2015

DYNAMICS OF IDENTITY THREATS IN ONLINE SOCIAL NETWORKS: MODELLING INDIVIDUAL AND ORGANIZATIONAL PERSPECTIVES

Romilla Syed
Virginia Commonwealth University

DYNAMICS OF IDENTITY THREATS IN ONLINE SOCIAL NETWORKS: MODELLING INDIVIDUAL AND ORGANIZATIONAL PERSPECTIVES

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at Virginia Commonwealth University.

by

Romilla Syed

Dissertation Chair: Gurpreet Dhillon, Professor,
Department of Information Systems

Virginia Commonwealth University
Richmond, Virginia
August 2015

Dedication

To my husband — You are a blessing. Without your unconditional love and support, I would have never seen the finish line.

To my daughter — You are a gift from heaven. Your curiosity keeps me moving.

I love you!

Romilla Syed,

Richmond, VA.

Acknowledgement

I have been blessed with an incredible family of advisors and friends, who over the years have bestowed trust and provided guidance. Thank you, first and foremost, to the members of my committee: Gurpreet Dhillon, Victoria Yoon, Jason Merrick, and Jason Levy. To Gurpreet, I thank you deeply for the opportunities you have provided me. You have a profound influence on me as an academic. Thank you for pushing me to see beyond obvious — a lesson that I will always value. To Victoria, thank you for the tremendous support and guidance. You are one of the most effective educators I have ever met. Thank you for introducing me to the 'design science' paradigm. To Jason Merrick, I am indebted to you in countless ways. Your modesty amazes me every time. Thank you for pushing me to 'getting it right' — a lesson that will stay with me forever. To Jason Levy, thank you for being an intellectual instigator. You taught me how to question the most fundamental assumptions and help me situate my thoughts. I am grateful to have met all of you. I look forward with great anticipation to future collaborations with all four of you.

Finally, to fellow doctoral students, my friends, thank you for everything. You were my strength in the hours of chaos. I look forward to many stimulating interactions for years to come.

Thank you All!

Romilla Syed,

Richmond, VA.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

DYNAMICS OF IDENTITY THREATS IN ONLINE SOCIAL NETWORKS: MODELLING INDIVIDUAL AND ORGANIZATIONAL PERSPECTIVES

By Romilla Syed, Ph.D.

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, at Virginia Commonwealth University.

Virginia Commonwealth University, 2015

Dissertation Chair: Gurpreet Dhillon, Professor
Department of Information Systems

Identity threats in Online Social Networks (OSNs) are real and unsettling. This dissertation examines identity threats perceived by individuals and organizations in OSNs. The research constitutes two major studies:

Research Study 1, entitled as *Social Identity Threats to Individuals in Online Social Networks,* examines the threats perceived by individuals in the identification mechanisms of OSNs. Using the concepts of Value Focused Thinking and the related methodology of Multiple Objectives Decision Analysis, the qualitative and quantitative value models are developed to explain the social identity threats perceived in OSNs and the utility of the protection mechanisms to avert the threats. The qualitative value model defines: 1) the value hierarchy i.e. the fundamental objectives to prevent threats to individuals' social identity; 2) the taxonomy of user responses, referred to as Social Identity Protection Responses (SIPR), to avert the social identity threats. The quantitative value model describes: 1) the utility of the current social networking

sites to achieve the fundamental objectives for preventing social identity threats; 2) the utility of Social Identity Protection Responses to avert social identity threats in OSNs.

The findings suggest that individuals perceive threats to the five aspects of social identity in OSNs. The corresponding objectives to minimize social identity threats include: *maximize enactment of social identity*; *maximize value of social identity*; *maximize meaning of social identity*; *maximize trust in OSNs*; *maximize normative ethics in OSNs*. A total of 15 fundamental objectives are defined to prevent the threats corresponding to the five aspects of social identity. The taxonomy referred to as Social Identity Protection Responses includes two types of responses: *self-recourse* and *external recourse*. Together the two response types encompass six types of alternatives. The utility scores of the current social networking sites suggest that large utility gaps exist in Status Quo with respect to preventing social identity threats to individuals. Finally, with respect to Social Identity Protection Responses, the utility of external-recourse emerged to be better than self-recourse; however, none of the alternatives ensure absolute prevention of social identity threats.

The findings suggest that there is a need to implement a mix of controls for preventing identity threats in OSNs. This study makes an important theoretical contribution to the social identity and identification literature by identifying the gaps between the values that users attribute to their social identities and the values that social networking sites endure in the identification mechanisms. The findings educate individuals about the types and sources of social identity threats prevalent in OSNs. Furthermore, the utility models help users decide which identity protection response is adequate to prevent a particular type of identity threat. The findings also inform organizations and policymakers about the value sensitive design of OSNs.

Research Study 2, entitled as *Reputation Threats to Organizations in Online Social Networks,* examines organizational identity threats in OSNs in the aftermath of a data breach. Conceptualizing the perceived threats as Information Security Reputation (ISR) threats, threat analysis is undertaken by examining the discourses related to the recent data breach at Home Depot and JPMorgan Chase in the popular microblogging website, Twitter. Specifically, the threat analysis identifies: 1) the dimensions of information security discussed in the Twitter postings; 2) the attribution of data breach responsibility and the related sentiments expressed in the Twitter postings; and 3) the subsequent diffusion of the tweets that threaten organizational reputation.

The results suggest that Twitterers discuss the five dimensions of organizational ISR: *Risk and Resilience Structure*; *Security Ethics and Practices*; *Structures of Governance and Responsibility*; *Response Readiness*; *Social and Moral Benevolence*. A large number of tweets attribute the data breach responsibility to the organizations. Overall, the tweets express more negative sentiment. However, tweets that attribute data breach responsibility carry more negative sentiments. Additionally, a large number of users share or seek information about the data breach. However, influential users (i.e. users with large number of followers) post lesser tweets albeit carrying negative sentiments. Finally, the results suggest that attribution of data breach responsibility and negative sentiments impact the count and speed of retweets.

By integrating the communication crisis and electronic Word of Mouth literature, this research makes an important theoretical contribution by explicating threats to the ISR of organizations in OSNs. The findings could inform the organizational strategy for social media reputation management and post-data breach intervention. Finally, this study demonstrates the use of novel data analytical techniques to derive insights from social media platforms.

Chapter 1: Introduction

1.1. Problem Definition

Prototypical questions such as 'Who are we?', 'Who am I?', 'What do I want others to know about me?', and 'What do others know about me?' have recently led to a flurry of research in the fields of management. Scholars from various disciplines have answered such questions using various theoretical and analytical lenses. Whitley et al. (2014) evaluate these questions as those related to identity and identification. *Identity* conceptualizes such questions as what individuals, groups, or organizations believe about themselves. *Identification,* on the other hand, is the mechanisms to define the idiosyncratic characteristics of self so as to provide assurances about the identity claims. Yet this simple and oversimplified segregation of identity and identification research is arbitrary especially in Online Social Networks (OSNs) where the two constructs are highly entangled (see Schultze 2014; Lyon 2009). In particular, the entanglement is evident in the presentation and the enactment of user identity that is shaped by the technological constraints of identification and the social needs of maintaining a positive identity (Schultze 2014; Schultze and Orlikowski 2010). Previous research acknowledges the positive impact of the entanglement from economic and social perspectives (e.g. Forman et al. 2008; Kim et al. 2012; Tsai and Bagozzi 2014); however, the negative implications of the entanglement have not received much attention. In particular, while OSNs provide mechanisms for a user to present and enact identity, such mechanisms are available to other social media users as well whose presentation and enactment could threaten the user's identity. Stated simply, how other social media users characterize a user's identity could cause a threat if such characterizations are contrary to or questions what the user projects. Empirical evidence suggests that individuals experience a myriad of identity threats in OSNs ranging from identity compromises (Levin 2013) to negative

or devalued treatment (Agranoff 2012). Likewise, organizations are increasingly concerned about their identity in OSNs as the information related to organizations trends instantly in OSNs providing an opportunity for users to share comments and opinions about the organization (Jansen et al. 2009; Coombs 2007). The big data breach at Target Corp. that exposed records of millions of customers, for example, faced a huge public wrath resulting in significant amount of negative Word-of-Mouth (WOM) (Pinsker 2014).

Currently, there is a problem in preventing the threats to the users emerging due to entanglement of identity and identification in OSNs. Informed by the theoretical concepts of social and organizational identity (Tajfel and Turner 1985; Albert and Whetten 1985), this dissertation argues that the social network users perceive identity threats if there is a disagreement between the values that inform users identity and the values that the social networking sites endure in the identification mechanisms. The overall objective of this dissertation is to explore the identity threats perceived by Online Social Network users. The overarching research question that this dissertation seeks to address is: *What identity threats users experience in Online Social Networks?* This dissertation answers this question by understanding the interaction between user identity and technology-based identification. Specifically, the threats are studied at two analytical levels, i.e. individuals and organizations. Consequently, this dissertation presents two research studies. The first study, entitled, "*Social Identity Threats to Individuals in Online Social Networks* " characterizes social identity threats faced by individuals in OSNs. The second study, entitled "*Reputation Threats to Organizations in Online Social Networks*" examines the threats to the organizational identity referred as reputation threats in OSNs in the aftermath of data breaches. In the following sections, an overview of the conceptualization of identity threat is presented followed by an introduction of

the two research studies. For each study, the research problem, the research questions, and the definitions of related terminology are presented. This chapter concludes with an overview of the subsequent chapters of this dissertation.

1.2. Overall Conceptualization of Identity Threat

Previous research establishes that online identity is a representation of user's offline identity and embodied experiences (Serfaty 2003; Madge and O'Connnor 2005). This *representational* view doesn't grasp the entanglement between users and technology that shapes embodied identities (Schultze 2014). To account for the influence of both online and offline experiences on the embodied identities, some scholars advance the concept of *performativity* view (e.g. Veerapen 201; Schultze and Orlikowski 2010). According to this view, user identity is constituted and constrained by the experiences in both real and virtual settings. Nevertheless, much of this research that seeks to understand the technological issues of identification and the social issues of user identities falls short by two perspectives.

Firstly, personal identity is not simply a role structure or in-group/out-group comparisons of self; it is a product of value commitments (Hitlin 2003). Hitlin argues that, theoretically values and personal identity are connected by the concept of authenticity- a primary self-motive. A user feels authentic if he or she enacts in keeping with the personal values, thus reflecting one's personal identity. This view of personal identity is consistent with that of organizational researchers who argue that identity is a question of self-reflection grounded in the organizational values. Decision makers introspect values to select a possible solution representative of the organizational values and identity (Albert and Whetten 1985). Secondly, there is long standing interest among researchers for promoting Value Sensitive Design of information systems to ensure user autonomy and freedom from bias (Friedman 1996). While autonomy helps users

achieve goals and promote values, bias-free technology prevents discrimination against certain users by denying desirable outcomes or assigning undesirable outcomes on unreasonable grounds. More recently, four different research strands that support the notion of Value Sensitive Design have emerged (see, Friedman and Kahn 2002, Friedman et al. 2013): Computer Ethics, Social Informatics, Computer Supported Cooperative Work, and Participatory Design. However, as Friedman (1996) states, "Values emerge from the tools that we build and how we choose to use them. Yet, in most of the current practice in designing computer technology and the related infrastructure of cyberspace, little is said about values" (pg. 17).

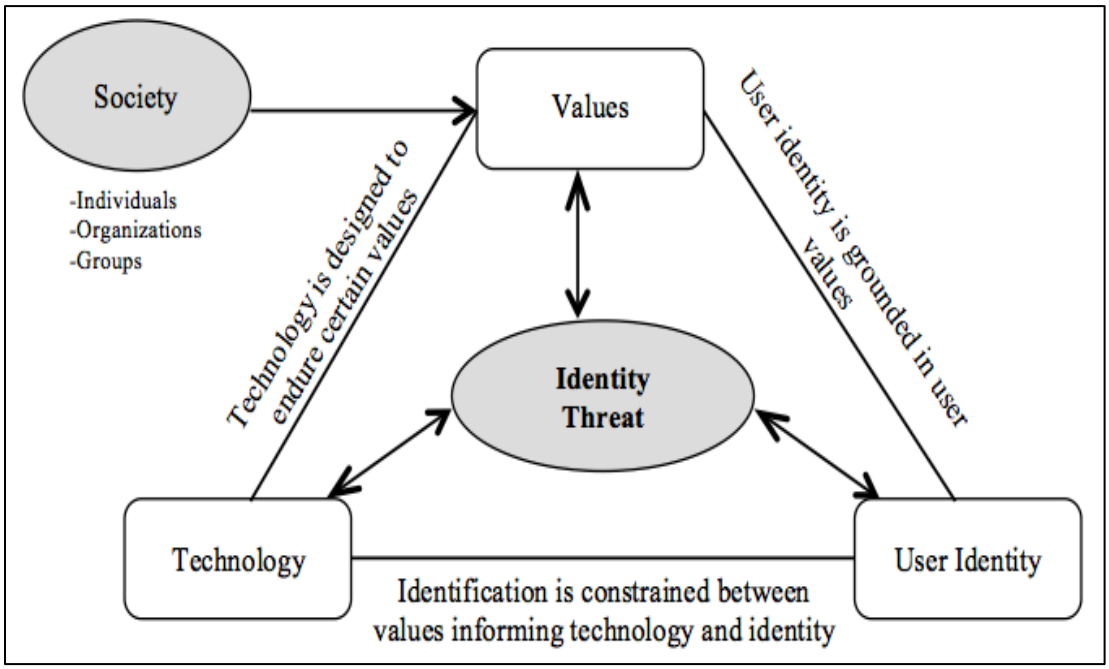


Figure 1: Conceptual Model of Social Identity Threat in Value-Identity-Technology (VIT) Entanglement

Given these two perspectives, it is apparent that the strife between users and technology emerges if there is a disagreement in the value structures between those of users and of technology. Especially, in the context of OSNs, users on the one hand project salient aspects of

their identity, and social networking sites on the other hand are designed to endure certain human values in the identification mechanisms that these sites support, creating a value gap between the users and the technology. This dissertation argues that the value gap between the identity of users and the identification mechanisms of OSNs could threaten the user's identity. The conceptual model of identity threat in Online Social Networks due to the entanglement of identity, technology, and values is presented in Figure 1.

1.2.1. Definitions

Values are the central beliefs expressed through specific behaviors (Rokeach 1973). Others scholars consider values as desirable goals that vary in importance and serve as guiding principles (Hitlin 2003; Schwartz 1992). For Keeney (1992), values are the priorities, ethics, tradeoffs, guidelines for actions, and attitudes toward risk.

Identity has at least three variations (Stryker and Burke 2000). While some scholars consider identity as a cultural or ethnic representation, others regard identity as representative of social category or group, yet others associate it to represent parts of self i.e. multiple roles played at personal level. On similar lines, Whitley et al. (2014) differentiate amongst three forms of identity as individual, organizational, and social. Individual identity is thought of as the personal characteristics and individual preferences. Social identity refers to an individual's perception about self as determined by his or her memberships with certain social groups. And finally, organizational identity is the understanding of members about the features of an organization. In this dissertation, the first research study operationalizes individuals' personal identity in terms of social identity whereas the second research study operationalizes organizational identity as the understanding of social network users about an organization and is referred to as reputation. The definitions are provided below in the respective sub-sections.

Technology in the context of this dissertation refers to the social networking sites that allow users identify themselves by creating a digital identity, connect with other users, and interact by sharing content (Ellison 2007)**.**

Identity Threat is defined as the "experiences appraised as indicating potential harm to the value, meanings, or enactment of an identity" (Petriglieri, 2011, pg. 644). In this dissertation, I argue that users perceive identity threats when their sense of self-projection is questioned in online social networks. The identity threats emergent in the Value-Identity-Technology triad presented in Figure 1 forms the basis of the two research studies presented in this dissertation.

1.3. Research Study 1: Social Identity Threats to Individuals in Online Social Networks

1.3.1. Research Problem

Online Social Networks (OSNs) offer a medium for individuals to project their identities in preferential ways, as how the individuals want themselves to be seen as or how other social network users should perceive them. However, the identification mechanisms in OSNs have emerged to be problematic to the idiosyncratic characteristics of the individuals' social identities. While individuals have greater control over the elements of identity presentation and enactment, social identity of individuals is largely dependent on how other social media users perceive the identity cues, over which the individuals have little control. Such loss of control in OSNs is eminent in the myriad of threats ranging from identity compromises (Levin 2013) to negative or devalued treatment (Agranoff 2012). This threat to the individual's sense of self-projection is largely because the boundaries in OSNs, within which individuals maintains their social identities, have been transformed. As McQuail (1991) argues, the formal structures and channels for information flow suggest a certain value structure with respect to identity. However, when these structures and channels get diffused or transformed, individual values

with respect to identity protection have no bearing (see McQuail 1991). The confusion caused is typically at three levels: 1) Confusion about personal values that define individual identity; 2) Concern about how identity is protected by various institutions; 3) Inability of the institutions to appreciate individual values regarding identity protection. Furthermore, while the magnitude of identity loss and its consequences has increased over the years, understanding of fundamental issues pertaining to the sources of identity threats and means of identity protection remains limited (Newman and McNally 2005; White and Fisher 2008). Much research on individual identity to date has focused on understanding the formation of digital identities and the impact of digital identities on individual behaviors in virtual communities (see Schultze 2014; Campbell et al. 2009); however, the impact of online experiences on the individual identity has received little attention. There is also some scattered research on the assurance of digital identities. However, the focus of this line of research is limited to either technology e.g., automated mechanisms to differentiate identities (Abbasi et al. 2008) or economic perspective e.g. determine the user willingness to pay for identity management (Roßnagel et al. 2014)

While existing research enhances our understanding about the formation, differentiation, and influence of digital identities, there is a limited research to understand the identity threats perceived by individuals in the identification mechanisms of OSNs. Similar observations has been made by Whitley et al. (2014) as well as the authors mention the implications of social networking sites on the identity of individuals. Informed by the theoretical concepts of social identity theory and identity threat (Stryker and Burke 2000; Tajfel and Turner 1985; Petriglieri 2011), this study argues that there is a gap between the values that inform individuals' social identity and the values that inform the identification processes in the OSNs, and the value gap in turn creates provisions for social identity threats to individuals. To this effect, the purpose of

this study is to identify and prevent the threats to individual identity due to identification mechanisms in OSNs. It is important to conduct this analysis as research suggests that social identity threats such as abusive behavior in social networking sites have negative repercussions on individual's digital and social identity (Whitley et al. 2014). Using the concepts and the techniques of Value Focused Thinking (VFT) and Multiple Objective Decision Analysis (MODA) (Keeney 1992; Keeney and Raiffa 1993), this study identifies the threats emergent in the gaps between the values informing the social identity of individuals and those endured by current social networks, and systematically identifies the objectives and alternatives for preventing social identity threats. More specifically, this study 1) defines the fundamental value hierarchy specifying the objectives to prevent threats to various aspects of individuals' social identity; 2) conducts a utility gap analysis to determine the extent to which current social networking sites prevent the identity threats; 3) identifies the alternatives referred as Social Identity Protection Responses to prevent the identity threats; 4) assesses the utility of the alternatives to prevent the social identity threats.

1.3.2. Research Questions

This study analyzes social identity threats experienced by individuals emergent in the gaps between the values that inform individuals' social identity and the values endured in the identification mechanisms of OSNs. Consequently, this study addresses the following four research questions:

RQ1: What are fundamental objectives to prevent threats to the various aspects of social identity of individuals in Online Social Networks?

RQ2: What are the user responses to prevent social identity threats in Online Social

Networks?

RQ3: What are the gaps between the values informing the social identity of the individuals and those supported by the identification mechanisms of current Online Social Networks?

RQ4: What are the most effective user responses to prevent social identity threats in Online Social Networks?

Using the concepts and techniques of Value Focused Thinking (VFT) and Multiple Objective Decision Analysis (MODA) as a unified decision-making framework, this study considers values and preferences of multiple stakeholders to address the four research questions. As has been argued by several scholars (Gregory and Keeney 1994), capturing stakeholder values provides a superior basis for decision-making. This analysis is more suitable for complex decision situations such as managing individual identity in OSNs involving multiple stakeholders, conflicting objectives, and uncertainty (Keen and Morton 1978).

To address the first research question, qualitative value modelling is used to define the fundamental value hierarchy. The value hierarchy defines the objectives to prevent the threats to various aspects of the social identity of individuals. The fundamental value hierarchy could inform social media organizations about the identification processes that are perceived to threaten the social identities of individuals and the corresponding objectives that could prevent those threats. It could also be helpful for individuals to understand the types of threats that exist in OSNs. To address the second research question, taxonomy of alternatives referred as *Social Identity Protection Responses (SIPR)*, is identified from the participant values and the existing literature. The alternatives define the recourses that individuals could pursue in case online experiences are perceived to be identity threatening. To address the third research question,

quantitative value modelling is used to assess the utility of the current social networking sites in preventing the identity threats. In particular, utility gap analysis is conducted to determine the effectiveness of current social networking sites to accomplish the fundamental objectives. This analysis is helpful for organizations to determine the scope of improvement in the social networking sites to prevent the social identity threats. It is also helpful for individuals to assess the level of risk to their social identities in OSNs. To address the fourth research question, quantitative value modelling is used to assess the utility of the Social Identity Protection Responses (SIPR). The utility analysis determines the extent to which different recourse types are effective in preventing a particular type of threat. This analysis is helpful for organizations to determine the appropriate strategies for preventing the social identity threats. It could also help individuals to choose the best available recourse to prevent a particular type of threat.

1.3.3. Definitions

Social identity, conceptualized in the field of social psychology, refers to the identifiable or categorical aspects of self. According to social identity theory, people classify themselves or others into various social categories ranging from group or organizational memberships to religious affiliations and gender or age-based cohorts (Tajfel and Turner 1985). Social identity theory defines two different aspects of identity: personal identity and social identification (Ashforth and Mael 1989). *Personal identity* represents the idiosyncratic characteristics such as bodily attributes, interests, and abilities etc. that allow individuals to define themselves in a larger social environment. In comparison, *social identification* allows to define oneself with respect to group characteristics. Identification is the perception of belongingness to a group. Although social identity theory explains the concepts of self and social categorization, it can be easily operationalized with respect to cyber identities. There is little doubt that OSNs allow the

projection of salient and pervasive aspects of digital identities by virtue of specifying profile attributes and group affiliations, and even by creating and sharing content.

1.4. Research Study 2: Reputation Threats to Organizations in Online Social Networks

1.4.1. Research problem

Organizations are increasingly using Online Social Networks (OSNs) as a medium to build strong brand and corporate presence. Given the large number of social media users, these networks serve as a bidirectional information communication medium between the organizations and the customers (Morrissey 2007). However, the unprecedented scalability and reachability of OSNs not only allow users to generate large amount of content but also disseminate that content to larger online population. Management scholars recognize that such characteristics of social media can be a source of threat to organizational identity. For example, previous research shows the potential of OSNs to influence the perceptions and opinions of stakeholders about the organizations by disseminating information to public, thereby reflect and affect organizations identity (Bampo et al. 2008; Rindova et al. 2007; Reynolds 2007). Confounding the threat is the possibility of social network users to malign an organization's identity. For example Dellarocas (2006) argues that online forums allow interested parties to manipulate information, such as praising own products or bad-mouthing competitors. Likewise, in 2004, Amazon.com revealed the identities of book reviewers due to software glitch. It was found that publishers, authors, and competitors write a significant number of reviews (Harmon 2004).

Informed by Brown et al. (2006), this study conceptualizes organization identity in OSNs as reputation. Reputation is defined as the aggregate stakeholders evaluation of how well an organization meets customers' expectations (Wartick 1992). Reputation in OSNs in its ubiquitous usage has a very intuitive appeal to organizations. Categorized as online reputation

systems, OSNs allow users engage in bi-directional information exchange and thereby generate large-scale electronic Word-of-Mouth (eWOM) networks around range of topics such as products, services, and even world events (Bampo et al. 2008; Dellarocas 2003; 2006). Research shows that through multiple exchanges, particularly in OSNs, eWOM reaches and shapes attitudes of individuals at a scale unparalleled by offline WOM (Brown et al. 2007). The interpersonal exchanges in OSNs hold "informational value" over and above the messages communicated by the organizations about themselves (Brown et al. 2007). OSNs thus exhibit powerful influence in shaping recipients opinion and subsequent decision-making. Consequently, organizations are becoming increasingly concerned about their reputation in OSNs of how well the organizations meet stakeholders' 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 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."[1] Crisis leads jarring stakeholders attribute the responsibility to organization and thereby create negative word of mouth (Coombs 2007). A higher level of attribution of crisis responsibility decreases the reputation score of the organizations.

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 data breach represents the single biggest security risk to an organization's reputation (Merritt 2014). A data breach not only puts customers' information at risk but also shakes their confidence in an organization's capability to protect

[1]http://www.freshfields.com/en/news/Half_of_businesses_unprepared_to_handle_'digital_age'_crises/

information. Furthermore, the recent surge of data breaches indicate that breach related information 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 Corp. that 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. Further due to emotional arousal stakeholders could engage in eWOM in OSNs influencing the perceptions and opinions of people beyond their immediate social connections. Informed by Situational Crisis Communication Theory (SCCT) (Coombs 2007), this study argues that, in order to contain threats to Information Security Reputation of organizations, it is important to understand the emotional and behavioral responses of OSN users following a data breach. Specifically, this study analyzes: (1) the aspects of information security reputation that social media users attribute responsible for the data breach; (2) the emotional response of users to data breaches; (3) the diffusion of reputation threatening tweets.

1.4.2. Research Questions

This study analyzes the Twitter postings related to the recent data breaches at Home Depot[2] and JPMorgan Chase[3] to identify the Information Security Reputation threats. For the organizations to perceive reputation threat, the Twitter postings have to deem an organization responsible for the data breach, should express negative sentiments, and the Twitter postings has to retweeted more. Consequently, this study addresses the following three research questions:

[2] http://www.wsj.com/articles/home-depot-confirms-data-breach-1410209720

[3]http://www.marketwatch.com/story/jp-morgan-says-about-76-million-households-affected-by-cyber-breach-2014- 10-02-17103316

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?

RQ3: What characteristics of eWOM following the data breach impact the subsequent diffusion of ISR threatening tweets?

Using 16,200 tweets from 9,702 users, a suite of novel data analytical techniques referred to as *Social Media Knowledge Discovery (SMKD)* process is employed to answer the three research questions. To address the first research question, a mixed methods approach is employed to identify the dimensions of Information Security Reputation of the organizations that the tweet postings indicate as ineffective to prevent the data breach. Specifically, probabilistic topic modelling technique and content analysis are employed to identify the dimensions of ISR. This series of analysis identifies the ISR dimensions of the organization that Twitterers are concerned post data breach. The findings could be used by the organizations to not only improve their overall security posture but also to prepare an adequate post-breach response.

To address the second research question, Twitter Annotation methodology is used to identify the tweets that attribute data breach responsibility to the organizations. Statistical tests are run to determine the association between the attribution of data breach responsibility and ISR dimensions. Next, the sentiments expressed in tweet postings are algorithmically analyzed. The accuracy of the algorithm is validated by manually coding the sentiments of a random sub-sample of tweets. Again, the statistical tests are run to determine the association between the sentiments and the data breach responsibility attribution. Furthermore, user level analysis is done to identify the "influential" users (i.e. users who have large number of followers and followees)

who engage in spreading attribution tweets. This series of analysis provided an insight into the extent to which overall attributions of breach responsibility and associated sentiments trend in Twitter post data breach. The findings could be used by organizations to assess the characteristics and severity of the attributions and sentiments, formulate a strategy for post data breach, and thus prevent reputational damage.

To address the third research question, regression analyses are run to examine whether the attribution of data breach responsibility and the associated sentiments increase the spread of such tweets. Specifically, the hypotheses test whether ISR dimensions, attributions, and sentiments increase retweet count (i.e. the number of times a tweet is retweeted) and reduce retweet latency (i.e. time lag between the tweet and its retweet). Several other factors such as content characteristics of tweets (e.g. url, hashtag) and contextual features of Twittterers (e.g. follower count, followee count, profile age) are controlled for. This series of analysis provide an insight into the factors that contribute to the diffusion of attribution tweets and negative sentiments in the event of a data breach. The findings could inform organizations about the scale at which reputation threatening tweets propagate in the social media and thus prepare a timely post-crisis response.

1.4.3. Definitions

Information Security Reputation, building on Wartick (1992), is the aggregate stakeholders evaluation of how well an organization meets customers expectations of protecting their personal information.

Crisis is defined as any unusual event that evokes a sense of threat to the high priority goals, image, legitimacy, profitability, or survival of organizations (Seeger et al. 2003).

Sentiments are the opinions, emotions, evaluations, attitudes, and behavior of people towards a particular subject or its characteristics (see Liu 2012).

Responsibility-Attribution, informed by Coombs (2006) theory of SCCT, refers to the extent to which stakeholders hold an organization accountable for the crisis. Coombs argue that the organizational crisis cause stakeholders exhibit various affective reactions depending on the crisis responsibility attributed to the organization. Stakeholders express sympathy if the organization is perceived to be a victim otherwise they experience anger. In case of a data breach, this study argues that jarred OSNs could attribute the breach responsibility to the organization.

Electronic Word-of-Mouth behavior is the engagement of Internet users in generating and exchanging opinions and experiences around various topics (Dellarocas 2003).

1.5. Dissertation Overview

This dissertation is organized around two large studies. In the subsequent chapters, informing theory and literature, research methodologies, research findings, and research implications and contributions are presented. An overview of the chapters follows.

In the chapter 2, *Informing Theory and Literature*, a review of background literature as pertinent to the two research studies is presented. Specifically, with respect to the first study, theories of personal and social identities are discussed. Further, based on earlier research, a link between identity and values is established. The concepts of individual identity threat are also discussed. Finally, the literature related to the two research streams of information systems i.e. information security and identity is reviewed.

With respect to the second research study, organizational identity from external stakeholder's perspective is discussed. Concepts of organizational reputation and reputation threat are presented. As the second study builds on the crisis perspective, a detailed review of Situational Crisis Communication Theory (SCCT) is presented followed by a discussion on the concepts of Online Social Networks and electronic Word-of-Mouth (eWOM). Finally a set of hypotheses related to the diffusion of Information Security Reputation (ISR) threats in Twitter is grounded in literature.

In the chapter 3, *Qualitative and Quantitative Value Modelling,* the concepts of values and value theory and its usefulness for decision analysis are discussed. In particular, the philosophy of Value Focused Thinking (VFT) and the technique for Multiple Objective Decision Analysis (MODA) are presented at length. The approach for building qualitative value model and quantitative value model is discussed. The characteristics of the data sources used for value modelling are also presented.

Chapter 4, *Social Media Knowledge Discovery Process and Techniques,* presents the mechanics of deriving knowledge from social media sites. This chapter proposes and initializes Social Media Knowledge Discovery (SMKD) process. This is followed by a discussion on the suite of social media analytics techniques employed for studying Information Security Reputation threat such as topic modelling, content analysis, tweet annotation, sentiment analysis, and regression analyses.

Chapter 5, *Identity-Identification Value Threat Analysis,* presents the results related to the individual level research study. This includes fundamental value hierarchy, Social Identity Protection Responses (SIPR), group utility functions, objective weights, and alternative scoring. Finally, utility gap analysis is presented to describe the gaps between the values informing social

identity of individuals and the values endured by current social networking site in their identification mechanisms. The theoretically grounded SIPR are then evaluated to identify the best possible user response for preventing threats to the social identity. The utility gaps in SIPR provide the insights into the new alternatives for preventing identity threats to individuals in OSNs.

Chapter 6, *Information Security Reputation (ISR) Threat Analysis,* presents the results related to the organizational level study. The findings discuss the dimensions of Information Security Reputation (ISR) of the organizations attributed responsible for the data breach. The emotional response of Twitterers in terms of sentiments expressed in tweets is also discussed. Finally, the behavioral response of Twitterers in terms of subsequent diffusion of reputation threatening tweets is discussed.

In the chapter 7, *Discussion and Conclusion,* the contribution of the two research studies is discussed. For each study, the contribution of the research to theory, practice, and methodology is presented. With respect to the first study, the findings extend the literature of identity management in Online Social Networks. The findings could inform the policies and strategies of organizations for protecting the values of individuals. With respect to the second study, the findings extend the literature about organization reputation threats in crisis situation. The findings could inform organization to manage their online reputation in the aftermath of data breaches. In concluding, the contribution of the two research studies to overall identity research is discussed. The limitations and future research directions are also discussed.

1.6. Conclusion

This chapter provides the conceptual underpinning of the identity threats in the OSNs. Specifically, the concepts related to the social identity threats to individuals and the reputation

threats to organizations are introduced. An overview of the two research studies to address various theoretically grounded research questions is presented. Finally, an outline of the dissertation chapters is discussed.

Chapter 2: Informing Theory and Literature

2.1 Introduction

This chapter presents a review of the literature pertinent to the two research studies. The review related to the individual perspective addresses the following five aspects: 1) theories of personal identity; 2) concepts of identity threat; 3) values and value theory; 4) current state of information security research; 5) current state of identity research in IS domain. For organizational perspective, the review includes: 1) theories of organizational identity; 2) concepts of reputation and reputation threat; 3) Online Social Networks (OSN) and Word of Mouth (WOM); 4) hypotheses related to the diffusion of reputation threatening tweets.

2.2. Research Study 1: Social Identity Threats to Individual in Online Social Networks

2.2.1. Theories of Personal Identity

The concept of identity cuts across several disciplines ranging from sociology, psychology, history, political science, and management science. Consequently, the term has gained different theoretical and conceptual meanings. While some scholars consider identity as a cultural or ethnic representation, others regard identity as representative of social category or group, yet others associate it to represent parts of self i.e. multiple roles played at a personal level. Together these connotations allow the analysis of identity at cultural, categorical, and personal levels (Stryker and Burke 2000). These distinctions are in line to what Whitley et al. (2014) differentiate amongst three forms of identity: *personal identity* i.e. the personal characteristics and individual preferences, *social identity* i.e. individual's perception about self, as determined by his or her membership with certain social groups; *organizational identity* i.e. the understanding of the members about the features of an organization. In the literature, personal

identity is analyzed from two main theoretical lenses: *identity theory* and *social identity theory*. A brief review of the two theories is presented below followed by a framework that unifies the two theories.

2.2.2. Identity Theory

In the literature, Identity Theory has been related to Symbolic Interactionism. Symbolic Interactionism purports that the behavior exhibited by people is in effect a result of social interactions and interpretations (Mead 1934; Blumer 1986). Literature also notes that identity is a social phenomenon embedded in the shared sense of belonging to a network that a person is associated to and becoming a part of those networks is a matter of choice dictated by the interpretation that a person draws outside the network (Stryker 1987). This view is consistent with that of Stryker and Burke (2000), as they note, "… social structures outside given social networks act as boundaries affecting the probability that persons will enter those networks" (pg. 285).

In the original formulation of identity theory, Stryker (1987) argues that the "…central proposition of identity theory is that 'large-scale' social structures affect commitment affects identity salience affects role performance" (pg.89). Thus, Identity Theory conceptualizes self as a structure of identities that are organized in a salient hierarchy. It conceptualizes internalization of as many identities as the number of roles played by a person in distinct social relationships. Social roles are the expectations associated to positions occupied in network of relationships and thus identities are the internalized role expectations. Furthermore, the identities are organized in salience of hierarchy depending on the probability of instantiating those within or across situations. Identity theory also recognizes that people enter more or less distinct relationships and therefore defines commitment as the cost of foregoing a particular identity and role; the salient

hierarchy of identities reflects the varying level of commitments with respect to various identities. Finally, the theory argues that the behavioral choices reflect alternate roles and particular identity within the salient hierarchy of identities.

2.2.3. Social Identity Theory

Social identity, conceptualized in the field of social psychology, refers to the identifiable or categorical aspects of self. According to social identity theory, people classify themselves or others into various social categories ranging from group or organizational memberships to religious affiliations and gender or age-based cohorts (Tajfel and Turner 1985). Ashforth and Mael (1989) argue that the social categorization provided by SIT serves two functions: First, it imposes cognitive order on the social structure, allowing a systematic mechanism to define and classify individuals. Second, it allows individuals to define or locate themselves within a larger social system.

Social identity theory defines two different aspects of identity: *personal identity* and *social identification* (Ashforth and Mael 1989). Personal identity represents the idiosyncratic characteristics such as bodily attributes, interests, abilities, etc. that allow individuals define themselves in a larger social environment. In comparison, social identification allows to define oneself with respect to group characteristics. Identification, thus, is the perception of belongingness to a group. Although social identity theory explains the concepts of self and social categorization, it is easily operationalized with respect to cyber identities. In particular, OSNs allow projection of salient and pervasive aspects of digital identities by virtue of specifying profile attributes and group affiliations, and even by creating and sharing content

Proposed by Tajfel and Turner (1985), Social Identity Theory (SIT) is based on the premises of two extreme forms of social behaviors-*intergroup* and *interpersonal*. The interpersonal

behavior is determined primarily by the interaction between two or more individuals based on their interpersonal relationships and personal characteristics. Interpersonal behavior is independent of the influences of social categories to which individuals may belong. In comparison to interpersonal behavior, intergroup behavior is determined by the interactions between two more individuals based on their memberships or affiliations to respective social categories. Intergroup behavior is independent of the interpersonal relationships and individual characteristics of the people involved. Along this interpersonal-intergroup continuum are the provisions for intergroup conflict. The more intense an intergroup conflict is, the more likely an individual belonging to the opposite groups will exhibit behavior as defined by her group memberships and not by the interpersonal relationships or individual characteristics. Tajfel and Turner (1985) argue that, social identity theory categorizes individuals with respect to their identification characteristics. These identifications are largely comparative and relational. To that effect, Tajfel and Turner propose following three theoretical principles: 1) Individuals strive to achieve or maintain positive social identity; 2) Positive social identity is based on the comparative evaluation between in-group and out-groups where the former is perceived positively differentiated from the latter; 3) In case of unsatisfactory social identity, individuals will either leave existing group and join some positively distinct group or strive to make their existing group more positively distinct.

2.2.4. Parallels Between Identity Theory and Social Identity Theory

Some scholars have drawn conceptual links between identity theory, social identity theory, and values. For example Hitlin (2003) argues that identity theory and social identity theory define the fundamental interplay between individuals and social world. Although both theories conceptualize self as defined by social roles and categorization, these theories posit an additional

level of *personal identity* informed by an individual's personal values (see, Hewitt 1997). Thus, Hitlin draws a conceptual bridge between values, personal identity, identity theory, and social identity theory as illustrated in Figure 2. Furthermore, Hitlin argues that personal identity is not simply role structure or in-group/out-group comparisons of self; it is a product of value commitments. Theoretically values and personal identity are connected by the concept of authenticity- a primary self-motive. One feels authentic when he/she behaves in keeping with his/her values, thus reflecting ones' personal identity. Finally, Hitlin argues that there are clearly similarities between values and personal identity with respect to the Schwartz (1992) five criteria for values. According to Hitlin, both values and identity have five characteristics: 1) are beliefs or concepts; 2) pertain to the desirable results of behaviors; 3) transcend specific situations; 4) determine selection and evaluation of acts, behaviors or situations; 5) are organized in order of relative importance These conceptualization of social identity and values fit well with respect to Keeney's (1992) conceptualization of stakeholder values (reviewed later). According to Keeney, values are ethical principles used as guidelines for evaluating choices. Values come in all forms- "ethics, desired traits, characteristics of consequences that matter, guidelines for action, priorities, value tradeoffs, and attitudes toward risk all indicate values" (pg. 7).

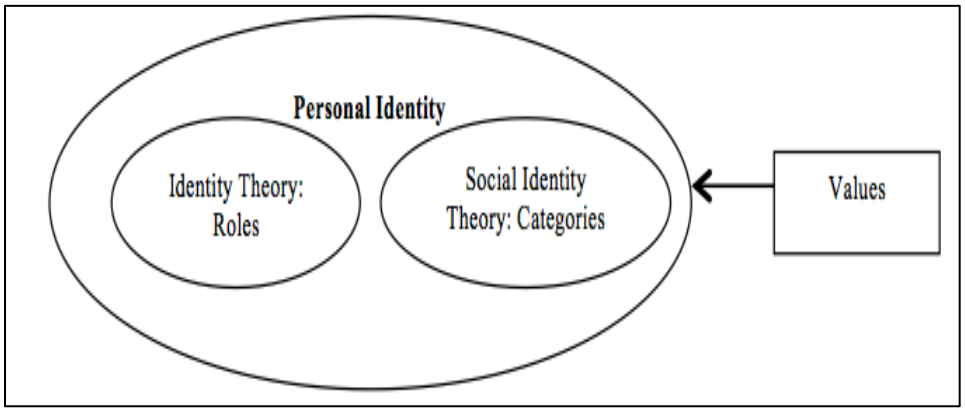


Figure 2: Conceptual Bridge Between Identity And Values (Conceptualized From Hitlin 1997)

2.2.5. Identity Threat

Perriglieri defines identity threats as the "experiences appraised as indicating potential harm to the value, meanings, or enactment of an identity" (Petriglieri 2011, pg. 644). Perriglieri argue that the definition not only encompasses the diverse aspects of threats as conceptualized by various disciplines but also sharpens its focus at three levels. First, the definition is grounded in individual's appraisal of the experiences as possible identity threats. Appraisal is a two-step process: primary and secondary appraisals. While primary appraisal evaluates the significance of an event with respect to personal well being, secondary appraisal determines the response to the threat. Second, this definition emphasizes assessing present cues that could possibly threaten the identity in future. Third, this definition incorporates the relation of threats to the value, meaning, and enactment of individual identity.

People value personal identities positively and thus appraise threats as devaluation of identity. Such devaluation could originate from in-group or out-group differences. With respect to meaning, Perriglieri argues that every identity is conceptualized in terms of some meaning. For example "a blacksmith may associate the meanings of "independence" and "skill" with his or her professional identity and make those meanings part of how he or she views him/herself" (pg. 646). Identity meaning is threatened when an individual appraises an experience that questions the link or association between the identity and the meaning(s). Finally, an individual appraises an experience as threatening if it prevents or limits the enactment of an identity in the future. The strongest threat is perceived if an individual appraises that the identity could not be enacted in future. Perriglieri argues that the threats to the enactment of identity occur due to competing demands from multiple identities. For example, a woman may appraise her professional identity to be threatened if its demand encroaches on the expression of her family role identities.

Within this background, Perriglieri discusses three main sources of threats. First, threats could originate from individuals themselves either due to conflicting identities or by taking identity-threatening action. Ashforth and Mael (1989) argue hat two identities conflict if the values, beliefs, norms, and demands inherent in the two identities are conflicting. Second, threats originate from the interpersonal interactions in social world. At group-level, individual may experience in-group threats in the interactions that question the individual's belongingness to the group. Out-group threats originate from the judgments that devalue the identity of competing or conflicting group to which an individual belongs. Third, threats originate from social world that are independent of individuals or groups. These include, for example traumatic incidents that threaten the identity of an individual. For example, natural accident could reduce prospective career opportunities. In the context of Online Social Networks (OSNs), individuals experience myriad of identity threats. It was recently reported that in the US there was a 32 percent increase in loss of personal identity complaints (Levin 2013). Additionally, OSNs also pose threats to the social identity of individuals due to the negative or de-valued treatment (see Agranoff 2012).

The coping process follows the threat appraisal process. Perriglieri differentiates between two types of coping processes: identity protection and identity restructuring. Identity protection mechanisms target source of the threat and encompass three types of responses: derogation, concealment, and positive-distinctiveness. Derogation means discrediting the source of the threats i.e. condemning the condemner. Concealment means to abandon the execution or exhibition of an identity that an individual appraises to be threatened in a particular context. Positive distinctiveness is an attempt to provide information for enhancing the positive perceptions of the identity and thereby change the outlook, attitude, or reaction of the individuals or groups towards such identity. In comparison to identity protection, identity restructuring

involves changing the aspects of a threatened identity and encompasses three types of responses: importance change, meaning change, and identity exit. Importance change means decreasing the importance of or downplaying an identity and thus eliminating the potential severity of harm. Meaning change involves change of expectations from an identity so as to eliminate the threat embedded in previous meanings. Finally, identity exit means abandoning the identity and disengaging from the role associated with a particular identity.

2.2.6. Values and Value Theory

The enriching role of *values* in social scientific research has long been recognized. Value concepts provide a richer perspective about human and social behavior. Typically values are considered as cultural manifestation of beliefs inherent to a particular group (Schein 1985a; 1985b). In the extant literature, there are several parallels drawn between values and emotions. While values are central beliefs expressed through specific behaviors (Rokeach 1973), emotions are feelings linked to specific behaviors (Gardner 1985). According to Holbrook (1986), values indicate preferences and are exhibited by affective emotional valence.

To information systems scholars, value-based research is not unknown. Over the years, several mainstream information systems (IS) theories grounded in values, both explicitly and implicitly have emerged. However, as Horley (2012) notes, "despite recognition as an important, potentially unifying construct within the social sciences and humanities, value lacks an overarching theoretical framework." Some notable progress is witnessed though. Tan and Hunter (2002), for instance, propose the personal construct theory as a means to study values, particularly with respect to different conceptions of systems developers. Originally proposed by Keeney (1992), the concept of value-focused thinking is introduced to IS scholars by Torkzadeh and Dhillon (2002). Nevertheless, a unified value theory is still a far-fetched call.

Hechter (1993) notes that the scholarly research in values has been limited because of several impediments - values in all forms are not directly observable; informing disciplines such as economics, psychology, and sociology hasn't contributed much to the understanding of values and value theory; processes to generate values are unclear. Consequently, Hechter makes a call for novel measurements effort for the definition and measurement of values. A common practice for explicating reliable set of values is to appropriately probe indigenous groups (see Leidner and Kayworth 2006). Scholars apply inferences to generate a common set of values (Fischhoff 1991). In the context of decision analysis, Keeney (1992), Gregory and Keeney (1994) were perhaps among the earlier scholars to define a theoretical basis for conceptualizing and operationalizing values.

Keeney's (1992) ambitions for a theory of values are greater than any other contributors in the field of decision analysis. He argues that values should be the main criteria for decision-making as the desirability of the consequences contingent to a decision problem is dependent on values. In lieu with earlier scholars, Keeney defines values as ethical principles that provide guidelines for the evaluation of choices. Values come in all forms- "ethics, desired traits, characteristics of consequences that matter, guidelines for action, priorities, value tradeoffs, and attitudes toward risk all indicate values" (Keeney 1992, pg. 7). Keeney defies alternate based decision-making that lacks value perspective and proposes a framework –Value Focused Thinking (VFT)- for utilizing values for decision-making. "Value-focused thinking involves starting at the best and working to make it a reality. Alternative-focused thinking is starting with what is readily available and the best of the lot" (Keeney 1992, pg. 6). Besides values, Keeney states two additional motivations for value-focused thinking. One, alternate-focused methodologies are not suitable for decision problems if the alternatives are unknown. Second,

unlike other decision methodologies, VFT doesn't start with a set of pre-specified alternatives but defines or changes them. The prime criterion for any decision situation is availability of alternatives. Keeney argues that if a decision situation has none or one alternative, it doesn't qualify for decision-making process. Therefore, before any decision making, there has to be an opportunity to create alternatives. VFT creates such decision opportunity by identifying alternatives grounded in values.

2.2.7. State of Information Security Research

Traditionally, security has been reviewed from multiple analytical lenses - technical, behavioral, managerial, philosophical, and organizational (Zafar and Clark 2009). In one of the earliest reviews, Baskerville (1993) discusses information systems security analysis and design methods. Specifically, three generations of methodological approaches are discussed: first generation – checklists; second generation - mechanist engineering; third generation - logical transformation. These three generations indicate a progression from the checklists for risk analysis to the engineering approaches for control and exposure analysis, and to the design of logical controls by virtue of abstraction. However, Baskerville (1993) suggests that early research on IS security was limited to the design of technological solutions. Furthermore, he makes an important call of not to give security an afterthought. Instead, IS security methodologies should be integrated with general system development methodologies.

In analyzing IS security literature, Dhillon and Backhouse (2001) critique the partial focus of security on the technical aspects. They were probably amongst the first few researchers who responded to the call made by Baskerville (1993) for integrating security methods with general IS development methodologies. Dhillon and Backhouse argue that information systems literature has socio- organizational focus whereas information security has been technically oriented.

Moreover, by organizing the information security research around the four paradigms of Burrell and Morgan (1979), the authors recommend security research to be analyzed from a socio-organizational perspective grounded in the interpretive paradigm. The authors argue that the checklists, controls, and evaluations are grounded in functionalist paradigm, which assumes the existence of reality. Furthermore, Dhillon and Backhouse argue that the context for traditional view of security has changed and hence considering organizations and security as objective reality doesn't capture the changed context. The authors make a call for social and behavioral oriented research as they note, "The prevention of such events therefore means more than just 'locks and keys' and must relate to the social groupings and behaviors" (pg.147).

Siponen (2001) analyzes the approaches to develop IS security from alternate approaches - Information/Data Base modelling approaches, responsibility approaches, and the security modified IS development approaches. The author argues that such an analysis is important because these approaches differ in the philosophical assumptions, and a comparative study will thus explicate the assumptions, strengths and weaknesses of these approaches. In analyzing the literature, Siponen reports that the research corresponding to the three paradigms can be traced to the disciplines of Data Modeling, IS, and Computer Science. The underlying philosophy for data modeling and computer science based approaches is positivism whereas IS has been influenced by both positivism and interpretive. Moreover, data modeling and computer science based approaches consider the development of security from technical perspective. In closing, Siponen acknowledges the need for a shift from technical to socio-technical or socio-organizational perspectives using interpretive research paradigm.

Siponen (2005) revisits the traditional approaches of Information Systems Security (ISS) development to identify the assumptions behind them and the future research directions. It is

reported that although scholars associate ISS methods to several generations, the ones related to early generations are more predominant. These include ISS checklists, ISS standards, maturity criteria, risk management, and formal methods. Siponen reports that the traditional methods are still common as they address fundamental features. The most prevailing objective of traditional ISS is oriented towards means-end, and as such more interpretive and critical studies are conducted. Moreover, the traditional methods are more inclined towards technical solution, and as such the socio-organizational perspective is not captured by traditional approaches. A call is made to conduct more of social ISS studies.

Zafar and Clark (2009) conducted a comprehensive survey of ISS research. The authors argue that the existing definition of security has been skewed; a more holistic perspective of ISS comprising of technology, people, and processes can't define security in a single sentence. Part of the problem is attributed to the focus of previous research that delineates Information Security from Information Systems. The research focus has been socio-philosophical, socio-organizational or technical. Zafar and Clark organize ISS literature around the constructs of Information Security Framework defined by IBM Corporation- IBM Information Security Capability Reference Model. Besides the eight themes of the framework, Zafar and Clark identify another emergent theme in ISS-economics. The level of analysis has been reported at individual, group, business, organization, and marketplace.

In a recent study, Crossler et al. (2012) acknowledge the skewed focus of ISS research on the technical issues. The authors argue that the much of the weaknesses in today's security approaches is due to delineation of user perspective. "Behavioral InfoSec research is a subfield of the broader InfoSec field that focuses on the behaviors of individuals which relate to protecting information and information systems assets … which includes computer hardware,

networking infrastructure, and organizational information" (pg. 91). To identify the research challenges and future directions of behavioral InfoSec research, the authors reached out to the participants of International Federation for Information Processing (IFIP) Working Group 8.11/11.13. Four categories of research areas are identified: 1) Separating insider deviant behavior from insider misbehavior; 2) Unmasking the mystery of the hacker world; 3) Improving information security compliance; 4) Cross-cultural InfoSec research.

It is clear from the review that repeated calls have been made to switch the focus to the behavioral aspects of information security. The study of values and human responses fits well within the behavioral aspect of information security research. In particular, Siponen (2000) notes "Emotions are an integral part of thinking and rational decision making. When people are confronted with a set of choices, emotional learning (past experiences) streamlines their decisions by eliminating some options and highlighting others …Consequently, security measures should aim at provoking emotions and appealing to them in order to affect attitudes and motivation in a positive manner" (pg. 37).

2.2.8. Identity Research In Information Systems

This section summarizes and discusses the identity research in Information Systems. To explicate the focus of existing research and the contribution of our study, a literature map (Figure 3) is designed. A literature map is a visual representation of the existing research (Creswell 2013).

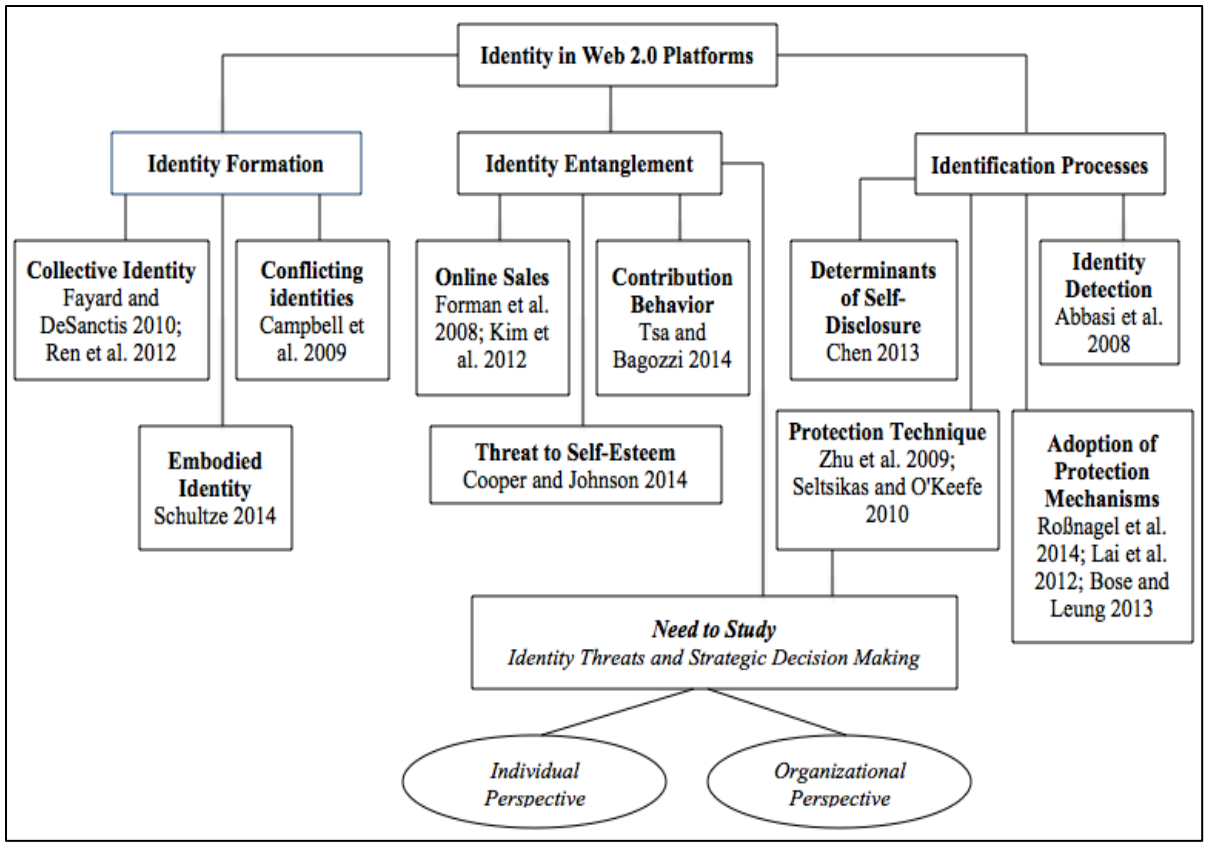


Figure 3: A Literature Map of Identity-Related Research in IS Domain

Table 1: Identity Research in Information Systems

No	Authors	Research Topic	Unit of Analysis*					Method	Theory	Themes
			I	D	G	O	S			
1	Whitley et al. 2014	Identity and Identification						Discourse	Identity theory	Discourse
2	Schultze 2014	Embodied identity	✔					Qualitative	Identity Performance: Representational and Performative Identity	Identity Formation
3	Campbell et al. 2009	Conflicting identity	✔					Qualitative	Critical Theory of Tribalism in virtual Communities	Identity Formation

4	Fayard and DeSanctis 2010	Collective identity			✔			Qualitative	Wittgenstein's concept of language games	Identity Formation
5	Forman et al. 2008	Relation between reviewers' identity and sales	✔					Econometrics	Social Identity theory	Identity Entanglement
6	Kim et al. 2012	Motivations to purchase digital items in virtual communities	✔					Statistical Analysis	Theory of self presentation	Identity Entanglement
7	Roßnagel et al. 2014	User's willingness to pay for Federated Identity Management	✔					Choice - based Cojoint Analysis		Identification
8	Abbasi et al. 2008	Technique to use stylometric similarity detection for trader identification	✔					Stylometric similarity detection system	Systemic functional linguistic theory	Identification
9	Ren et al. 2012	Collective identity	✔		✔			Field and Laboratory Experiment	Theory of common identity and common bond	Identity Formation
10	Tsai and Bagozzi 2014	Determinants of we-intentions and their impact on contribution behavior in virtual communities	✔		✔			Quasi-experimental study	Theory of collective intentionality	Identity Entanglement
11	Seltsikas and O'Keefe 2010	Electronic identity management in e-government systems	✔					Qualitative		Identification

12	Bose and Leung 2013	Impact of adopting identity theft counter measures by firms				✔		Statistical Analysis	Theory of dynamic capabilities and the principle of shareholder value maximization	Identification
13	Cooper and Johnson 2014	Threat to self esteem in seller-buyer negotiations		✔				Statistical Analysis	Theory of self-esteem	Identity Entanglement
14	Zhu et al. 2009	Identity Protection technique	✔					Algorithms		Identification
15	Chen 2013	Stimuli and inhibitors to members self disclosure	✔					Statistical Analysis	Information Disclosure Behavior	Identification
16	Lai et al. 2012	Factors that influence consumers adoption of identity protection practices	✔					Statistical Analysis	Coping theories: the process view and the style or personality view.	Identification

*I=Individual, D=Dyad, G=Group, O=Organization, S=Society

As obvious from the literature map, the concept of identity is sporadically studied in IS. The search on identity research in online networks fetched only 16 papers (see, Table 1). Other scholars have also called attention to such lack of research in IS. For example Whitley et al. (2014) note that although identity is being researched in various disciplines such as organization sciences, strategic management, and psychology, it is sporadically studied in information systems. The authors express surprise given the significance of identity to issues that are highly relevant to IS. "This is surprising given the significance of identity to a variety of issues that have received considerable attention from information systems researchers such as group and organizational sense-making... the shaping of organizational practices and change...

organizational learning ... and knowledge work..." (pg. 18). Furthermore, Whitley et al. (2014) argue that unlike management scholars who study identity purely from organizational perspective, IS scholars could provide thoughtful insights on the interaction of technology and organizational identity.

Overall, identity-related literature falls into three categories: identity formation, identity entanglement, and identification processes. Within *identity formation* category, it is Campbell et al. (2009) who study the lack of trust and cohesion in online social communities. The study shows that manipulative behavior could not only damages the ideals of a community but also increases stock price volatility and sends false market signals. The authors provide an interpretive account of the formulation and reformulation of three distinct identities in online financial investment forums: big man, sorcerer, and trickster. Furthermore, Campbell et al. discuss the role of power positions to control manipulative and exploitative behaviors of dishonest participants, thereby establishing the ground to reconsider design and governance procedures of online communities. Just like Campbell et al. (2009), Schultze (2014) conceptualize multiple identity perspective by studying embodied identities in social networking environments. In this qualitative study, Schultze explores the role of physical and digital identities, the relationship between the two, and the impact of the two types of identities on the embodied identity. Schultze observes the entanglement of online representation and real life performance in the behavior of entrepreneurs who enact embodied identities in both real and virtual environments. Another related aspect of identity, the emergence of collective identity, is also studied by IS researchers. For example, Fayard and DeSanctis (2010) study the construction of collective identity and culture through discussions on online forums. Like wise Ren et al. (2012) show experimentally that the identity and the bonding processes increase attachment

among the participants of online communities. Overall the research in this category focuses on the emergence of personal or collective identities at individual level.

With the ubiquity of OSNs, researchers realize the impact of these platforms on various other phenomenon. *Identity entanglement* category represents studies that analyze the impact of identifiable information on various social and economic aspects. In one of the earliest studies Forman et al. (2008) study the influence of revelation of reviewers' identity on product sales. This study shows that the reviewer's self-disclosure is positively related to the perceived helpfulness of the product review and the product sale. In a related study Kim et al. (2012) study the determinants of purchases of digital items in the virtual communities. Among many other factors individual identity in terms of expressive or symbolic power is reported to influence the purchasing behavior. Besides product sales, identity revelation influences the contribution behavior in virtual communities. For example, Tsai and Bagozzi (2014) in their quasi-experimental study analyze the determinants of the contribution behavior in small friendship groups. It is found that the social identity along with the group norms, attitudes, and anticipated emotions influence the contribution behavior, and the contribution behavior in turn influences we-intentions. Finally, the negative aspects of the entanglement have also received some attention. For example Cooper and Johnson (2014) study the threats to the self-esteem of negotiators in an instant messaging environment. Although, this study acknowledges the threats to self-esteem, it does not test the influence of the threat on the participant's identity. Overall, the research in entanglement category recognizes the complex interplay among social network, user identity, and other social and economic aspects.

The need for the protection and the assurances of identities has led to another stream of research, which is referred to as *identification processes*. In particular, scholars analyze the

factors determining the adoption of identity protection practices and disclosure mechanisms. For example Roßnagel et al. (2014) study user willingness to pay for Federated Identity Management - an alternative to password based sign-on in virtual communities and electronic commerce websites. Likewise, Bose and Leung (2013) study the impact of the adoption of the identity theft measures on the market value of ecommerce firms. In a related study Lai et al. (2012) study the factors influencing the adoption of identity protection practices by the consumers. There is also some research around the stimuli and inhibitors to member's self-disclosure (see Chen 2013). Finally, informed by the design science paradigm, few scholars propose the techniques to detect and protect individual identities. For example, Abbasi et al. (2008) propose a stylometric technique to identify traders based on feedback comments posted in an online reputation system. With respect to the protection strategies Zhu et al. (2009) propose an identity protection mechanism in the data mining techniques. In a related study, Seltsikas and O'Keefe (2010) study the digital identity management in e-government systems. The authors identify ten themes of identity management and map them to the theoretical framework.

Clearly the existing research has enhanced our understanding about identity and identification in social network environments. However, based on the analysis, the existing research falls short by five perspectives: 1) Much of the existing research analyzes identity at individual-level. Other units of analysis have not been studied. Particularly OSNs impact the identities of organizations and groups and therefore presents a compelling avenue to study. 2) Although, existing research acknowledges the threats to identity in OSNs, the focus is limited to the personal identifiable information. Threats to the social identity of individuals have not received attention. Moreover, the identity protection focuses on the adoption and not on the definition of mechanisms. The protection measures by themselves are not empirically validated.

3) Identity and identification represent two distinct strands of research; however, there is a considerable overlap between the two due to increased intervention of technology. More specifically, the negative implications on identity due to the entanglement need to be researched. Whitley et al. (2014) made a similar call as they note the negative implications of social networking sites on the identity of individuals. The authors assert that multiple identities, fake identities, abusive behavior, fraud, tension between personal and professional identities etc. impact user identities in the social networking sites. 4) Identity threat is a societal concern and raises methodological challenges. Scholars argue that sensitivity to such concerns often cause significant bias in reported research results (see Whitley et al. 2014). Given these challenges, the data for this dissertation is collected from multiple sources (individuals and social media). In particular, multi- and mixed-methods approach is adopted to alleviate the bias problem. 5) Finally, the concepts of social network and identity have broader applicability; an interdisciplinary approach to understand the relation of two could provide richer insights. To this effect, this dissertation conceptualizes threats to both personal and social identity of individuals and then defines the objectives to prevent the perceived threats. Moreover, the research builds on the theories and techniques from several disciplines including sociology, decision analysis, and information system.

2.3. Research Study 2: Reputation Threats to Organizations in Online Social Networks

2.3.1. Theories of Organizational Identity

Organizational identity, unlike organization sciences and strategic management, is sporadically studied in information systems. Whitley et al. (2014) express surprise given the significance of identity to issues that are being highly relevant to IS. The authors argue that unlike management scholars, who study identity purely from organizational perspective, IS

scholars could provide thoughtful insights on the interaction of technology and organizational identity.

> *This is surprising given the significance of identity to a variety of issues that have received considerable attention from information systems researchers such as group and organizational sense-making... the shaping of organizational practices and change... organizational learning ... and knowledge work...(Whitley et al. 2014, pg. 18).*

The concept of organizational identity is defined from two perspectives (Albert and Whetten 1985; Whetten 2006). Firstly, organizations use identity to define and characterize aspects of self. For organizations, identity is a question of self-reflection grounded in its values. Organizational decision makers introspect values to select a possible solution that is representative of organizational identity. Albert and Whetten (1985) note:

> *With respect to organization's use of concept, a prototypical sequence leading to questions regarding identity might be the following: an organization may decide which of several new products to market, which of several companies to acquire, which of several divisions to sell, or how to absorb a 20% budget cut internally. In short, organizations face choices of some consequences. Debate surrounding the alternatives is usually carried out, at least ideally, in terms of some model of rationality in which questions of information, probability, and expected utility dominate the discussion. When these considerations are not sufficient to resolve the question, and the importance of the question is inescapable, questions of information will be abandoned and replaced by questions of goals and values. When discussion of goals and values becomes heated, when there is deep and enduring disagreement or confusion, someone may well ask an identity question: "Who are we?" ,*

"What kind of business are we in?" or "What do we want to be?" (Albert and Whetten 1985, pg. 264-265).

Furthermore, Albert and Whetten argue that when the question of identity requires to reflect on organization's culture, philosophy, market position or membership, the answer should suffice three requirements: 1) features that captures the essence of organization - criterion of claimed central character; 2) features that differentiate the organizations from others - criterion of claimed distinctiveness; 3) features that exhibit continuity over time - criterion of claimed temporal continuity.

Secondly, researchers use identity to conceptualize and operationalize certain aspects of an organization. Authors argue that all three criteria are necessary and sufficient to operationalize organizational identity. While criterion of claimed central character provides an important distinction to an organization, there is no theory that defines the dimensions of distinction. It is left up to the judgment of decision-makers to determine central character. Albert and Whetten acknowledge the threats to organizational identity when the characteristics are debated openly, as they cite the example of acquiring a new company as opposed to debating a case in court. In the latter case the outcome of the discussion between adversaries could have serious ramifications on the identifiable characteristics of organization. How an organization should defend or disambiguate such identity threatening statements is a question of research, note the authors.

With respect to the criterion of claimed distinctiveness, authors notes that organizations face two issues in differentiating themselves. First relates to distinguishing between public and private identity. The authors argue that greater the difference between public and private identity, the more its effectiveness will be impaired. Such organizations will face difficulties in garnering

support required for the survival. Second relates to conveying the identity to others. Authors note that although organizations disseminate identity information in terms of press releases and annual reports, identity is also reflected by means of signs and symbols. Such symbolic identifiers could be threatening as well. With respect to the second research study, both issues of identity are relevant as OSNs allow projecting identity that could be different than the intended identity. Moreover, the textual identification processes could be a threat to the intended identity of an organization. Finally, with respect to criterion of claimed temporal continuity, authors are concerned about loss of identity and its consequences. From organizational perspective, identity loss could threaten the existence of business.

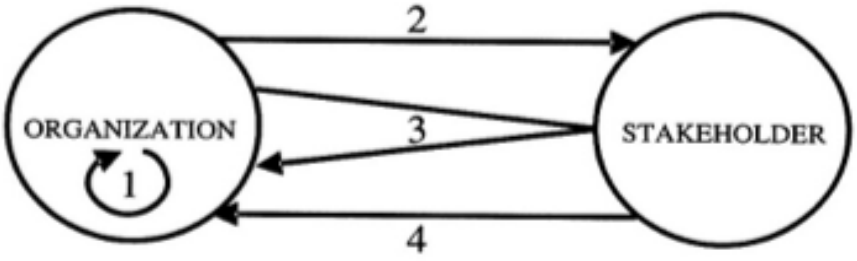
2.3.2. A Framework for Understanding Organizational identity, Image, and Reputation

Due to increased interest of scholars across various disciplines an inconsistent terminology has emerged over the years. Recently, Brown et al. (2006) proposed a framework to guide scholars who study the concepts of organizational identity, reputation, and image. Based on the literature review Brown et al. (2006) argue that organizational researchers broadly study three research questions: (1) what do various stakeholders know or believe about a focal organization? (2) How does focal organization develop, use or change this information? (3) How do stakeholders respond to what they know about the focal organization? The authors argue that addressing these questions is important from both individual and organizational perspectives. For example, organization will be interested to know both customer responses and employee responses for launching a new product. Furthermore, the authors emphasize that the interdisciplinary research on these concepts is required for two reasons. Firstly, previous research shows that organizational identity, image, and reputation influence the performance of an organization. Two, corporate identity and associations are broader topics that could be

understood from the insights provided by multiple disciplines. To that effect, Brown et al. note that it is worthwhile to develop a consistent terminology around these concepts. A review of literature allowed the authors to conceptualize four viewpoints operationalized as research questions. These are shown in Figures 4.a. and 4.b.

Given these four views, the authors argue that scholars have adopted varied terminology. To address this problem, a framework as shown in Figure 5.b is proposed. It has two dimensions, the first dimension represents if the research considers all or partial set of organizational aspects as proposed by Albert and Whetten's (1985) definition of organizational identity (i.e. centrality, endurance and distinctiveness - CED). The second dimension represents the level of analysis, i.e. individual vs. organizational. At individual level, the focus of the four viewpoints is to study the individual perspective about an organization. In this case an organizations' image, reputation, or identity is a mental conceptualization of an individual. In contrast, organizational analysis views organizational identity, image or reputation as organizational characteristic.

FIGURE 1
Key Organizational Viewpoints



1 "Who are we as an organization?"
2 "What does the organization want others to think about the organization?"
3 "What does the organization believe others think of the organization?"
4 "What do stakeholders actually think of the organization?"

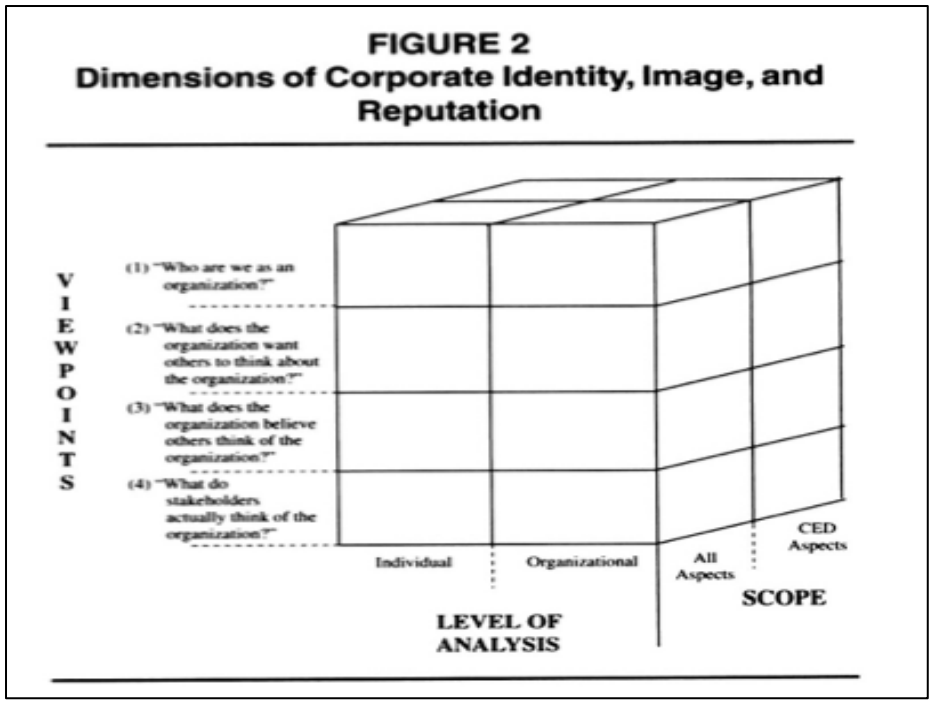


Figure 4.a: Key Organizational Viewpoints **Figure 4.b:** Dimensions of Corporate identity

(Adapted from Brown et al. 2006)

Table 2 provides a summary of the four views. The first viewpoint is about the perceptions of organization held by insiders. The authors' recommend the use of word *identity* to characterize the first viewpoint. Moreover, for organizational level analysis, *organizational identity* is appropriate whereas at individual level of analysis, *perceived organizational identity* or *organizational identity associations* are suggested terminology. The second viewpoint concerns about what image or association organizations intends to communicate. While the intended associations are the attributes of an organization that managers want stakeholders to view as strong associations, intended image is the constrained set of attributes that a manager wants stakeholders to view most salient. The authors recommend the use of *intended image* as the term to reflect management's view of how stakeholders should perceive the importance of the organization. Third viewpoint concerns about views that outsiders hold about the organizations.

At collective or organizational level, such a view is referred as *construed associations* and at individual level it is referred as *construed image*. The fourth viewpoint is concerned about how stakeholders view and respond to organizations. The authors recommend using the term *corporate or organizational association* to represent all information that an individual holds about an organization and the term *reputation* to represent the organizational association of individuals outside the organization. Furthermore, the authors differentiate between image and reputation. While *image* represent what organizational members want other stakeholders to believe about an organization, *reputation* is the actual perception of the organization held by external stakeholders. With this framework in mind, the second research study operationalizes the fourth viewpoint i.e. the reputation of organization in Online Social Networks.

Table 2: Unified Terminology (Borrowed from Brown et al., 2006)

TABLE 2
Proposed Unifying Terminology

Viewpoint	*Brief Description*	*All Aspects*	*CED Aspects*
"Who are we as an organization?"	Mental associations about the organization held by organizational members	Member organizational associations	Identity
"What does the organization want others to think about the organization?"	Mental associations about the organization that organization leaders want important audiences to hold	Intended associations	Intended image
"What does the organization believe others think of the organization?"	Mental associations that organization members believe others outside the organization hold about the organization	Construed associations	Construed image
"What do stakeholders actually think of the organization?"	Mental associations about the organization actually held by others outside the organization	Corporate (organizational) associations	Reputation

NOTE: For each viewpoint, the proposed terminology applies to both the individual and organizational levels of analysis. CED = central, enduring, and distinctive.

2.3.3. Theory: Situational Crisis Communication Theory

A growing body of literature on crisis communication aims to understand the interrelationships between crisis situation, stakeholder perceptions, and response strategies. Scholars argue that crisis impacts an organization's reputation and that 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 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 organizational 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 could assess the level of reputation threat i.e. the potential damage an organization's reputation could suffer in case no action is being taken. SCCT posits that three factors shape reputational threat: initial crisis responsibility, crisis history, and prior stakeholder relationship.

Crisis responsibility is the amount of the damage caused by the crisis that stakeholders attribute to the organization. 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, accidental, and intentional. In the case of victim cluster the organization is viewed as being a victim of crisis and stakeholders thus attribute low responsibility to the organization. This includes mostly natural events such as 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 scenario, 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. Finally, Coombs argue that crisis history and prior relational reputation moderate reputation threat. While crisis history indicates if an organization had similar crisis before, prior relational reputation is how well the organization have treated stakeholders in similar or other crises situations. Both factors could intensify reputation threat as stakeholders increasingly attribute crisis responsibility if the organization has history of crises or unfavorable prior relational reputation. However, a good crisis history and a relational reputation could also serve as a buffer to prevent reputation loss during crisis.

Crisis manager in preparing post crisis response considers these three factors to evaluate the reputational threat due to a crisis. The first step to assess reputational threat is to determine how much of the initial crisis responsibility stakeholders attribute to the organization. As the attributions increase, the reputation decreases. This step allows crisis manager to determine if an organization is considered to be a victim cluster, accidental cluster or intentional cluster. The second step is to assess the crisis history and prior relational reputation. As Coombs argue that although an organization may be considered a victim, a history of crisis and/or poor prior relational reputation will generate same degree of reputation threat as an accidental cluster.

2.3.4. Reputation and Reputation Threat

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 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 including 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 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 and smaller and non-U.S. based companies are not rated. These weaknesses imply the need for an alternate mechanism to better understand 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).

2.3.5. Online Social Networks (OSNs) 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 Pew Research, by January 2014, 74% of all Internet users used social networking sites, which represented a 32% increase

since Sept 2013[4]. Research shows that the diffusion of information on 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 recipients' opinions and decision-making. Moreover, research indicates that people trust the disinterested opinions of individuals beyond their immediate social networks (Duana et al. 2008).

The broad reach of electronic WOM afforded by OSNs, on the one hand provides tremendous power to consumers while on the other hand puts company's brand image at risk (Reynolds 2006). Management scholars recognize the potential of media to reflect and affect organizations reputation and disseminating the perceptions to public, thereby influencing stakeholders' perceptions and opinions about the organization (Rindova et al. 2007). The potential of online networks to influence opinions has serious implication on an organization's reputation. Referred as *online reputation mechanisms,* these platforms allows individuals to

[4] http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/

engage in bi-directional communication capabilities to generate large-scale word-of- mouth networks by sharing opinions and experiences on a wide range of topics such as companies, products, services, and even world events (Dellarocas 2006).

Previous research shows the efficacy of Twitter to impact word of mouth branding (Jansen et al. 2009). Attention economy, a new paradigm influenced by social networking sites, forces companies to compete for seeking attention of potential customers (Davenport and Beck 2002). As Jansen et al. argue microblogging services such as Twitter is a new forum to understand attention economy as consumers share brand-affecting opinions in short messages, from anywhere in the world to anyone connected to Twitter at a scale previously unparalleled. Few scholars also question the credibility of information on social networks. For example, Dellarocas (2006) argue that the characteristics of online forums allow interested parties to manipulate the information such as praising own products and bad-mouthing competitors for their own strategic purpose. In another incidence, in 2004, Amazon.com revealed the identities of book reviewers due to software glitch. A large number of reviews are written by publishers, authors, and competitors (Harmon 2004). There is no doubt that credibility of the information source and the strong reviews can impact stakeholder's response, nevertheless negative WOM presents a reputational threat in comparison to positive WOM (Coombs and Holladay, 2007).

Although a number of social networking sites have emerged overtime, in this study I am particularly interested in the most popular microblogging site - *Twitter* for its efficacy in generating large-scale eWOM. Twitter allows users - *Twitterers* post short messages up to 140 characters, which are referred to as *tweets*. Tweets can be sent and retrieved from several interfaces including web and mobile clients. Users create profiles by providing basic information such as name, email id, and location. User profiles and tweets can be set as public or private.

Any Twitter user can see public profiles and tweets whereas only those who have permission can see private profiles and tweets.

Twitter deserves serious research attention for 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 as a medium to harvest information about the crisis situation - *situational awareness* (Vieweg et al. 2010). In times of organizational crisis, diffusion or propagation of crisis information has unique implications on organizations reputation. Twitter has several features that make it indispensible 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 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 it easier to consume and re(produce) tweets. Furthermore, messages can be asynchronously noninvasive as individuals can decide whom to receive tweets from. Finally, tweets are archived and are searchable by web engines.

2.3.6. Diffusion of Information Security Reputation Threats-Hypotheses Development

Word of Mouth (WOM) has long been recognized as a powerful influence in shaping the attitudes of consumers (Brown and Reingen 1987). Although research shows that a number of other factors influence the consumers' evaluation of WOM such as source credibility, strong or. ambiguous comments etc. (Herr et al. 1991; Laczniak et al. 2001), marketers perceive negative WOM as a threat and positive WOM as a benefit. In the context of organizational crisis, stakeholders engage in negative WOM if the crisis responsibility is attributed to the organization

and/or stakeholders experience negative emotions. Coombs (2006) theory of SCCT posits that when an organization faces crisis, stakeholders exhibit various affective reactions depending on the crisis responsibility attributed to the organization. However, stakeholders experience anger if an organization is attributed responsible for the crisis as the crisis is contrary to stakeholders' expectation of how an organization should protect their interests (Hearit 2006; Coombs and Holladay 2007). Building on SCCT, this study argues that in times of a data breach stakeholders engage in negative WOM if the breach responsibility is attributed to the organization. Furthermore, the emotional arousal such as anger tips the scales of stakeholders in relaying negative comments about the data breach and the organization. Thus, increased attribution and negative sentiments represent negative WOM, which poses threat to organizations reputation (see Figure 5).

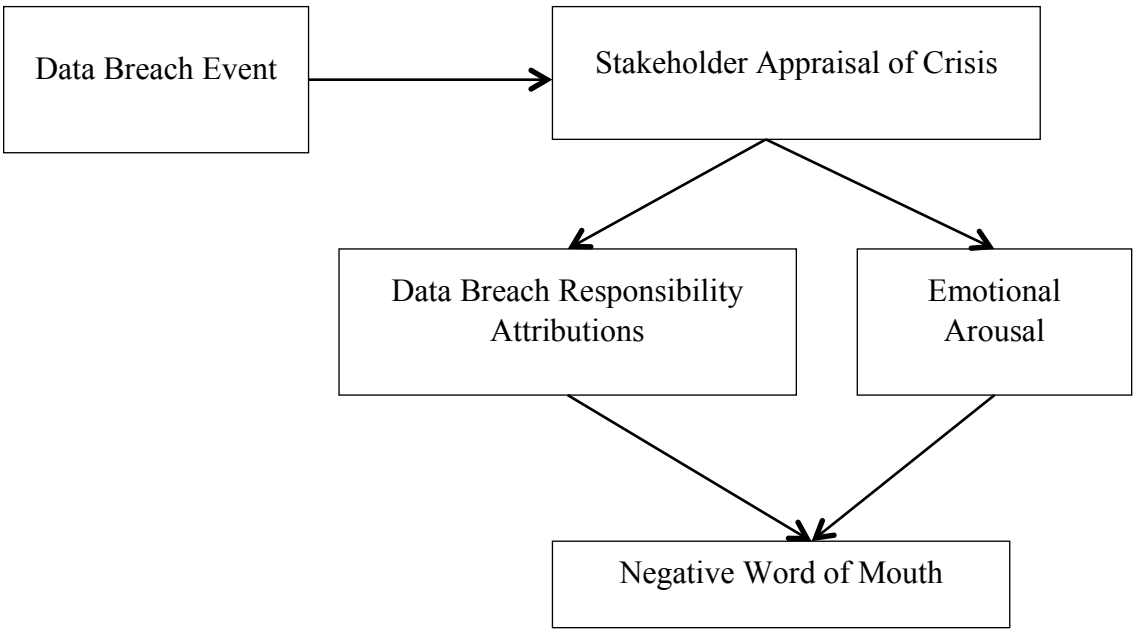


Figure 5: Conceptual Model for Information Security Reputation Threat

Contemporary psychologists have a consensus on the broad nature of emotions. Fischer et al. (1990) define emotions as "complex functional wholes including appraisals or appreciations,

patterned physiological processes, action tendencies, subjective feelings, expressions, and instrumental behavior" (pg. 85). Fischer et al. associate the action tendencies to emotions; the action tendencies arise when individuals perceive that their goals or concerns are being advanced or hampered in some way. Individuals sense some notable change by appraising the event with respect to their concerns or coping potential. The appraisal allows determining if the notable change promotes or interferes concerns. Individuals experience positive emotions if the event facilitates goal attainment and vice-versa. Likewise, individuals appraise the event with respect to their coping potential. A positive or negative emotion occurs depending on how an individual can cope with the event. Depending on the outcome of the appraisal process, individuals experience and exhibit action tendencies or behavioral reactions. Fisher et al. state that the action tendencies could permeate behavior such as feeling good, or raising attention to injustice.

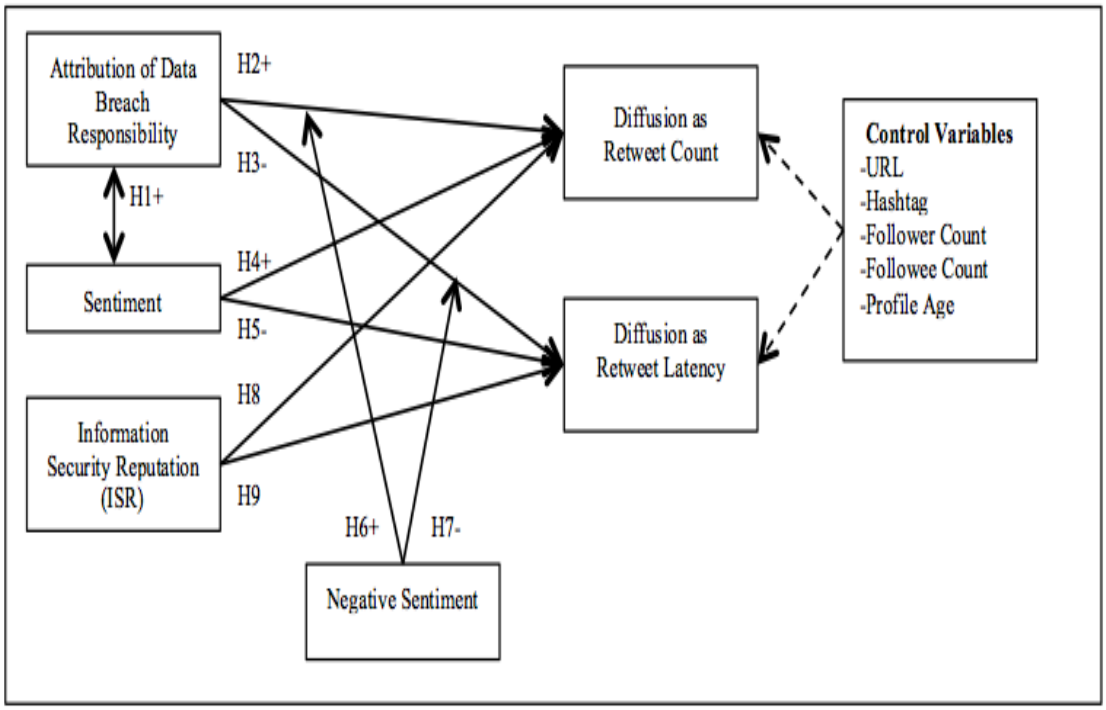


Figure 6: Research Model

Similar to Fisher et al., Coombs (2006; 2007) argue that the appraisal of crisis event causes individuals to experience emotions and consequently take actions. The greater attribution of crisis responsibility triggers more negative emotions in stakeholders. The arousal of negative emotions further cause stakeholders to engage in negative word of mouth or take actions that sever their interactions with the organization. In the context of Internet enabled communication, the action tendencies transcend into negative WOM in case stakeholders experience emotional arousal due to crisis situation. Previous research suggests a link between emotional arousal and negative communication dynamics. For example, dissatisfied consumers are more likely to engage in interpersonal WOM about products and services than satisfied customers (Richins 1984). Moreover, negative WOM has stronger effect on customer assessment of organizations reputation than positive WOM (Laczniak et al. 2001; Mizerski 1982). Based on these findings it is logical to assume that data breaches are contrary to stakeholder expectation about an organization's responsibility to protect their personal identifiable information. The announcement of data breach consequently arouses negative emotions when the organization is attributed responsible for the data breach. Consequently, we hypothesize:

H1: The association between attribution of data breach responsibility and sentiments is stronger for tweets with negative sentiments than for those with positive sentiments.

A large body of research in social and behavioral sciences study the spread of moods and behavior among network of people. Largely referred as behavioral or emotional contagion, it is the phenomenon by which people copy or imitate the behavioral or emotional responses. The term contagion has its roots in Latin word *contagio*, which means, 'to have contact with.' Psychologists define contagion as "the spread of ideas, feelings and, some think, neuroses through a community or group by suggestion, gossip, imitation etc." (Sutherland 1995).

Furthermore, Marsden (1998) states that although contagion is commonly conceived in biological sense, the concept came first to be known as a social phenomenon through the work of James Mark Baldwin (1894), Gabriel Tarde (1903), and Gustave Le Bon (1895). However, the empirical research to study the phenomenon of social transmissions began only in 1950. In the social scientific literature social contagion is defined as "the spread of affect or behavior from one crowd participant to another; one person serves as the stimulus for the imitative actions of another" (Lindzey and Aronson 1985). According to Marsden (1998), contagion refers to the social transmission, by contact, of biological diseases or sociocultural states. In general, the social contagion research can be classified into two major areas: emotional contagion and behavioral contagion. Studies related to emotional contagion analyze the spread of moods whereas the ones related to behavioral contagion analyze the spread of behavior. This research study is concerned about emotional contagion. The original definition is by McDougall (1920) who defines emotional contagion as "the principle of direct induction of emotion by way of the primitive sympathetic response". Much later Sullins (1991) defines it as "the process by which individuals seem to catch the "mood" of those around them."

In crisis situation, SCCT posits that the crisis responsibility and negative emotions cause stakeholders to take adverse actions against the organization ranging from engaging in negative word of mouth to severing interactions with the organization (Coombs, 2007). Furthermore, those angered by crisis situation may share their displeasure by posting negative messages about the organization. Coombs and Holladay (2007) state that, “Just as viral marketing hopes to spread favorable information from person-to-person, negative word-of-mouth spreads unfavorable information from person-to-person. The result is that the crisis has a potential effect on behaviors well beyond those who experienced the crisis or learned about the crisis through the

news media" (pg. 304). In the context of Internet enabled communications, negative word of mouth has greater reach and higher shelf life. Research suggests that social media technology increases the diffusion of negative word of mouth, which in turn effects the interpretation of messages by the receivers (Walther and D'Addario 2010; Harris and Paradice 2007; Riordan and Kreuz 2010).

Research suggests that information diffuses in social networks due to its structural properties and social reinforcement (Centola 2010). In other words, the network structure of social media spreads messages and emotions beyond immediate associates impacting on how receiver interprets and behaves. Moreover, the social reinforcement of behavior in networks further promotes the diffusion and adoption of behaviors. Informed by SCCT, stakeholders engage in attribution of breach responsibility, if they perceive the event as jarring. The social reinforcement coupled with network structure of OSNs would further diffuse the attribution information across larger population within the network. Consequently, the attribution messages will receive reinforcement and attention within the social network and therefore positively affect subsequent information diffusion. This leads to conjecture a positive relationship between the attributions articulated in tweets and their likelihood to spread through the Twitter network. Furthermore, informed by previous research on information diffusion (Yang and Counts 2010; Stieglitz and Dang-Xuan 2013), it is reasoned that the increased attributions impact the speed of subsequent diffusion of attribution tweets. Therefore, the following two hypotheses are proposed:

H2: Twitter postings attributing data breach responsibility are retweeted more often.

H3: Twitter postings attributing data breach responsibility have shorter retweet time latency.

Just like attribution of responsibility, emotions affect the spread of negative WOM in crisis (Coombs 2007). As discussed before, the network structures affect the diffusion of emotional responses among people. Previous studies suggest that the articulated sentiments (positive or negative) in messages might diffuse in the network causing subsequent comments or replies (Huffaker 2010; Stieglitz and Dang-Xuan 2013). Based on the above findings it can be inferred that the attribution and emotionally loaded messages may lead to more attention and arousal. In other words, emotionally laden attribution messages are retweeted more by Twitterers. Consequently, the following two hypotheses are proposed:

H4: The larger the total amount of sentiment (positive or negative) an attribution Twitter posting exhibits, the more often it is retweeted.

H5: The larger the total amount of sentiment (positive or negative) an attribution Twitter posting exhibits, the shorter is the retweet time latency.

Psychologists posit that the negative events have greater impact on individuals than the positive events (Baumeister et al. 2001). Specifically, when an individual confronts equal measures of good and bad events, the psychological effect of the negative events outweigh those of the positive events. More recently, the hypothesized effect of emotional messages on viral diffusion has been quantified. For example, Berger and Milkman (2010) analyzed a sample of 6,956 articles from New York Times to determine the affect of sentiments on the possibility of an article to make into the New York Times list of "most-emailed articles." The authors conclude a strong relation between the sentiment affect of a News article and the possibility of sharing it. The authors found that although the positive articles are shared more than the negative articles, but the articles containing negative content like anger or anxiety are more likely to be

shared. Drawing on these insights, it is posited that the attribution messages carrying negative sentiments will diffuse more than the attributions messages with positive or neutral sentiments. This leads to formulate the following two hypotheses:

H6: Twitter postings attributing data breach responsibility and negative sentiment are retweeted more often.

H7: Twitter postings attributing data breach responsibility and negative sentiment have shorter retweet time latency.

According to SCCT, reputation threat is shaped by the initial crisis responsibility. An increased level of attribution of crisis responsibility reduces the reputation score. Crisis managers conduct the initial assessment based on the crisis responsibility (see, Coombs 2007). Extant literature in mass media provides a rational for crisis types as crisis frames (Druckman 2001). Media communication involves two types of frames: communication frame i.e. words used to communicate the information, and cognitive frame i.e. interpretation that an individual draws from information. Cooper (2002) argues that the framing of a message shapes the definition, causes, attributions, and solutions to crisis. In other words, message framing emphasizes certain aspects of the event, causing the recipients of the messages to focus their attention on those salient aspects of the message (Druckman 2001). Coombs (2007) state that each crisis type is a frame and provides cues about certain aspects of the crisis. Based on these findings, it is argued that data breach related messages in OSNs are frames that provide cues about various information security dimensions of the organization. Depending on the attributions, some of the information security dimensions will be salient and may receive more attention in social media. Consequently the following two hypotheses are derived:

H8: Retweet count of Twitter postings varies for the Information Security Reputation (ISR) dimensions.

H9: Retweet latency of Twitter postings attributing data breach responsibilities varies for the Information Security Reputation (ISR) dimensions.

2.4. Conclusion

This chapter provided an overview of the literature pertinent to the study of identity threats in OSNs. A review of theories for studying individual and organizational identity is presented. Specially, identity theory, social identity theory, and theory of organizational identity are reviewed. Concepts related to identity threat are also discussed. Besides the fundamental theories of identity and identity threats, several other theoretical concepts with respect to reputation, sentiments, social networks, and value theory are reviewed. A review of information security research is provided to explicate the state of research. Furthermore, research related to identity in information systems is also reviewed. Both information security and identity research indicate that identity threats in OSNs have not received much attention. Finally, set of hypotheses predicting the diffusion of Information Security Reputation threatening tweets are presented. This literature review forms the basis for the two research studies that this dissertation reports.

Chapter 3: Qualitative and Quantitative Value Modelling

3.1. Introduction

Just like in any scientific discipline, scholars in the field of information systems engage in activities with the goal of explaining phenomena, which is more commonly called science. Nagel (1979) asserts that science purports "systematic and responsibly supported explanation" (pg. 15). To Nagel, explanations answer the questions. If asked and investigated correctly, each explanation contributes to the progress of the scientific knowledge. Nevertheless the scientific community reserves the right to determine if valid questions are asked and if valid rules are applied to investigate the truth of a theory (Kuhn 1996). One of the critical decisions for the advancement of the scientific knowledge is the selection of appropriate research approach to study the topic. Several factors inform this selection—philosophical assumptions, research design, research methods, and research problem (Creswell 2013). The purpose of this chapter is to discuss these factors with respect to the first research study i.e. social identity threats to individuals in Online Social Networks (OSNs).

3.2. Philosophical Worldview

It is convenient to conceptualize the scientific research in terms of assumptions related to reality—*ontology*, knowledge of reality—*epistemology*, and ways of seeking the reality—*methodology* (Guba 1990). Although the underlying philosophical assumptions remain largely hidden in many research projects, they still play an important role in the scientific inquiry. However, as Creswell (2013) notes, it is better to explicate the espoused philosophical worldview to justify the choice of research approaches. Based on Guba (1990, pg. 17), a worldview represents " a basic set of beliefs that guide action." Scholars have used various

terms to refer worldview such as paradigms, epistemology/ontology, and even research methodologies. Depending on the researcher's worldview or belief, a qualitative, quantitative, or mixed methods approach is embraced. Informed by Creswell (2013), there are four worldviews: postpositivism, constructivism, transformative, and pragmatism (see, Table 3).

Table 3: Four Worldviews (Adapted from Creswell, 2013)

Postpositivism	**Constructivism**
• Determination • Reductionism • Empirical observation and measurement • Theory verification	• Understanding • Multiple participant meaning • Social and historical construction • Theory generation
Transformative	**Pragmatism**
• Political • Power and justice oriented • Collaborative • Change-oriented	• Consequences of actions • Problem-centered • Pluralistic • Real-world practice oriented

This dissertation adopts a pragmatic worldview derived from the work of pragmatists such as Peirce, James, Mead, and Dewey (Cherryholmes 1992). Pragmatism as a worldview arises out of actions, situations, and consequences rather than antecedent conditions (Creswell 2013, pg. 10). Under this worldview researcher focuses on the research problem and uses all available research methods to understand the problem. Pragmatism is the thus the philosophical underpinning for mixed methods research. There are several philosophical tenets to pragmatism (see Creswell 2013): 1) Pragmatism doesn't require commitment to any particular ontological and epistemological assumption, thus allowing mixed method researchers to draw from both qualitative and quantitative methodologies. 2) Pragmatism grants freedom to researchers to choose methods, techniques, and procedures that serve the need best. 3) Pragmatism does not see

reality as one type of entity. In this way mixed method researchers can collect and analyze data using multiple approaches. 4) Pragmatism allows researchers to look at *what* and *how* questions with respect to the intended consequences. This provides a rational for mixing qualitative and quantitative data in mixed methods studies. Creswell (2013) argues, "for the mixed methods researcher, pragmatism opens the door to multiple methods, different worldviews, and different assumptions, as well as different forms of data collection and analysis" (pg. 11).

In information systems, mixed methods approach is well accepted. The first research study uses sequential mixed method approaches by conducting qualitative value modelling followed by quantitative value modelling. Exploratory nature of the qualitative phase allows understanding what identity threats are perceived by the individuals in the context of OSNs and how can such threats be prevented. It is important to conduct exploratory studies, particularly in light of the call made by scholars such as Pavlou (2011) and Whitley et al. (2014). To this effect, this research study justifies the use of mixed methods approach for three reasons: 1) It allows to leverage both qualitative and quantitative data and thus overcome limitations of each approach. 2) It is a sophisticated approach to study new types of research problems. 3) It provides a basis for rich meta-inferences (Venkatesh et al. 2013).

Once the researcher embraces a particular worldview and the type of study to conduct (qualitative, quantitative, or mixed methods), the next step is to design the inquiry. "Research designs are types of inquiry within qualitative, quantitative, and mixed methods approaches that provide specific direction for procedures in a research design" (Creswell 2013, pg. 12). Research design is also called as *strategies of inquiry* (Denzin and Lincoln 2011). This dissertation adopts a pragmatic worldview and uses mixed methods approach. Per Creswell (2013), there are three basic types of mixed methods research design: convergent parallel, explanatory sequential, and

exploratory sequential. Furthermore, these three basic forms could be combined to design advanced research approaches.

Convergent parallel mixed methods design allows the convergence or merger of quantitative and qualitative data for the comprehensive analysis. Both forms of data are collected in parallel, which is then integrated to allow overall interpretation. Explanatory sequential mixed methods design is the one in which researcher first collects and analyzes quantitative data. The results of quantitative analysis are then followed up and explained in detail by qualitative data collection and analysis. In comparison, exploratory sequential mixed methods design operates in the reverse sequence; researcher first collects and analyzes qualitative data followed by quantitative phase. Finally, the three types of design methods could be used to model advanced mixed methods design such transformative, embedded or multiphase, see Creswell (2013) for details. In the following sections, the research design and research method i.e. forms of data collection and data analysis procedures for the individual level study are presented. Specifically, the concepts and the technique for Value Focused Thinking and Multiple Objectives Decision Analysis as a unified decision analysis framework are discussed.

3.3. Value Theory and its Usefulness for Decision Analysis

Early research by Rokeach (1973; 1979) points to the usefulness of values as enduring perspectives that remain stable over a period of time and hence are a useful means to aid decision-making. In a similar vein, England (1967) also argues that values are preferences for a certain outcome. Such arguments were also central to the earlier interactionist perspectives in motivational psychology. Values are also considered as cultural manifestation of beliefs inherent to a particular group (Schein, 1985a; 1985b). To information systems scholars, value-based research is not unknown. Over the years, several mainstream information systems theories

grounded in values, both explicitly and implicitly have emerged. However, as Horley (2012) notes, "despite recognition as an important, potentially unifying construct within the social sciences and humanities, value lacks an overarching theoretical framework." Some notable progress is witnessed though. Tan and Hunter (2002) propose the personal construct theory as a means to study values, particularly with respect to different conceptions of systems developers. Originally proposed by Keeney (1992), the concept of value-focused thinking is also not new to IS scholars, e.g. see Torkzadeh and Dhillon (2002). Nevertheless, a unified value theory for IS research is still a far-fetched call.

Hechter (1993) notes that the scholarly research in values has been limited because of several impediments. Amongst many challenges, values in all forms are not directly observable, informing disciplines such as economics, psychology and sociology hasn't contributed much to the understanding of values and value theory and processes to generate values are unclear. Consequently, Hechter makes a call for novel measurement efforts for the definition and measurement of values. A common practice for explicating reliable set of values is to appropriately probe indigenous populations (see Leidner and Kayworth 2006). Scholars then apply inferences to generate a common set of values (Fischhoff 1991). In the decision analysis discipline, Keeney (1992) and Gregory and Keeney (1994) were perhaps among the earlier scholars to define a methodological basis for conceptualizing and operationalizing values.

Keeney's ambitions for value theory are greater than any other scholars in the field of decision analysis. He argues that values should be the main criterion for decision-making as the desirability of the consequences contingent to a decision problem is dependent on values. Keeney defines values as ethical principles that provide guidelines for the evaluation of choices. Values come in all forms — "ethics, desired traits, characteristics of consequences that matter,

guidelines for action, priorities, value trade offs, and attitudes toward risk all indicate values" (Keeney 1992, pg. 7). Keeney defies alternative-based decision-making that lacks value perspective and proposes a framework—Value Focused Thinking—for utilizing values for decision-making. Unlike many decision processes that start with alternatives to define objectives, Value Focused Thinking (VFT) uses values to identify alternatives. By focusing on values, decision makers overcome the constraints imposed by alternate focused thinking. In other words, alternate focused thinking is constrained and reactive whereas value-focused thinking is constraint free and proactive. To that effect VFT is a philosophy to make better decisions and relies on three main ideas: 1) Elicit values of stakeholders to identify objectives; 2) Identify better alternatives from the values; 3) Use values to evaluate alternatives using Multiple Objectives Decision Analysis technique.

Keeney (1992) mentions that VFT has nine benefits (pg. 24), which are self-explanatory. However, there are two additional motivations for applying VFT for studying identity threats in OSNs: One, it provides a transparent and a systematic approach to identify the better alternatives. This study sets the stage for future research agenda to identify better alternatives for preventing social identity threats to individuals. Two, the development of value model using value-focused thinking requires collaborative analysis amongst multiple stakeholders. Various stakeholders come together to identify objectives and build a value model (Raiffa 1982). This collaborative analysis allows the stakeholders to discuss underlying problems and the values and objectives of the stakeholders rather than being defensive about a particular objective (Merrick and Garcia 2004). Identifying the values of multiple stakeholders such as social network users and security experts resonates well with respect to the first research study.

3.4. Methodology for Multiple Objectives Decision Analysis (MODA)

The importance of theorizing about values and related decision analysis is more important today than has been the case in the past. Today's networked society and increased interdependence of businesses requires consideration of multiple stakeholder views. Multiple Objectives Decision Analysis (MODA) approach allows the consideration of multiple stakeholders' values and preferences. As has been argued by several scholars (Gregory and Keeney 1994), capturing stakeholders' values provides a superior basis for decision-making. This analysis is more suitable to complex decision situations involving multiple stakeholders, conflicting objectives and uncertainty (Keen and Morton 1978). Multiple Objectives Decision Analysis (MODA) is a mathematical technique to implement the ideas of Value Focused Thinking. This technique is also referred as multiple attribute utility theory, multiple attribute value theory, and multiple attribute preference theory. Keeney and Raiffa (1993) and later Kirkwood (1997) discuss the technique at length.

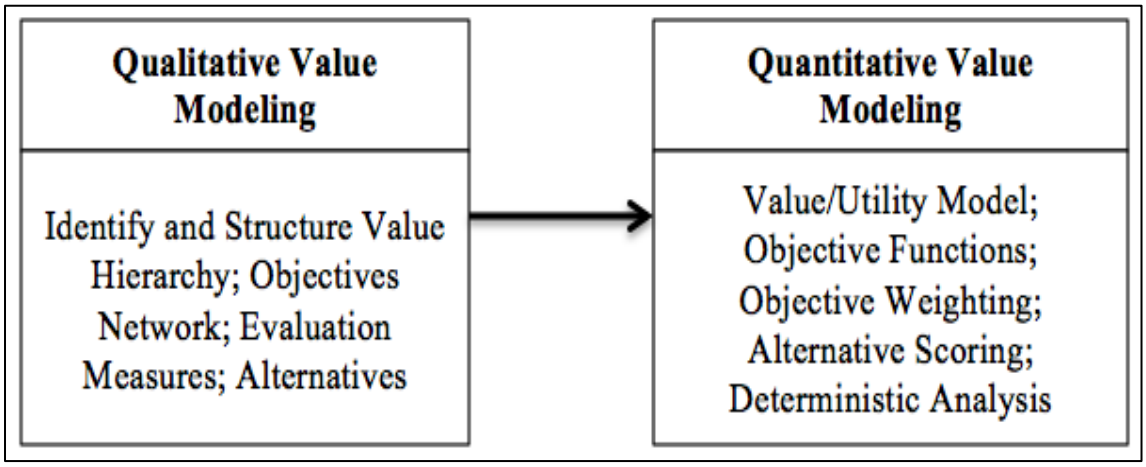


Figure 7: MODA Based Explanatory Sequential Mixed Methods Research Design

Overall the approach involves qualitative value modelling and quantitative value modelling. Figure 7 provides an overview of the MODA within the perspective of exploratory sequential mixed methods approach. The qualitative value modelling begins with identifying the overall objective followed by the value hierarchy that describes the fundamental objectives to be achieved for the decision situation. The evaluation measures also refereed as attribute levels to assess the degree of attainment of the fundamental objectives are then defined. Finally, the best set of feasible alternatives is identified from the values. Within the quantitative value modelling, first using the evaluation measures, single-dimensional objective functions are assessed for the objectives. The value hierarchy is weighted to indicate the relative importance i.e. values of the fundamental objectives. The alternatives are scored with respect to the objectives. Finally, deterministic analysis identifies the value gaps between the ideal alternative and best possible alternative. In the following paragraphs, the approach is presented and illustrated in detail. For each step, the characteristics of data are also discussed.

3.4.1. Qualitative Value Modelling

The qualitative value modelling determines the overall success of value-focused thinking. As qualitative value modelling forms the basis of quantitative value modelling, latter stages add little value if the values of right kind of stakeholders are not modeled. The steps to structure and develop qualitative value model are presented below.

Elicit Values and Objectives

The first step in the qualitative value modelling is to identify the individuals whose values are to be modeled. The first research study is concerned about the social identity threats perceived by individuals in Online Social Networks (OSNs), therefore this phase models the

values of common OSN users. The values are then used to identify objectives for a given decision situation, i.e. *Minimize Social Identity Threats in Online Social Networks*. There are various ways to identify values and objectives. The obvious one is to engage in a discussion with the stakeholders and determine what would they like to achieve in a given situation. In the decision analysis literature, scholars define three standards for identifying objectives: gold, platinum, and silver (see Parnell et al. 1998). The gold standard determines the objectives from several documents such as policy and planning documents or literature review. The platinum standard is one when the senior stakeholders and decision-makers are interviewed to identify objectives. Finally, the silver standard is the one when stakeholder representatives or subject matter experts are interviewed. Additionally, Keeney (1992) recommends that objectives could be elicited from more than one source such wish list, alternatives, problems and shortcomings, consequences, goals, constraints, and guidelines, different perspectives, strategic objectives, generic objectives, structuring objectives and quantifying objectives. The details about these strategies could be found in Keeney (1992).

Table 4: Data Sources for MODA

Phase	**MODA Activity**	**Data Source (Number of Participants)**
Qualitative Value Modelling	Identify Objectives	Literature Review (NA) Interviews (67) Focus Group (22)
	Identify Alternatives	Values and Literature Focus Group (5)
Quantitative Value Modelling	SDUF	Online Social Network Users (11)
	Swing Objectives	Security Experts (19)
	Score Alternatives	Security Experts (18)

In this research study, a combination approach is used to generate objectives. The approach begins with the literature review to identify what aspects of social identity could be threatened. Informed by Petriglieri (2011), social media users could perceive identity threats if the online experiences indicate potential harm to the value, meaning, or enactment of their identities This allows identifying three higher-level aspects of social identity that could be threatened: *value, meaning,* and *enactment*. Next a series of interviews were conducted to elicit values of typical online social network users that they perceive to be threatened in OSNs. The values were converted into objectives as described in the following paragraphs. A total of 15 fundamental objectives that emerged from the data analysis were then mapped to the three aspects of the social identity.

To elicit values, the intention was to identify a large number of social media users who would fit an average profile. McCracken (1988) is used as a guide to select interviewees. The starting point was to recruit working executives participating in a continuing education program at a large US based University. The candidates were recruited based on their age, gender, and years of experience in using social networking sites. Our respondents, all located in the US, had an average age of 35 years (20-25 years: 35 respondents; 26-35 years: 40 respondents; 36-50 years: 40 respondents; 50 and older: 32 respondents). Nearly 52% were women and 48% were males. Average user experience in using social networking was 3 years with at least 2 active social network memberships. On average each user visited a social platform site at least twice a week for either personal reasons or business and other professional purposes. A total of 67 interviews were conducted between January 2014 and November 2014. Each interview lasted an average of 90 minutes. All interviews were recorded.

This interview process follows Fischhoff's (1991) three guiding principles for participants to articulate their values. First, the participants are given enough time to think through questions during an interview. In case a participant struggles in framing a response, suitable probes are introduced (e.g. share your experiences when you felt a post made by your friend was inappropriate and did your other friends reacted negatively to the post? What measures did you take to prevent the damage?) Second, the aim of value elicitation is to identify a comprehensible set of consequences, which helps at later stage to define the objectives. The objectives themselves need to be commensurable into a common set. Third, the participants are pooled from different walks of life, which will allow multiple and diverse perspectives to be incorporated into the value set. The project was undertaken following an approval from the Institutional Review Board. The respondents were asked to think freely as to what they thought threaten their social identity in the context of OSNs. Suitable probes were used to uncover the latent values. The research process for value hierarchy is shown in Figure 8.

Following Keeney, interview data is converted into common form values, which were then clustered and redundancies were removed. A total of 67 interviews resulted in 1054 raw values, which after eliminating redundancies were reduced to a total of 584 clean values. These were further consolidated, largely based on values emanating a similar meaning, to a total of 395 values. Each of the values was then converted into an objective. Keeney (1992) suggests adding a directional preference in forming the objectives. There is typically a many to one relationship, i.e. many values may result in one objective. The process of creating objectives from values is exemplified in Figure 9.

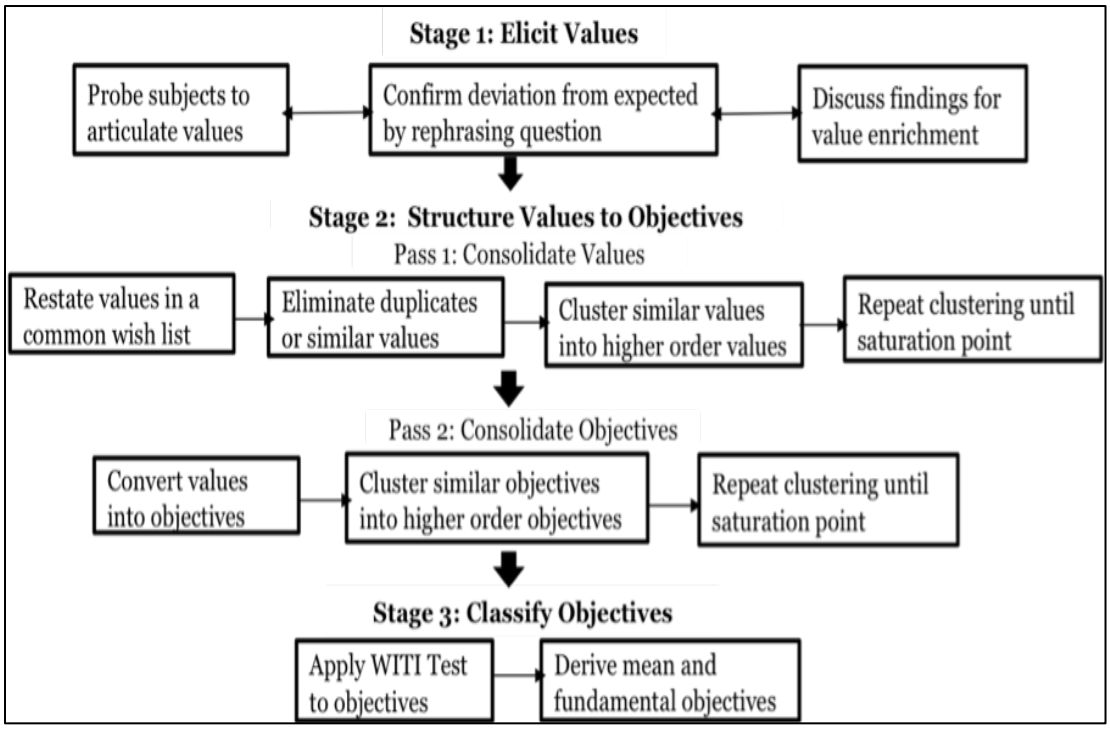


Figure 8: Value Elicitation and Value Hierarchy Development Process

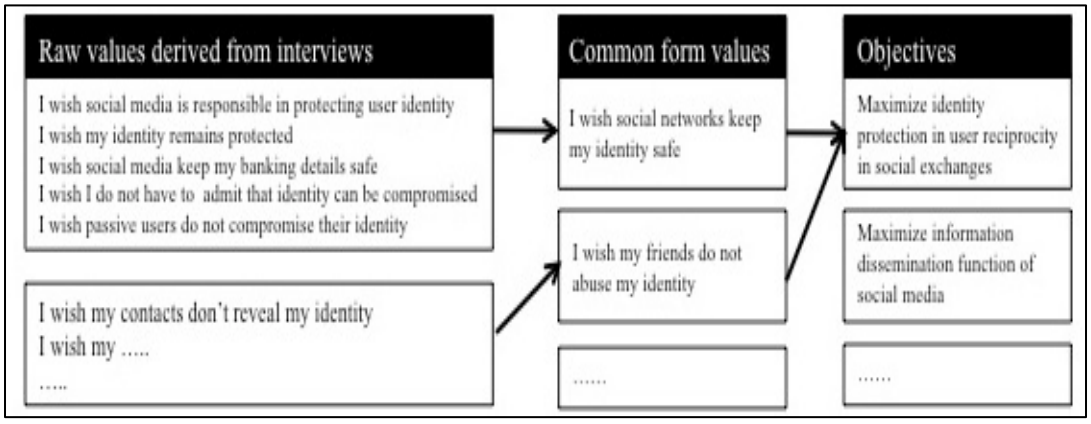


Figure 9: Process to Convert Values to Objectives

Define Value Hierarchy

For any decision analysis situation, the objectives need to be structured logically. The structuring of objectives results in fine-grained understanding of what decision makers need to care about. There are two major outcomes of the structuring process: fundamental objectives and

means objectives. While the fundamental objectives represent the aspects of a particular decision situation, the means objectives define the mechanisms to accomplish the fundamental objectives. The fundamental objectives are organized in a hierarchical tree structure referred to as *value hierarchy*. Each low level objective is an answer to the question "what aspects of the corresponding higher level objective are important?" The higher-level objectives are defined by the set of corresponding lower level objectives. The lower level objectives should be mutually exclusive and collectively characterize the higher-level objective. Each higher-level objective should have at least two lower level objectives. The fundamental objectives hierarchy can be structured top-down or bottom-up. Top-down structuring requires answering the question, "what aspects of the higher-level objective are important?" Bottom-up structuring requires answering, "are specific cases of what?"

It is ultimately the fundamental objectives that guide the development of value model. However, in the process, decision analysts also creates a means-ends network in which each lower level objective is an answer to the question, "How can the corresponding higher level objective be achieved?" The relationship between objectives is causal; the lower-level objectives are a means or causal factors to the higher-level objectives. There may be only one mean objective to a higher-level objective. Keeney (1992) suggest that the means-ends objectives network can be structured top-down or bottom-up. Top-down structuring of objectives requires answering the question, "How better to achieve a particular objective?" Bottom-up structuring follows "Why is it Important Test (WITI)" test. The structuring process classified the clusters of objectives into fundamental and means.

Keeney asserts that it is important to know when the objectives hierarchy and the objectives network are complete and further structuring could be stopped. For fundamental objectives

hierarchy, the decomposition of lower-level objectives continues until the objectives could be measured by reasonable attributes. Thus, the search for attributes may further lead to the decomposition of objectives hierarchy. The desirable properties for fundamental objectives include: essential, controllable, complete, measurable, operational, decomposable, non-redundant, concise, and understandable (Keeney 1992, pg. 82). For means-ends network, Keeney suggests that the natural stopping point is when the alternatives or classes of alternatives are encountered.

In the subsequent steps, when the analysis of alternatives is conducted, the fundamental objectives hierarchy and means-ends network has to be connected. The fundamental objectives hierarchy represents a set of objectives over which attributes are defined. The value or utility model is then developed to evaluate consequences of fundamental objectives.

As stated before, the 15 fundamental objectives were mapped to the three aspects of social identity i.e. value, meaning, and enactment. In August 2014, a focus group session was conducted to further validate the fundamental objectives hierarchy. Focus group was comprised of 22 graduate students from Computers and Information Security Program (CISP) in a large US based University. All the students have experience of using online social networks for personal or professional purposes. The session lasted for 3 hours. The session allowed validation and restructuring of the objectives hierarchy. Besides the three aspects of social identity, two additional aspects were defined i.e. *normative ethics* and *trust*. In the final synthesis a total of 15 fundamental objectives were clustered into 5 aspects of social identity

Specify Evaluation Measures —Attributes

The fundamental objectives hierarchy represents a set of objectives over which the attributes

are defined. An attribute measures the degree of attainment of an objective. Kenney (1992) proposes three types of attributes for measuring the effectiveness of objectives: natural, constructed, and proxy. Natural attributes have common interpretation such as dollar value or age. For example, the objective for increasing financial gain could be measured in dollar value. Often times a natural attribute may not be available to measure a very subjective objective. Such subjective objectives have uncertain outcomes and are thus measured using utility instead of value. For uncertain objectives, constructed attributes with carefully defined indexes are used to measure them. For example, *maximize benevolent use of OSNs* can be measured on a categorical scale. In case both natural and constructed attributes are not feasible, proxy attributes could be defined to measure an objective. For example, the proxy attribute for measuring attractiveness of OSN user could be the 'number of likes' on the profile picture. Keeney notes that there are three main desirable properties of attributes; they should be measurable, operational, and understandable.

For the value hierarchy, constructed attributes are chosen to represent the degree of attainment of the objectives. The range of each attribute is specified between Low and High. Clear descriptions of the levels help decision makers state their preferences clearly. The attributes are measured on a common scale, i.e. utility ranges between 0 and 1 with 0 being the utility of most undesirable attainment level of an objective and 1 being the utility of the most desirable attainment level of an objective. Table 5 provides an example of one such constructed attribute for the fundamental objective; *maximize compliance to the norms of social media network*. The attribute level ranges between Low with utility 0 and High with utility 1. In the next step, the decision makers are asked to state their utility preferences for attaining an objective at different levels of evaluation measures.

Table 5: Example of a Constructed Attribute Definition

Objective: Maximize compliance to the norms of social media network	
Attribute Level	**Attribute Definition**
Low	Poor compliance to standard norms
Low-Medium	Some compliance to standard norms
Medium	Compliance to standard norms
Medium-High	Some compliance to extra norms
High	Full compliance to extra norms

Identify Alternatives

Unlike alternative-focused thinking that models the decision situation based on pre-identified alternatives, value focused thinking generates alternatives based on decision-makers' values. Keeney (1992) notes that several inputs could trigger the generation of alternatives—strategic objective, fundamental objectives hierarchy, means-ends network, attributes, and/or objective functions**.**

Following Clemen and Terrence (2001) and Kirkwood (1997), strategy-generation tables are also used for generating alternatives. The analyst identifies the decision elements i.e. how a particular objective could be accomplished and the characteristics of decision elements i.e. what options are available for the decision element. The decision elements are then sequenced by importance or time. The several potential strategies could be suggested using permutations and combinations of characteristics features; however, the analyst chooses the most promising ones with respect to the overall objective.

With respect to the first research study that aims to minimize social identity threats in OSNs, the decision elements and the characteristics are identified from values and objectives. Based on the strategy-generation tables approach, a preliminary set of alternatives is identified. Next the

existing literature is reviewed to identify the measures for protecting identity. Finally, a focus group session was conducted in December 2014 to further validate and identify alternatives for better preventing social identity threats. The focus group was comprised of two security experts from the industry and three from academia. The session lasted for about 2 hours. Moreover, the identified alternatives were further used to refine the objectives hierarchy. Keeney recommends using both existing and hypothetical alternatives as a source to identify objectives. The alternatives derived in the focus group session were used to identify further objectives for preventing identity threats. For the existing alternatives, subjects were probed to think of what the purpose of a particular alternative is. The purpose was then identified as an objective. For the hypothetical alternative, subjects were asked to state a perfect alternative to accomplish a particular objective and what implications it could have. In the final synthesis, six alternatives grounded in individual values and literature is proposed. The alternatives are referred to as *Social Identity Protection Responses (SIPR)* and are discussed in the Chapter 5.

3.4.2. Quantitative Value Modelling

Define Mathematical Model

MODA uses many forms of mathematical equations to model decision makers' preferences over possible outcomes. The simplest and most commonly used form is the additive value mode and can be written as:

$$v(x_1, x_2, \ldots, x_n) = w_1 v(x_1) + \cdots + w_n v(x_n) = \sum_{i=1}^{n} w_i v_i(x_i), where \sum_{i=1}^{n} w_i = 1$$

where $v(x_1, x_2, \ldots, x_n)$ is the value function used to rank alternatives, $v(x_i)$ are single dimensional value functions, and w_i is the weight of each evaluation measure with respect to overall preference (Keeney and Raiffa 1993).

However, instead of value function, one could use utility function in case there is uncertainty involved with the outcome of alternatives for attaining the fundamental objectives (Keeney 1992). For the first research study, consequences of the alternatives are uncertain therefore utility functions are used to measure the risk preferences of the users. Per Keeney and Raiffa (1976), a simple utility-independent multi-attribute utility function is represented as:

$$u(x_1, x_2, \dots, x_n) = \sum_{i=1}^{n} k_i u_i(x_i) + \sum_{i=1}^{n} \sum_{j>i} k_{ij}\, u_i(x_i) u_j(x_j)$$

$$+ \cdots + k_n\, u_1(x_1) u_2(x_2) \dots u_n(x_n)$$

where n is the number of attributes, $u_i(x_i)$ is a single-attribute utility function for attribute $(X_i)$and $k_1, k_2, \dots, k_n$ are normalizing constants representing a decision maker's preferences.

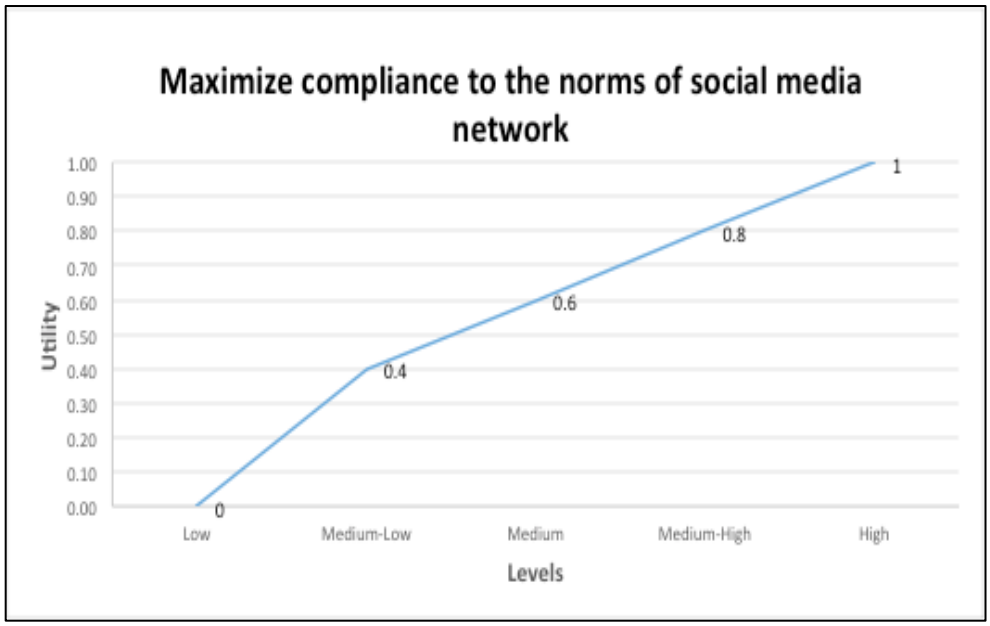
The main assumption of additive function is that the evaluation measures are preferentially independent (see Kirkwood 1997; Keeney and Raiffa 1993). According to this condition, a pair of attributes $\{X_1, X_2\}$ is preferentially independent of other attributes $\{X_3, \dots X_n\}$ if the preference order for consequences depends only on the change in the levels of X_1 and X_2, while holding all other attributes fixed at a certain level. The lowest-level objectives in the value hierarchy for minimizing social identity threats of OSN users are determined to be mutually preferential independent i.e. the preference for any subset of objectives is not affected by the level of any other subset of objectives. Simply stated, the desire for improvement of each objective is for a different reason. Thus, an additive utility function is suitable representation of the preferences for the fundamental objectives in the value hierarchy.

Create Single-Dimensional Group Utility Function

In the additive objective function, single-dimensional utility functions formalize the subjective preferences of the decision makers for the attainment of objectives. A utility function

represents the decision maker's preference for the consequences and lotteries (Keeney and Raiffa 1993). There are several techniques to elicit functions such as mid-value splitting and certainty equivalence (see Keeney and Raiffa 1993; Clemen and Reilly 2001). The decision analyst interviews the stakeholders to elicit the shape of the function using lottery procedure as described by Keeney and Raiffa (1993). The assessment of utility function starts by assigning the lowest and highest utility to least and most preferred consequences respectively. This is followed by a series of questions to assess the utilities of other levels relative to the two extremes. For example, the fundamental objective *maximize compliance to the norms of social media network* is measured at five levels as shown in Table 3.3. The utility of level Low is set to '0' and level High is set to '1' as greater level of compliance is preferred. In comparison, for the fundamental objective *minimize abysmal behavior in social media network,* the utility of level Low is set to '1' and level High is set to '0' as lesser level of abysmal behavior is preferred. The analyst then assesses the utility for other three levels as probability π such that the stakeholder is indifferent to the lottery and outcome associated with a particular level. A monotonically increasing single dimensional utility function represent the preference of a decision maker who prefers greater amount to a lesser amount, whereas a monotonically decreasing single dimensional function represent the preference of stakeholder for lesser amount to larger one (see Figures 10.a and 10.b.).

For this study, SDUFs are elicited with 12 graduate students. Each participant is using online social media for at least two years. Aggregating SDUFs generates the group utility function for each objective. More specifically, 15 group utility functions are created corresponding to the 15 leaf-level fundamental objectives.



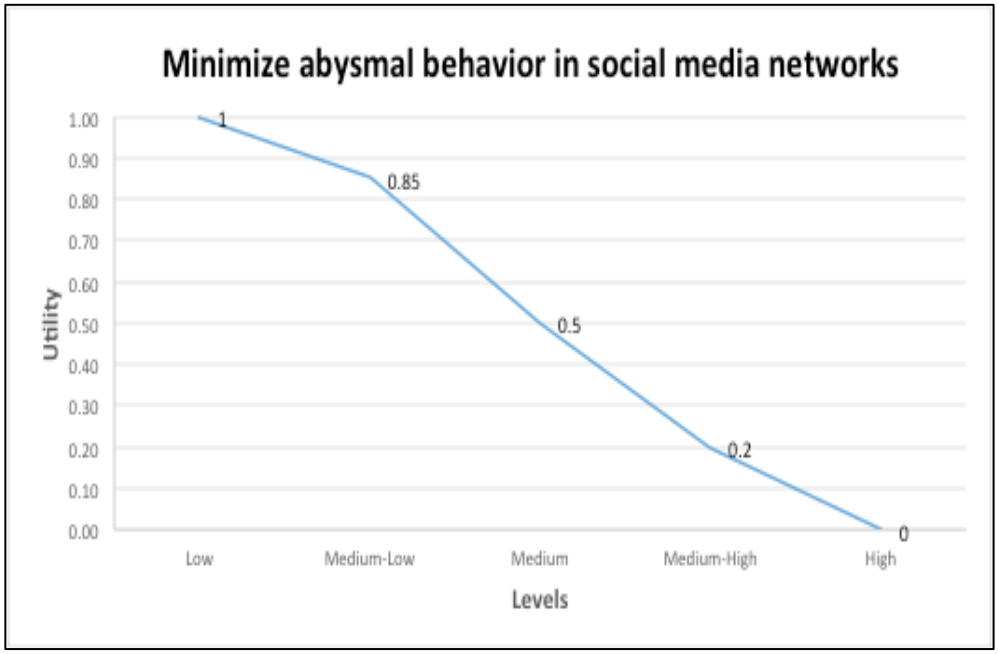


Figure 10.a: Example of Monotonically Increasing Single Dimensional Utility Function (SDUF)

Figure 10.b: Example of Monotonically Decreasing Single Dimensional Utility Function (SDUF)

Assign Weights to the Objectives

The value hierarchy is comprised of several objectives to which a decision maker may have different preferences. To account for varying preferences across the fundamental objectives, decision makers must weigh each objective within the hierarchy to indicate their relative preferences. Although various weighting techniques are available in literature, such as fixed-point scoring, paired comparison, judgment analysis, and the expected value, this research study, following Kirkwood (1997), uses swing weighting technique to elicit objective weights. Using this technique, the objectives are swung from their worst evaluation score to their best evaluation score in order of relative preference. Specifically, a decision maker is asked to imagine that all objectives are set at their worst levels of attainment, which one of the objectives will the respondent like to swing to best possible level. The chosen objective gets the highest weight. Next the decision maker is asked to choose two most important objectives and specify the relative weights. The relative weights are then normalized so that the assessments sum to one. This process is continued until all objectives at all levels of the value hierarchy are weighted. The weights of the objectives indicate how much of the overall value users ascribe to different objectives in the hierarchy in the most ideal situation. With respect to research study 1, the weights represent the 'Utopian OSN' in which all the objectives are met with respect to user values.

Score the Alternatives

Once the mathematical model is vetted, the next step is to score the alternatives on either value measures or probability score depending on the certainty or uncertainty of outcomes. Alternative scoring not only measures each alternative but also identifies the value or utility gaps i.e. chances to create better alternatives (Parnell 2007). Parnell suggests three scoring

mechanisms: scoring by alternative champions, scoring by scoring panel, and scoring by alternative champions reviewed by scoring panel. This research study implements the second approach; however, the scoring panel was comprised of both champions i.e. the subject-matter experts and "reviewers" who ensured that the bias is controlled. The scoring was conducted in a focus group session comprised of around 22 participants. Five of the participants are senior security professionals, three are the security researchers, and whereas others are graduate students in Computer and Information Systems Security program at a large US based university.

Deterministic Analysis

The deterministic analysis of the alternatives allows comparing various alternatives with respect to their level of achievement of the objectives. Two types of analysis are employed to gain the insight into the alternatives for minimizing social identity threats in OSNs: *stacked bar charts* and *utility gaps*. Stacked bar charts show the relative contribution of each alternative with respect to attainment of the fundamental objectives. Utility gaps are extracted from stacked bar charts and represent the difference between the utility attained by an alternative for a particular objective and the utility of the objective attained in the 'Utopian OSN'. It is at this point the means objectives are analyzed for the improvement of the utility gaps (for example, see Merrick et al. 2005) Using means-ends network, one could graphically represent how each means objective could lead to the achievement of other objectives, specifically focusing on ones with largest utility gaps. Usually, an in-depth discussion with all stakeholder groups is conducted to identify the most accurate and feasible means-objectives.

3.5. Conclusion

This chapter provided an overview of the research design and the methodologies pertinent to the study of identity threats to individuals in OSNs. The philosophical assumptions and the research design for the individual level study are discussed. The data collection and the analysis procedures are presented. The rational for the design, methodologies, and methods are grounded into the research problem and the theoretical foundations.

The exploratory nature of this research allows questioning what values users attribute to their social identity and how those values could be threatened. In particular, the proposed objectives to prevent threats to the social identity of users in OSNs are derived from user values and previous research. The objective functions and evaluation of the alternatives allows formulating tradeoffs among the objectives and determining suitability of alternatives to achieve the objectives. Thus the first research study switches the focus from normative to exploratory or descriptive findings (Smith et al. 2011; Bélanger and Crossler 2011). Moreover, the sequential mixed method based research design adopted in this study leverages the benefits of both qualitative and quantitative approaches of data analysis.

Chapter 4: Social Media Knowledge Discovery Process and Techniques

4.1. Introduction

The explosion of data on the Internet has attracted interest of many enterprises to collect data at the most granular level. The knowledge buried in large data sets can prove invaluable to the business performance. Consequently, there is a need for efficient mechanisms to collect, prepare, analyze, visualize, manage, and preserve large collections of data and information. From the perspective of organizational reputation management in the event of data breach, it is inevitable to ignore what customers or external stakeholders believe or know about the organization. Fortunately, with the availability of online social media and novel data analytical techniques, it is possible to tap on to the social media conversations and derive knowledge for better managing the reputation and the customer expectation in the aftermath of a data breach. With that motivation, this chapter presents the mechanics of deriving knowledge from social media sites. Specifically, this chapter proposes and initializes Social Media Knowledge Discovery (SMKD) process. This is followed by a discussion on the suite of social media analytics techniques employed for studying Information Security Reputation (ISR) threats to organizations.

4.2. Social Media Knowledge Discovery (SMKD) Process

The Knowledge Discovery in Databases (KDD) process is a standard practice of data creation, storage, transformation, and application In their seminal work, Fayyad et al. (1996a, b) note KDD as a "non trivial process of searching through large amount of computerized data to identifying valid, potentially useful, and ultimately understandable patterns." At a very high level KDD involves five major steps: selection, preprocessing, transformation, data mining, and

interpretation/evaluation. This study adopts and modifies the KDD process to discover knowledge from the social media and is referred as *Social Media Knowledge Discovery (SMKD)* (See Figure 11). The purpose of each step involved in SMKD is discussed below. Moreover, the process is initialized by demonstrating the extraction and interpretation of the data from Twitter. R-Hadoop environment is deployed to collect, cleanse, transform, and analyze the data. The data analytics reference architecture is presented in Figure 12. R-Hadoop allows to apply deep analytical capabilities offered by R to massive datasets stored in Hadoop Distributed File System (HDFS), thus exploiting the parallelism of Hadoop and analyst friendly environment of R (Das et al. 2010).

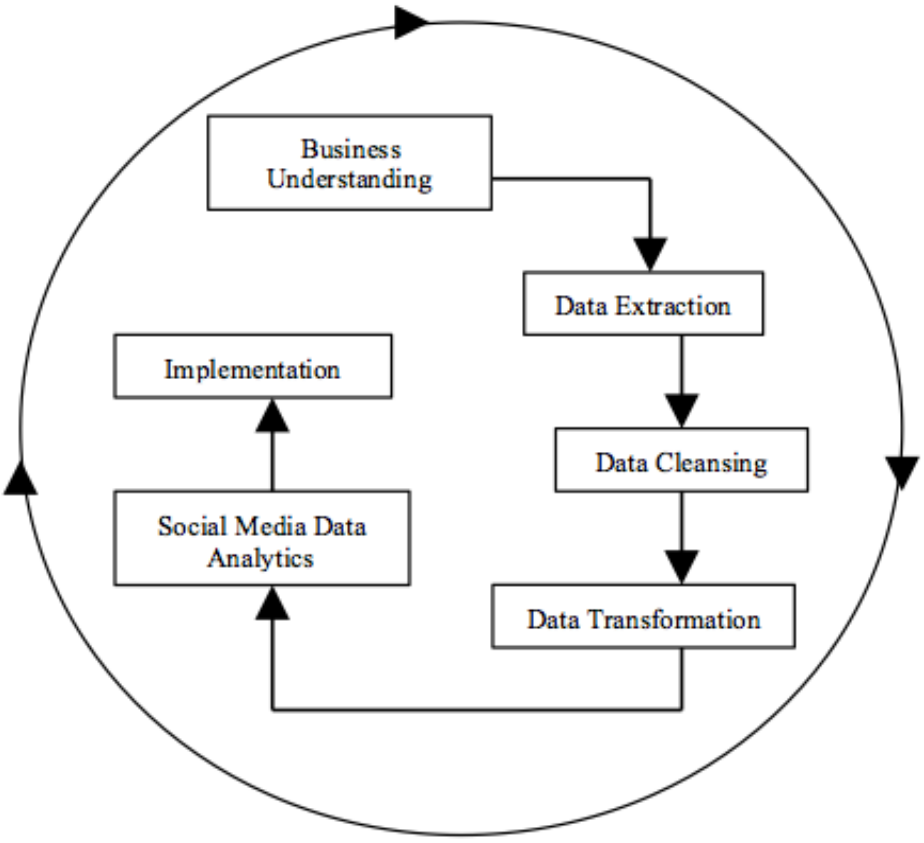


Figure 11: Social Media Knowledge Discovery (SMKD) Process Model©

Data Extraction

Similar to the KDD, the first step in SMKD is to extract the data of interest. Many social networking sites allow API streaming to connect to their data reservoir. For example Facebook's Graph API and Twitter API allows to stream data from their sites. The second research study theorizes about the Information Security Reputation (ISR) threats an organization perceives in Twitter in the event of data breach. Consequently, Twitter postings posted after the announcement of data breaches are of interest. The tweets published on Twitter's public message board are collected using *twitteR* package available in R library. The *twitteR* package provides an interface to connect to the Twitter's Search API (Gentry 2013). The relevant tweets are searched using hashtags. Twitter uses # character appended to a word or a phrase to relate the tweets by a common theme or a topic e.g. #HDBreach #ChaseHack. The tweets are downloaded in comma separated values (csv) format on to the virtual box. From here, the dataset is uploaded to Hadoop Distributed File System (HDFS) for subsequent processing and analysis.

The tweets are collected immediately after the data breaches were announced. The first data set is related to HomeDepot breach covering a period from Sept 8, 2014 to Oct 30 2014. The second data set is related to JPMorgan Chase breach spanning over four weeks from Oct 3 to Oct 31. The profile information of the authors of tweet postings — Twitttерers such as follower count, following count, and profile creation date is also collected. A brief description of the variables is presented in the Table 6.

Data Cleansing

The collection of raw data i.e. corpus is usually not ready to be analyzed. A cleansing process over the corpus is performed to assure reasonable quality. The two main cleansing operations involves disregarding irrelevant tweets i.e. tweets that don't discuss anything related to the

problem of interest and disregarding redundant tweets i.e. tweets posted by same user at the same time. Hive queries along with the *tm* package available in R library provides a framework to apply a multitude of existing methods for cleansing and transforming text data.

Table 6: Variables used for the analyses

Variable	Description
text	The tweet message posted
created	Date on which the tweet was posted
id	User ID of the tweet author
screenname	Screen name of the tweet author
rt_count	Number of times a tweet is retweeted
is_rt	Set to *True* if the posting is a retweet otherwise set to *False*
follower_count	Number of Twitter users that follow the tweet author
followee_count	Number of Twitter users that the tweet author follows
profile_created	Date on which tweet author created his or her Twitter account
Calculated Variables	
hashtag	Set to *True* if the tweet text has hashtag otherwise set to *False*.
url	Set to *True* if the tweet text has URL otherwise set to *False*.
profile_age	Number of days tweet author holds an account. It is calculated by subtracting the *created* from *profile_created*
Latency	Lag between the times a tweet is posted and it is retweeted. It is calculated in minutes
Polarity	Sentiment valence (positive, negative or neutral) of a tweet posting
Sentiment	Sentiment score of a tweet posting
Attribution	Binary variable set to 1 if tweet attributes data breach responsibility to the organization otherwise set to 0
ISR	ISR category that the tweet belongs to

Total 39,416 tweets related to the data breaches at Home Depot and JPMorgan Chase are mined. Hive queries are used to remove the 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 doesn't discuss anything related to data breaches. Such tweets are identified by first listing the most frequent words in the tweet corpus. Text mining package *tm* is used to identify words that occur at least 50 times. A quick

glance at words allows identifying irrelevant words for example *sweepstakes*, *letsgogameday*, etc. Hive queries are written to rule out the tweets corresponding to these keywords reducing the final number of tweets to 16,200.

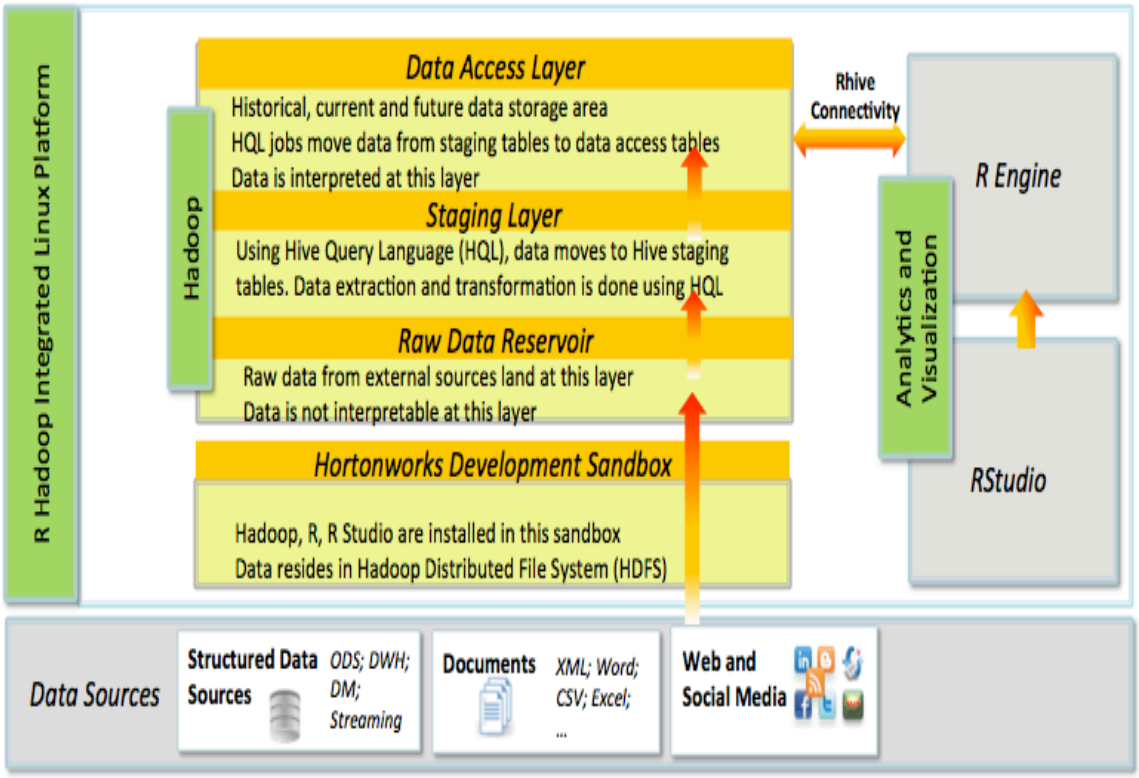


Figure 12: Data Analytics Reference Architecture©

Data Transformation

Once the relevant corpus is available, certain modifications may be required to suffice the needs of the research study. The *tm* package provides several functions to perform standard transformation on text such as converting text to lower or upper case, deleting numbers, stripping whitespaces, removing stopwords, and stemming. Besides, one may need to create metadata to annotate the corpus with additional information. For example, tweets have predefined attributes such as author, created, etc. However, based on the requirements, one can extend it with an

arbitrary number of tags.

For the Twitter data set related to this study, the basic transformations are done using *tm* package. Additionally, Hive Query Language (HiveQL) — a SQL like declarative language is used to calculate the values for few other columns such as hashtag, URL, profile_age, latency, ISR, and attribution. Interested reader can refer to Thusoo et al. (2010) for an introduction to HiveQL. Sentiment and polarity is calculated by adopting Jeffrey Breen's approach as discussed in section 4.2.4.

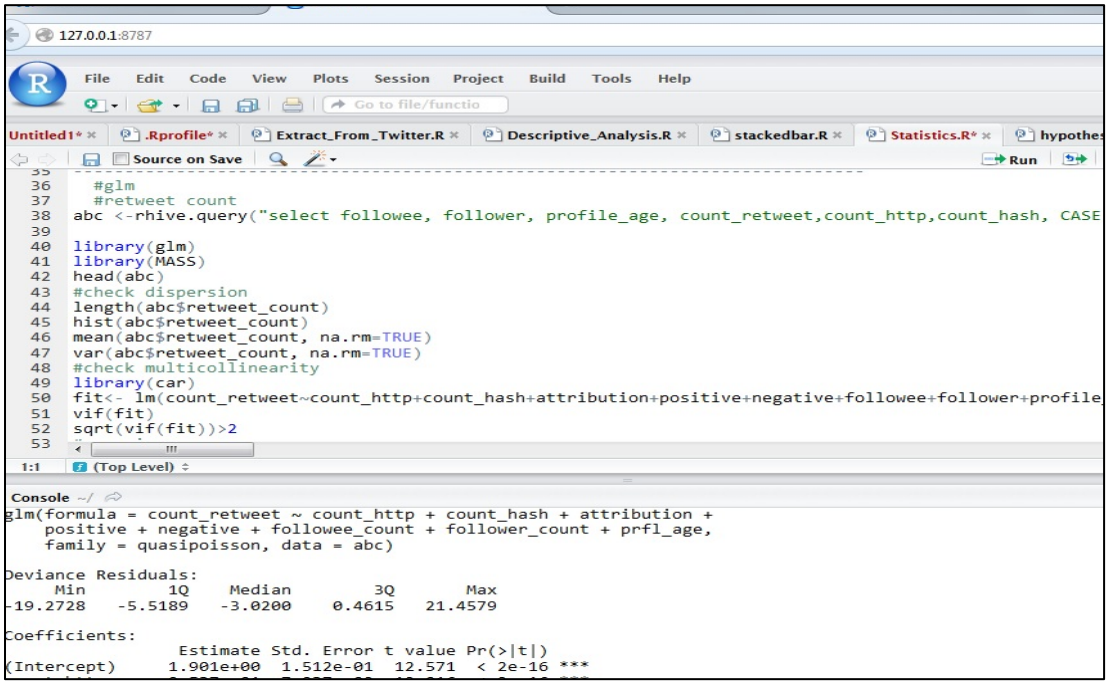


Figure 13: A screenshot to illustrate use of R-Studio for data analysis

Social Media Data Analytics

Unlike KDD, this step is not referred as "data mining" because social media analytics could involve a range of sophisticated analytical techniques such as text analysis, simulation, optimization, statistical analyses etc. According to Gartner's 2013 Analytics Capabilities

Framework, there are four types of analytical techniques each answering a different question from data (Kart et al. 2013): descriptive, diagnostic, predictive, and prescriptive analytics. The techniques employed for understanding the threats to ISR of organizations are discussed in the next section.

Implementation

The final step is to rollout the action-plan and implement the changes based on the insights offered by the analytical results. The plan should illustrate the type of organizational changes needed to achieve the proven analytics value. LaValle et al. (2013) state three capability levels based on the motive for analytics prowess: (1) *aspirational* i.e. basic use of analytics to justify day to day or future actions; (2) *experienced* i.e. rigorous use of analytics to guide day to day or future actions; (3) *transformed* i.e. rigorous use of analytics to prescribe day to day or future actions. Depending on the level, the implementation plan is designed to closely link the insights to business strategy and embed into organizational processes so that value could be achieved in terms of guiding organizational decisions and actions.

4.3. Social Media Data Analytics Techniques

A suite of data analytical techniques are employed with respect to the research questions that the second research study attempts to answer. Figure 14 illustrates the approaches combined for the purpose of second research study.

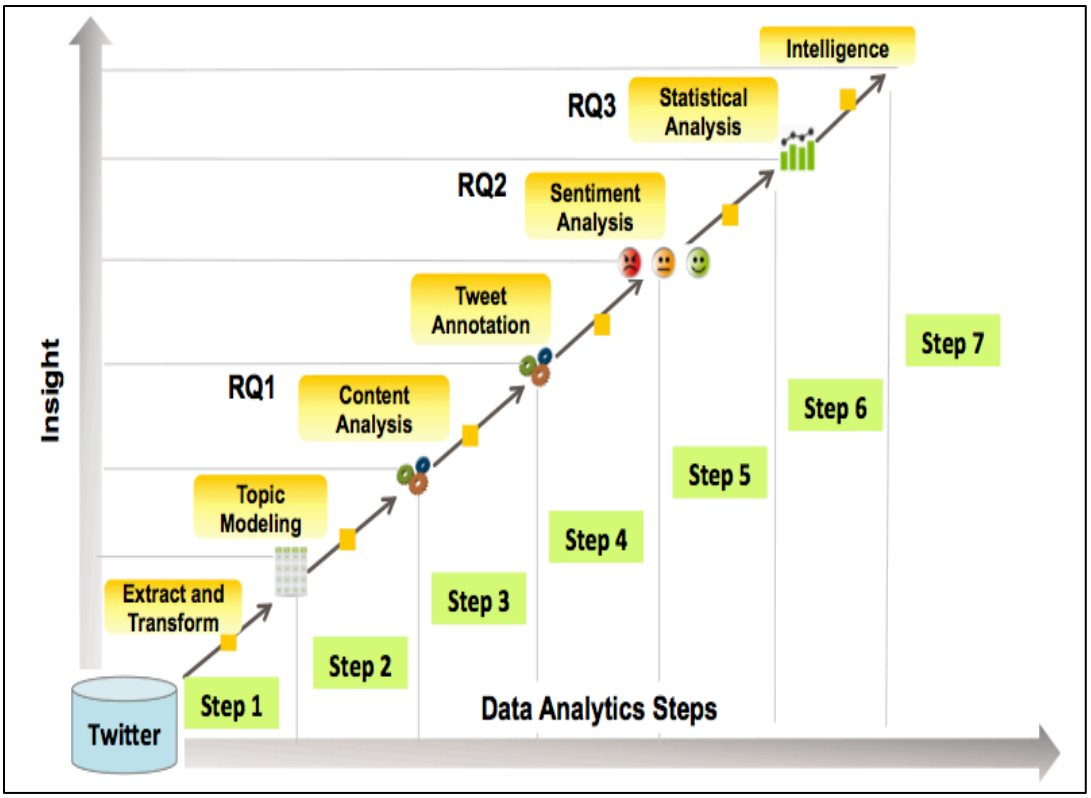


Figure 14: Social Media Knowledge Discovery Techniques ©

4.3.1. Topic Modelling

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 1999). Moreover, it becomes increasingly difficult to identify the structure or pattern of the content as the size of text grows (Blei 2012). To overcome the difficulty of analyzing large text corpuses, machine-learning researchers developed a suite of algorithms known as probabilistic topic modelling. Probabilistic modelling techniques are statistical approaches for analyzing the text documents to discover and annotate words around the thematic pattern. The advantage of topic modelling 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 modelling techniques generate semantically coherent and interpretable topics by enumerating most probable words corresponding to each topic Furthermore, topic modelling 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-modelling approaches are available, this study employs Latent Dirichlet Allocation (LDA) (Blei et al. 2003; Blei 2012) technique to identify the dimensions of ISR discussed in Twitter postings. LDA has many advantages over other topic modelling 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 referred to as "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, LDA technique generates the number of topics by associating words with one or more topics with a certain probability. The technique 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*, available in R library, is used for fitting topics (Hornik and Grun 2011). With respect to Twitter data set, LDA treats each tweet as a single document. LDA is run multiple times by varying the number of topics to be generated. The algorithm is run for

15, 25, 50, 75, and 100 topics. However, given that tweets are short in length, the model with 15 topics is chosen. Other researchers have acknowledged such difficulties with a 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 are systematically analyzed and the topics are labeled. The topics are grouped by common higher-level theme, which is referred to as topic category. To validate the topic model, content analysis of a random sub-sample of tweets is conducted. The approach to content analysis is discussed in the following subsection.

4.3.2. Content Analysis: Grounded Theory Approach

To complement the results of LDA, a content analysis of tweet postings is performed using the grounded theory methodology (Strauss and Corbin 1988). Grounded theory takes an inductive approach to category and thematic development. For this, a random 20% sub-sample of tweets (3,240 tweets) that were analyzed previously by topic modelling technique is selected. The tweet postings are read several times while being informed by the 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. The process of creating categories and themes is illustrated in Table 7. A brief description of the grounded theory from information systems research perspective follows.

Grounded theory is a type of qualitative research method that builds a theory by grounding it extensively in data. Grounded theory is independent of underlying epistemology and can be used in positivist, interpretive, or critical studies (Urquhart et al. 2010). Unlike other qualitative research methods, grounded theory research allows continuous interplay between data collection and analysis. Urquhart et al. (2010) argue that grounded theory is not just a technique

for coding but also a comprehensive method for developing theory. The authors provide guidelines for conducting and evaluating grounded theory based research in information systems. Four distinct characteristics of grounded theory differentiate it from other qualitative research methods, assert Urquhart et al. Firstly, the main purpose of grounded theory is to build a theory. The researcher needs to be cognizant of the context in which the theory is developed. Secondly, the researcher should not pre-formulate the hypothesis. This research method forbids the researcher to preconceive ideas from literature, as that will defeat the core purpose of grounded theory. In other words, grounded theory aims for theory formulation not for theory verification. Thirdly, there is greater emphasis on joint interaction between data collection and data analysis; data is jointly collected, compared and coded. The idea is to gain fresh analytical ideas that emerge during coding; these ideas then redefine the data collection. Finally, data is sliced by virtue of different analytical sampling. This provides an ability to the researcher to define categories and their properties.

The process starts with the researcher's initial hunches that inform her area of inquiry or *substantive area.* Following this, the researcher extracts initial *slices of data* and defines conceptual categories as the first elements of the 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 the grounded theory.

Table 7: Example of codes, sub-categories, categories and a theme from content analysis of tweet postings

Theme: Risk and Resilience Structure		
Codes	Sub-Category	Category
cracked 10 companies in addition to morgan; hackers also hit over a dozen other financial firms; JPMorgan Chase hackers tried infiltrating other institutions; Hackers Who Breached @JPMorgan Hacked 9 Other Banks.	Inadequate protective controls	Lack of Robust Security Controls to Safeguard Customer Data
What security lessons did we learn from the JP Morgan Chase breach?; CTO, discusses how the @HomeDepot #breach could have been prevented; We knew hackers would move beyond software and focus on hardware. Home Depot should have known better; Home Depot Breach signals the end of excuses to not update your business security.	Security measures shortfall	
breach affects 76 million consumers.; Businesses members affected by the recent #HomeDepotBreach; cyberattack affects million households; size matters; HomeDepotBreach could turn out to be one of the biggest in history.	High magnitude of impact	Capability of Causing Catastrophic Damage
The rate companies get breached; Large breaches dominating headlines these days; 2014 - The Year of Hacks; First #Target now #JPMorganChase who next? If we do business and dating electronically we run the risk of getting burned; jpmorgan breach is just another in an all too long line of large breaches.	Large scale vulnerability	
And another one bites the dust; Could #homedepot Fall Further?; Damn. It's about time to get a checkbook again.; I despise checkbooks and buying stamps to pay bills.; I am tired of companies like #JPMorganChase taking 4 to 6 months before telling #customers that they have been exposed to #IDTheftChat.	Disappointed customers about organization's doing	Concerns about Organization's Role in Victimizing Customers
My debit card has been #hacked. Thanks #HomeDepotBreach; Has #Cybersecurity Become Cheap?; I plan to boycott your stores; Thanks #HomeDepot. You owe me a weekend's worth of lost frequent flier miles! And the hour spent reporting fraud!	Expressing discontent through angry messages	

4.3.3. Twitter 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 is conducted. The approach is described as follows.

Firstly, the tweet text is analyzed to classify corresponding tweets into five ISR dimensions. A database column 'ISR' is created and populated using Hive queries. The Hive queries search for tweets by topic words using the findings from topic modelling and content analysis phases. Tweets that do not fall into any of the categories are then labeled as 'NA.' To validate the results of automated annotation, 1% of random sub-sample of tweets is 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 update the 'attribution' column to 'True' or 'False'. To accomplish this, the tweet corpus is generated i.e. the collection of tweet text. The *tm* package available in the R library is used to transform and analyze the tweet corpus (Hornik and Grun 2011). 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) is 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 case of Twitter

dataset, each tweet is treated as a document and the words in each tweet are treated as terms. The DTM has 16,200 documents with 8,821 terms. Finally, an ordered list of terms by frequency is obtained to identify the most frequent and least frequent terms. The threshold for least frequent terms is set as 50, i.e. a word occurs at least 50 times in the tweet corpus. Using the set threshold, 465 terms 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 are manually analyzed to identify words that indicate the attribution of data breach responsibility. A total of 308 such attribution terms are 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 are manually annotated. The accuracy of attribution responsibility for the complete data set is 98.7%

4.3.4. 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). With the advancement of Natural Language Processing techniques coupled with the outburst of opinionated data in social media, sentiment analysis is becoming very popular in the disciplines of management, economics, and social science (e.g. Stieglitz and Dang-Xuan 2013; Jansen et al. 2009). Particularly in the context of social platforms sentiment analysis is applied to several research problems. Examples range from studying the impact of mood on the stock prices (e.g., Baker and Wurgler 2006), to the effect of review ratings on the product sales (e.g., Chevalier and Mayzlin 2006), and the diffusion of politically

oriented messages (Stieglitz and Dang-Xuan 2013). However, the nascence of the field of social media monitoring and analysis is evident in the confounding and confusing terminology. Pang and Lee (2008) assert that the words such as sentiments, subjectivity, and opinions are common in literature. Consequently, the research streams have come to be known as sentiments analysis, opinion mining, or subjectivity analysis.

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, this study uses Jeffrey Breen's[5] approach for sentiment analysis. 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 i.e. to classify a tweet as being positive, negative or neutral. I used the opinion lexicon in English with 2,006 positive words and 4,783 negative words by Hui and Liu, which is available on http://www.cs.uic.edu/~liub/FBS/sentiment-analysis.html. Furthermore, following Breen, the lexicon is enhanced with the domain specific words. The words analyzed using *tm* package previously are added to positive or negative word lists. The sentiment score for a tweet is calculated as:

Sentiment score = number of positive words - number of negative words

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 are manually coded using Breen's approach. The results of

[5] http://jeffreybreen.wordpress.com/2011/07/04/twitter-text-mining-r-slides/

this manual coding are compared with those of the automated approach. The intercoder agreement between the manual and algorithmic coding is quite high (Cohen's $\kappa = 0.92$).

4.3.5. Statistical Analysis

To test for H1 that postulates a strong association between data breach responsibility attributions and sentiments, the following two variables for each tweet are constructed:

a) A binary variable to indicate whether the tweet message attributes the responsibility of the data breach to the organization: *attribution*; and
b) The sentiment valence of a tweet message: *polarity*.

To test H1, chi-square test of independence is performed to determine the association between attributions of data breach responsibility and sentiments. Chi-square test of independence is used when there are two nominal variables and the researcher wants to test whether the proportions of one variable varies with respect to the different values of other variable. Chi-Square test is appropriate for large samples size.

To test for other hypotheses that postulate relationship of data breach responsibility attribution and/or sentiment with retweet response in terms of both retweet quantity (positive relationship) and retweet latency (negative relationship), four additional variables were constructed:

a) Number of times a tweet has been retweeted: *rt_count*;
b) Time elapsed between the tweet and corresponding retweet: *latency* (in minutes);
c) Total sentiment score of a tweet: *sentiment*
d) A dummy variable for Information Security Reputation dimension: *ISR*

Previous research concludes that both *content features* (i.e. URLs and hashtags) and *contextual features* of tweets (i.e. user followers, user followees and age of the user account) impact the retweet behavior in Twitter (Suh et al. 2010). Thus, the following five control variables are added to the analyses:

a) A binary variable to indicate whether a tweet mentions at least one hashtag: *hashtag*

b) A binary variable to indicate whether a tweet contains a URL: *url*

c) Number of users who follow the tweet author: *follower_count*

d) Number of users that the tweet author follows: *followee_count*

e) Number of days tweet author holds the Twitter account (This is calculated by subtracting the date of tweet posted from the date of account is created): *profile_age*

H2, H4, and H6 predict that the attribution and/or sentiment increase retweet count. To test these hypotheses, Generalized Linear Models (GLM) are applied to predict the dependent variable *rt_count.* As *rt_count* represents count data, Poisson regression, a special case of Generalized Linear Model is applied. However, as the data set indicates overdispersion problem i.e. variance of the data is more than the mean, Poisson Quasi-MLE (Gourieroux et al. 1984) also known as GLM with a log link is applied. Poisson QMLE is a robust technique to model overdispersed data. It requires log-transformation of the dependent variable and exponential transformation of coefficients for the interpretation of effect sizes. The *glm* package available in R library is used to run the model using R Studio. The regression model for H2 is as follows:

$$Log_e(rt\_count) = \beta_0 + \beta_1 attribution + \beta_2 polarity + \beta_3 url + \beta_4 hashtag + \beta_5 Log_e(follower\_count) + \beta_6 Log_e(followee\_count) + \beta_7 (profile\_age)$$

To test for H4, the model is run only for the tweets where 'Attribution' is true. This reduces the sample size to 7,778. The model for H4 is as follows:

$$Log_e(rt\_count) = \beta_0 + \beta_1 sentiment + \beta_2 url + \beta_3 hashtag + \beta_4 Lo\square_e(follower\_count) + \beta_5 Log_e(followee\_count) + \beta_6(profile\_age)$$

To test for H6, an interaction variable *attribution * negative* is included to determine the impact of negative sentiments on *rt_count*. The regression model is as follows:

$$Log_e(rt\_count) = \beta_0 + \beta_1 attribution + \beta_2 negative + \beta_3(attribution * negative) + \beta_4 url + \beta_5 hashtag + \beta_6 Log_e(follower\_count) + \beta_7 Log_e(followee\_count) + \beta_8(profile\_age)$$

H3, H5, and H7 predict whether attribution and/or sentiment impact retweet latency. As the dependent variable *latency* is a continuous time variable, Ordinary Least Square (OLS) regression is applied. Multicollinearity is checked and none is observed. To account for nonnormality, the dependent variables are log-transformed before applying OLS regression. Results of the Shapiro–Wilk test for normality applied on the log-transformed variables suggest that the null hypothesis of normal distribution cannot be rejected. To test for H3, the model is ran for the tweets where retweet count > 0, this reduces the sample size to 6,423. The regression model for H3 is as follows:

$$Log_e(latency) = \beta_0 + \beta_1 attribution + \beta_2 polarity + \beta_3 url + \beta_4 hashtag + \beta_5 Log_e(follower\_count) + \beta_6 Log_e(followee\_count) + \beta_7(profile\_age)$$

Again, to test for H5, the model is ran only for the tweets where attribution is 'True' and retweet count > 0. This reduces the sample size to 3,023. The model for H5 is as follows:

$$Log_e(latency) = \beta_0 + \beta_1 sentiment + \beta_2 url + \beta_3 hashtag + \beta_4 Log_e(follower\_count) + \beta_5 Log_e(followee\_count) + \beta_6(profile\_age)$$

Again for H7, to account for sentiment effect on retweet *latency*, an interaction variable *attribution* * *negative* is included. The model was run on tweets with retweet count > 0. The regression model is as follows:

$$Log_e(latency) = \beta_0 + \beta_1 attribution + \beta_2 negative + \beta_3(attribution * negative) + \beta_4 url + \beta_5 hashtag + \beta_6 Log_e(follower\_count) + \beta_7 Log_e(followee\_count) + \beta_8(profile\_age)$$

Finally, H8 and H9 predict the diffusion of Twitter postings for the five ISR dimensions. H8 is run for all the tweets whereas H9 is run for only retweets. To test the variance of retweet count and the retweet latency for the ISR dimension, the regression models are as follows:

$$Log_e(rt\_count) = \beta_0 + \beta_1 ISR + \beta_2 polarity + \beta_3 url + \beta_4 hashtag + \beta_5 Log_e(follower\_count) + \beta_6 Log_e(followee\_count) + \beta_7(profile\_age)$$

$$Log_e(latency) = \beta_0 + \beta_1 ISR + \beta_2 polarity + \beta_3 url + \beta_4 hashtag + \beta_5 Log_e(follower\_count) + \beta_6 Log_e(followee\_count) + \beta_7(profile\_age)$$

4.4. Conclusion

Creating an analytics capability doesn't require outrageous investment. Several open-source tools offer the capability to perform high-end analytics. This chapter presents Social media Knowledge Discovery process that uses the open source R-Hadoop framework for deriving knowledge from social media. The exploratory design of study allows answering what Information Security Reputation (ISR) threats prevail in social networks for organizations that face data breaches. The content analysis and topic modelling allows identifying various ISR dimensions, tweet annotation methodology annotates the tweets that attribute the data breach responsibility to the organizations, sentiment analysis gauges the associated sentiments, and finally statistical analyses test the diffusion of ISR threatening tweets.

Chapter 5: Identity-Identification Value Threat Analysis

5.1. Introduction

The purpose of this chapter is to present the results of Value Focused Thinking and Multiple Objectives Decision Analysis. The outcome of the qualitative value modelling includes the fundamental value hierarchy for minimizing threats to the social identity of individuals in Online Social Networks (OSNs), the evaluation attributes, and the alternatives for preventing identity threats referred to as Social Identity Protection Responses (SIPR). The outcome of quantitative value modelling includes the single dimensional group utility functions, the objective weights, and the alternative scores. Finally, the utility gap analysis is presented identifying the alternatives that best accomplish the fundamental objectives to minimize social identity threats to individuals in Online Social Networks.

5.2. Qualitative Value Modelling

5.2.1. Fundamental Value Hierarchy

The qualitative data analysis shows that five aspects of social identity are threatened in OSNs and the corresponding objectives are: *maximize enactment of social identity*, *maximize meaning of social identity*, *maximize value of social identity*, *maximize trust in online social networks*, and *maximize normative ethics*. The sub-objectives corresponding to each of these five aspects represent distinct fundamental objectives to minimize the relevant threats in OSNs (see Figure 15). Each of the five aspects of social identity and the corresponding fundamental objectives to minimize threats are discussed below:

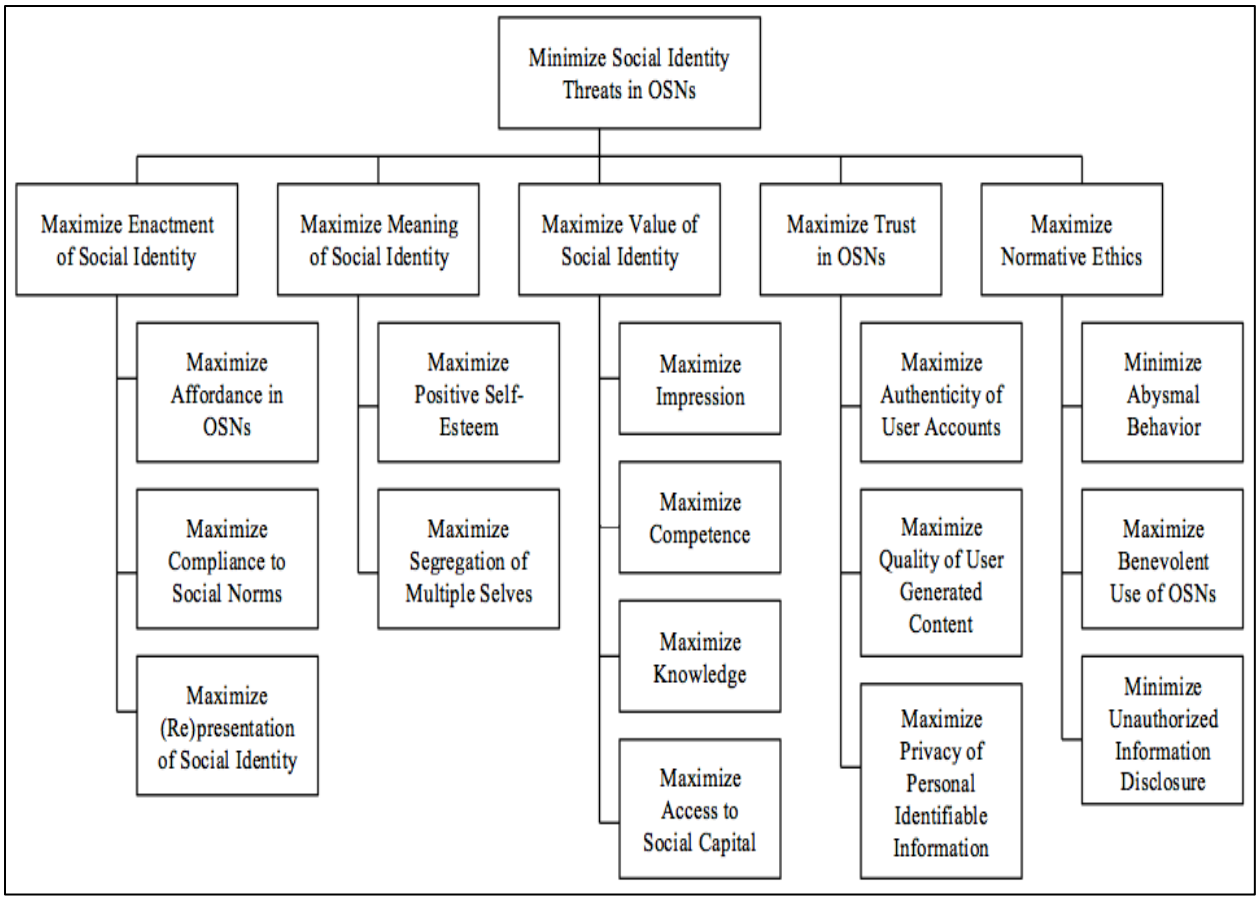


Figure 15: Social Identity Value Hierarchy

5.2.1.1. Maximize Enactment of Social Identity

Social networks provide a mechanism for people to identify themselves and construct their personal identities (Higgins and Kram 2001; Schultze 2014). Specifically, the trust, reciprocity, and interdependence in social networks reflect and shape the identities of individuals (Higgins and Kram 2001; Swann 1987; Mead 1934). Furthermore, as part of social interaction, individuals perform their identities sanctioned in a particular milieu (Goffman 1959). However, individuals could appraise certain experiences as identity threatening if the experiences limit or prevent the performance or enactment of an identity. Sociologists have studied such situations arising for example due to chronic diseases (Breakwell 1993), personal loss (Neimeyer et al.

2002), encroachment of demands from competing identities (Rothbard 2001), and overemphasis of personal identity over social identity or vice versa (Kreiner et al. 2006). On similar lines, OSNs provide disembodied environment to facilitate identity performances (Boyd and Heer 2006); however, individuals could experience or perceive threats in enacting certain identities. The data analysis indicates that threats to the identity enactment in OSNs stems from limited technology affordance, non-compliance to social norms, and restrictions in representing identities. Consequently, the three objectives to maximize identity enactment are: *maximize affordance in OSNs*, *maximize compliance to social norms*, and *maximize re(presentation) of social identity*.

Maximize Affordance in OSNs

Affordance is the "strengths and weaknesses of technology with respect to the possibilities they offer the people that might use them" (Gaver 1991, pg. 79). Individuals can enact their identities if OSN technology affords the needs of user identification. Besides generic identification mechanisms such as creating digital profiles (Zhao et al. 2008), the interactions and events in OSNs are perceived as affording an opportunity to satisfy certain individual goals e.g. creating humor or expressing moral perspective (Thelwall et al. 2011). Scholars distinguish these two aspects identification afforded in online social media as *exhibitions* and *performances* (see Hogan 2010) and there often is a mismatch between the two (see Acquisti and Gross 2006). In this study affordance to exhibit and perform identities emerged as a fundamental objective. The values emanated by the participants suggest an intricate relationship between affordance and identification; however, the threats to the affordance emanate due to constrained identity construction and performance. The individuals not only have to construct selves by defining who they are within the limited options provided by OSNs but also to ensure that their actions reflect

the constructed definitions. The respondents note the tension between presentation and performance afforded in OSNs. One in particular states:

> *I believe identifying oneself by stating discreet characteristics [name, gender, and age] is a limited construction of identity. Although, I provide regular status updates, and share personal or professional content to flesh out my identity a little more, tension arises between the options provided by online media to define identity and the requirements of an individual to construct social identity. I personally feel challenged in acting true to my online persona; I choose words very carefully while expressing my views in these forums.*

Maximize Compliance to Social Norms

Social influence literature maintains that individuals look to social norms to gain an understanding of and respond adequately to uncertain social situations (Cialdini and Goldstein 2004). A large number of studies indicate that social norm compliance typically requires a punishment threat for violators (e.g. Sober and Wilson 1998; Fehr and Gächter 2002; Boyd et al. 2003). Research shows that the people often comply with social norms conditional on compliance of others (Fischbacher et al. 2001), and thus even a minority of violators could potentially trigger widespread dissolution of disobedience. The data analysis shows that users fear the non-compliance to the "traditional" social norms in online networks. Additionally, lack of controls in social networks reinforces non-compliance and that such violations are common in online networking. In particular, one of the participants mentions:

> *Traditionally shame and embarrassment forced people to behave within social limits; however, the physical and psychological distance in virtual forums has redefined what now is considered stigma or dishonor. I prefer to talk about the certain issues only with the*

closest family or friends rather than in the social forums. Public fame and shame is dependent on like/unlike clicks.

Maximize Re(presentation) of Social Identity

The expression of social identity is not a static process. Scholars argue that along the life span of humans, there could be events or situations that force individuals to adapt to the environmental opportunities and demands (e.g. Hormuth 1990; Ruble 1994). Moreover, such adaptations are more than momentarily changes; an individual may undergo a fundamental change to her central identity (Deaux 1993). Specifically, social identity is supported by network of interrelationships (Abrams 1992) and such interrelationships could change during times of transition (Hormuth 1990), which in turn impact an individual's identity. Ethier and Deaux (1994) argue that the previous identity may no longer be valid or reflective in the new context. Thus maintaining an identity in a new context requires an individual to develop new bases for supporting that identity and, in the process, detach the previous identity from its supports in the former context. The data analysis reveals the need for users to reposition their identities and the limitations of current social networking technology to forego previous identity. The below stated comment from one of the participants captures the essence of the challenges in the representation of social identity:

I admit that part of being young is saying and doing nonsensical things. Whatever we tweet today may not make any sense in the next five years. Ironically, both users and social networking technology don't consider this "five year rule." People have found a way to deal with it simply by creating multiple profiles. However, I recommend being careful in creating multiple "throwaway" profiles. Although, social networks allow individuals to create multiple personas, it is easy to track and link those by following an individual's

digital traces. We should bear in mind that Internet does not have any expiration date which in turn could deter the reflection of maturing personalities.

5.2.1.2. Maximize Meaning of Social Identity

Each identity of an individual is conceptualized as "What it be to be X" (Petriglieri 2011). For example, Anteby (2008) mentions that a blacksmith may conceptualize the meaning of "independence" and "skill" with respect to his/her identity. However, identity threat is perceived if an individual experiences the disassociation of meanings from the identity. Petriglieri (2011) argues that identity meaning can be threatened if an individual's actions contradict the association between the identity and its current meaning. For example a blue-collar worker threatens the association of "craftsmanship" to the identity by performing non-creative jobs (Newman 1988) or the stagnant nature of one's job may threaten the meaning of "progress" associated to professional identity (Elsass and Ralston 1989). In the context of OSNs, identity meaning could be threatened if the performance afforded in such networks is perceived to be contrary to what a particular identity claims. From theoretical perspective, these networks are front stage in which explicit individual performances are displayed and observed (Pearson 2009), and identity threat is experienced if the observers perceive an individual's performance contrary to his or her identity claims. The data analysis suggests that social identity means self-esteem and multiple roles/identities enacted by users in OSNs. Consequently, users perceive threats to the meaning of their social identities if online experiences threaten the aspects of self-esteem or multiple self-identities. Consequently maximization of identity meaning in OSNs involves two sub-objectives: *maximize positive self-esteem* and *maximize segregation of multiple selves.*

Maximize Positive Self-Esteem

Social identity theory posits that positive self-esteem is a fundamental motivation for identification (Turner 1982). Individuals experience lowered self-esteem if the meaning of the ascribed identity is threatened. For example stigmatization based on group identity results in lower self esteem (Ethier and Deaux 1994). To prevent negative evaluations, individuals engage in conscious and deliberate attempts to seek social acceptance, build positive relationships, and thus enhance self-esteem (Cialdini and Goldstein 2004). Scholars argue that individuals with both high and low self-esteem strive to behave consistently with their actions, statements, commitments, beliefs, and self-ascribed traits (Zywica and Danowski 2008). The data analysis suggests that social media users perceive threats to their self-esteem depending on how other users evaluate the ascribed identities. For example, as indicative from the comments of a participant, people join and share information on these networks to enhance self-esteem and thereby build meaningful identities.

> *I am highly connected in online media for one reason that my connections receive my opinions positively. The feedback comments on my posts make me feel in control of my existence and that I am indulging in meaningful activities. The key is to keep a positive two-way communication with the community.*

On the contrary, another participant points out the elements of social media that she perceives to lower her self-worth and identity:

> *I have always been on the higher side of the body weight. The pictures of my skinny friends make me upset as they collect 100 plus likes. My feeling of wanting to be accepted gets intense as I get in the space of social media.*

Maximize Segregation of Multiple Selves

Identity is a fluid and a dynamic construct that on the one hand forms associations among people while on the other hand differentiates an individual (Citrin et al. 2001). Research suggests that there is strife between multiple dimensions of an individual's identity. For example, Roberts (2005) argue that the professional image in an organization setting is defined by both personal and social identity of an individual. However, people perceive identity threat if they are categorized or associated to stereotypical characteristics of one of the dimensions of their identities. On similar vein, Branscombe et al. (1999) note people, if treated based on their gender, political, or religious affiliations, feel victimized by being judged by certain social identities and not by unique individual traits. The respondents in this study echo the sentiment of being judged by one of the different perspectives of their personalities, and thereby perceive threats to the meanings of different identities. In particular, a communication manager at a large financial company notes:

> *Balancing professional and personal identities using same social media account is tricky. To keep things simple, I have decided to untangle the two. I believe in personalizing profession but not making it personal. So I share content on behalf of my company using my professional account and my personal content in my personal space. However, I have to be on my toes in dealing with people who try to get personal in my professional space and vice-versa.*

5.2.1.3. Maximize Value of Social Identity

People value their personal identity to sustain sense of self-worth (Gecas 1982). Petriglieri (2011) argues that more negative an identity is valued, less self-worth an individual perceives from it, and vice-versa. The devaluation of identity usually stems from in-group/ out-group

differences (Tajfel and Turner 1979). At group-level, an individual may experience in-group threats in the interactions that question the individual's belongingness to the group. Out-group threats originate from the judgments that devalue the identity of competing or conflicting groups to which an individual belongs (Ashforth and Meal 1989). Examples of this stream of research include devaluation of identity of people belonging to different nations (Fiol et al. 2009), races (Roberts 2005) or professions (Ashforth and Kreiner 1999). In online social networks negative and devalued treatment is common (e.g. see Dellarocas 2006; Schultze 2014). The data analysis suggests that users value gain in impression, knowledge, outreach, and access to social capital within the online social networks. Consequently, any experience that is perceived to threaten or limit these gains devalues individuals' social identity. Therefore, to minimize threats to individuals' social identity, four aspects of value are to be maximized: *maximize impression*, *maximize knowledge*, *maximize outreach*, and *maximize access to social capital*.

Maximize Impression

According to psychological literature, impression management is the process to control the impressions about individuals (Leary et al. 1990). Impression not only determines the perceptions, evaluations, and treatment of others towards an individual but also how an individual views self. Unlike self-presentation, impression management is broader and more encompassing concept. For example Schneider (1981) points out that both self and third party may manage an individual's impression. This duality of impression management fits well within the online social networking paradigm. While technology allows individuals to emphasize on the positive aspects of their identity, the notions about one's identity is also formed by how other social media users characterize the individual's identity. The respondents acknowledge the conundrum faced by people in their attempts to control self-impression as they note:

There is a constant need for us to be connected all the time and present the best "cyberface." Much of this need arises from the fact that everyone in my social network does so, which creates an opportunity to compare myself with others. Yet, sometimes, after seeing my glamorous and rare photos, some of my online friends feel "instagram envy." Tackling envious comments is very stressful.

Maximize Knowledge

Engagement in social networks is defined by the extent to which users communicate and create and share content (Kietzmann et al. 2011). Research suggests that the diversity of users involved in the social interaction is crucial. For Noteboom (2006), user diversity entails both the number of users involved in the learning process, and the skill and knowledge they possess. The diversity in online social networks allows individuals derive informal learning and develop an identity by demonstrating technological fluency, digital citizenship, and communicative and cultural competence (e.g. see Borau et al. 2009; Greenhow and Robelia 2009). However, a parallel stream of research studies the sharing behavior in virtual communities (see Lee and Ma 2012). The data analysis suggests that users draw benefits from knowledge networks in social media; however, sharing and learning is inhibited if the users do not participate actively. One of the participant states:

Contributing to community is about people, not technology. Most of my content posted in these platforms does not trigger public interactions from others and thus nobody notices my participation. Public participation and engagement is important not only for my content to spread in the network but also that people will come to know about my personality and professional expertise. Highlighting the good work of others increases visibility and is more powerful than simply hitting like button in private.

Maximize Outreach

The tendency of people to form groups based on common interest is inherent to human society and the way such groups form and evolve attract the attention of a large number of social science researchers (Coleman 1990). In particular, network analysis techniques allow understanding the dynamics of online outreach by exploiting the structure and content in these networks (Backstrom et al. 2006). In his seminal work on the strength of weak ties, Granovetter (1983) suggests that network structures could deprive individuals of the information embedded in the distant parts of the social network. However, the network confinement not only deprives an individual from various forms of social capital exchanged in these networks but also alienates the individual from the group. As such the mechanism of outreach to build online relationships is fundamental to achieving value from social identification. As one of the participant notes:

> *Having a presence on online social networks is important to increase reach and exposure of my entrepreneurial identity. But to drive my ideas, I rely on "network of values" rather than "network of humans." I need people who care about the information I share online.*

Maximize Access to Social Capital

The concept of social capital has gained wide popularity in the disciplines of social sciences. Social capital is conceptualized as the goodwill engendered by social structures and relations (Portes 1998). In describing the effects of social capital, Portes notes that social capital based structure have both positive and negative implications. In the positive sense, social capital imposes social control and provides social support and benefits through extended networks. However, from negative perspective, social capital based structures exclude outsiders from networks, impose excessive demands on group members, and restrict individuals' freedom.

In online social networking literature, social capital research is gaining currency. From individual perspective, a person draws on the resources from other members of the network to which he or she belongs. These resources can come in several forms — useful information, personal relationships, organized groups, and employment connections (Granovetter 1973; Paxton 1999). Moreover, research suggests that various forms of social capital are related to individual's psychological well being, such as self-esteem and satisfaction with life (Bargh and McKenna 2004; Helliwell and Putnam 2004) and knowledge contribution (Wasko and Faraj 2005). The participants in this study not only acknowledge the usefulness of social web to create good social capital for the benefit of communities but also are cognizant of bad social capital. One participant in particular expresses the dual side of social capital in social media as he notes:

> *As a father and a practitioner, I believe that everyone should learn about the risks and opportunities of social media before publishing their accounts. I like to teach my kids not only how to find the information that is relevant to them and reliable but also how to prevent themselves from being exposed to any type of risks prevalent in the use of social networking technologies. I'm concerned that if we don't pay attention enough to these issues starting from now, our children might lose all sense of privacy, and consequently will find it hard to build their own identity.*

5.2.1.4. Maximize Trust in Online Social Networking

Trust is considered as a lubricant for cooperation (Arrow 1974), source of social order (Parsons 1937), driver of efficiency in economic and non-economic transactions (Coleman 1988), and mobilizer for social capital (Paxton 1999). The concept of fiduciary trust fits well within the context of social networking sites. Barber (1983) defines it as the belief that individuals carry out their obligations and responsibilities and place others' interest before their

own. On similar lines, trust in social networks is the belief that users will behave within the social norms and will not exploit other members (Juan et al. 2007). Moreover, research suggests a strong association between trust and identity. For example, consumers identify with trustworthy organization to communicate self-identity and enhance self-esteem, (see Keh and Xie 2009). The respondents in this study perceive threats to their social identity due to the lack of trust in three fundamental identification mechanisms of OSNs: member authentication, information credibility, and processes to protect user information. Consequently, to protect social identify in OSNs, the respondents emphasize on trust building mechanisms grounded in three aspects of social networks: *maximize authenticity of users*, *maximize quality of user generated content*, and *maximize privacy of personal identifiable information*.

Maximize Authenticity of Users

An authentic individual is committed to personal values and roles chosen by him or her freely and self-consciously (Tajfel 1978; Hitlin 2003). However, being authentic, i.e. being true to self presents two confounding challenges to identification in OSNs. Firstly, social identity and authenticity are opposite concepts. Social identity theorists posit that identity is defined by the social and historical context beyond the control of an individual (Hogan and Cheek 1983). Such lack of control in defining the social identity of individuals is perceived to threaten the individual authenticity in OSNs. The respondents in this study acknowledge the loss of control on self-authenticity as they note:

> *Impersonation is one of the many risk in being on social media. It happened to a friend of mine and it took quite some time to rescue her profile. There was a lot of negative commenting going on against her. It was really sad to see someone sink so low to do this to someone. I learnt to keep my profile private and only connect with people I know and trust.*

Secondly, authenticity and trust are interrelated. In the real world context, the better the two individuals know each other, the more they trust each other. Revealing identifiable information about oneself ensures authenticity, thus builds trust. Credentials Networks is for example an approach for handling trust and authenticity in distributed networks (see Jonczy and Haenni 2005). The respondents in this study expressed concern about the authenticity of friendship-networks. As the comment below notes:

> *I like to share on social media if something upsets or bothers me. Usually, these kinds of posts get the swarm. People empathize, disagree, debate, or share advice and experiences. However, I really dislike the passive, aggressive, and unauthentic posts. Even the nicest of people are prone to this now and then. I'm totally me on social media but I am connected with people who I'm not afraid to be me with. If you build a trustworthy and supportive friends list then there is no need to worry.*

Maximize Quality of User Generated Content

The popularity of social media has transformed the users from content consumers to content creators. An emerging body of research examines the relationship between information quality and trust and its impact on human decision-making (e.g. Gefen et al. 2003; Pavlou and Gefen 2004). Additionally, research shows that identity-descriptive information influences the consumers' perception about the review and product information, for example (see Forman et al. 2008). However, the quality of social media content remains to be a challenge (Agichtein et al. 2008). For example, the faulty swine flu tweets caused a widespread panic in the general public. Likewise the popularity of social bots to run campaigns and spread misinformation and propaganda exposes the vulnerability in OSNs (Boshmaf et al. 2011). More recently, a study shows that most of the tweets and retweets related to outbreak of Ebola in West Africa contained

misinformation and that misinformation spreads more than the correct information (Oyeyemi et al. 2014). The respondents' of this study trust the information shared in OSNs albeit with caution. In particular, some of the respondents are careful of relating to bogus information:

> *With the availability of social media, traditional news reporting has been abandoned. Both news agencies and common people are so caught up with being the first to share the news that the credibility of the news and source is often ignored. One needs to realize the importance of checking the facts first before sharing any information online. Not only a large majority of our society uses social media as their main source of news in this generation, but also information sharing patterns set the credibility of the source, including people.*

Maximize Privacy of Personal Identifiable Information

Building consumer trust by enforcing privacy practices is well-researched area. For example, Fair Information Practices (FIP) is regarded important in defining customer trust and behavior (Culnan and Armstrong 1999; Kim and Mauborgne 1997). On the contrary, Robershaw and Marr (2006) show that people falsify personal information if they do not receive reasonable guarantee of data protection against unwanted marketing communications. In online networks, trust and privacy concerns have also received some attention (e.g. see Dwyer et al. 2007). In particular, scholars suggest a decentralized architecture that capitalizes the trust relationships in social networks, and thereby cope with the problem of trust-building and privacy-preserving mechanisms (Cutillo et al. 2009). Furthermore, research shows that users fake their identities for privacy enhancement (Gross and Acquisti 2005). The data analysis suggests that users conceal their identifiable information for lack of trust in the protection mechanisms of OSNs. The behavior is echoed in the following comment of a participant:

I am a parent of two teenagers who are being over-informed and over-tweeted. I warned them against sockpuppeting. The idea is that, to improve online privacy, we change our usernames and email addresses frequently so that social media sites don't build a history of our activities. Of course, this is only a small part of the things we you can do to improve online privacy, but it's a good start. Tools such as 'Fake Name Generator' work great for both sham and genuine users.

5.2.1.5. Maximize Normative Ethics

The ubiquity of social networking sites has revealed several ethical issues ranging from employer surveillance (Albrechtslund 2008) to accessing private information for marketing purposes (Gross and Acquisti 2005). Similar to Light and McGarth (2010), this study concurs that although previous studies acknowledge the ethical issues in the use of social networks, the values governing the human behavior and the technological use has not been studied. Many ethical studies adopt a normative perspective that sees moral behavior as a legitimate human concern. For example Orlikowski and Iacono (2001) purport ethical information technology that allows people to control the behavior of the technology and prevent undesirable outcomes. More recently, a related stream of research examining the ethical and legal responsibilities — *ethicolegal responsibilities* in using OSNs has emerged. For example, Batchelor et al. (2012) examine the ethical dilemma in OSNs where users have impaired or reduced ability to understand the implications of sharing health related data. The authors argue that vulnerable people such as those suffering from dementia and their caretakers face uncertainty in managing consent, data protection, online identity, and legal liabilities. The respondents in this study confront identity threats due to three types of normative ethical issues emergent in the use of OSNs: abysmal behavior, non-benevolence, and unauthorized information disclosure.

Consequently, the three objectives to maximize normative ethics are: *minimize abysmal behavior*, *maximize benevolent use of social networks*, and *minimize unauthorized information disclosure*.

Minimize Abysmal Behavior

Although online social media offers numerous benefits, it also has a "dark side." Increasingly, there are evidences of users engaging in online networks for purposes of bullying, stalking, propaganda, derogation, and profanity to name a few (e.g. see Chretien et al. 2009; Ellison et al. 2007; Willard 2007; Kowalski and Limber 2007; Gross and Acquisti 2005). The respondents in this study perceive identity threats due to abysmal behavior of users. One in particular notes:

> *As my mother says that there is a time and a place for everything. I think social media is not the place for profanity. I believe it is okay to be negative if one has a good reason but not just to vent. Save that venting and f-bombs for your family and close friends and in private!*

Maximize Benevolent Use of Social Networks

Recent studies suggest that a fair number of nonprofit organizations have incorporated OSNs to reach out to key public (e.g. Waters et al. 2009). In particular Briones et al. (2011) provide an evidence of the effectiveness of OSNs for American Red Cross to communicate with the community. Likewise, the use of online networks for spreading situational awareness in times of natural disasters (Veil et al. 2011), epidemics (Househ 2015), health issues (Greene et al. 2011), among others is well acknowledged. However, as mentioned before there is considerable concern about the intent of users and the quality of information spread on these networks. For example in Haitian earthquake, research shows a significant difference in morality between the information disseminated by nonprofits and media and both failed to involve public effectively

(Muralidharan et al. 2011). Likewise, in Ebola outbreak, a significant amount of misinformation was tweeted (Oyeyemi et al. 2014). At individual level, the effectiveness of social media in spreading awareness is well regarded by the participant in this study; however, the lack of benevolent trait in some users poses a threat. The ethical conundrum is noted in the comments of one the participants who says:

> *Good deeds are good deeds irrespective of the fact whether they are performed in the real or virtual world. There are many of my connections on LinkedIn who freely share their knowledge, and provide recommendations and professional support. They have no motive other than to help. Then there are nasty users such as gangs and hate groups who are on the lookout for recruiting youth and spreading propaganda.*

Minimize Unauthorized Information Disclosure

In one of earliest study, Culnan and Armstrong (1999) raise questions about the procedural fairness in online commerce. The authors note that, "fair information practices are procedures that provide individuals with control over the disclosure and subsequent use of their personal information. They are global standards for the ethical use of personal information and are at the heart of U.S. privacy laws" (pg. 107). The current procedures of information consumption and utilization are puzzling to social network users. Research shows that marketers collect information for behavioral targeting (Palmer and Koenig-Lewis 2009) and to intercept one's close friends or connections (Leskovec et al. 2007). These concerns cause respondents of this study fear about divulging their identity. One in particular notes:

> *Everyone points to marketers and advertising agencies. That's just tip of the iceberg. As a consumer of social networking services, I have no idea of what's really going on out there. Even the policies of social networking sites don't really provide any guarantee.*

5.2.2. Evaluation Measures

The evaluation measures were selected in a focus group session comprised of the security experts and the researchers. The measures are listed in Table 8. Following Merrick et al. (2005), to ensure that common OSN users will understand the evaluation measures, simple measures were chosen over the complex ones.

Table 8: The Evaluation Measures

Fundamental Objectives	Evaluation Measures	Desired Level
Affordance in OSNs	Degree of features for user's self presentation and performance*	High
Compliance to Social Norms	Degree of compliance to basic and advanced rules+	High
Re(presentation) of Social Identity	Degree of controls to prevent digital trace of user information+	High
Positive Self-Esteem	Degree of positive Word-of-Mouth shared in the network+	High
Segregation of Multiple Selves	Degree of control to delink multiple identities of a user*	High
Impression	Degree of features to build positive impression*	High
Knowledge	Degree of resources to improve user's knowledge *	High
Outreach	Degree of the features to expand user's social network*	High
Access to Social Capital	Degree of access to resources offering emotional or spiritual type of support+	High
Authenticity of User Accounts	Degree of legitimate and identifiable user accounts+	High
Quality of UGC	Degree of accurate and complete information +	High
Privacy of PII	Degree of confidentiality of information maintained+	High
Abysmal Behavior	Degree of profanity and derogation+	Low
Benevolent Use	Degree of provisions to promote social good not for profit*	High
Unauthorized Information Disclosure	Degree of information sold or accessed without user consent+	Low

*Measured at 3 Levels: Low, Medium, and High; + Measured at 5-Levels: Low, Med-Low, Medium, Med-High, and High

5.2.3. Alternatives: Social Identity Protection Responses (SIPR)

The value hierarchy identifies the objectives for preventing threats to the social identity of individuals. These objectives present a decision opportunity to institutionalize measures for accomplishing the overall fundamental objective i.e. *minimize social identity threats in OSNs*. To accomplish the objective, this study introduces the notion of *Social Identity Protection Responses (SIPR)* and defines it as the set of responses to prevent social identity threats in OSNs. In particular, SIPR involves two broad types of responses to prevent social identity threats in OSNs (see Figure 16). The first response type referred to as *self-recourse* involves certain behavioral actions to neutralize the identity threats that social network users perceive in the social exchange and self-presentation. However, reflecting on the user values, the respondents believe that their actions may not always yield favorable results. There is a greater need for reactive and proactive measures enforced by technology and governing bodies. Consequently, another response type referred to as *external recourse* is defined, in which social networking sites and third-party organizations monitor and prevent identity threats. The response types are discussed below at length.

5.2.3.1. Self-Recourse

Individuals pursue behavioral efforts to negate the potential harm in case an OSN experience is appraised to be identity threatening, (Major and O'Brien 2005). The extant literature identifies three major coping strategies for perceived identity threats: *retaliation*, *concealment*, and *positive distinctiveness*.

Retaliation to the source of threat is the basic behavioral response to protect individual's identity. In the sociology literature, various types of retaliation acts have been studied. For example Sykes and Matza (1957) mention "condemnation of the condemner" technique to shift

the focus from individuals' identity to the motives of the attacker. The discrediting of the source of identity threat that Petriligiri (2011) refers as derogation reduces the severity of the threat in sex-based harassments, for example (Berdahl 2007; Maass et al. 2003).

In the privacy literature, scholars have noted that individuals respond to privacy threats by either refusing to provide information or falsifying information (Son and Kim 2008). In similar vein, an individual conceals the idiosyncratic characteristics of the threatened identity. To prevent the harm, an individual could completely hide the identity in a particular context, suppress the associated characteristics of the threatened identity, or appear to be someone who possesses non-threatened identity (Tajfel, 1978; Roberts, 2005).

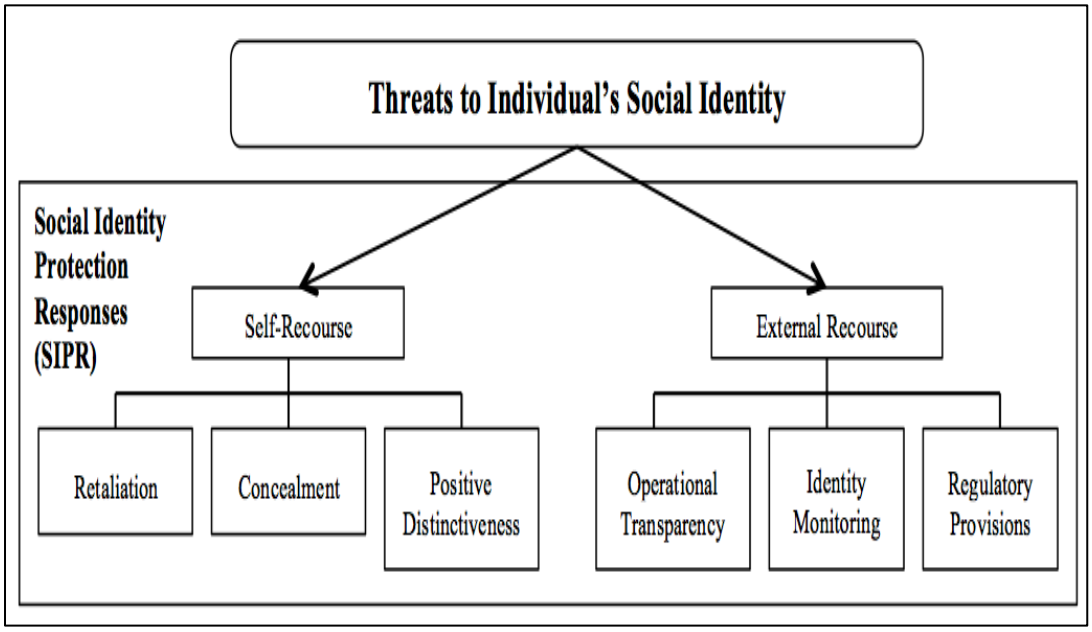


Figure 16: A Typology of Social Identity Protection Responses (SIPR)

Finally, an individual can prevent identity threat by emphasizing positive distinctiveness (Ellemers et al. 2002). Rather than concealing the identity or condemning the source, an individual presents positive information about the threatened identity. The individual attempts to

educate others about the value of the threatened identity and displays pride in associating to the identity (Creed and Scully 2000; Ely 1995).

5.2.3.2. External Recourse

While individuals could take certain actions to prevent harm to their identities, scholars believe that the prevention efforts need to be considered at several other levels spanning businesses, legislative bodies, and policy makers (Milne et al. 2004). Although there is some effort on part of companies in forming coalitions with government agencies such as Federal Trade Commission[6] to fight online identity theft and fraud, preventing harm to the social identity in OSNs is still a challenge. Information security literature recommends that organizations implement not only technological controls, but institutionalize principles of responsibility, integrity, trust and ethics (Dhillon and Backhouse 2000). Similarly, this study proposes a mix of technical and social controls to circumvent social identity threats in OSNs. Broadly the controls provide protection by *identity monitoring*, *operational transparency,* and *regulatory provisions*.

The misuse of identity-related information is a growing concern. In recent years, researchers from academia and industry have introduced solutions and tools to monitor different aspect of identity on web. For example, Symantec Corporation defines a system to protect individual's identifiable information (Satish and Hernacki 2014). Furthermore, this system monitors the information on web for the potential reputational impact for individuals. Likewise, Mashima and Ahamad (2008) propose a user-centric system referred as OpenID Monitor. Informed by such technological designs, this study proposes identity monitoring as an external recourse to prevent social identity threats in OSNs.

[6] http://www.consumer.ftc.gov/topics/privacy-identity

The aggregation of social information in OSNs has become a lucrative source for behavioral researchers and marketers. However, unauthorized data aggregation has raised identity and privacy concerns. Paradoxically, users share information to traverse the social graph and information; however, exposing individual identity invites various problems including reputation, stalking, spamming and phishing (Zhang et al. 2010). Although the Terms of Service of OSNs discourage acts that could jeopardize the individual's identity, social networking sites assume no liability for the content or behavior of users (Lievens 2012). While some considerable efforts are underway to revise the policies for preventing identity harm (Livingstone and Gorzig 2014), the participants of this study recommend design feature to keep users informed about the vulnerability level of their identities. Past research suggests that keeping consumers updated about the operational status increases the perceived value of the service (Buell and Norton 2011). Consequently, operational transparency is proposed as another mechanism to keep users informed about the vulnerability status of their profiles and offer suggestions to prevent the potential harm.

In a recent study Roßnagel et al. (2014) analyze the users' willingness to pay for federated identity management, a mechanism to share user's authentication information across several domains. The results suggest that consumers do not value secure design features as much as they value a system in which an intermediary takes responsibility for the protection of user data. In the consumer complaint literature, dissatisfied customers generally take recourse by involving third-party organizations (Brown and Swartz 1984). Especially, legal provisions to protect data privacy such as HIPAA and COPPA have been a force for organizations to demonstrate compliance. In the US, there are also laws for example to protect minors from obscenity on the

Internet[7]. Consequently, this study proposes that social networking sites would become serious to protect the user identity if the sites are required to comply by certain regulatory provisions.

5.3. Quantitative Value Modelling

5.3.1. Group Utility Functions

The Single Dimensional Utility Functions (SDUFs) were assessed individually for the eleven participants. For each participant, the utilities for all the 15 leaf-level objectives were assessed using lottery elicitations. Figures 17.a shows monotonically increasing SDUFs for the objective *maximize compliance to the norms* i.e. higher compliance have more utility and Figure 17.b shows monotonically decreasing SDUFs for the objective *minimize abysmal behavior* i.e. lower abysmal behavior has more utility. Averaging the utilities of the SDUFs of the participants generates the group utility functions corresponding to the 15 fundamental objectives. Figure 18 shows the Single Dimensional Group Utility Functions (SDGUFs) for the15 leaf-level fundamental objectives. Table 9 shows the quartile average of the utilities of the fundamental objectives. The values indicate the variation in the utility of the objectives amongst the participants.

Table 9: Quartile Averages of Single Dimensional Utility Functions (SDUFs)

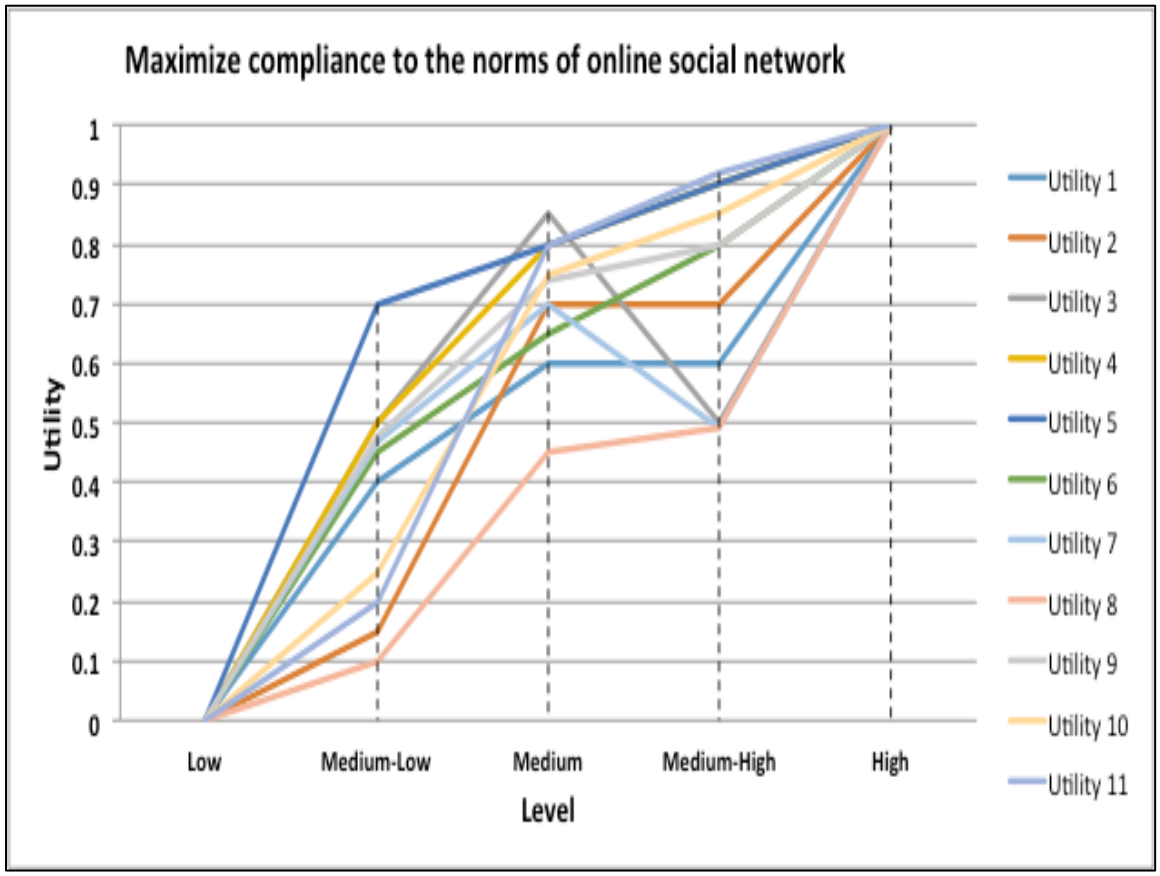
		Quartiles					
Objectives	**Range***	**Min**	**5%**	**25%**	**75%**	**Max**	**Average**
Affordance in OSNs	L	0	0	0	0	0	0
	M	0.35	0.41	0.58	0.70	0.85	0.58
	H	1	1	1	1	1	1
Compliance to Social Norms	L	0	0	0	0	0	0
	ML	0.10	0.23	0.45	0.49	0.70	0.39
	M	0.45	0.68	0.74	0.80	0.85	0.70
	MH	0.49	0.55	0.80	0.88	0.92	0.73
	H	1	1	1	1	1	1

[7]http://www.justice.gov/criminal/ceos/citizensguide/citizensguide_obscenity.html

Re(presentation) of Social Identity	L	0	0	0	0	0	0
	ML	0.10	0.20	0.30	0.45	0.75	0.36
	M	0.35	0.43	0.55	0.65	0.85	0.57
	MH	0.50	0.55	0.80	0.83	0.95	0.73
	H	1	1	1	1	1	1
Positive Self-Esteem	L	0	0	0	0	0	0
	ML	0.10	0.15	0.35	0.45	0.80	0.37
	M	0.35	0.50	0.55	0.65	0.80	0.57
	MH	0.30	0.65	0.80	0.80	0.90	0.69
	H	1	1	1	1	1	1
Segregation of Multiple Selves	L	0	0	0	0	0	0
	M	0.20	0.50	0.60	0.75	0.80	0.57
	H	1	1	1	1	1	1
Impression	L	0	0	0	0	0	0
	M	0.25	0.50	0.65	0.73	0.95	0.62
	H	1	1	1	1	1	1
Knowledge	L	0	0	0	0	0	0
	M	0.20	0.38	0.60	0.68	0.70	0.51
	H	1	1	1	1	1	1
Outreach	L	0	0	0	0	0	0
	M	0.45	0.67	0.75	0.80	0.80	0.69
	H	1	1	1	1	1	1
Access to Social Capital	L	0	0	0	0	0	0
	ML	0	0.225	0.35	0.48	0.85	0.38
	M	0.40	0.50	0.60	0.71	0.90	0.62
	MH	0.45	0.80	0.85	0.85	0.95	0.78
	H	1	1	1	1	1	1
Authenticity of User Accounts	L	0	0	0	0	0	0
	ML	0	0.20	0.25	0.63	0.80	0.38
	M	0.35	0.50	0.60	0.70	0.85	0.60
	MH	0.15	0.78	0.85	0.93	0.95	0.73
	H	1	1	1	1	1	1
Quality of User Generated Content	L	0	0	0	0	0	0
	ML	0	0.18	0.35	0.44	0.80	0.35
	M	0.25	0.58	0.65	0.68	0.90	0.61
	MH	0.70	0.75	0.85	0.90	0.95	0.83
	H	1	1	1	1	1	1
Privacy of Personal Identifiable Information	L	0	0	0	0	0	0
	ML	0	0.23	0.30	0.48	0.90	0.38
	M	0.30	0.40	0.45	0.66	0.93	0.55
	MH	0.40	0.63	0.80	0.86	0.98	0.73
	H	1	1	1	1	1	1
Abysmal Behavior	L	0	0	0	0	0	0
	ML	0	0.15	0.20	0.40	0.80	0.31
	M	0.10	0.45	0.50	0.63	0.85	0.51
	MH	0.30	0.65	0.75	0.80	0.90	0.68

	H	1	1	1	1	1	1
Benevolent Use	L	0	0	0	0	0	0
	M	0	0.53	0.60	0.65	0.75	0.56
	H	1	1	1	1	1	1
Unauthorized Information	L	0	0	0	0	0	0
Disclosure	ML	0	0.20	0.25	0.40	0.90	0.35
	M	0.30	0.40	0.45	0.58	0.80	0.51
	MH	0.40	0.75	0.80	0.85	0.98	0.76
	H	1	1	1	1	1	1

*L=Low, ML=Medium-Low, M=Medium, MH=Medium-High, H=High



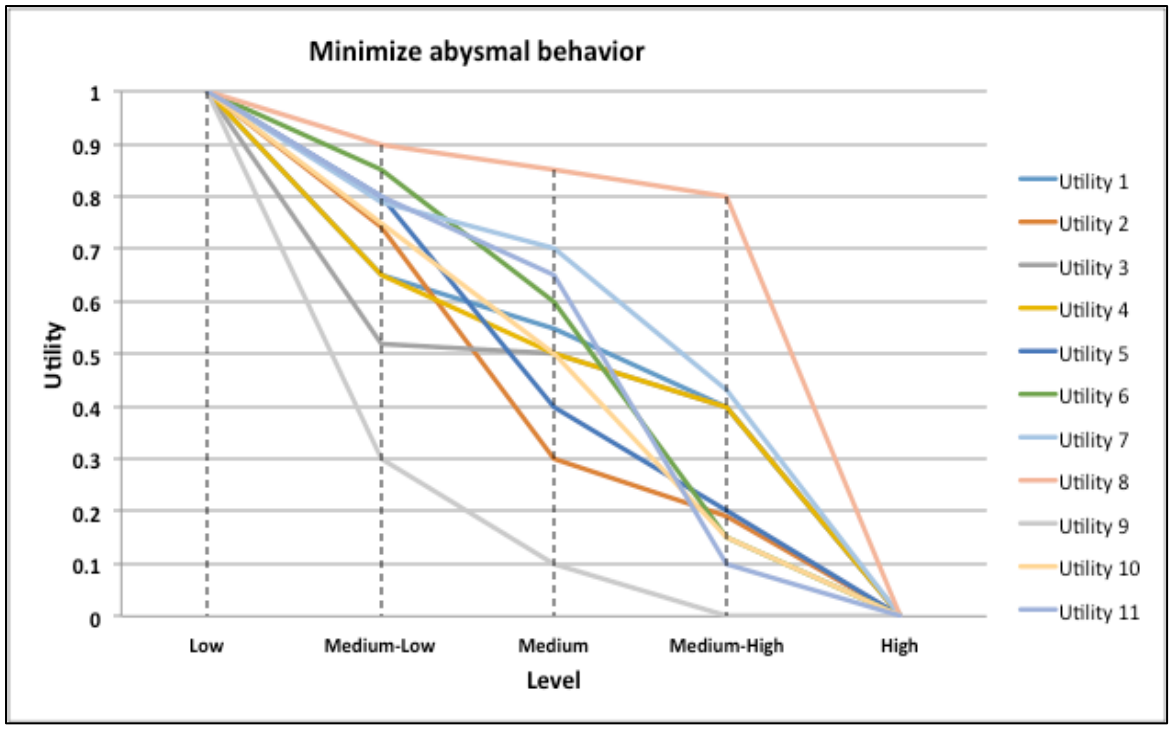


Figure 17.a**:** Monotonically Increasing SDUFs **Figure 17.b:** Monotonically Decreasing SDUFs

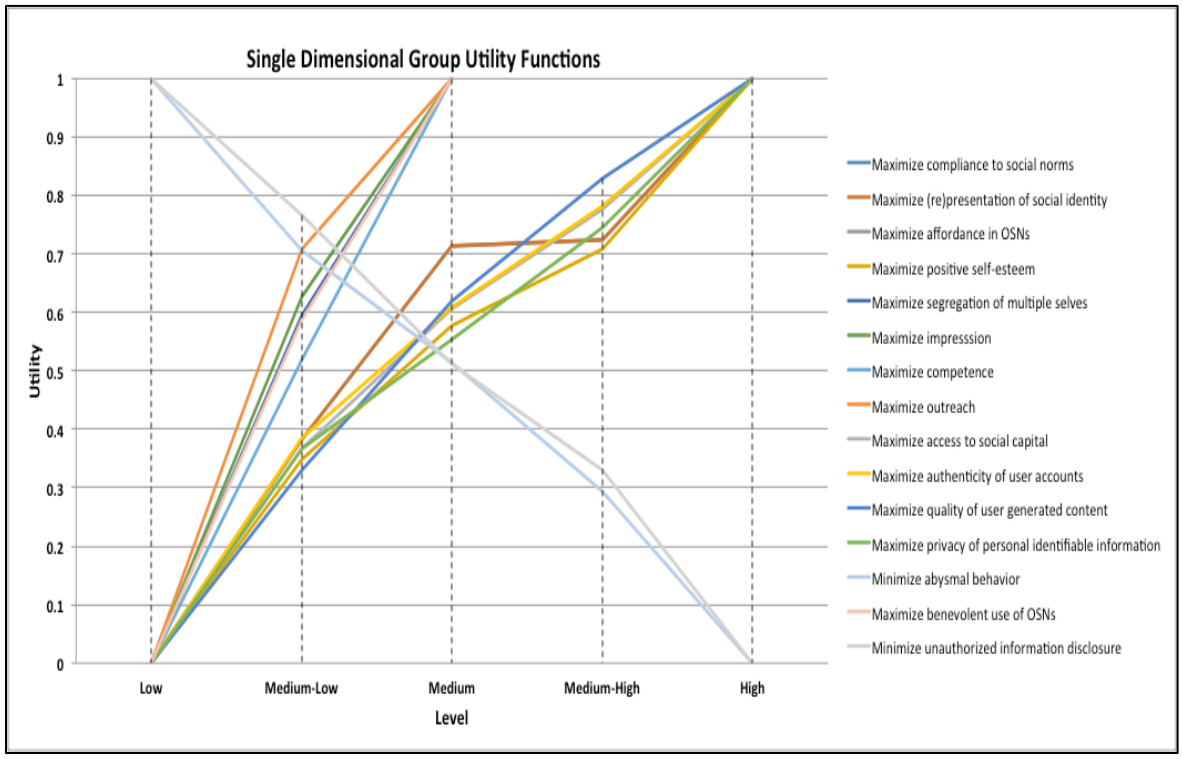


Figure 18: Single Dimensional Group Utility Functions for 15 Leaf-Level Objectives

5.3.2. Objective Weights

The swing weighting technique is used to determine the relative weights for the objectives. Figure 19 shows the relative weights of the fundamental objectives at each level. The sum of the weights at each level equals to one. Clearly, the weights show that social media users have ordered preferences to prevent threats to various aspects of their social identities.

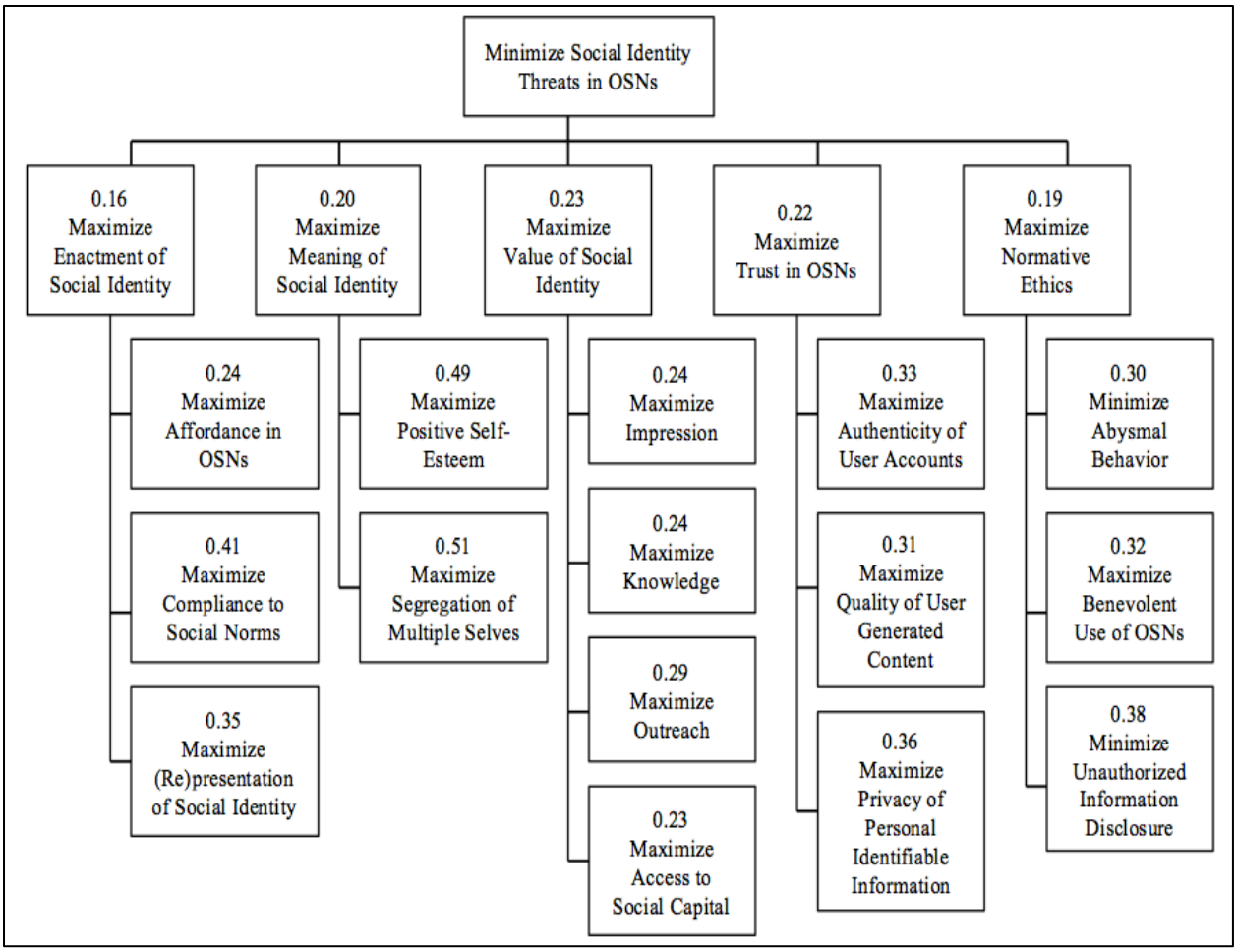


Figure 19: Swing Weights for the Fundamental Value Hierarchy

As expected, users prefer preventing threats to the value of social identity followed by ensuring trust building mechanisms in social networks and preventing threats to the meaning of social identity. In comparison, normative ethics and threats to the enactment of social identity

have lower preferences. For each of the five higher-level objectives, the values ascribed to the corresponding sub-objectives indicate a preferential order. The preference structure could help organizations strategize about the prevention of the social identity threats in OSNs. Overall, the weights represent the maximum value that users ascribe to the objectives in an ideal social networking site. In this study, we refer such an ideal OSN as 'Utopian OSN'. Following Merrick et al. (2005), a Utopian OSN is defined as a hypothetical perfect OSN that fulfills all the objectives to their best levels. The values of Utopian OSN serve as a benchmark to assess the performance of current social networking sites referred to as 'Status Quo' and other alternatives i.e. Social Identity Protection Responses.

5.3.3. Alternative Scoring

The determination of the utility of the objectives corresponding to the six alternatives involes three steps: (1) Assess utility of the objectives — this analysis is done already and Single Dimensional Group Utility Functions are defined; (2) Add the uncertainty by determining the probability distribution of the alternatives; (3) Determine the utility scores by modelling single dimensional group utility functions and probability distribution using Monte Carlo Simulation.

Table 10: Probability Scores of Retaliation

Objective: Maximize affordance in OSNs **Evaluation Measure:** Degree of features for user's self presentation		
Level	**Description**	**Probability**
Low	High constraints imposed by OSN on user membership and role-playing	0.35
Medium	Some constraints imposed by OSN on user membership and role-playing	0.50
High	No constraints imposed by OSN on user membership and role-playing	0.15

To account for the uncertainty in the model, the alternatives are scored using probability elicitation. For each alternative, the probability score of accomplishing a particular objective at different evaluation levels is elicited. For example, consider scoring the alternative *Retaliation* with respect to the objective *maximize affordance in OSNs*. The objective is measured at three levels: low, medium, and high. The description of the levels is provided in Table 10. At each level, the participant's belief about the probability that the given alternative will accomplish the objective is elicited. For example, to elicit the score for low-level, the participant is asked *if retaliation is allowed in OSNs, what is the probability that it will not constraint exhibiting identity characteristics or performing roles related to a particular identity?* The sum of the probabilities equals one. The probabilities for all the 15 leaf-level fundamental objectives are elicited with respect to the six alternatives i.e. Social Identity Protection Responses. Besides evaluating SIPRs, the current social networking sites referred as Status Quo are also evaluated with respect to the fundamental objectives. The scores for Status Quo will help to understand the efficacy of current social networking sites in preventing the identity threats.

A total of 18 individuals participated in the alternative scoring exercise. The individual probabilities are averaged to generate the overall score for the alternatives. Table 11 presents the descriptive statistics of the probabilities. Once the probabilities are determined, the overall utility of the alternatives is determined using Monte Carlo Simulation. Specifically, *RiskDiscrete* function available in @Risk software allows to model uncertain quantities with discrete values and corresponding probabilities. Finally, *RiskMean* function provides the average of the utilities generated by the simulation.

Table 12 shows that the overall utility of Status Quo is 36%. All the five aspects of social identity have a scope of utility improvement by over 50%; however, the objective *maximize*

normative ethics is the one with maximum improvement possible by 68.5%. Figure 20 graphically displays the utility improvement gaps.

Table 11: Mean, Mode and Standard deviation of Probability Scores

	Status Quo	Retaliation	Concealment	Positive Distinctivene	Operational Transparency	Identity Monitoring	Regulatory Provisions
Affordance	1.93 2 0.78	1.91 1 0.84	2.07 2 0.79	1.86 1 0.79	2.01 2 0.81	1.97 2 0.80	2.03 3 0.82
Compliance	3.29 3 1.33	3.18 5 1.40	3.18 4 1.40	3.04 4 1.46	3.21 5 1.42	3.47 5 1.45	3.15 5 1.45
Re(presentation)	3.09 4 1.49	3.53 4 1.28	3.32 5 1.34	3.09 5 1.44	3.24 4 1.32	3.02 1 1.44	2.98 1 1.45
Positive self-esteem	3.35 5 1.40	3.26 4 1.30	3.13 2 1.38	2.99 1 1.46	3.24 4 1.31	3.07 5 1.47	3.11 3 1.30
Multiple-selves	2.22 3 0.77	2.13 3 0.82	2.10 3 0.82	1.93 2 0.76	1.99 2 0.79	1.87 1 0.78	1.86 1 0.79
Impression	2.11 3 0.83	2.04 3 0.85	2.13 3 0.81	2.25 3 0.80	2.25 3 0.82	2.14 3 0.81	2.11 3 0.81
Knowledge	2.19 3 0.76	1.91 1 0.88	1.98 1 0.85	2.19 3 0.82	2.07 3 0.86	2.23 3 0.81	2.12 3 0.83
Outreach	1.99 1 0.82	1.97 1 0.85	1.91 1 0.84	2.08 3 0.81	1.97 1 0.83	2.11 3 0.80	1.96 1 0.83
Social Capital	3.43 4 1.28	3.05 4 1.40	3.02 4 1.40	3.19 4 1.41	3.25 3 1.32	3.13 4 1.49	3.02 4 1.43
Authenticity of users	3.07 1 1.44	3.02 1 1.46	2.86 1 1.44	3.54 5 1.35	3.20 4 1.35	3.01 5 1.52	2.83 1 1.39
Quality of UGC	3.09 3 1.40	3.10 4 1.45	3.25 4 1.40	3.21 4 1.40	3.15 5 1.43	3.06 5 1.51	2.89 1 1.48
Privacy of PII	3.02 3	2.91 1	3.09 3	3.05 3	3.23 5	3.43 5	3.13 4

	1.34	1.54	1.42	1.40	1.46	1.47	1.39
Abysmal behavior	3.17 4 1.37	3.12 3 1.28	3.10 5 1.43	3.35 5 1.38	3.37 5 1.39	3.24 4 1.37	3.18 5 1.42
Benevolent use	2.18 3 0.82	2.10 3 0.83	1.93 1 0.87	2.08 3 0.83	2.28 3 0.79	2.02 2 0.79	2.06 3 0.83
Information disclosure	2.88 1 1.47	3.19 5 1.54	3.26 5 1.43	3.01 1 1.44	3.18 3 1.42	3.22 5 1.47	3.08 5 1.50

Table 12: Scores and Utility

Objectives	**Utopian OSN**	**Status Quo**	**% Utility Attained**
Maximize Enactment of Social Identity	0.16	0.06	37.5%
Maximize Meaning of Social Identity	0.20	0.07	35%
Maximize Value of Social Identity	0.23	0.09	39%
Maximize Trust in OSNs	0.22	0.08	36%
Maximize Normative Ethics	0.19	0.06	31.5%
Total Utility	1	0.36	36%

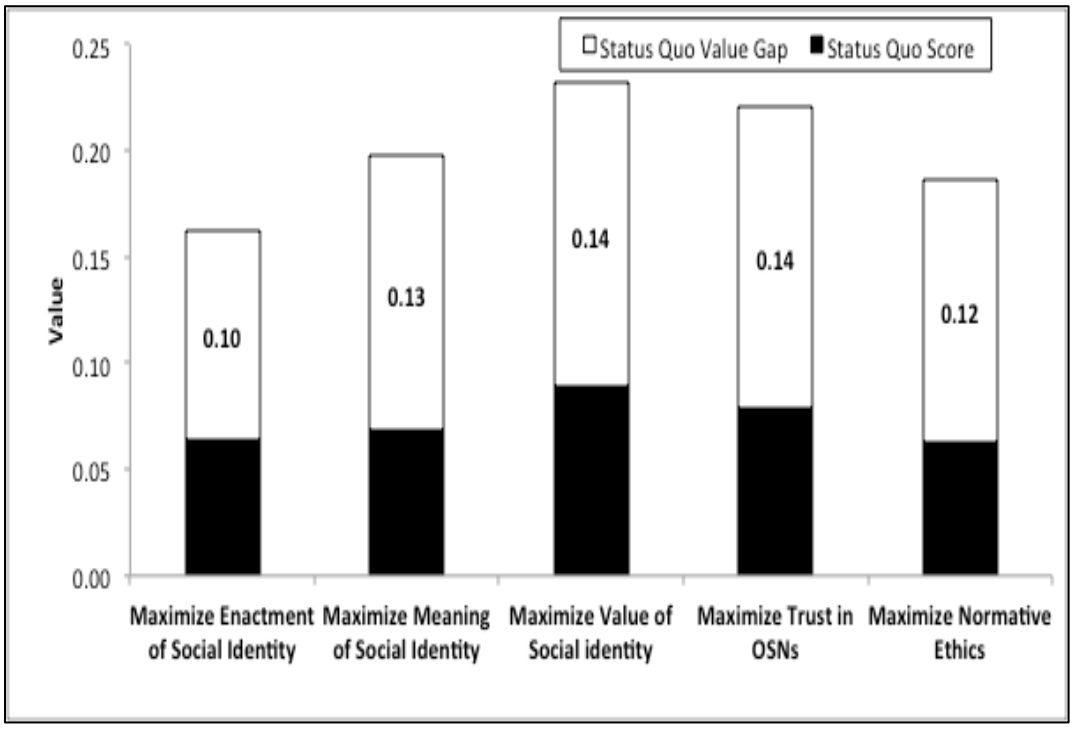


Figure 20: Utility Gaps for Status Quo

5.3.4. Utility Gap Analysis

Utility gap analysis identifies the objectives that have the most scope of improvement and the alternatives that could meet those gaps. Table 13 lists the utility scores for the alternatives (i.e. SIPR) and Status Quo. Figure 21 visually displays the utility scores and utility gaps. Amongst the SIPR, *Regulatory Provisions* achieves the maximum utility followed by *Identity Monitoring* and *Retaliation*. Table 14 presents the utility scores and utility gaps for the value hierarchy with respect to six SIPR. Amongst the three self-recourse alternatives, *Retaliation* achieves maximum utility for the three objectives: enactment, trust and ethics. Amongst the three external recourse alternatives, *Identity monitoring* best achieves three objectives: enactment, meaning and value whereas *Operational transparency* achieves ethics better than other SIPRs. Figures 22a-e graphically shows the utility gaps in the SIPR.

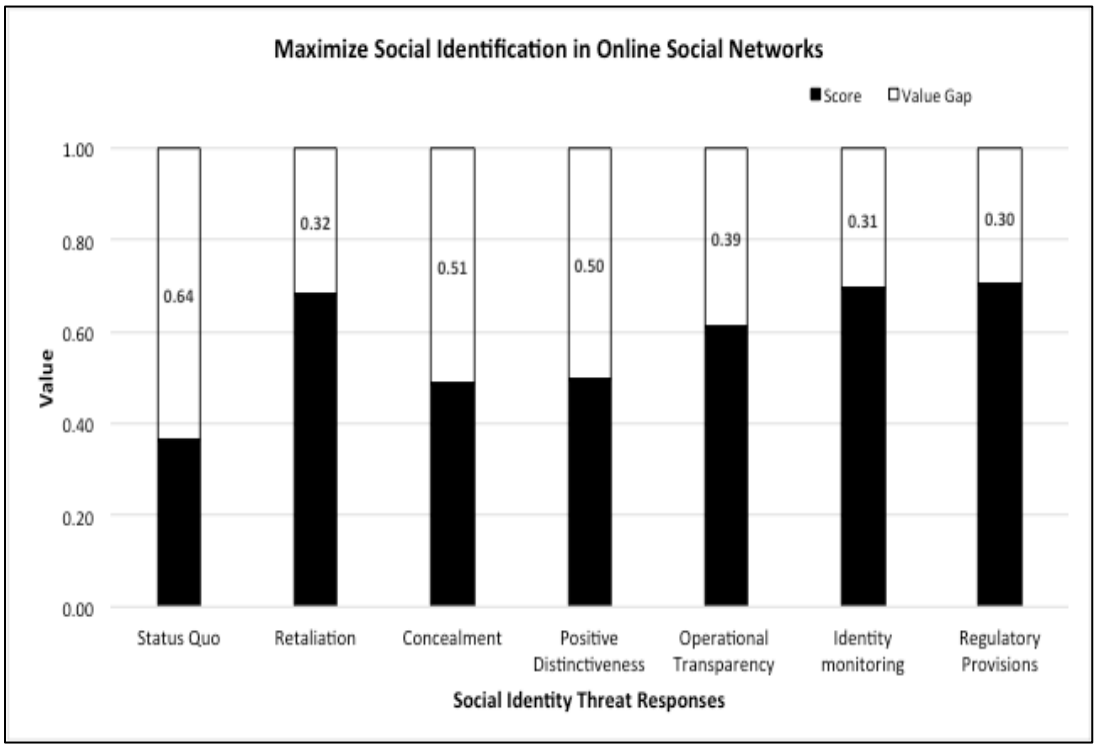


Figure 21: Overall Utility Gaps for the SIPR and Status Quo

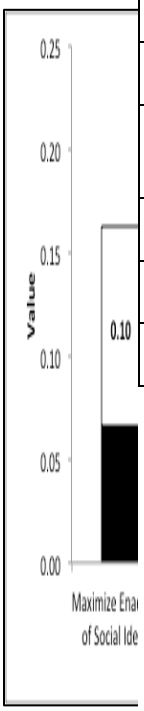
Table 13: Utility Score and the Utility Gaps of the Alternatives

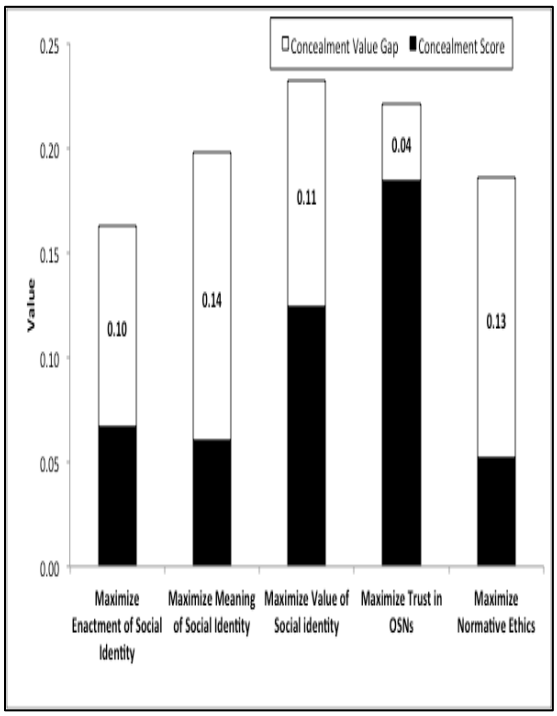
Alternatives	**Utility Score**	**Utility Gap**
Status Quo	0.36	0.64
Retaliation	0.68	0.32
Concealment	0.49	0.51
Positive Distinctiveness	0.50	0.50
Operational Transparency	0.61	0.39
Identity Monitoring	0.69	0.31
Regulatory Provisions	0.70	0.30

Table 14: Scores and Utility Gaps for the Fundamental Value Objectives

Objectives	**Social Identity Protection Responses (SIPR)**													
	Status Quo		Retaliation		Concealment		Positive Distinctiveness		Operational Transparency		Identity Monitoring		Regulatory Provisions	
	Scr.	UG	Scr.	UG	Scr.	UG	Scr.	UG	Scr.	UG	Scr.	UG	Scr.	UG
Maximize Enactment	0.06	0.10	0.07	0.10	0.07	0.10	0.07	0.10	0.09	0.07	**0.14**	**0.02**	0.10	0.06
Affordance	0.59	-0.35	0	0.24	0	0.24	0	0.24	0.59	-0.35	1	-0.76	0	0.24
Compliance	0.00	0.41	0.38	0.03	1.00	-0.59	0.38	0.03	0.71	-0.30	1.00	-0.59	0.72	-0.31
Re(presentation)	0.71	-0.37	0.71	-0.37	0.00	0.35	0.71	-0.37	0.34	0.01	0.56	-0.22	1.00	-0.65
Maximize Meaning	0.07	0.13	**0.17**	**0.03**	0.06	0.14	0.06	0.14	0.10	0.10	**0.16**	**0.04**	0.13	0.07
Positive self-esteem	0.71	-0.22	0.71	-0.22	0.00	0.49	0.00	0.49	1.00	-0.51	0.58	-0.09	0.71	-0.22
Multiple-selves	0.00	0.51	1.00	-0.49	0.60	-0.08	0.60	-0.08	0.00	0.51	1.00	-0.49	0.60	-0.08
Maximize Value	0.09	0.14	0.14	0.09	0.12	0.11	0.14	0.09	0.16	0.07	**0.19**	**0.04**	**0.21**	**0.02**
Impression	0.00	0.24	0.63	-0.38	0.63	-0.38	0.00	0.24	0.63	-0.38	1.00	-0.76	1.00	-0.76
Knowledge	1.00	-0.76	0.00	0.24	1.00	-0.76	1.00	-0.76	1.00	-0.76	1.00	-0.76	1.00	-0.76
Outreach	0.00	0.29	1.00	-0.71	0.00	0.29	1.00	-0.71	0.71	-0.42	0.71	-0.42	0.71	-0.42
Social Capital	0.61	-0.38	0.78	-0.55	0.61	-0.38	0.37	-0.14	0.37	-0.14	0.61	-0.38	1.00	-0.77

Maximize Trust	0.08	0.14	**0.21**	**0.02**	0.18	0.04	**0.19**	**0.03**	0.17	0.05	0.15	0.07	0.16
Authenticity of users	0.78	-0.45	0.78	-0.45	0.78	-0.45	1.00	-0.67	0.61	-0.28	0.78	-0.45	0.39
Quality of UGC	0.33	-0.02	1.00	-0.69	1.00	-0.69	0.62	-0.31	0.62	-0.31	1.00	-0.69	1.00
Privacy of PII	0.00	0.36	1.00	-0.64	0.74	-0.38	1.00	-0.64	1.00	-0.64	0.37	0.00	0.74
Maximize Normative ethics	0.06	0.12	**0.10**	**0.09**	0.05	0.13	0.03	0.15	**0.10**	**0.09**	0.05	0.13	**0.10**
Abysmal behavior	0.70	-0.40	0.29	0.01	0.51	-0.21	0.00	0.30	0.70	-0.40	0.51	-0.21	0.51
Benevolent use	0.00	0.32	1.00	-0.68	0.00	0.32	0.59	-0.27	1.00	-0.68	0.00	0.32	0.59
Information disclosure	0.33	0.05	0.33	0.05	0.33	0.05	0.00	0.38	0.00	0.38	0.33	0.05	0.51





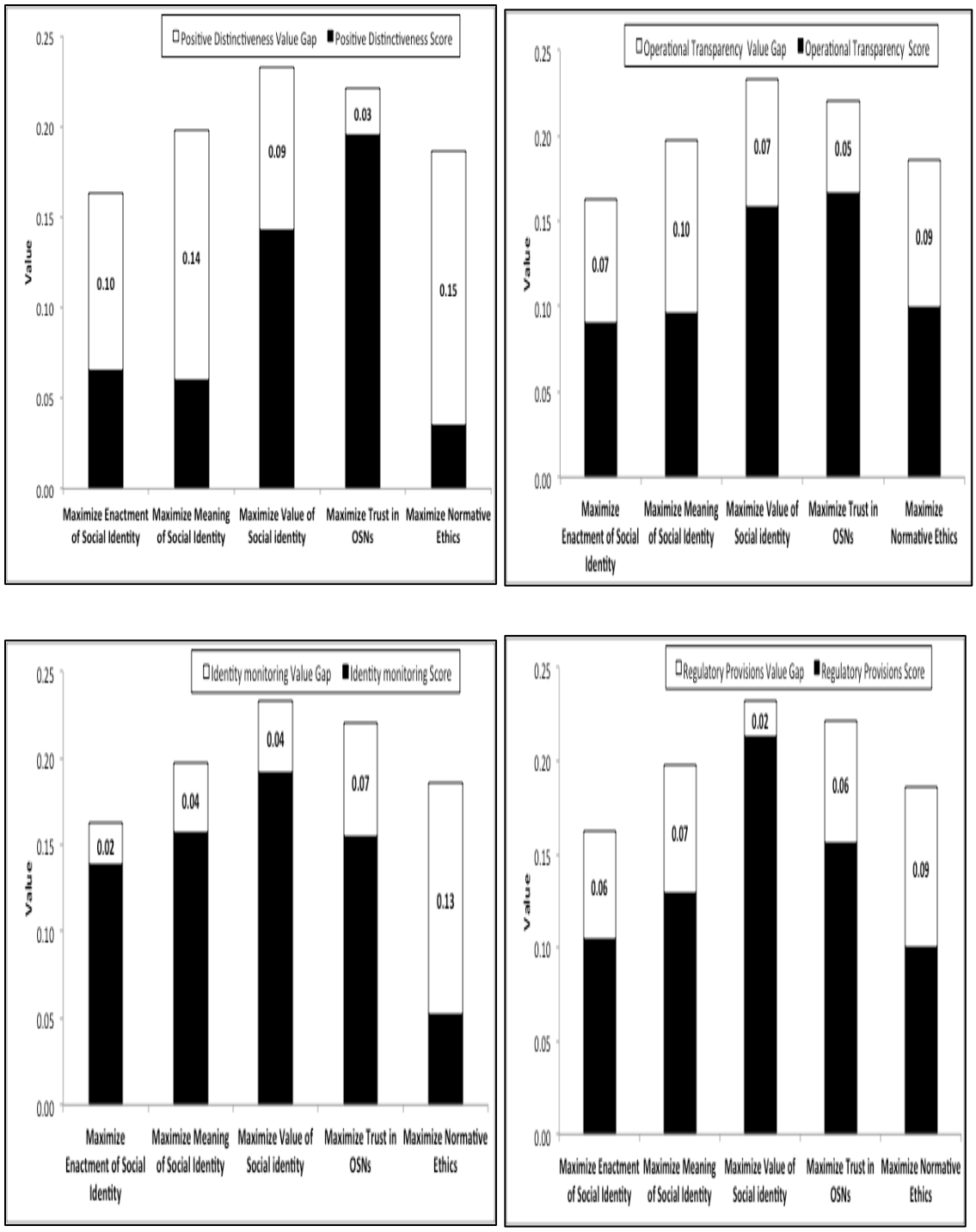


Figure 22.a-e: Utility Gaps for Social identity Protection Responses

5.4. Conclusion

Identification of oneself in OSNs with other users who share common attributes and interests is an important aspect of social networking. However, certain experiences in OSNs could threaten the objective of individual identification. In this chapter, the results of Value Focused Thinking and Multiple Objective Decision Analysis to minimize social identity threats to individuals in OSNs are presented. The utility scores of theoretically grounded alternatives are evaluated and the alternatives that best accomplish the objectives are identified.

Chapter 6: Information Security Reputation (ISR) Threat Analysis

6.1. Introduction

The purpose of this chapter is to present the results of the second research study that examines the reputation threats to organizations in the aftermath of data breaches. The main results that are discussed include: (1) Information Security Reputation (ISR) dimensions as interpreted from Topic Modelling and Content Analysis techniques; (2) Sentiments associated with the Twitter postings using sentiment analysis; (3) Attribution of data breach responsibility using Twitter annotation methodology; (4) hypotheses testing related to the diffusion of reputation threatening tweets.

6.2. Results of Social Media Data Analytics

6.2.1. Topic Model

The topic model discriminates among 15 different topics. Table 15 lists the topics and the corresponding top 8 words that describe each topic. The analysis of the words and the topics resulted into seven topic categories: *Situational Awareness*; *Catastrophic Implications; Preventive Means; Future Assurance; Negative Word-of-Mouth; Social Justice; Moral Responsibility.*

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). *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). *Preventive Means* provides information about the proactive and reactive measures 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).

Table 15: Words, Topics and Categories

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

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). *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). *Social Justice* topics discuss the need for indictment (e.g. indict, hacker) and punishment (e.g. life, sentence, hacker). Finally, *Moral Responsibility* includes topics that raise a voice against the event demanding the organization's attention to the situation (protect, members, heck) and offer information to victims (e.g. free, monitor, prevent).

6.2.2. Content Analysis

The summary of the content analysis is presented in Table 16. 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*; *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.

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 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). Several scholars note that exclusive focus on the technological solutions doesn't ensure information security (Dhillon and Backhouse 2001; Siponen 2005). The risk reduces when organizations implement mix of technical and behavioral controls. The need to integrate risk and resilience mechanisms into the organizational culture to prevent security breaches is well echoed in Twitter postings. The 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 that 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 being 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. 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 modelling 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, organizational information security governance involves 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). The findings emphasize the need for accountability and governance structure to ensure security of data. With respect to the topic modelling results, the following topic categories describe this dimension: Social Justice and Future Assurance. Results suggest that Twitteres, on the one hand, voice the need for regulating data protection mechanisms, and competitors, on the other hand 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 that forensic principles should be integrated into the security tools, training, and techniques for intelligence gathering. Furthermore, Casey notes

that it is important to do for four reasons: 1) To determine when and how the intruders breached the computer system; 2) To appraise what sensitive information was exposed; 3) To determine the intruder's intent; 4) 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. As Coombs (2007) argues that crisis creates a need for information and that it is in the interest of organization's reputation to initiate the communication in order to address the physical and psychological concerns of the stakeholders. The results suggest 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-modelling category that complements this dimension is Preventive Means. The exemplar tweets that infer ineffective response strategy state:

> *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 about 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. The topic modelling results describe this dimension with the Moral Responsibility category. Some of the tweets in this category that criticize company's capability and social responsibility state:

> *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.*

Table 16: Dimensions of Information Security Reputation (ISR)

Content Analysis Results			
First-Order Codes	Second-Order Themes	Aggregate ISR Dimension	Corresponding Topics
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	Situational Awareness; Catastrophic Implications
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	Concerns about Organization's Role in Victimizing Customers		

Organizations doing			
Suspecting Engagement in Unethical Business Practices; Suspecting Company's Intentions	Suspicions About Company's Ethics and Intentions	Security Ethics and Practices	Negative Word-of-Mouth
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 Regulation Through Litigation	Structures of Governance and Responsibility	Social Justice; Future Assurance
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	Preventive Means
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	Moral Responsibility
Spreading Unsubstantiated Information; Mocking Behavior Towards the Crisis Situation	Posting Unsubstantial Negative Remarks		

6.2.3. Data Breach Responsibility Attributions

The five ISR dimensions trigger a varying amount of tweets (see Table 17). A significantly higher proportion of tweets (62%) discuss Security Ethics and Practices of the organizations, followed by 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%). Moreover, a higher percentage of users (57%) tweeted about Security Ethics and Practices followed Risk and Resilience Structure (29%). Comparatively, a lower percentage of users tweeted about the rest of the three ISR dimensions.

Table 17: Tweet and User Frequencies and Percentages

Security Effectiveness Dimensions	Tweets (%)	Users* (%)
Risk and Resilience Structure	3,655(23)	2940(29)
Security Ethics and Practices	10,020(62)	5824(57)
Structures of Governance and Responsibility	351(2)	230(2)
Response Readiness	146(1)	113(1)
Social and Moral Benevolence	2,028(13)	1061(10)
Total	16,200(100)	10,168(100)

**Users tweet on more than one dimension*.

Table 18: Frequency of attributions for ISR dimensions

	Attributions		
ISR Dimensions	**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 18 describes the frequencies of the tweets for the 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.

Table 19: Post-hoc Analysis for ISR Dimensions

ISR Dimensions	Chi-square	P value
Risk & Resilience Structure vs. Security Ethics & 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*

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 19 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 Structure than any other dimension. Also, 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.

6.2.4. ISR Dimensions and Sentiments

This study uses Jeffrey Breen's approach to calculate the sentiment. Results show that 32% of tweets (5,138) have neutral sentiment or mixed sentiment (see, Table 20). 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 20. 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.

Table 20: Sentiment Analysis of ISR Dimensions

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 and 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)

Furthermore, user level analysis is conducted to identify the distribution of sentiments. As shown in Tables 21 and 22, users across all the group-levels tweet more negative sentiments. Moreover, users with the number of followers and followees belonging to the three groups (1-99; 100-499; 500-1,999) post maximum number of tweets and have more negative sentiment. These user

groups are of high interest to organizations as the tweets will comparatively reach and negatively influence large number of users.

Table 21: Analysis of Tweet Sentiment by User Followers

User group (no. of followers)	Users (%)	Tweets (%)	Positive (%)	Negative (%)	Neutral (%)
0	77(1)	112(1)	17(15)	67(60)	28(25)
1-99	1797(19)	2,414(16)	263(11)	1386(57)	765(32)
100-499	2867(31)	4,311(28)	555(13)	2411(56)	1345(31)
500-1,999	2567(28)	4,963(32)	507(10)	2900(58)	1556(31)
2,000-4,999	985(11)	1,616(10)	166(10)	873(54)	577(36)
5,000-9,999	424(5)	1,061(7)	247(23)	497(47)	317(30)
>10,000	582(6)	939(6)	114(12)	524(56)	301(32)
Total	9299(100)	15,416(100)	1869(12)	8658(56)	4889(32)

Table 22: Analysis of Tweet Sentiment by User Followees

User group (no. of followees)	Users (%)	Tweets (%)	Positive (%)	Negative (%)	Neutral (%)
0	214(2)	360(2)	49(14)	198(55)	113(31)
1-99	1512(16)	2197(14)	240(11)	1226(56)	731(33)
100-499	3100(33)	5631(37)	594(11)	3360(60)	1677(30)
500-1,999	3238(35)	5207(34)	737(14)	2760(53)	1710(33)
2,000-4,999	881(9)	1461(9)	178(12)	789(54)	494(34)
5,000-9,999	198(2)	312(2)	37(12)	191(61)	84(27)
>10,000	156(2)	248(2)	34(14)	134(54)	80(32)
Total	9299(100)	15,416(100)	1869(12)	8658(56)	4889(32)

6.2.5. Hypotheses Testing

The descriptive statistics relevant to the variables used for regression analyses is presented in Table 23. On average, a tweet is retweeted 13 times and in 9.47 minutes after the initial posting. There are more negative tweets (polarity:1=positive, 2=negative, and 3=neutral) and on average the sentiment score is 4.11. A tweet on average has two URLs (1.93) and 5 hashtags (4.78). Most of tweets are related to second ISR dimension i.e. Security Ethics and Practices. On

average a user has 1,832 followers and 1,325 followees. A typical user holds Twitter account for an average of 1,235 days i.e. 3.4 years.

Table 23: Summary statistics of variables relevant for regression analyses

n=16,200	Mean	Standard Deviation
Dependent Variables		
rt_count	12.92	21.25
latency (minutes)	9.47	499.53
Independent Variables		
sentiment	4.11	3.05
ISR (dummy)	2.19	1.17
attribution (dummy)	0.48	0.50
polarity (dummy)	2.19	0.64
url (dummy)	1.93	0.46
hashtag(dummy)	4.78	6.03
follower_count	1832.49	1055.47
followee_count	1324.79	834.02
profile_age(days)	1235.33	801.57

The sentiments for the tweets that attribute breach responsibility are also analyzed. As shown in Table 24, 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 for H1 that predicts 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 25).

Table 24: Sentiment Analysis for Attribution Tweets

Attribution	Positive (%)	Negative (%)	Neutral (%)
Yes	785 (38)	4908 (54)	2085 (41)
No	1270 (62)	4099 (46)	3053 (59)
Total	2055 (13)	9077 (56)	5138 (32)
Chi-square=344.443, df=2, P <0.000			

Table 25: Post-hoc Analysis for Sentiments and Attributions

	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

The correlation matrix for the independent variables for whole data set is shown in Table 26. The Variance Inflation Factor (VIF) for the data sample doesn't indicate multicollinearity problem. Poisson Quasi-MLE is run with *rt_count* as the dependent variable to test for H2 that hypothesizes relationship between attributions of data breach responsibility and retweet count. The results are reported in Table 27. The coefficient of attribution ($b = 0.262$, $p < 0.01$) is highly significant. The data sample supports that Twitter postings that attribute data breach responsibility tend to trigger more retweets. The magnitude of the impact of independent variables can be inferred from the exponential transformations of the coefficients as shown in the column exp(b). For example, the coefficient of attribution means that holding all other predictor variables constant, the attribution increases the retweet count by 1.299 times i.e. 30% more retweets. The coefficient for neutral is -0.122. This means that compared to negative sentiment the expected log count reduces by 0.12. The coefficient for positive is -0.265. This means compared to negative sentiment the expected log count reduces by 0.26. Among the control

variables profile_age, hashtag and follower_count are significant. However, hashtag and follower_count reduce the log count by -0.290 and -0.103 whereas follower profile_age increases the log count by 0.060.

Table 26: Correlation matrix of Independent Variables (Full Sample)

	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
Attribution	1								
Polarity	0.03*	1							
Hashtag	0.01	-0.01	1						
url	-0.07*	-0.02*	-0.03*	1					
follower_count	0.00	0.00	0.00	0.00	1				
followee_count	0.00	0.00	0.00	0.01	0.08*	1			
profile_age	-0.02*	0.04*	-0.05*	-0.03*	0.09*	0.10*	1		
sentiment	0.13*	-0.08*	-0.02	-0.04*	0.01	0.00	-0.04*	1	
ISR	0.13*	0.01	-0.01	-0.14*	-0.02	-0.01	0.07*	0.14*	1

** Significant at the 0.05 percent level*

Table 27: Poisson Quasi-MLE Results for H2

Independent Variables	*B*	exp(*b*)	SE	CI: 2.5%-97.5
Attribution	0.262***	1.299	0.023	0.216, 0.308
Neutral	-0.122***	0.885	0.026	-0.173, -0.070
Positive	-0.265***	0.767	0.038	-0.341, -0.190
url	-0.001	0.999	0.030	-0.060, 0.058
Hashtag	-0.290 ***	0.748	0.023	-0.337, -0.243
log(follower_count)	-0.103***	0.902	0.007	-0.119, -0.885
log(followee_count)	0.015	1.015	0.010	-0.004, 0.036
profile_age	0.060***	1.061	0.011	0.037, 0.829
Constant	0.844***	2.325	0.086	0.673, 1.012

*Significance codes: *** 0.01 ** 0.05*

H4 hypothesizes that larger the amount of sentiment score an attribution message has, the higher the number retweets. To test this hypothesis, regression analysis is run for only the tweets where attribution is 'True'. Consequently, the number of tweets reduces to 7,778. Result for Poisson QMLE is reported in Table 28. The coefficient of *sentiment* is highly significant (b=1.389, p <0.000). This means holding all other predictor variables constant, the sentiment score increases the retweet count by 300% (exp(1.389)=4.010). Among the control variables

URL increases the log count by 0.382 and hashtag reduces the log count by -1.433 are significant.

Table 28: Poisson Quasi-MLE Results for H4

Independent Variables	*b*	exp(*b*)	SE	CI: 2.5%-97.5
Sentiment	1.389***	4.010	0.098	1.198, 1.584
url	0.382***	1.465	0.114	0.164, 0.615
Hashtag	-1.443 ***	0.236	0.090	-1.623, -1.270
log(follower_count)	-0.015	0.985	0.018	-0.052, 0.020
log(followee_count)	0.035	1.035	0.024	-0.013, 0.084
profile_age	-0.011	0.989	0.030	-0.069, 0.048
Constant	-0.034	0.966	0.239	-0.508, 0.430

*Significance codes: *** 0.01 ** 0.05*

Table 29: Poisson Quasi-MLE Results for H6

Independent Variables	*b*	exp(*b*)	SE	CI: 2.5%-97.5
attribution	0.145***	1.156	0.035	0.590, 0.936
Negative	0.056	1.057	0.034	-0.011, 0.123
*attribution * negative*	0.207***	1.230	0.048	0.112, 0.303
url	-0.028	0.971	0.030	-0.087, 0.031
Hashtag	-0.310 ***	0.733	0.023	-0.357, -0.263
log(follower_count)	-0.103***	0.901	0.007	-0.119, -0.088
log(followee_count)	0.015	1.016	0.010	-0.004, 0.036
profile_age	0.060***	1.062	0.011	0.037, 0.083
Constant	0.764***	2.147	0.088	0.590, 0.936

*Significance codes: *** 0.01 ** 0.05*

H6 tests the interaction between negative sentiments and attribution of data breach responsibility. (*attribution * negative*). Poisson QMLE is run for all the tweets. The results are shown in Table 29. The coefficient for the interaction terms is significant (b= 0.207, p <0.01). The results suggest that Twitter messages with negative sentiment and attributions trigger 1.23 times i.e. 23% more retweets. Thus, the data sample supports H6. Moreover, the control variables hashtag, follower_count, and profile_age are found significant. More specifically, an increase of 10 percent in the number of followers reduces the retweet count by 1.03 (-0.103

*0.1= -1.03). Likewise, one unit increase in hashtag reduces the log count by 0.310. Finally, one unit increase in profile_age increases the log count by 0.060.

H8 predicts that the retweet count varies by ISR dimensions. The results of Poisson QMLE are reported in Table 30. With respect to ISR1 i.e. Risk and Resilience Structure, all other dimensions except ISR4 are significant. This means compared to ISR1, ISR2 reduces the log count by -0.435 i.e. 35%, ISR3 reduces the log count by -0.873 i.e. 58%, and ISR5 reduces the log count by -0.440 i.e.36%. Besides, with respect to negative sentiment, both neutral and positive sentiments are significant. Among the control variables profile_age, hashtag and follower_count are significant. To determine if ISR is overall statistically significant, Chi-square test is done. The overall sample has a chi-square value of 49. 08 with four 4 degrees of freedom giving a p-value < 5.615e-10. The test indicates that ISR, taken together, is a statistically significant predictor of retweet_count.

Table 30: Poisson Quasi-MLE Results for H8

Independent Variables	*b*	exp(*b*)	SE	CI: 2.5%-97.5
ISR2	-0.435***	0.647	0.027	-0.4888, -0.381
ISR3	-0.873**	0.417	0.110	-1.098, -0.663
ISR4	-0.285	0.751	0.114	-0.519, -0.068
ISR5	-0.440***	0.643	0.040	-0.520, -0.362
Neutral	-0.073**	0.928	0.026	-0.125, -0.022
Positive	-0.188***	0.828	0.038	-0.264, -0.112
url	-0.007	0.992	0.029	-0.065, 0.051
Hashtag	-0.349 ***	0.705	0.025	-0.398, -0.300
log(follower_count)	-0.098***	0.906	0.007	-0.113, -0.083
log(followee_count)	0.016	1.016	0.010	-0.003, 0.037
profile_age	0.054***	1.056	0.011	0.003, 0.037
Constant	1.299***	3.666	0.087	1.127, 1.469

*Significance codes: *** 0.01 ** 0.05*

The correlation matrix for the reduced sample i.e. only retweets is shown in Table 31. The sample size reduces to 6,423. Multicollineraity test indicates that it is not a problem for the

reduced data set. H3 hypothesizes that Twitter posting implying attributions of data breach responsibility have shorter retweet time latency. The dependent variable *latency* represents time and is log transformed for OLS regression. The results are reported in Table 32. The coefficient of attribution ($b = 0.531$, $p < 0.01$) is significant. However, it increases the retweet latency by 70% (=(exp(0.53)-1)*100). This indicates that Twitter posts that attribute data breach responsibility tend to be retweeted slower by almost 70 % times than the ones that don't attribute organizational responsibility. The data sample thus doesn't supports H3. In comparison to negative sentiment, one unit increase in positive sentiments increases the latency by 19%. In comparison to negative sentiment, one unit increase in neutral sentiment reduces the latency by 52%. The control variables URL is significant for retweet latency. More specifically, one unit increase in the number of URL reduces the latency by 28 %.

Table 31: Correlation Matrix of Independent Variables (Reduced Sample)

	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
attribution	1								
Polarity	0.08*	1							
Hashtag	0.06*	-0.11*	1						
url	-0.12*	-0.11*	0.11*	1					
follower_count	-0.02	0.01	-0.01	-0.01	1				
followee_count	-0.03*	-0.01	0.01	0.01	0.02	1			
profile_age	-0.02	0.11*	-0.06*	-0.04*	0.08*	0.12*	1		
sentiment	0.07*	-0.18*	0.06*	0.01	0.00	0.00	-0.08*	1	
ISR	0.21*	-0.03*	0.16*	-0.05*	-0.02	0.01	0.05*	0.17*	1

** Significant at the 5 percent level*

H5 hypothesizes that the sentiment score reduces the retweet latency. The OLS regression is run for only tweets where retweet count is > 0 and attribution is True, reducing the number of tweets to 3023. The results are presented in Table 32. Although overall model is significant, the coefficient of sentiment is not significant. Therefore, the data sample doesn't support H5.

H7 predicts associations between sentiments of the attribution messages and retweet latency is stronger for tweets with negative sentiment. This affect is estimated by adding the interaction between attribution and negativity (*attribution * negative*), which implies that the sentiment polarity moderates retweet latency. The results are shown in Table 32. The coefficient for the interaction term is significant (b= -1.335, p <0.01). The results suggest that messages with negative sentiment and attributions reduces latency by 74% =((exp(-1.335)-1)*100). The data thus support H7. Among the control variables one unit increase in hashtag increases the latency by 40% whereas one unit increase in profile_age reduces the latency by 8%.

Table 32: OLS Regression results for H3, H5, H7, and H9

Dependent variable: *latency*								
Independent Variables	H3		H5		H7		H9	
	b	SE	*b*	SE	*b*	SE	*b*	SE
Attribution	0.531***	0.080			1.274***	0.122		
Positive	0.175	0.122					0.315	0.124
Neutral	-0.735***	0.091					-0.756***	0.092
Negative					1.064***	0.112		
*attribution*negative*					-1.335***	0.169		
sentiment			-0.169	0.411				
url	-0.328**	0.101	0.759	0.450	-0.109	0.102	-0.357***	0.099
Hashtag	0.152	0.082	0.124	0.287	0.339***	0.084	0.524***	0.090
followee_count	-0.006	0.030	0.009	0.135	-0.003	0.038	-0.013	0.037
follower_count	-0.015	0.038	-0.004	0.120	-0.012	0.030	-0.012	0.029
profile_age	-0.083	0.037	-0.047	0.133	-0.084**	0.037	-0.042	0.037
ISR2							0.218	0.102
ISR3							-0.210	0.329
ISR4							-1.958***	0.400
ISR5							-1.177***	0.140
Constant	9.355***	0.295	9.002***	1.061	8.311***	0.302	9.230***	0.300
Adjusted R^2	0.053		-0.016		0.057		0.080	
Number of Obs.	16200		3023		6423		6423	
p-value	< 0.000		0.781		< 0.000		< 0.000	

Notes: The reduced sample contains only tweets that triggered at least one retweet.
*Significance codes: *** 0.01 ** 0.05*

H9 predicts that the retweet latency varies by the ISR dimension. The results are reported in Table 32. With respect to ISR1, ISR2 increases the retweet latency by 24% whereas ISR4 and ISR5 reduce retweet latency by 95% and 69%. ISR3 is not significant. Besides, with respect to

negative sentiment, one unit increase in neutral sentiments reduces the latency by 53%. Among the control variables URL and hashtag are significant. One unit increase in hashtag increases the retweet latency by 68% whereas one unit increase in URL reduces the latency by 30%. A summary of the results of all the hypotheses is presented in Table 33.

Table 33: Summary of Hypothesis Testing

Hypothesis	Description	Support?
H1	*The association between attribution of data breach responsibility and sentiments is stronger for tweets with negative sentiments than for those with positive sentiments.*	Yes
H2	*Twitter postings at reattributing data breach responsibility are retweeted more often.*	Yes
H3	*Twitter postings attributing data breach responsibility have shorter retweet time latency.*	No
H4	*The larger the total amount of sentiment (positive or negative) an attribution Twitter posting exhibits, the more often it is retweeted.*	Yes
H5	*The larger the total amount of sentiment (positive or negative) an attribution Twitter posting exhibits, the shorter is the retweet time latency.*	No
H6	*Twitter postings attributing data breach responsibility and negative sentiment are retweeted more often.*	Yes
H7	*Twitter postings attributing data breach responsibility and negative sentiment have shorter retweet time latency.*	Yes
H8	*Retweet count of Twitter postings varies for Information Security Reputation (ISR) dimensions.*	Yes
H9	*Retweet latency of Twitter postings varies for Information Security Reputation (ISR) dimensions*	Yes

6.3. Conclusion

This chapter presents the results of Social Media Knowledge Discovery (SMKD) process applied for studying the Information Security Reputation (ISR) threats in Online Social Network (OSNs). Dimensions of ISR emergent from Topic Modelling and Content Analysis are discussed. The results for attribution of data breach responsibility and associated sentiments in

Twitter postings are presented. Finally, the empirical analyses to test the diffusion reputation threatening tweets are presented.

Chapter 7: Discussion & Conclusion

7.1. Introduction

This chapter summarizes the findings corresponding to the two research studies. The contribution of each research study to theory, practice, and methodology is discussed. The limitations and the future research directions are also discussed. Finally, drawing on the insights provided by the two research studies presented in this dissertation, the chapter concludes by discussing the challenges and the opportunities in the quest of examining the complex interplay between identity and identification in online social networking.

7.2. Research Study 1: Social Identity Threats to Individuals in Online Social Networks

7.2.1. Research Findings

Using the concepts of Value Focused Thinking (VFT) and the technique of Multiple Objectives Decision Analysis (MODA), this research study analyzes the threats to the social identity of individuals in OSNs. Table 34 summarizes the findings for the four research questions. Overall, the analysis reveals that the current social networking sites significantly threaten the social identity values of individuals. The taxonomy of Social Identity Protection Responses are perceived to avert the threats to some extent; however, there is a need to define better measures for the protection of individual values toward their social identity.

Table 34: Summary of the Findings for Research Study 1

Research Question	Research Findings
RQ1: What are fundamental objectives to prevent threats to the various aspects of social identity of individuals in Online Social Networks?	Using the qualitative data analysis of user values and informed by the theory and literature on social identity and identity threats, this study defines five fundamental objectives to minimize threats to the social identity of individuals in OSNs: maximize enactment of social identity, maximize meaning of

	social identity, maximize value of social identity, maximize trust in social networks, and maximize normative ethics in social networks. For each fundamental objective, a set of sub-objectives is defined. Together the 15 sub-objectives ensure minimization of social identity threats to individuals in Online Social Network (OSNs)
RQ2: What are the user responses to prevent social identity threats in Online Social Networks?	Informed by the value hierarchy and the existing literature, this study defines taxonomy of responses to prevent social identity threats in OSNs. The taxonomy, referred to as Social Identity Protection Responses (SIPR), encompasses self-recourse and external-recourse as preventive responses. Self-recourse involves three types of alternatives: retaliation, concealment, and positive distinctiveness. And the external recourse involves three types of alternatives: identity monitoring, operational transparency, and regulatory provisions
RQ3: What are the gaps between the values informing the social identity of the individuals and those supported by the identification mechanisms of current Online Social Networks?	By comparing the utility scores of the current OSNs referred to as Status Quo with that of perfect social network referred to as Utopian OSN, the gaps indicate that the current social networking platforms significantly lack endurance of user values for all the 15 fundamental sub-objectives. The net utility of Status Quo is 36%. The percentage utility of the five aspects of social identity for the Status Quo is: - Maximize Enactment of Social Identity: 37.5% - Maximize Meaning of Social Identity: 35% - Maximize Value of Social Identity: 39% - Maximize Trust in OSNs: 36% - Maximize Normative Ethics: 31.5%
RQ4: What are the most effective user responses to prevent social identity threats in Online Social Networks?	By conducting the utility gap analysis, this study describes the utility of the Social Identity Protection Responses (SIPR) to prevent the threats related to the 15 fundamental sub-objectives. The net utility of the SIPR is as follows: - Retaliation: 68% - Concealment: 49% - Positive Distinctiveness: 50% - Operational Transparency: 61% - Identity Monitoring: 69% - Regulatory Provisions: 70% Although there is a variation in the utility of the alternatives for preventing social identity threats, none of the alternatives ensure complete protection

7.2.2. Implications on Theory

Social Identity Value Hierarchy

The concept of identity threat has received considerable attention from identity researchers across different disciplines including IS, management, and sociology. Past research in IS conceptualizes and operationalizes individual identity as discreet characteristics of personal identifiable information. This is partly because the identity literature in IS domain explicitly or implicitly focuses on the personal identifiable information and ignores the threats to the social identity of individuals. Furthermore, traditionally identity and identification represent two distinct research strands; however, there is a considerable overlap between the two due to increased intervention of technology. Whitley et al. (2014) make a similar observation as they note the implications of social networking sites on the identity of individuals. The authors mention several problems emergent in social networking platforms including multiple identities, fake identities, abusive behavior, fraud, tension between personal and professional identities etc. The threats in the entanglement of individual identity and the identification mechanisms afforded in OSNs has not received its due attention from IS scholars.

Given the state of the existing research, theorizing about identity and identity threat concepts is not new. However, the objectives to prevent identity threats to the social identity better defines what values of individuals' social identity are threatened in OSNs and how can those threats be prevented. To this effect, the fundamental value hierarchy defined in this study provides a comprehensive framework to understand and plan for the nuances of the social identity threats in the social media landscape. The relative importance of the objectives elicited using swing-weighting technique further prioritizes the objectives for the prevention of identity threats in the technology-driven identification. It is expected that the value hierarchy will mark the starting

point for the researchers to further theorize about the sources of identity threats and the protection measures.

Social Identity Protection Responses Taxonomy

Past research in the IS domain primarily focuses on: 1) definition of the technical measures for identity protection; and 2) analysis of the adoption of identity protection measures (Roßnagel et al. 2011; Lai et al. 2012; Bose and Leung 2013; Abbasi et al. 2008). However, the research falls short of understanding the values that are threatened and use those values as a basis for defining measures. Moreover, little attention has been paid to an array of behavioral responses of users to prevent the perceived identity threats that stem due to identification mechanisms in online social networks. This lack of research is problematic because it is not only important to understand what aspects of identity are threatened in OSNs but also to know how users respond to those identity threats. Together the two aspects have an impact on the user identification and ultimately on the utility of social networking sites.

This study, by drawing on social identity literature coupled with individual values, provides a systematic analysis into the Social Identity Protection Responses (SIPR). In defining the taxonomy, it theorizes why a particular type of response is similar to and distinct from other types of responses. The findings of this study indicate that the SIPR are generally adequate to prevent certain types of identity threats. In particular, the utility scores for SIPR provide an understanding about what type of response is adequate to best achieve an objective preventing a particular type of social identity threat. Thus, it is expected that the taxonomy will serve as a useful starting point for an in-depth examination of the prevention measures for social identity threats.

Utility of Social Identity Threat Responses for Preventing Identity Threats

The growth and popularity of social networks makes it difficult for people to stay abreast of the available choices and features in the social networking platforms. However, when examining the ecology of various OSNs, it becomes clear that while these sites have a common goal of social identification, a careful balance is struck among the identification objectives. Nevertheless, none of the today's OSNs ensure identification with absolute identity protection. The utility gap analysis helps understand the efficacy of the current social networking sites in accomplishing the fundamental objectives encompassing prevention of social identity threats. Although several scholars admit the prevalence of identity threats in social networking sites (e.g. Whitley et al. 2014), no research till date examines the intensity of those threats. By performing the utility gap analysis of Status Quo with respect to Utopian OSN, this research provides an empirical evidence of the seriousness of threats in current OSNs. Additionally, the utility gap analysis of Social Identity Protection Responses provides an understanding about the effectiveness of several behavioral responses in containing the identity threats in current OSNs. Overall the utility gap analysis sets the research agenda for identifying better identity protection mechanisms in OSNs.

7.2.3. Implications on Practice

This research provides several practical insights for social networking users, social networking organizations, and policy makers. From user perspective, the findings educate about the myriad of identity threats prevalent in social networks. The SIPR provide a decision framework for users to choose the most effective recourse in order to circumvent a potential social identity threat. From organizational perspective, the fundamental objectives serve as a baseline for the value-sensitive design of OSNs. Further the utility gaps in current social

networks provide an insight about the utility of the platforms in protecting the values that users attribute to their social identities. Finally, the SIPR provides insights about how organizations could facilitate identity protection. Especially, the utility gaps in SIPR indicate a need for organizations to define more robust controls in the social identification mechanisms of OSNs. Overall the findings will guide the identity protection initiatives of online social networking organizations. Lastly, the objectives could serve as a basis for the policy analysis. The lawmakers could decide what actions need to be taken that would best serve the strategic objective of preventing identity threats in OSNs and increasing the usefulness of OSNs.

7.2.4. Implications on Methodology

Value Focused Thinking (VFT) and Multiple Objectives Decision Analysis (MODA) allow to question what values of users are threatened in the online social identification and how can such values be protected. Furthermore, the exploratory nature of this research study identifies the adequate user responses to prevent the identity threats. Thus, this study heeds to the calls made by scholars to switch the focus from the normative to the exploratory and descriptive designs (Smith et al. 2011; Bélanger and Crossler 2011). Moreover, the sequential mixed method design to build the qualitative and the quantitative value models provide rich meta-interference (Venkatesh et al. 2013). While the qualitative value modelling allows developing fundamental value hierarchy and Social Identity Protection Responses, the quantitative value modelling allows conducting utility gap analysis to measure the efficacy of the protection responses in order to avert identity threats in OSNs. Finally, although VFT and MODA are well-established methodologies in the discipline of Decision Analysis, this research study is first of its type to incorporate both to IS-related research, thus bridging the methodological distances between the two disciplines.

7.2.5. Limitations and Future Research

This research has three limitations. Firstly, the fundamental objectives are measured using the constructed attributes that are subjective in nature. Although Keeney (1978) recommends natural attributes, the unavailability of such attributes for the objectives hierarchy forced to create constructed ones. However, the focus group session served to validate the attributes and ensured that they provide a decent measurability of the objectives. Secondly, the effectiveness of the current social networking sites in preventing the identity threats is assessed in generic sense. The utility scores for Status Quo generalize the efficacy level across various social networking platforms. However, the levels and types of identity threats vary across the social media landscape i.e. Twitter vs. Facebook vs. Google+. Furthermore, it is reasonable to expect that, when faced with identity threats in a particular social media website, a user is likely to engage in certain forms of SIPR mainly based on an individual's experiences within the social network. Consequently, there is a scope to replicate the study in different online social networks in order to validate the value hierarchy and the utility of the identity protection responses. Finally, the analysis of the means objectives to achieve the fundamental value objectives is not within the scope of this research study.

This study opens up several interesting avenues for future research. From theoretical perspective, one of the interesting directions is to test the causal relationship between the identity threats and the behavioral responses. A nomological model of the identity threats as the antecedents of the protection responses will allow the empirical validation of how the antecedents differentially affect different types of behavioral responses. Another avenue for future research is to develop better alternatives for the prevention of identity threats. The utility gaps indicate that none of the recourse types absolutely prevent the perceived threats. Although

the external recourse emerged to be better than the self-recourse, future study need not only to define better alternative but also differentiate the effect of those alternatives in preventing the threats. Such insights could be helpful to redesign features of social networking sites informed by user values. Finally, this study could extend into validating the social identification objectives and protection responses. Especially informed by Dhillon and Torkzadeh (2002), the instruments for measuring identity threats and responses could be defined.

7.3. Research Study 2: Reputation Threats to Organizations in Online Social Networks

7.3.1. Research Findings

The second research study conceptualizes, operationalizes, and validates the threats to the Information Security Reputation (ISR) of the organizations in the aftermath of data breaches. Table 7.2 summarizes the findings corresponding to the three research questions addressed in this study. Using the exploratory analysis of Twitter postings, this study identifies five major dimensions of Information Security Reputation (ISR). 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 previous literature, which argues that the important events are associated with negative sentiments (Thelwall et al. 2011). Furthermore, the higher percentage of neutral sentiments is also 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. Moreover, both attributions and sentiment score increase the retweet count albeit not quickly. However, negative attribution tweets are retweeted more and faster.

Table 35: Summary of the Findings for Research Study 2

Research Question	Research Findings
What dimensions of organizational Information Security Reputation (ISR) are discussed in Twitter postings following a data breach?	The discourse among Twitter users questions the five major dimensions of ISR: Risk and Resilience Structure, Security Ethics and Practices, Structures of Governance and Responsibility, Response Readiness, and Social and Moral Benevolence A large proportion of tweets are related to Security Ethics and Practices (62%), followed by Risk and Resilience Structure (23%) and Social and Moral Benevolence (13%). In comparison, a lower proportion of tweets correspond to Structures of Governance and Responsibility (2%) and Response Readiness (1%) On similar vein, a large number of users tweet about Security Ethics and Practices (57%), followed by Risk and Resilience Structure (29%) and Social and Moral Benevolence (10%). A lesser number of users tweet about Structures of Governance and Responsibility (2%) and Response Readiness (1%)
What are the characteristics of responsibility-attributions and user-sentiments expressed in Twitter Postings related to ISR dimensions?	Overall 48% tweets attribute the data breach responsibility to the organizations Twitter users attribute varying proportion of attributions for the five ISR dimensions. However, there are more attributions for Risk and Resilience Structure (63%). The attribution for the rest of the four dimensions vary between 37% to 45% With respect to the sentiments, 56% tweets are negative, 32% are neutral, and 13% are positive Overall, there are more negative sentiment tweets for all the five ISR dimensions: Risk and Resilience Structure (77%); Response Readiness (60%); Structures of Governance and Responsibility (53%); Security Ethics and Practices (50%); Social and Moral Benevolence (47%) Finally, there are significantly more cases of attribution in those tweets that express negative sentiment than those tweets that

	express positive sentiment or neutral sentiment
What characteristics of eWOM following the data breach impact the subsequent diffusion of ISR threatening tweets?	Twitter postings that attribute data breach responsibility tend to trigger 30% more retweets but increases retweet latency by 70% Sentiment score increases the retweet count by 300% but doesn't reduce the retweet latency Twitter messages with negative sentiments and attributions trigger 23% more retweets and reduce latency by 74% With respect to Risk and Resilience Structure - Security Ethics and Practices reduces retweet count by 35% and increases retweet latency by 24% - Structures of Governance and Responsibility reduces retweet count by 58% - Response Readiness reduces retweet latency by 95% - Social and Moral Benevolence reduces retweet latency by 69% and reduces retweet count by 36%

7.3.2. Implications on Theory

Organizational Information Security Reputation

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 the mechanisms that could threaten that reputation. Furthermore, the attribution of breach responsibility coupled with emotional arousal in social media intensifies 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 to prevent security incidents. However, a robust organization requires a plan for post data breach as well. The data analysis shows that while Risk and Resilience Structure 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. Moreover, post breach strategy is more important in light to our findings about the spread of reputation threats in Twitter. This study shows that information security planning requires an outward focus. Such a planning should consider controlling the diffusion of attributions and negative emotions that could otherwise increase the risk to the security reputation of organizations.

Crisis in Online Social Networks

In the age of online social media, it is easier for customers to create and disseminate negative Word-of-Mouth post crisis. Companies are getting increasingly worried about negative WOM as it could hurt their reputation and profitability (Boyd 2000; Tucker and Melewar 2005). Therefore, to adequately prepare for reputation management, it is important for organizations to

understand the communication dynamics on social networks in the event of data breach. The use of Situational Crisis Communication Theory (SCCT) to analyze Twitter postings demonstrates that the theory originally developed to analyze the organizational crisis, can be adapted for the social media analysis. By understanding the attributions of data breach responsibility and associated sentiments of Twitter postings, this study shows that such tweets diffuse in the online networks at high rate. Specifically, by differentiating between the two mechanisms of diffusion i.e. the number of retweets and the latency of retweets, this study shows that reputation-threatening tweets can not only reach to larger population but can reach faster.

In applying the theory beyond its original application domain, the findings from this study highlight an area of the modification. SCCT posits that crisis triggers negative word of mouth if the stakeholders attribute responsibility to the organization. The diffusion of nWOM is important factor to determine reputational effect. The findings from this study indicate that the diffusion can be assessed by the amount of nWOM i.e. the number of times a tweet is retweeted by different people and the speed at which nWOM is generated i.e. the latency in retweeting. For these reasons, it is suggested that the *amount* and *rate* as the two indicators of the diffusion of negative WOM be theoretically positioned to assess reputation threat in OSNs.

7.3.3. Implications on Practice

The findings from this study have two major implications for practice. Firstly, this study provides practical insight into what aspects of ISR in OSNs need to be managed. 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 quantifiable information will

allow crisis manager to assess the reputation threat and adequately prepare and communicate post breach response for managing reputation of a secure and trustworthy organization.

Secondly, this study emphasizes the need to revise the most popular measure of organization's reputation—*Fortune rating* by integrating public opinion from social media. Scholars critique *Fortune rating* for that it ignores the customer's perspective (Deephouse 2000). However, high profile data breaches not only make headlines of the popular press but also cause provisions for the offending organization to be subjected to public outrage and reputation loss (see Albergotti 2014; Pinsker 2014). Despite the reputation loss after the massive data breach in 2013, Target Corp. maintains its Fortune rating. In 2013, *Fortune* reported Target's reputation score of 36, same as of 2012. This indicates the need to revise the procedures to evaluate reputation score of organizations, especially after the crisis strikes an organization and stakeholders react to it.

7.3.4. Implications on Methodology

In information security research, various scholars have repeatedly made calls to conduct more exploratory studies (e.g. see Bélanger and Crossler 2011; Smith et al. 2011). Further, there is also a momentum to mix qualitative and quantitative methods for richer interpretations (Venkatesh et al. 2013). Finally, the availability of social media data provides an opportunity to overcome the biases of reported data. Past research shows that observational data not only provides richer insight into human behaviors but also overcomes cognitive limitations (see Eagle et al. 2009). Given the need to understand the public reaction to data breaches, this study derives richer meta-inferences for ISR by subjecting the observational data from Twitter to exploratory and confirmatory analysis. In other words, this study heeds to the calls of earlier scholars to investigate what and how ISR is threatened in OSNs by leveraging the public discourse and

behavior of Twitterers. Moreover, this study conceptualized a model referred to as Social Media Knowledge Discovery (SMKD). The model supports various phases of knowledge discovery — from the extraction of data from social media to the processing and analysis of data for deriving useful insights. The big data architecture to support the SMKD is also presented. The use of integrated R-Hadoop environment is utilized to leverage the storage and processing power of the software suite. Finally, the model is instantiated using Twitter data set.

7.3.5. Limitations and Future Research

The Twitter postings allow the 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 the data and the 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, their characteristics, and the propagation of threats 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 the 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 research 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.

Finally, this study applies Latent Dirchichet Allocation (LDA) algorithm for Topic Modelling that according to few scholars may not work well with the Twitter data set due to the short length of tweets (see Zhao et al. 2011). To overcome this limitation, this study follows the recommendations from previous studies and aggregates all the tweets before running LDA (Weng et al., 2010). Although, as Zhao et al. (2011) argue this treatment doesn't consider a single tweet as a topic, the aggregation technique performs well for the purposes of this study.

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 for managing reputation of organizations that face data breaches. More specifically, decision analysis techniques will be applied to assess the significance of various alternatives for managing reputation risks in online social networks. Finally, there also exists a greater scope of developing models for automatic tagging of tweets. For example, this study uses a combination approach to annotate tweets that attribute data breach responsibility. In future, the annotated tweets will be utilized for training automatic annotation algorithm for Twitter data.

7.4. Conclusion

The ubiquitous use of online networking sites has led to unprecedented increase in the user-generated content. Additionally, the micro-processes within these networked structures permeate the content beyond ones immediate social connections. The scalability and reachability of the content have several implications on the identities of social media users. Amongst many such implications, this dissertation examines the identity threats perceived by the individuals and the organizations in the social media based identification. Drawing on the insights provided by this dissertation, this section discusses the complex interplay between identity and identification in online social networks. Three key arguments give direction to this discussion, and each of them provides anchors for information systems researchers who wish to investigate identity in online social platforms.

Firstly, identity is not only the discreet characteristics of user's personality but also the performances relevant to the salient aspects of the identity. In online networks, the identity definition takes variety of forms including symbolic expressions (such as displaying avatars, images etc.) and textual expressions (such as specifying name, gender, or interests). Besides, online networks allow users perform the purposeful actions or behaviors relevant to the traits of the defined identity. The purposeful expression or suppression of salient identity characteristics and identity performances is beneficial as well as challenging. While users could self-define and perform their identities so as to gain social acceptances and draw benefits from the social groups, to be acceptable as a social member generally requires an acceptance of the identity by other members. The second research study demonstrates the social rejection of organization identity as secure and trustworthy after the data breach. The benefits and challenges of social acceptance and rejection of user identities is an interesting direction to explore.

Secondly, identity is socially constructed. It is the product of both self-characterization and external characterization. The threat emerges due to the lack of synergy between the two, however. As sociologist would posit, some identities—both external markers and performances—are perceived to be superior over others. Likewise, in social media identities could be glamorized or defamed. This dissertation demonstrates that what others say have greater impact on the user's identity and identification in social media. For example, in the first research study participants expressed concerns about the threats to the their self esteem and impression and note that the abysmal behavior is commonly experienced. The second research study shows how the thoughts and actions of social media users could hurt the reputation of organizations. An interesting direction to explore is how social media affords the (dis)association between how one represents self to others and how others perceive one. In particular, the definition of social and technical controls to negate the negative effect of the social construction of identities requires its due attention.

Thirdly, identity is a reflection of values. The question "who am I" forces to think about identity as external markers of self such as race, gender, or ethnicity. However, the meaning of identity is much deeper than such characterizations. It is also a reflection of our ideologies and values. Social media provides a medium to reflect the ideologies and values. However, as stated before, the differences and contradictions in the identity characterizations is indeed a conflict of the value system amongst users. Currently social networking sites discourage or encourage certain values as evident from the utility gaps presented in the first research study. Consequently, there arises a need to (re)design these platforms in order to account for the human values. The first research study demonstrates how to elicit the values and identify objectives for ensuring those values, the next step is to design or integrate those values into technology. However, there

is also a need to conduct similar analysis for different contexts, stakeholders, and purposes. The integration of comprehensive and principled values in the social network ecosystem is an interesting and challenging direction to pursue.

In conclusion, it is important to establish resiliency more important than ever in today's networked society that exposes us to the risks previously unknown. While information systems researchers have explored some of the important aspects of identity and identification, this dissertation demonstrates the scope of examining the negative effects due to the entanglement of the two concepts. Better technical and behavioral controls are required to protect the user identities and enhance the identification in social media. As this dissertation demonstrates, information systems researchers have much to contribute to this research stream.

References

Abbasi, A., Chen, H., and Nunamaker, J. F. 2008. "Stylometric identification in electronic markets: Scalability and robustness," *Journal of Management Information Systems* (25:1), pp. 49-78.

Abrams, D. 1992. "Processes of social identification," in *Social psychology of identity and the self-concept,* G. M. Breakwell (ed.), London: Surrey University Press, pp. 57-99.

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.

Acquisti, A., and Gross, R. 2006. "Imagined communities: Awareness, information sharing, and privacy on the Facebook," in *Privacy enhancing technologies*, Springer Berlin Heidelberg, pp. 36-58.

Agichtein, E., Castillo, C., Donato, D., Gionis, A., and Mishne, G. 2008. "Finding high-quality content in social media," in *Proceedings of the 2008 International Conference on Web Search and Data Mining*, ACM, pp. 183-194.

Agranoff, C. 2012. "Online Reputation -- Losing in Court Thanks to Facebook and Twitter," (available at http://www.huffingtonpost.com/craig-agranoff/online-reputation_b_1305013.html).

Albert, S., and Whetten, D. A. 1985. "Organizational identity," *Research in organizational behavior*, pp. 263-295.

Albergotti, R. 2014. "Furor Erupts Over Facebook's Experiment on Users," (available at http://online.wsj.com/articles/furor-erupts-over-facebook-experiment-on-users-1404085840).

Albrechtslund, A. 2008. "Online social networking as participatory surveillance," *First Monday* (*13*:3).

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*.

Anteby, M. 2008. "Identity incentives as an engaging form of control: Revisiting leniencies in an aeronautic plant," *Organization Science* (19:), pp. 202–220.

Arrow, Kenneth. 1974. *The Limits of Organization*, Norton.

Ashforth, B. E., and Kreiner, G. E. 1999. ""How can you do it?": Dirty work and the challenge of constructing a positive identity," *Academy of Management Review* (24:), pp. 413–434.

Ashforth, B. E., and Mael, F. 1989. "Social identity theory and the organization," *Academy of management review* (*14*:1), pp. 20-39.

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

Backstrom, L., Huttenlocher, D., Kleinberg, J., and Lan, X. 2006. "Group formation in large social networks: membership, growth, and evolution," in *Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining,* ACM, pp. 44-54.

Baker, M., and Wurgler, J. 2006. "Investor sentiment and the cross-section of stock returns," *The Journal of Finance* (61:4), pp. 1645-1680.

Baldwin, J. M. 1894. "Imitation: A chapter in the natural history of consciousness," in *Mind* (3:), pp. 25-55.

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.
Barber, B. 1983. *The Logic and Limits of Trust*, Rutgers University Press: New Brunswick.
Bargh, J., and McKenna, K. 2004. "The Internet and social life," *Annual Review of Psychology* (55:1), pp. 573-590.
Baskerville, R. 1993. "Information systems security design methods: implications for information systems development," *ACM Computing Surveys (CSUR)* (25:4), pp. 375-414.
Batchelor, R., Bobrowicz, A., Mackenzie, R., and Milne, A. 2012. "Challenges of ethical and legal responsibilities when technologies' uses and users change: social networking sites, decision-making capacity and dementia," *Ethics and information technology* (14:2), pp. 99-108.
Baumeister, R.F., Bratslavsky, E., Finkenauer, C., and Vohs, K.D. 2001. "Bad is stronger than good," *Review of General Psychology* (5:4), pp. 323–370.
Bélanger, F., and Crossler, R.E. 2011. "Privacy in the digital age: A review of information privacy research in information systems," *MIS quarterly* (35:4), pp. 1017-1042.
Berdahl, J. L. 2007. "Harassment based on sex: Protecting social status in the context of gender hierarchy," *Academy of Management Review* (32:), pp. 641-658.
Berger, J., and Milkman, K. 2010. "Social transmission, emotion, and the virality of online content," *Wharton Research Paper*.
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.
Blumer, H. 1986. *Symbolic interactionism: Perspective and method*, University of California Press: Berkeley.
Borau, K., Ullrich, C., Feng, J., and Shen, R. 2009. "Microblogging for language learning: Using twitter to train communicative and cultural competence," in *Advances in Web Based Learning–ICWL,* Springer Berlin Heidelberg, pp. 78-87.
Bose, I., and Leung, A. C. M. 2013. "The impact of adoption of identity theft countermeasures on firm value," *Decision Support Systems* (55:3), pp. 753-763.
Boshmaf, Y., Muslukhov, I., Beznosov, K., and Ripeanu, M. 2011. "The socialbot network: when bots socialize for fame and money," in *Proceedings of the 27th Annual Computer Security Applications Conference*, ACM, pp. 93-102.
Boyd and J. Heer, 2006. "Profiles as conversation: Networked identity performance on Friendster," in *Proceedings of the Hawai'i International Conference on System Science (HICSS–39)*.
Boyd, R., Gintis, H., Bowles, S., and Richerson, P. J. 2003. "The evolution of altruistic punishment," *Proceedings of the National Academy of Sciences*, (*100*:6), pp. 3531-3535.
Boyd, N. 2000. "Crisis management and the internet," *Ivey Business Journal* (64: 3), pp. 3-17.
Branscombe, N. R., Ellemers, N., Spears, R., and Doosje, B. 1999. "The context and content of social identity threat"
Breakwell, G. M. 1983. *Threatened identities,* Wiley: Chichester, UK.
Briones, R. L., Kuch, B., Liu, B. F., and Jin, Y. 2011. "Keeping up with the digital age: How the American Red Cross uses social media to build relationships," *Public Relations Review* (37:1), pp. 37-43.

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, T. J., Dacin, P. A., Pratt, M. G., and Whetten, D. A. 2006. "Identity, intended image, construed image, and reputation: an interdisciplinary framework and suggested terminology," *Journal of the Academy of Marketing Science* (34:2), pp. 99-106.
Brown, J. J., and Reingen, P. H. 1987. "Social ties and word-of-mouth referral behavior," *Journal of Consumer research*, pp. 350-362.
Brown, S. W., and Swartz, T. A. 1984. "Consumer Medical Com- plaint Behavior: Determinants of and Alternatives to Malpractice Litigation," *Journal of Public Policy and Marketing* (3:1), pp. 85-98.
Buell, R. W., and Norton, M. I. 2011. "The labor illusion: How operational transparency increases perceived value," *Management Science* (57:9), pp. 1564-1579.
Burrell, G., and Morgan, G. 1979. *Sociological paradigms and organizational analysis,* Heinemann: London.
Campbell, J., Fletcher, G., and Greenhill, A. 2009. "Conflict and identity shape shifting in an online financial community," *Information Systems Journal* (19:5), pp. 461-478.
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* (3:), pp. 13-16.
Centola, D. 2010. "The spread of behavior in an online social network experiment," *Science* (329:5996), pp. 1194-1197.
Cherryholmes, C. H. 1992. "Notes on pragmatism and scientific realism," *Educational Research*, pp. 13-17.
Chen, R. 2013. "Living a private life in public social networks: An exploration of member self-disclosure," *Decision Support Systems* (55:3), pp. 661-668.
Chevalier, J. A., and Mayzlin, D. 2006. "The effect of word of mouth on sales: Online book reviews," *Journal of marketing research* (43:3), pp. 345-354.
Chretien, K. C., Greysen, S. R., Chretien, J. P., and Kind, T. 2009, "Online posting of unprofessional content by medical students," *JAMA* (302:12), pp. 1309-1315.
Chung, S. and Liu, S. 2011. *Predicting Stock Market Fluctuations from Twitter*, Berkeley, California.
Cialdini, R. B., and Goldstein, N. J. 2004. "Social influence: Compliance and conformity," *Annual Review of Psychology* (55*:)*, pp. 591-621.
Citrin, J., Wong, C. and Duff, B. 2001. "The Meaning of American National Identity: Patterns of Ethnic Conflict and Consensus" in *Social identity, intergroup conflict, and conflict reduction,* Ashmore, R. D., Jussim, L. J., & Wilder, D. (eds.), Oxford University Press: USA.
Clemen,R. T.,and Terence, R. 2001. *Making Hard Decisions with Decision Tools Suite Update 2004 Edition*, Duxbury Press: Pacific Grove, CA.
Coleman, James S. 1988. "Social Capital in the Creation of Human Capital," *American Journal of Sociology* (94:), pp. 95-120.
J. Coleman. 1990. Foundations of Social Theory, Harvard.

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.
Cooper, R. B., and Johnson, N. A. 2014. "So close yet no agreement: The effects of threats to self-esteem when using instant messaging and audio during seller–buyer negotiations," *Decision Support Systems* (57:), pp. 115-126.
Cooper, A.H. 2002. "Media framing and social movement mobilization: German peace protest against INF missels, the Gulf War, and NATO peace enforcement in Bosnia," *European Journal of Political Research* (41:), pp. 37–80.
Creed, W. E. D., and Scully, M. A. 2000. "Songs of ourselves: Employees' deployment of social identity in workplace encounters," *Journal of Management Inquiry* (9:), pp. 391–412.
Creswell, J. W. 2013. Research design: Qualitative, quantitative, and mixed methods approaches, Sage.
Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2012. "Future directions for behavioral information security research," *Computers & Security*.
Culnan, M. J. and Armstrong, P. K. 1999. "Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation," *Organization Science* (10:1), pp. 104–115.
Cutillo, L. A., Molva, R., and Strufe, T. 2009. "Safebook: A privacy-preserving online social network leveraging on real-life trust," *Communications Magazine, IEEE* (47:12), pp. 94-101.
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.
Davenport, T.H., and Beck, J.C. 2002. *The attention economy: Understanding the new currency of business*, Harvard Business Press: Cambridge, MA.
Deaux, K. 1993. "Reconstructing social identity," *Personality and Social Psychology Bulletin* (19:), pp. 4-12.
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.
Dellarocas, C. 2006. "Strategic manipulation of internet opinion forums: Implications for consumers and firms," *Management Science* (52:10), pp. 1577-1593.
Dellarocas, C. 2003. "The digitization of word of mouth: Promise and challenges of online feedback mechanisms," *Management Science* (49:10), pp. 1407-1424.
Denzin, N. K. and Lincoln, Y. S. (eds.) 2011. *The SAGE handbook of qualitative research* (4th ed.), Sage: Thousand Oaks, CA.
Dhillon, G., and Backhouse, J. 2001. "Current Directions in Information Security Research: Toward Socio-Organizational Perspectives," *Information Systems Journal* (11:2), pp. 127-153.
Dhillon, G., and Backhouse, J. 2000. "Technical opinion: Information system security management in the new millennium," *Communications of the ACM* (43:7), pp. 125-128.

Dowling, G. 2002. Creating Corporate Reputations: Identity, Image, and Performance, Oxford University Press: New York.
Druckman, J.N. 2001. "The implications of framing effects for citizen competence," *Political Behavior* (23:3), pp. 225–256.
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.
Dwyer, C., Hiltz, S., and Passerini, K. 2007. "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace," in *the Proceedings of AMCIS*, pp. 339.
Eagle, N., Pentland, A. S., and Lazer, D. 2009. "Inferring friendship network structure by using mobile phone data," in the *Proceedings of the National Academy of Sciences* (106:36), pp. 15274-15278.
Ellemers, N., Spears, R., and Doosje, B. 2002. "Self and social identity," *Annual Review of Psychology* (53:), pp. 161-186.
Ellison, N. B., Steinfield, C., and Lampe, C. 2007. "The benefits of Facebook "friends: Social capital and college students' use of online social network sites," *Journal of Computer-Mediated Communication* (12:4), pp. 1143-1168.
Ellison, N. B. 2007. "Social network sites: Definition, history, and scholarship," *Journal of Computer-Mediated Communication* (13:1), pp. 210-230.
Elsass, P. M., and Ralston, D. A. 1989. "Individual responses to the stress of career plateauing," *Journal of Management* (15:), pp. 35-47.
Ely, R. J. 1995. "The power in demography: Women's social constructions of gender identity at work," *Academy of Management Journal* (38:), pp. 589–634.
England, G. W. 1967. "Personal value systems of American managers," *Academy of Management Journal* (10:1), pp. 53-68.
Ethier, K. A., and Deaux, K. 1994. "Negotiating social identity when contexts change: Maintaining identification and responding to threat," *Journal of personality and social psychology* (*67*:2), pp. 243.
Fayard, A. L., and DeSanctis, G. 2010. "Enacting language games: the development of a sense of 'we-ness' in online forums," *Information Systems Journal* (20:4), pp. 383-416.
Fayyad, U. M., Piatetsky-Shapiro, G., and Smyth, P. 1996a. "Knowledge Discovery and Data Mining: Towards a Unifying Framework," in *KDD* (96:), pp. 82-88.
Fayyad, U., Piatetsky-Shapiro, G., and Smyth, P. 1996b. "From data mining to knowledge discovery in databases," *AI magazine* (17:3), pp. 37.
Fehr, E., and Gächter, S. 2002. "Altruistic punishment in humans," *Nature* (415:6868), pp. 137-140.
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.
Fischbacher, U., Gächter, S., and Fehr, E. 2001. "Are people conditionally cooperative? Evidence from a public goods experiment," *Economics Letters* (71:3), pp. 397-404.
Fischer, K. W., Shaver, P. R., and Carnochan, P. 1990. "How emotions develop and how they organize development," *Cognition and emotion* (4:2), pp. 81-127.
Fischhoff, B. 1991. "Value elicitation: is there anything in there?" *American Psychologist* (46:8), pp. 835-847.

Fiol, C. M., Pratt, M. G., and O'Connor, E. J. 2009. "Managing intractable identity conflicts," *Academy of Management Review* (34:), pp. 32–55.
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*, Harvard Business School Press: Boston, MA.
Forman, C., Ghose, A., and Wiesenfeld, B. 2008. "Examining the relationship between reviews and sales: The role of reviewer identity disclosure in electronic markets," *Information Systems Research* (19:3), pp. 291-313.
Friedman, Batya. 1996. "Value-sensitive design," *interactions* (3:6), pp. 16-23.
Friedman, B., Kahn, P., and Borning, A. 2002. "Value sensitive design: Theory and methods," *University of Washington technical report*, pp. 02-12.
Friedman, B., Kahn Jr, P. H., Borning, A., and Huldtgren, A. 2013. "Value sensitive design and information systems," in *Early engagement and new technologies: Opening up the laboratory*, Springer Netherlands, pp. 55-95.
Gardner, R. C. 1985. Social psychology and second language learning: The role of attitudes and motivation. London: Edward Arnold.
Gaver, W. W. 1991. "Technology affordances," in Proceedings of the SIGCHI conference on Human factors in computing systems, ACM, pp. 79-84.
Gecas, V. 1982. "The self concept," *Annual Review of Sociology* (8:), pp. 1-33.
Gefen, D., Karahanna, E., & Straub, D. W. 2003. "Trust and TAM in online shopping: An integrated model," *MIS quarterly* (27:1), pp. 51-90.
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 *the Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies: short papers*, Association for Computational Linguistics, pp. 42-47.
E. Goffman, 1959. *The presentation of self in everyday life*, Doubleday: Garden City, N.Y.
Gourieroux, C., A. Monfort, and A. Trognon, 1984. "Pseudo Maximum Likelihood Methods: Theory," *Econometrica* (52:), pp. 681-700.
Granovetter, M. 1983. "The strength of weak ties: A network theory revisited," *Sociological theory* (1:1), pp. 201-233.
Granovetter, M. S. 1973. "The strength of weak ties," *American Journal of Sociology* (78:6), pp. 1360-1380.
Greene, J. A., Choudhry, N. K., Kilabuk, E., and Shrank, W. H. 2011. "Online social networking by patients with diabetes: a qualitative evaluation of communication with Facebook," *Journal of general internal medicine* (26:3), pp. 287-292.
Greenhow, C., and Robelia, B. 2009. "Informal learning and identity formation in online social networks," *Learning, Media and Technology* (34:2), pp. 119-140.
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.
Gregory, R., and Keeney, R. L. 1994. "Creating policy alternatives using stakeholder values," *Management Science* (40:8), pp. 1035-1048.

Gross, R., and Acquisti, A. 2005. “Information revelation and privacy in online social networks,” in *the Proceedings of the 2005 ACM workshop on Privacy in the electronic society,* ACM, pp. 71-80.
Guba, E. G. 1990. “The alternative paradigm dialog” in *The Paradigm Dialog*, E. G. Guba (ed.), Sage: Newbury Park, CA, pp. 17–30.
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.
Harmon, Amy. 2004. Amazon glitch unmasks war of reviewers, New York Times.
Harris, R. B., and Paradice, D. 2007. “An investigation of the computer-mediated communication of emotions,” *Journal of Applied Sciences Research* (3:12), pp. 2081-2090.
Hearit, K.M. 2006. Crisis Management by Apology: Corporate Response to Allegations of Wrongdoing, Lawrence Erlbaum Associates: Mahwah, NJ.
Hechter, M. 1993. "Values research in the social and behavioral sciences," in *The origin of values,* M. Hechter, L. Nadel, and R. E. Michod (eds.), Aldine: New York, pp. 1-28
Helliwell, J. F., and Putnam, R. D. 2004. “The social context of well-being,” *Philosophical Transactions of the Royal Society* (359:1449), pp. 1435-1446.
Herr, P. M., Kardes, F. R., and Kim, J. 1991. “Effects of word-of-mouth and product-attribute information on persuasion: An accessibility-diagnosticity perspective,” *Journal of consumer research*, pp. 454-462.
Hewitt, J. P. 1997. Self and Society: A Symbolic Interactionist Social Psychology, Allyn & Bacon: Boston, MA.
Higgins, M.C. and Kram, K.E. 2001. “Reconceptualizing mentoring at work: a developmental network perspective,” *Academy of Management Review* (26:2), pp. 264-88.
Hitlin, S. 2003. “Values as the core of personal identity: Drawing links between the two theories of self,” *Social Psychology Quarterly* (66:), pp. 118–137.
Hogan, B. 2010. “The presentation of self in the age of social media: Distinguishing performances and exhibitions online,” *Bulletin of Science, Technology & Society*, 0270467610385893.
Hogan, R., and Cheek, J. M. 1983. “Identity, authenticity, and maturity,” in *Studies in social identity*, pp. 339-357, Praeger: New York.
Holbrook, M. B. 1986. “Aims, concepts, and methods for the representation of individual differences in esthetic responses to design features,” *Journal of Consumer Research*, pp. 337-347.
Horley, J. 2012. "Personal Construct Theory and Human Values," *Journal of Human Values* (18:2), pp. 161-171.
Hormuth, S. E. 1990. *The ecology of the self: Relocation and self-concept change,* Cambridge University Press: Cambridge, England.
Hornik, K., and Grün, B. 2011. “topicmodels: An R package for fitting topic models,” *Journal of Statistical Software* (40:13), pp. 1-30.
Househ, M. 2015. “Communicating Ebola through social media and electronic news media outlets: A cross-sectional study,” *Health informatics journal*, 1460458214568037.
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.

Hsu, M-H. and Kuo, F-Y. 2003. "An investigation of volitional control in information ethics," *Behavior and Information Technology* (22:), pp. 53–62.
Huffaker, D. 2010. "Dimensions of Leadership and Social Influence in Online Communities," *Human Communication Research* (36:4), pp. 593-617.
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.
Jonczy, J., Haenni, R. 2005. "Credential networks: a general model for distributed trust and authenticity management," in *the Annual Conference on Privacy, Security and Trust*, PST'05: 3rd, Ghorbani, A., Marsh, S., eds., St. Andrews, Canada, pp. 101–112
Juan Juan, H. A. N., Zheng, R. J., and Yunjie, X. U. 2007. "The effect of individual needs, trust and identification in explaining participation intentions in virtual communities," in *Hawaii international conference on system sciences (HICSS '07),* Big Island: AIS.
Kart, L., Linden, A., and Schulte, W. R. 2013. *Extend Your Portfolio of Analytics Capabilities*, Gartner Group, Stamford, CT.
Keen, P. G., and Morton, M. S. S. 1978. *Decision support systems: an organizational perspective* (35:), Addison-Wesley: Reading, MA, pp. 19-30
Keeney, R. L. 1992. *Value-focused thinking*, Harvard University Press: Cambridge, Massachusetts.
Keeney, R. L., and Raiffa, H. 1993. Decisions with multiple objectives: preferences and value trade-offs. Cambridge university press.
Keh, H. T., and Xie, Y. 2009. "Corporate reputation and customer behavioral intentions: The roles of trust, identification and commitment," *Industrial Marketing Management* (38:7), pp. 732-742.
Kietzmann, J. H., Hermkens, K., McCarthy, I. P., and Silvestre, B. S. 2011. "Social media? Get serious! Understanding the functional building blocks of social media," *Business horizons* (54:3), pp. 241-251.
Kim, H. W., Chan, H. C., and Kankanhalli, A. 2012. "What motivates people to purchase digital items on virtual community websites? The desire for online self-presentation," *Information systems research* (23:4), pp. 1232-1245.
Kim, W.C. and Mauborgne, R. 1997. "Fair process: managing in the knowledge economy," *Harvard Business Review* (75:4), pp. 65-75.
Kirkwood, C. W. 1997. Strategic decision making: Multiobjective decision analysis with spread-*Sheets,* Duxbury: Belmont, CA.
Kowalski, R. M., and Limber, S. P. 2007. "Electronic bullying among middle school students," *Journal of adolescent health* (41:6), pp. 22-30.
Kreiner, G. E., Hollensbe, E. C., and Sheep, M. L. 2006. "Where is the "me" among the "we"? Identity search for optimal balance," *Academy of Management Journal* (49:), pp. 1031–1057.
Kuhn, T. S. 1996. *The structure of scientific revolutions*, University of Chicago press.
Kurland, N. B. 1995. "Ethical intentions and the theories of reasoned action and planned behavior," *Journal of Applied Social Psychology* (25:), pp. 297–313.

Laczniak, R. N., DeCarlo, T. E., and Ramaswami, S. N. 2001. "Consumers' responses to negative word-of-mouth communication: An attribution theory perspective," *Journal of Consumer Psychology* (11:1), pp. 57-73.
Lai, F., Li, D., and Hsieh, C. T. 2012. "Fighting identity theft: The coping perspective," *Decision Support Systems* (52:2), pp. 353-363.
Lange, D., Lee, P. M., and Dai, Y. 2011. "Organizational reputation: A review," *Journal of Management* (37:1), pp. 153-184.
LaValle, S., Lesser, E., Shockley, R., Hopkins, M. S., and Kruschwitz, N. 2013. "Big data, analytics and the path from insights to value," *MIT Sloan Management Review* (21*)*.
Leary, Mark R., and Robin M. Kowalski. "Impression management: A literature review and two-component model," *Psychological bulletin* 107.1 (1990): 34.
Le Bon, G. 1895-1903. *The Crowd: A Study of the Popular Mind*, T. Fisher Unwin: London.
Lee, C. S., and Ma, L. 2012. "News sharing in social media: The effect of gratifications and prior experience," *Computers in Human Behavior* (28:2), pp. 331-339.
Lee, A. S. 1989. "A scientific methodology for MIS case studies," *MIS Quarterly*, pp. 33-50.
Leidner, D. E., and Kayworth, T. 2006. "Review: a review of culture in information systems research: toward a theory of information technology culture conflict," *MIS quarterly* (30:2), pp. 357-399.
Leskovec, J., Adamic, L. A., and Huberman, B. A. 2007. "The dynamics of viral marketing," *ACM Transactions on the Web (TWEB)* (1:1), pp. 5.
Levin, A. 2013. "12.6 Million Reasons Why Identity Theft Matters," (available at http://www.huffingtonpost.com/adam-levin/126-million-reasons-why-i_b_2788870.html).
Lievens, E. 2012. Bullying and sexting in social networks from a legal perspective: Between enforcement and empowerment, Katholieke Universiteit: Leuven,
Light, B., and McGarth, K. 2010. "Ethics and social networking sites: a disclosive analysis of Facebook," *Information Technology & People* (23:4), pp 290-311.
Lindzey, G. and Aronson, E. (eds.) (1985). Handbook of Social Psychology: Group Psychology and the Phenomena of Interaction (3rd Ed.), Random House: New York.
Liu, B. 2012. "Sentiment analysis and opinion mining," *Synthesis Lectures on Human Language Technologies* (5:1), pp. 1-167.
Livingstone, S., and Görzig, A. 2014. "When adolescents receive sexual messages on the internet: Explaining experiences of risk and harm," *Computers in Human Behavior* (33:), pp. 8-15.
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.
Lyon, D. 2009. Identifying Citizens: ID Cards as Surveillance, Polity: Cambridge.
Maass, A., Cadinu, M., Guarnieri, G., and Grasselli, A. 2003. "Sexual harassment under social identity threat: The computer harassment paradigm," *Journal of Personality and Social Psychology* (85:), pp. 853–870.
Madge, C., and O'Connor, H. 2005. "Mothers in the making? Exploring liminality in cyber/space," *Transactions of the Institute of British Geographers* (30:1), pp. 83-97.
Major, B., and O'Brien, L. T. 2005. "The social psychology of stigma," *Annu. Rev. Psychol.* (56*:)*, pp. 393-421.
Manning, C. D. 1999. Foundations of statistical natural language processing, H. Schütze (Ed.), MIT press.

Mashima, D., and Ahamad, M. 2008. "Towards a user-centric identity-usage monitoring system," in *The Third International Conference on Internet Monitoring and Protection, ICIMP'08,* IEEE, pp. 47-52.
Marsden, P. 1998. "Memetics and social contagion: Two sides of the same coin," *Journal of Memetics-Evolutionary Models of Information Transmission* (2:2), pp. 171-185.
McCraken, G. D. 1988. *The long interview*, Sage: Newbury Park, CA.
McDougall, W. 1920. *The Group Mind*, Knickerbocker Press: New York.
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.
McQuail, D. 1991. Mass communication theory: An introduction, Sage: Barcelona.
Mead, George H. 1934. *Mind, Self and Society,* University of Chicago Press: Chicago.
Merrick, J. R., Parnell, G. S., Barnett, J., and Garcia, M. 2005. "A multiple-objective decision analysis of stakeholder values to identify watershed improvement needs," *Decision Analysis* (2:1), pp. 44-57.
Merrick, J. R. W. and M. Garcia 2004. "A value focused thinking approach to watershed improvement," *Journal of the American Planning Association* (70:3), pp. 313–328.
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).
Milne, G. R., Rohm, A. J., and Bahl, S. 2004. "Consumers' protection of online privacy and identity," *Journal of Consumer Affairs* (38:2), pp. 217-232.
Mimno, D. and McCallum, A. 2007. "Mining a digital library for influential authors," in *the 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 *the Proceedings of the 24th international conference on Machine learning,* ACM, pp. 633-640.
Mishra, A. N., Anderson, C., Angst, C. M., and Agarwal, R. 2012. "Electronic health records assimilation and physician identity evolution: An identity theory perspective," *Information Systems Research*, (23:3-part-1), pp. 738-760.
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), pp. 215-241.
Mizerski, R. W. 1982. "An attribution explanation of the disproportionate influence of unfavorable information," *Journal of Consumer Research*, pp. 301-310.
Morrissey, B. 2007. "Social media sites replacing microsites in marketing mix," *Brandweek* (5:), pp. 41-48.
Muralidharan, S., Rasmussen, L., Patterson, D., and Shin, J. H. 2011. "Hope for Haiti: An analysis of Facebook and Twitter usage during the earthquake relief efforts," *Public Relations Review* (37:2), pp. 175-177.
Nagel, E. 1979. *The Structure of Science*, Hackett: Indianapolis, IN.
Neimeyer, R., Prigerson, H., and Davis, B. 2002. "Mourning and meaning," *American Behavioral Scientist* (46:), pp. 235-251.
Newman, G. R., and McNally, M. M. 2005. "Identity theft literature review," *US Department of Justice*.

Newman, K. S. 1988. *Falling from grace,* University of California Press: Berkeley and Los Angeles.
Nooteboom, B. 2006. "Innovation, learning and cluster dynamics," *Clusters and Regional Development*, pp. 137-163.
Orlikowski, Wanda J., and C. Suzanne Iacono. 2001. "Research commentary: Desperately seeking the "IT" in IT research—A call to theorizing the IT artifact," *Information systems research* (12:2), pp. 121-134.
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 *the HLT-NAACL*, pp. 380-390.
Oyeyemi, S. O., Gabarron, E., and Wynn, R. 2014. "Ebola, Twitter, and misinformation: a dangerous combination?," *BMJ* (349*)*, pp. 6178.
Palmer, A., and Koenig-Lewis, N. 2009. "An experiential, social network-based approach to direct marketing," *Direct Marketing: An International Journal* (3:3), pp. 162-176.
Pang, B., and Lee, L. 2008. "Opinion mining and sentiment analysis," *Foundations and trends in information retrieval* (2:1-2), pp. 1-135.
Parnell, G. S. 2007. "Value-focused thinking using multiple objective decision analysis: *Methods for conducting military operational analysis: Best practices in use throughout the Department of Defense*," Military Operations Research Society: Alexandria, VA, pp. 619-656.
Parnell, G., H. Conley, J. Jackson, L. Lehmkuhl, and J. Andrew (1998). "Foundations 2025: A framework for evaluating future air and space forces," *Management Science* (44:10), pp. 1336–1350.
Parsons, Talcott. 1937. *The Structure of Social Action*, McGraw Hill.
Pavlou, P. A. 2011. "State of the information privacy literature: where are we now and where should we go," *Mis Quarterly* (35:4), pp. 977-988.
Pavlou, P. A., and Gefen, D. 2004. "Building effective online marketplaces with institution-based trust," *Information Systems Research* (*15*:1), pp. 37-59.
Paxton, P. 1999. "Is social capital declining in the United States? A multiple indicator assessment," *American Journal of Sociology* (105:1), pp. 88–127.
Pearson, E. 2009. "All the World Wide Web's a stage: The performance of identity in online social networks," *First Monday*, (14:3).
Petriglieri, J. L. 2011. "Under threat: responses to and the consequences of threats to individuals' identities," *Academy of Management Review* (*36*:4), pp. 641-662.
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.
Pinsker, B. 2014. *"Consumers vent frustration and anger at Target data breach,"* (available at http://www.reuters.com/article/2014/01/14/us-target-consumers-idUSBREA0D01Z20140114).
Portes, A. 1998. "Social capital: Its origins and applications in modern sociology," *Annual review of sociology* (*24*:1), pp. 1-24.
Raiffa, H. 1982. *The art and science of negotiation*, Harvard University Press: Cambridge, MA.
Ramagopalan, S., Wasiak, R., and Cox, A. P. 2014. "Using Twitter to investigate opinions about multiple sclerosis treatments: a descriptive, exploratory study," *F1000Research*, *3*.

Ren, Y., Harper, F. M., Drenner, S., Terveen, L. G., Kiesler, S. B., Riedl, J., and Kraut, R. E. 2012. "Building Member Attachment in Online Communities: Applying Theories of Group Identity and Interpersonal Bonds," *Mis Quarterly* (36:3), pp. 841-864.
Reynolds, G. 2007. An army of Davids: How markets and technology empower ordinary people to beat big media, big government, and other Goliaths, Thomas Nelson Inc.
Richins, M. L. 1984. "Word-of-Mouth Communication as Negative Information," in *Advances in Consumer Research*, T. Kinnear (ed.), Association for consumer Research, Provo, UT, pp. 697-702.
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.
Riordan, M. A., and Kreuz, R. J. 2010. "Emotion encoding and interpretation in computer-mediated communication: Reasons for use," *Computers in human behavior* (26:6), pp. 1667-1673.
Roberts, L. M. 2005. "Changing faces: Professional image construction in diverse organizational settings," *Academy of Management Review* (30:4), pp. 685-711.
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.
Robertshaw, G.S., and Marr, N.E. 2006. "The implications of incomplete and spurious personal information disclosures for direct marketing practice," *J. Database Mark. Cust. Strategy Manag*., (13:3), pp. 186–197.
Roßnagel, H., Zibuschka, J., Hinz, O., and Muntermann, J. 2014. "Users' willingness to pay for web identity management systems," *European Journal of Information Systems* (23:1), pp. 36-50.
Rokeach, M. 1979. "The two-value model of political ideology and British politics," *British Journal of Social and Clinical Psychology* (18:2), pp. 169-172.
Rokeach, M. 1973. *The nature of human values*, Free Press: New York.
Rothbard, N. P. 2001. "Enriching or depleting? The dynamics of engagement in work and family roles," *Administrative Science Quarterly (*46:), pp. 655–684.
Ruble, D. 1994. "A phase model of transitions: Cognitive and motivational consequences," in *the Advances in social psychology,* M. Zanna (ed.), Academic Press: San Diego, CA, pp. 163-214.
Satish, S., and Hernacki, B. 2014. *U.S. Patent No. 8,868,719*, U.S. Patent and Trademark Office: Washington, DC.
Schein, E. H. 1985a. "How Culture Forms, Develops and Changes," in *Gaining Control of the Corporate Culture*, R. H. Kilmann, M. J. et al. (eds.), Jossey-Bass, San Francisco, pp. 17-43.
Schein, E. H. 1985b. *Organizational Culture and Leadership*, Jossey-Bass: San Francisco, CA.
Schneider, D. J. 1981. "Tactical self-presentations: Toward a broader conception," in *Impression management theory and social psychological research,* J. T. Tedeschi (ed.), Academic: New York, pp. 23-40.
Schultze, U. 2014. "Performing embodied identity in virtual worlds," *European Journal of Information Systems* (23:1), pp. 84-95.
Schultze, U. and Orlikowski, W. 2010. "Virtual worlds: a performative perspective on globally-distributed, immersive work," *Information Systems Research* (21:4), pp. 810–821.

Schwartz, S. H. 1994. "Are there universal aspects in the structure and contents of human values?," *Journal of social issues* (50:4), pp. 19-45.
Schwartz, S. H. 1992. "Universals in the content and structure of values: Theoretical advances and empirical tests in 20 countries," *Advances in experimental social psychology* (25:1), pp. 1-65.
Seeger, M. W., Sellnow, T. L., and Ulmer, R. R. 2003. *Communication and organizational crisis*, Greenwood Publishing Group.
Serfaty, V. 2003. "Me, myself and I: online embodied identity in America," *Research and North American English (RANAM)* (*3*:), pp. 35-47.
Seltsikas, P., and O'Keefe, R. M. 2010. "Expectations and outcomes in electronic identity management: the role of trust and public value," *European Journal of Information Systems* (19:1), pp. 93-103.
Sheffi, Y. 2005. The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage, MIT Press: Boston, MA.
Silverman, G. 2011. Secrets of Word-of-Mouth Marketing: How to trigger exponential sales through runaway word of mouth, American Marketing Association: New York.
Smith, H.J.; Dinev, T.; and Xu, H. 2011. "Information privacy research: An interdisciplinary review," *MIS Quarterly* (35:4), pp. 989-1016.
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.
Siponen, M. T. 2001. "An analysis of the recent IS security development approaches: descriptive and prescriptive implications," *Information Security Management-Global Challenges in the Next Millennium*, Idea Group, pp. 101-124.
Siponen, M. T. 2000. "A conceptual foundation for organizational information security awareness," *Information Management & Computer Security* (8:1), pp. 31-41.
Sykes, G. M., and Matza, D. 1957. "Techniques of neutralization: A theory of delinquency," *American Sociological Review* (22:), pp. 664–670.
Sober, E., and Wilson, D. S. (eds.). 1999. *Unto others: The evolution and psychology of unselfish behavior*, Harvard University Press.
Solms, V. B., and Solms, V. R. 2004. "The 10 deadly sins of information security management," *Computers & Security* (23:5), pp. 371-376.
Son, J. Y., and Kim, S. S. 2008. "Internet users' information privacy-protective responses: A taxonomy and a nomological model," *Mis Quarterly*, pp. 503-529.
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.
Stieglitz, S., and Dang-Xuan, L. 2013. "Emotions and information diffusion in social media-Sentiment of microblogs and sharing behavior," *Journal of Management Information Systems* (29:4), pp. 217-248.
Strauss, A., and Corbin, J. M. 1998. Basics of Qualitative Research: Grounded Theory Procedures and Techniques, A: Sage, Newbury Park.
Stryker, S., and Burke, P. J. 2000. "The past, present, and future of an identity theory," *Social psychology quarterly*, pp. 284-297.
Stryker, S. 1987. "Identity theory: developments and extensions," in *Self and identity: perspectives across the lifespan,* pp. 89-104.

Suh, B., Hong, L., Pirolli, P., and Chi, E. 2010. "Want to be retweeted? Large scale analytics on factors impacting retweet in Twitter network," in *the Proceedings of the 2nd IEEE International Conference on Social Computing*, A. Pentland (ed.), Los Alamitos, CA: IEEE Computer Society, pp. 177-184.

Sullins, E.S. 1991. "Emotional contagion revisited: Effects of social comparison and expressive style on mood convergence," Personality and Social Psychology Bulletin (17:), pp. 166-174.

Sutherland, S. (ed.) 1995. *Macmillan Dictionary of Psychology*, Macmillan Press: London.

Swann, W.B. Jr. 1987. "Identity negotiation: where two roads meet," *Journal of Personality and Social Psychology* (53:6), pp. 1038-51.

Tajfel, H. C., and Turner, J. C. 1985. "The social identity theory of intergroup behavior," in *Psychology of intergroup relations,* S. Worchel and W. G. Austin (eds.), (2:), Chicago: Nelson-Hall, pp. 7-24.

Tajfel, H. 1978. *The social psychology of minorities,* Minority Rights Group International: London.

Tan, F. B., and Hunter, M. G. 2002. "The Repertory Grid Technique: A method for the study of cognition in information systems," *MIS Quarterly* (26:1), pp. 39-57.

Tarde, G. 1903- 1963. *The Laws of Imitation*, Mass: Peter Smith.

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.

Torkzadeh, G., and Dhillon, G. 2002. "Measuring factors that influence the success of Internet commerce," *Information Systems Research* (13:2), pp. 187-204.

Tsai, H. T., and Bagozzi, R. P. 2014. "Contribution behavior in virtual communities: cognitive, emotional and social influences," *MIS Quarterly* (38:1), pp. 143-163.

Tucker, L., and Melewar, T. C. 2005. "Corporate reputation and crisis management: The threat and manageability of anti-corporatism," *Corporate reputation review* (7:4), pp. 377-387.

Turner, J. C. 1982. "Towards a cognitive redefinition of the social group," *Social identity and intergroup relations*, pp. 15-40.

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. "Leveraging unstructured information using topic modeling," in *the International Conference on Management of Engineering & Technology,* Portland PICMET*,* IEEE, pp. 955-961.

Veerapen, M. 2011 "Encountering oneself and other: a case study of identity formation in second life," in *Reinventing Ourselves: Contemporary Concepts of Identity in Virtual Worlds*, Peachey, A. and Childs, M., (eds), Springer, London, pp. 81–100.

Veil, S. R., Buehner, T., and Palenchar, M. J. 2011. "A Work-In-Process Literature Review: Incorporating Social Media in Risk and Crisis Communication," *Journal of contingencies and crisis management* (19:2), pp. 110-122.

Venkatesh, V., Brown, S. A., and Bala, H. 2013. "Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems," *Mis Quarterly* (37:1), pp. 21-54.

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.

Walther, J. B., and D'Addario, K. P. 2001. "The impacts of emoticons on message interpretation in computer-mediated communication," *Social science computer review* (*19*:3), pp. 324-347.
Wartick, S. 1992. "The relationship between intense media exposure and change in corporate reputation," *Business & Society* (31:), pp. 33–49.
Wasko, M. M., and Faraj, S. 2005. "Why should I share? Examining social capital and knowledge contribution in electronic networks of practice," *MIS quarterly*, pp. 35-57
Waters, R. D., Burnett, E., Lamm, A., and Lucas, J. 2009. "Engaging stakeholders through social networking: How nonprofit organizations are using Facebook," *Public Relations Review*, (*35*:2), pp. 102-106.
Weiner, B. 1986. An Attributional Theory of Motivation and Emotion, Springer Verlag: New York.
Weng, J., Lim, E. P., Jiang, J., and He, Q. 2010. "Twitterrank: finding topic-sensitive influential twitterers," in *the Proceedings of the third ACM international conference on Web search and data mining*, ACM, pp. 261-270.
Whetten, D. A. 2006. "Albert and Whetten revisited: Strengthening the concept of organizational identity," *Journal of Management Inquiry* (15:3), pp. 219-234.
White, M. D., and Fisher, C. 2008. "Assessing Our Knowledge of Identity Theft The Challenges to Effective Prevention and Control Efforts," *Criminal Justice Policy Review* (19:1), pp. 3-24.
Whitley, E. A., Gal, U., and Kjaergaard, A. 2014. "Who do you think you are? A review of the complex interplay between information systems, identification and identity," *European Journal of Information Systems* (23:1), pp. 17-35.
Willard, N. E. 2007. Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress, Research Press.
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.
Yang, J., and Counts, S. 2010. "Predicting the speed, scale, and range of information diffusion in Twitter," in *the Proceedings of the Fourth International AAAI Conference on Weblogs and Social Media*, W. Cohen and S. Gosling (eds.), AAAI Press: Palo Alto, CA, pp. 355–358.
Zafar, H., and Clark, J. G. 2009. "Current state of information security research in IS," *Communications of the Association for Information Systems* (24:1).
Zhang, C., Sun, J., Zhu, X., and Fang, Y. 2010. "Privacy and security for online social networks: challenges and opportunities," *Network, IEEE* (24:4), pp. 13-18.
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 *the Advances in Information Retrieval*, Springer Berlin Heidelberg, pp. 338-349.
Zhao, S., Grasmuck, S., and Martin, J. 2008. "Identity construction on Facebook: Digital empowerment in anchored relationships," *Computers in human behavior* (24:5), pp. 1816-1836.
Zhu, D., Li, X. B., and Wu, S. 2009. "Identity disclosure protection: A data reconstruction approach for privacy-preserving data mining," *Decision Support Systems* (48:1), pp. 133-140.
Zywica, J., and Danowski, J. 2008. "The faces of Facebookers: Investigating social enhancement and social compensation hypotheses; predicting Facebook™ and offline popularity from sociability and self-esteem, and mapping the meanings of popularity with semantic networks," *Journal of Computer-Mediated Communication* (14:1), pp. 1-34.

Vita

Romilla Syed was born in India. She received Masters of Science in Information Systems in 2011 from Virginia Commonwealth University, USA. Before graduate school, she worked for six years in Information Technology Services Industry for various clients spanning across India, UK, and USA. Her research interests include cybersecurity, data analytics, and social networks. Her work has been published and presented in various journals and conferences including *Decision Support Systems*, *International Conference on Information Systems*, *International Federation for Information Processing*, among others.