reputation: How reputation helps attain and sustain superior profitability," in *the Proceedings of the Conference on Corporate Reputation, Image, & Competitiveness*, New York University, New York.
Seeger, M. W., Sellnow, T. L., and Ulmer, R. R. 2003. *Communication and organizational crisis*, Greenwood Publishing Group.
Sheffi, Y. 2005. The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage, MIT Press, Boston.
Silverman, G. 2011. Secrets of Word-of-Mouth Marketing: How to trigger exponential sales through runaway word of mouth, AMACOM Div American Mgmt Assn.
Siponen, M. T. 2005. "An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice," European Journal of Information Systems (14:3), pp. 303-315.
Solms, V. B., and Solms, V. R. 2004. "The 10 deadly sins of information security management," *Computers & Security* (23:5), pp. 371-376.
Sterbenz, J. P., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., and Smith, P. 2010. "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," *Computer Networks* (54:8), pp. 1245-1265.
Strauss, A., and Corbin, J. M. 1998. Basics of Qualitative Research: Grounded Theory Procedures and Techniques, Newbury Park, A: Sage.
Thelwall, M., Buckley, K., and Paltoglou, G. 2011. "Sentiment in Twitter events," *Journal of the American Society for Information Science and Technology* (*62*:2), pp. 406-418.
Urquhart, C., Lehmann, H., and Myers, M. D. 2010. "Putting the 'theory' back into grounded theory: guidelines for grounded theory studies in information systems," *Information systems journal* (*20*:4), pp. 357-381.
Uys, J. W., Du Preez, N. D., and Uys, E. W. 2008, July. "Leveraging unstructured information using topic modeling," in *Management of Engineering & Technology, Portland International Conference on* (pp. *PICMET,* IEEE, pp. 955-961.
Vieweg, S., Hughes, A. L., Starbird, K., and Palen, L. 2010. "Microblogging during two natural hazards events: what twitter may contribute to situational awareness," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* ACM, pp. 1079-1088.
Wartick, S. 1992. "The relationship between intense media exposure and change in corporate reputation," *Business* & *Society* (31:), pp. 33–49.
Weiner, B. 1986. An Attributional Theory of Motivation and Emotion, Springer Verlag, New York.
Workman, M., Bommer, W. H., and Straub, D. 2008. "Security lapses and the omission of information security measures: A threat control model and empirical test," *Computers in Human Behavior* (24:6), pp. 2799-2816.
Zhao, W. X., Jiang, J., Weng, J., He, J., Lim, E. P., Yan, H., and Li, X. 2011. "Comparing twitter and traditional media using topic models," in *Advances in Information Retrieval*, Springer Berlin Heidelberg, pp. 338-349.