Analysis of Data Breach Induced Trauma: An Exploratory Study

Steven "Doc" Simon
Robert Perkins
Mercer University, Atlanta, GA
Simon_sj@mercer.edu

Abstract

Data breaches - security incidents - have become an everyday occurrence with hundreds of millions of consumers having their lost personal identification information (PII), had their credit and debit card numbers stolen, and their credit compromised. Despite the risk, consumers continuously swipe their cards and share their personal information regularly. This study examines the impacts of trust and distrust on consumer intentions in this environment. More than 1000 consumers involved in technology-driven transactions comprise the data sample. Trust, distrust, and their antecedents are investigated to determine if the trauma induced by data breaches on consumers has an impact on the levels of trust and distrust and consumer behaviors.

Key words: Trust, distrust, trauma, consumer behavior, consumer intentions, security, data breach, hacks

INTRODUCTION

In 2014, a total of 79,790 cyber security incidents *were reported* in 61 countries (Verizon 2015). In the United States 43% of companies *reported* a data breach. An estimated $93 Billion was stolen from U.S. consumers between 2000 and 2014 (Javelin Strategy & Research 2015). The widely publicized system breach at Home Depot exposed over 56 million customer records. Anthem's security lapse cost 80 million of its consumers and employees their personal information with similar losses at Ebay (145 million), JPMorgan (76 million), Court Ventures (200 million), Sony (77 million), AOL (92 million), and TJ Maxx (94 million). These attacks are not restricted to business as illustrated with the US government's Office of Personnel Management's (OPM) breach placing the security clearance and background information of over 22 million individuals at risk and the US military's loss of 70 million veteran's records. This phenomenon is not exclusive to any one country, continent, socio-economic class, or ethnic group. In South Korea, nearly 20 million people, almost 40% of the population had their personal data stolen and their credit cards compromised (Thornhill 2014). The magnitude of this crisis can be measured in media coverage. 'Data breach' has become a term of everyday vernacular with *The New York Times* publishing more than 700 related articles in 2014, a 560% increase over 2013 (Verizon 2015). Despite the litany of successful cyber-attacks and media coverage, individuals are continuously swiping their credit and debit cards, engaging in e-commerce transactions (many on unsecured connections), and providing a wealth of personal information to business, government, doctors, insurers, and almost anyone who asks for it. This extraordinary behavior in light of the obvious lack of security has prompted the authors to investigate trauma induced, technology-driven consumer behavior and transaction[1] intention as it relates to trust and distrust and their antecedents.

Interestingly, of the 70 million individuals impacted by the 2013 Target breach only 35% indicated that their trust and behavior towards Target had changed (Bizrate Insights 2014). Trust is a widely researched construct that has been linked to all economic transactions and interpersonal exchanges (Mayer et al 1995, Gambetta 1998, Gefen 2004, Alga 2014). In a related technology-driven area, the role of trust in e-commerce is highly correlated with consumer intentions and purchase behavior (Kim et al 2004, Pavlou and Gefen 2005, Wu and Tsang 2008). Less understood and researched is distrust – the unwillingness to be vulnerable to others (Benamati et al 2010). Some researchers believe that distrust is a distinct construct from trust and not just ends of the same continuum (Lewicki et al 1998).

This exploratory study investigates the behavior of individuals as a result of the trauma induced by data breaches (hacks). The study reviews the literature associated with trauma and behavior change. Next, we develop an understanding of trust, distrust, and their antecedents. The literature review is followed by an explanation of the methodology of the research, explaining

[1] For the purposes of this work, transactions refer to any monetary exchange or the providing of any personal identification information (PII) to include credit or debit card numbers, social security numbers, medical information, etc.

sample, participants, and data analysis. To conclude this study, the findings are reviewed with a discussion closing the paper.

TRAUMA AND BEHAVIOR CHANGE

When an event, or series of events, causes a lot of stress, it is called a traumatic event. A person's response to a traumatic event may vary. Physical and behavioral responses include feelings of fear, grief, depression, dizziness, and changes in appetite and sleep pattern as well as modification of normal activities (CDC 2015). Trauma includes responses to powerful one-time incidents like accidents, natural disasters, crimes, surgeries, deaths, and other violent events. It also includes responses to chronic or repetitive experiences such as child abuse, neglect, combat, urban violence, concentration camps, battering relationships, and enduring deprivation. This definition intentionally does not determine whether a particular event is traumatic; that is up to each survivor. This definition provides a guideline for the understanding of a survivor's experience of the events and conditions of his/her life. There are two components to a traumatic experience: the objective and the subjective (Allen 1999):

"It is the subjective experience of the objective events that constitutes the trauma - the more you believe you are endangered, the more traumatized you will be. Psychologically, the bottom line of trauma is overwhelming emotion and a feeling of utter helplessness. There may or may not be bodily injury, but psychological trauma is coupled with physiological upheaval that plays a leading role in the long-range effects" (Allen 1999, p.14). In other words, trauma is defined by the *experience of the survivor*. Trauma comes in many forms, and there are vast differences among people who experience trauma. But the similarities and patterns of response cut across the variety of stressors and victims, so it is very useful to think broadly about trauma.

Trauma - extremely negative life-changing events – has been studied for many years and across a variety of disciplines. While the circumstances that induced the trauma vary, the common finding throughout the research is that those affected by trauma have aspects of their behavior modified. This behavior change manifests itself in things as simple as changes in daily routines to extremes such as suicidal tendencies. As indicated above, behavioral modification varies by individual and their perception of the severity of the trauma. At the most extreme end of this continuum and recently widely studied is PTSD (Post Traumatic Stress Disorder). A number of studies have demonstrated that combat veterans diagnosed with PTSD have exhibited changes (some extreme) to their behavior (Rooney et al 2007, O'Hare and Sherrer 2009, Korn and Zukerman 2011, Borders et al 2012, Brenner et al 2015). Studies have not been limited just to combat veterans but to others including children who have experienced war or terror related trauma (Mels et al 2013, Malzoon et al 2016). The mental trauma and behavioral changes experienced by individuals in the studies listed above are found to be quite similar to those

experienced by individuals experiencing physical trauma such as traumatic brain injury (TBI) (Arciniegs and Wortzel 2014, McGee et al 2016).

Trauma of course is hardly limited to war or terror-related incidents. Rzeszutek et al (2015) and Stone (1998) illustrated that Emergency Medical Technicians (EMTs) experienced similar behavioral changes as a result of their repeated exposure to traumatic events, while Zhai et al (2015) showed behavior modification in children after natural disasters such as earthquakes. Medical researchers have discovered that individuals who suffer traumatic afflictions experience changes in their beliefs, as well as social, relationship, and consumer behaviors (Chatzisarantis and Hagger 2008, Studley and Chung 2014, Ponce et al 2015, Berry et al 2015). In less dire circumstances, trauma has been shown to manifest similar – although less sever - behavioral outcomes. For instance, driver behavior – particularly reckless driving and speeding - moderates after said drivers receive tickets (Elliott et al 2007). Tourists modify their intentions to travel and/or visit specific locations based on both man-made and natural traumatic events (Wang and Ritchie 2013).

Consumer research has also contributed to this extensive cross disciplinary study. Steenkamp and Maydeu-Olivares (2015) showed that consumers change established behavior patterns as a result of traumatic external forces. Stefanska and Bilinska-Reformat (2015) found a direct impact between consumer behaviors including spending with global crises. Other studies discovered a direct link between consumer purchase intentions and exposure to negative life altering events (Pavia and Mason 2004) including terror incidents (Jebarajakirty and Lobo 2014). While Li (2015) demonstrated direct changes in purchase intentions as a result of negative events related to health and safety concerns. Recent data from the Association for Financial Professionals Risk Survey (2015) suggests that a majority (57%) of consumers in the United States stated they would either reduce or discontinue their relationship with a company that had been suffered a cyber-attack after learning of the data breach.

Although few studies have explored trauma and behavior change as it relates to data theft, the topic of identity theft has been discussed for decades (Bielski 2001). According to the US Department of Justice's Bureau of Justice Statistics (2015), well over 100 million Americans have had their personal identification information placed at risk each year with over 15 million suffering identity theft. The average identity theft incident costs the consumer $5000 and over 600 hours to correct with some cases causing irreparable damage to a consumer's credit and ruining their lives (US Department of Justice 2014). Seventy percent (70%) of those impacted report never being able to completely correct the negative impacts (Identity Theft Resource Center 2015). A 2009 Gallup poll showed that 67% of those surveyed were deeply concerned about the loss of their personal information with one in seven directly impacted. Further, over 36% of those impacted by data breaches and identity theft suffer severe emotional distress (US Department of Justice 2012).

The impact from the loss of one's personal information or identity certainly meets the classic definition of trauma. The increasing number of incidents and the growing impact on consumers not to mention the overall economic impact should be of growing concern to consumers and organizations alike. The authors posit that like others suffering trauma we expect those impacted by data breaches to modify their behavioral intentions and behavior. Specifically, we believe that those who have been directly impacted will exhibit measureable changes towards those entities involved in their levels of trust and distrust, their behaviors, and any future business or purchase intentions.

TRUST

Trust can be thought of as the glue that holds society together. It is a defining feature of most economic and social transactions in which uncertainty is present (Pavlou 2003). Trust is commonly invoked by individuals, businesses and organizations, as well as governments. Trust is mentioned in mottos, slogans, pitches, and even appears on US currency. It is a pervasive concept that has been widely studied across disciplines and yet a common definition has eluded researchers and practitioners alike.

Gambetta (1988) stated that when a trust-related topic is discussed, trust is always considered a fundamental or crucial element – one that we cannot do without in human interactions. Trust is generally crucial in business and social interactions that are characterized by dependence of one party on another. It is a common perception, that trust is one of the key and perhaps most important factors in completing a transaction and thus of economic trade (Alga 2014). In these transactions, trust – in part - binds all parties together based on the expected utility or return from the interaction (Ganesan 1998, Mayer et al 1995). Trust has been linked to consumer confidence with consumers willing to transact with organizations they trust more than those who they do not (Keen 2000). Gefen (2004) suggests that trust caters to a basic need to predict, understand, and control the social environment while attempting to determine the behavior of others and foresee the outcomes of actions.

Trust is the foundation of commerce (Su and Han 2003) and is important because it helps consumers overcome perceptions of risk (McKnight et al 2002). When conducting commerce as in all social interactions, trust is a mechanism that is employed to reduce uncertainty (Su and Han 2003) and complexity (Luhmann 1979, Gefen et al 2003). Trust in online merchants has been positively associated with their attitude towards the store and intent to conduct transactions (Macintosh and Lockshin 1997, Jarvenpaa and Tractinsky 1999, Kim et al 2004). Ba and Pavlou (2002) argue that trust refers to the subjective assessment of one party that another party will perform a particular transaction according to his or her confident expectations, in an environment characterized by uncertainty. Lack of trust has a negative consequence for consumers both online (Wu and Tsang 2008) and in the physical environments. Consumers whose trust is

deficient will not engage in financial transactions (Hoffman et al 1999). In e-commerce, a number of studies (Hoffman et al 1999, Liu et al 2005, Pavlou 2005) have shown that trust is a major barrier to acceptance and inhibits Internet transactions (Kim et al 2004).

Trust has traditionally been difficult to define (Rousseau et al 1998) and has been regarded as a "confusing pot-pourri" (Shapiro 1987). McKnight et al (2002) call for conceptual clarity and quote Keen et al (1999), " .. the basic conclusion in all these fields [is] trust is becoming more and more important, but we really cannot say what it exactly is' (pp. 4-5). The reason for this confusion (McKnight et al 2001) is that researchers have conceptualized trust within a narrow perspective in their specific field. Economists view trust from the reputation of the parties and the impact on transactions (Cave 2005). The key to successful economic transactions is avoiding opportunistic behavior (Williamson 1985). Managerial and marketing researchers focus on strategies for consumers and trust building (Fogg 2002) using trust as a mediator of the influence of a company's actions on consumer behavior (Johnson 2007). Mayer et al (1995) define trust as the "willingness of one party to be vulnerable to the actions of another based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (p 712). Human computer interaction views the relationship between the user and system usability (Riegelsberger et al 2005), while information systems researchers investigate system adoption, acceptance, and use[2]. Lee and Turban (2001) hold that trust is the willingness of a consumer to be vulnerable to the actions of an Internet merchant in an Internet shopping transaction, based on the expectation that the Internet merchant will behave in certain agreeable ways. Sociologists investigate trust from an interpersonal and group perspective (Salovery and Rothman 2003) with Rotter (1971) defining trust as a generalized expectancy held by an individual that the word of another can be relied upon. Zucker (1986) suggests that trust is a set of expectations shared by all involved in an exchange, which encompass social rules.

For purposes of this work, trust is not a behavior or a choice, but a psychological condition and can be defined as the willingness to be vulnerable under conditions of risk and interdependence (Bhattacharya 1998). McKnight et al (2002) proposed three means to measure trust – willingness to provide personal information, willingness to engage in a purchase, and willingness to act on provided information. This study focuses on willingness to provide personal information and willingness to engage in a business transaction in trusting intentions. Further McKnight et al (1998) indicate that trusting beliefs directly influence trust intentions. This relationship between trust and intentions/behaviors has been pervasive across the literature and disciplines (Macintosh and Lockshin 1997, Jarvenpaa and Tractinsky 1999, Kim et al 2004, Pavlou and Gefen 2005, Liu et al 2006, Wu and Tsang 2008, Ho and Chau 2013). The higher

[2] Several prior studies have provided a meta-analysis of the trust literature (see Gefen et al 2003, Rousseau 1998, Johnson 2007, Kim and Tadisina 2007).

the trusting beliefs, the more likely they (consumers) are to interact (Luhmann 1979). Prior research has also found that trust is a predictor of consumer behavior (Bhattacherjee 2002, McKnight et al 2002). Therefore,

Hypothesis 1: Trust will be negatively influenced as a result of personal experience with data breaches.

DISTRUST

Prior research has mainly focused on trust and largely ignored distrust, partly because of the assumption that trust and distrust are two ends of one continuum (Schoorman et al 2007, Komiak and Benbasat 2008, Benamati et al 2010, Ou and Sia 2010, Chau et al 2013, Seckler et al 2015). Early studies (Rotter 1967) viewed distrust as the opposite of high trust. This conceptualization of distrust as a single dipolar construct has been questioned (Lewicki et al 1998). They state that distrust is a distinct construct from trust and that low trust is not equivalent to high distrust with the two constructs actually coexisting. To support this assumption, they extend Luhmann (1979) and suggest that trust and distrust have different consequences and develop a model which helps explain how both trust and distrust reflect the complexities and risks associated with interpersonal and business relationships. Trust focuses on more positive emotional reactions (*hope, faith, confidence, assurance*) toward others, while distrust is based in negative overtones (*fear, skepticism, cynicism, vigilance*) (Lewiciki et al 1998, Benamati et al 2010).

Although both trust and distrust serve as mechanisms to reduce complexity and uncertainty (Kramer 1999), distrust may exert a more critical role for consumers (Ou and Sia 2010). In most people the desire to avoid a negative outcome is stronger than seeking a potentially more positive one (Moody et al 2014), suggesting that distrust should provide stronger motivations and behaviors (Chau et al 2013). Trust in the workplace has been found to foster improved working relationships and performance (Dirks and Ferrin 2001) while distrust of institutionalized roles and structures lead to greater negative consequences (Sitkin and Roth 1993).

Akin to trust, distrust simplifies an individual's decision-making process by determining which high risk or undesirable outcomes should be avoided. Trust reduces complexity by enabling individuals to take actions that expose them to risk while distrust reduces complexity, encouraging individuals to take protective actions to reduce risk (Benamati et al 2010). In other words, trust and distrust balance each other leading a decision-maker to a state of equilibrium and potential action. Trust without distrust might lead to a consumer who fails to take full account of the risks associated with a decision. In the context of this work, a consumer that freely provides personal identification information (PII) on all occasions might find their identity compromised. This is not to suggest that trust is good and distrust is bad, a simplistic view that has been pervasive in organizational and social research (Lewicki et al 1998). Distrust can be thought to represent caution before or after taking an action. A famous example is Ronald

Reagan's quote "Trust but Verify," during arms negotiations. While distrust is not explicitly mentioned it is implied and in this context not viewed as negative or bad but merely responsible and a means to reduce uncertainty which in turn led to an agreement. It has been further suggested (Benamati et al 2010) that trust and distrust need not vary simultaneously. Lewicki et al (1998) state that it is possible to like and dislike, to love and hate, and may be possible to trust and distrust. Fein (1996) suggested that when trust and distrust interact simultaneously, distrust predominates because of the disproportionate weighting of negative outcomes. In this case, one might trust a company and its products but have minimal trust in their IT support systems as a result of a data breach or failure to protect personal information.

If distrust is a distinct construct from trust, then focusing exclusively on trust may explain only part or provide a bias estimation of behavior (McKnight et al 2004, Benamati et al 2010, Ou and Sia 2010). This study therefore assumes that trust and distrust exist as separate yet related constructs allowing the authors to study the constructs independently and interdependently as they relate to intentions and behavior. We follow prior definitions of distrust, the negative expectations regarding an action, "the positive expectation of injurious action" (Luhmann 1979, p72), or "fear of, a propensity to attribute sinister intentions to, and a desire to buffer oneself from the effects of another's conduct" (Lewicki et al 1998, p 439).

Hypothesis 2: Distrust will be positively influenced as a result of personal experience with data breaches.

ANTECEDENTS TO TRUST AND DISTRUST

This section examines the primary antecedents of distrust and trust as independent and inter-related components of the trust/distrust model. While the antecedents of trust have been studied, little research has explored the antecedents of distrust (Moody et al 2014). Since trust and distrust are distinct constructs, they should have antecedents that differ (Lewicki et al 1998, Benamati et al 2010) and in one of few studies, Seckler et al (2015) showed that trust and distrust are affected by different antecedents.

The research literature features the following six antecedents: disposition to trust or distrust, situational abnormality, trustworthiness/reputation, knowledge, and environmental scanning. In addition, we have created another antecedent, defensive posture. The aim is develop a comprehensive model, thereby leading to a better understanding of how trust and distrust are developed.

Disposition to trust or distrust

"Disposition to trust is a general not situation specific, inclination to display faith in humanity and to adopt a trusting stance toward others" (Gefen 2000, p 728). Disposition to trust does not imply that others are trustworthy, only that they are more willing to depend on others (McKnight and Chervany 2001). Conlon and Mayer (1994) found the willingness to trust was significantly related to behavior and performance.

Disposition to trust has an impact on the formation of trust, especially when consumers have insufficient information or are in unfamiliar or abnormal situations (Gefen 2004, Zhou and Tian 2010). The concepts have been linked to faith in humanity and the assumptions of people and organizations in general. In contrast, disposition to distrust is also a persistent view that a person holds across situations, irrespective of the others involved (McKnight et al 2001, Zhaou and Tian 2010, Moody et al 2014). This concept implies a general unwillingness to depend on or become vulnerable to others (McKnight et al 2004).

Both dispositional trust and distrust develop over a lifetime as a result of learned outcomes from varied experiences (Rotter 1971, McKnight et al 2004, Merritt et al 2013). Furthermore, both constructs are thought to be relatively stable, although not static (Mayer et al 1995, Merritt and Ilgen 2008) and may change as individuals experience both positive and negative experiences. The degree or severity of an experience could yield a greater impact. Therefore, we expect that as with trust and distrust, disposition to trust and distrust may not vary simultaneously. A person with high disposition trust is more likely to trust others than a person with low dispositional trust, while an individual with high dispositional distrust is likely to be more distrustful. Therefore, we hypothesize that:

Hypothesis 3: Disposition to trust will be negatively influenced as a result of personal experience with data breaches.

Hypothesis 4: Disposition to distrust positively influenced as a result of personal experience with data breaches.

Reputation

Company reputation reflects the amount of regard that stakeholders, particularly customers, assign to the company (Fombrun and Rindova 2000). The literature recognizes that reputation plays a critical and primary role in building productive customer relations (Garbarino and Johnson 1999, Hennig-Thurau et al 2002, Abimbola and Vallester 2007). Fombrun (2005) noted that customers judge companies constantly, adding that reputation is widely seen as a powerful intangible corporate asset, which the leaders of well-respected companies actively measure and work to enhance. While a strong and positive reputation must be earned slowly with superior

quality and service to customers, it is generally recognized that it can be lost very quickly (Hall 1993).

Keh and Xie (2008) examined the relationship of corporate reputation to trust and purchase intent in Chinese companies. Their findings showed that reputation was very strongly related to trustworthiness and with a positive link to the customers' intent to purchase. The strength of the relationship suggests that it is a major component of overall corporate reputation. Consequently, higher levels of trust can exercise a significant and favorable impact on customer behavior.

Reputation has been categorized as a factor through which individuals build cognitive trust (McKnight et al 1998) and view an organization as trustworthy (Jarvenpaa et al 2000, Kim 2012). An established reputation has been linked to integrity and ability – an organization that is capable and insures its products and services (Mayer et al 1995, Lin et al 2006). Therefore, from the literature:

Hypothesis 5: Reputation will be negatively influenced as a result of personal experience with data breaches.

Environmental Scanning

Environmental scanning is the search or exposure to information that assists the consumer in reducing uncertainty or insures that the parties adhere to general rules and social norms (Pavlou 2002). Scanning the environment to gather information is a way to diminish uncertainty, protect the consumer, potentially reduce consumer dissonance, and improve performance (Daft et al 1988, Elenkov1997, Albarracin and Wyer 2000, Winn and Jondet 2008, Jogartnam and Wong 2009). If there is doubt or suspicion on the part of a decision maker/consumer, they become more attentive to cues that revel negative information (Schul et al 2004). Similarly, monitoring is thought to be a basic part of institutional structure (Zucker 1986). It has been viewed as a means to reduce speculation, thereby protecting parties from malicious intent (Mayer et al 1995). Given the 24-hour news cycle and the recent publicity and reporting of data breaches, individuals have easy access to information on cyber security, stolen information, and identity theft. Those stories are frequent front-page news across all media outlets. We believe that the more consumers are exposed to "bad news" the more information they will require and seek. Additionally, research has shown that individuals generally weight negative events more heavily than positive ones of comparable magnitude (Bloom and Price 1975, Slovic 1993, Connelly et al 2012). Therefore:

Hypothesis 6: Environmental scanning will be positively influenced as a result of personal experience with data breaches.

Defensive Posture

This study introduces a new construct, defensive posture, as an antecedent of trust and distrust. We view defensive posture as the steps an individual takes to protect themselves from potential harm. This construct may be either proactive or reactive in nature, depending on the individual's experiences. Proactively a consumer who has not been the victim of a data breach might review their bank and credit card accounts periodically, insuring that there has been no fraudulent activity. A consumer who has lost information during a breach might take the same action adding active behaviors – restricting the use of credit cards, reducing social media presence, or subscribing to a credit monitoring service.

Knowledge has been recognized as one of the most important cognitive factors influencing behavioral processes (Jeng & Fesenmaier 2002, Vogt & Fesenmaier 1998) and consumer behavior (Klink and Daniel 2001) and is a key component of defensive posture. Selnes and Howell (1999) found that decision-making behavior and information processing differ between customers with high and low levels of knowledge. Court et al. (2009) - in a study on decision-making patterns of 20,000 customers in five industries - concluded that the traditional model of a sales driven push tactics of company marketers was no longer accurate. A new kind of buyer had emerged, the knowledgeable customer, who behaved differently. Knowledgeable customers reached out and pulled in helpful information about the company and its products, initiating 67% of buying transactions.

Knowledge plays a central role in many theoretical models of attitude because it is hypothesized to influence behavior (Barber et al 2009). Hadar et al. (2013) investigated the impact of subjective knowledge states on financial decision-making with findings showing that when customers felt less confident in their knowledge, they were less likely to make a risky investment. With high levels of knowledge, consumers are confident in their own ability to undertake information-searching tasks (Schmidt et al 1996) with results leading to higher levels of trust, which reinforce their purchase behavior (Alba and Hutchinson 1987, Crowley and Mitchell 2003). Low knowledge holders are limited in their ability to collect and assimilate relevant information for evaluating options (Malhotra 1983) contributing to longer searches with poorer results impacting their purchase behavior.

Consumer researchers have extensively investigated the role of knowledge on behavior with issues ranging from knowledge measurement (Brucks 1985), the effects of knowledge on search (Bettman and Park 1980), product judgments (Maheswaran et al. 1996) and choice (Mitchell and Dacin 1996). Researchers have found that experts and novices differ in the amount, content, and organization of their knowledge and as a result exhibit large variances when performing some tasks. Knowledge is a multidimensional construct comprising three categories: 1) subjective knowledge – familiarity, 2) objective knowledge – expertise, and 3) product experience - possession (Bettman and Park 1980, Johnson and Russo, 1984, Brucks 1985, Sujan 1985, Alba and Hutchinson 1987, Ratchford 2001, Park and Moon 2003). Hence, subjective knowledge

equates to the familiarly with the laws and structural procedures in place to safeguard their information, objective knowledge is expertise but focused on the understanding of the nature of the technology related to information transmission and protection, while experience relates to the conduct of the transaction gained through use. This study incorporates knowledge that would protect an individual from the dangers present in technology-driven transactions.

Therefore:

> *Hypothesis 7: Defensive posture will positively influenced as a result of personal experience with data breaches.*

METHODOLOGY

The authors surveyed over 1000 consumers to understand the impacts of data breaches. The questionnaire was derived from pervious literature (see review above) with a number of questions rewritten to make them more applicable to this study's intent. The initial instrument consisted of just over a hundred (7 point scale, Likert-type) items including demographic information. The instrument was initially pilot tested with a group of approximately 250 individuals drawn from a population representing the desired sample. As a result of the pilot test, the analysis of the data, and feedback from subjects, the instrument was reduced by one half with redundant items eliminated and the wording of several questions modified. The resulting instrument was then retested and after very minor changes, a final instrument was made available. The first page of the questionnaire explained to participants the intent and objectives of the study and provided them with some contextual background for the work. It further explained that the research was for academic purposes only and that any information provided would be held in strictest confidence.

Participants

Participants were recruited into the study utilizing business and institutional contacts of the researchers and their associates. The only conditions for participation was that participants must be over the age of 18, hold a credit card that they were responsible, and have either completed a) an Internet transaction, b) used a credit card at any merchant – on-line or otherwise, or c) provided personal information to any organization (business or otherwise). While not excluding students, this study sought participants from the general population insuring more representative sample. Further, the sample was not restricted to any group or country although the majority of responses came from the United States.

The sample was composed of 384 (37%) females and 652 (63%) males with a mean age of 36.8 years (standard deviation 12.6). Participants had the following education make-up – 1.2 % no

high school degree, 6.9 % high school completion, 19.2 % some college work, 12.5 % associates degree, 39.2% bachelor degree, and 21% graduate degree. The questionnaire also collected income demographics with 43.9% having income of less than $75000 per year, 38.4% between $75000 & $150000, 9.7% between $150000 & $200000, and 8.1% in excess of $200000.

Analysis

Surveys were taken and collected via a controlled access website. For this sampling, 1036 fully completed and useable surveys were obtained. Exploratory factor analysis was the first step in the analysis process. Using SAS, the data resolved a nine factor model. Eight factors described in the literature including – trust, distrust, disposition to trust, disposition to distrust, trustworthiness/reputation, defensive posture, environmental scanning, and intentions - plus an additional factor that we have termed technology trust. The resolved factors were distinct and demonstrated clear discriminant validity. The next step was to establish internal consistency of the factors themselves. Cronbach's alpha found that the internal consistency of each factor was acceptable (see Table 1).

Since this exploratory research is concerned with the impact of trauma (cyber hacks/data breaches) on consumer behavior, the sample was then parsed by those directly experiencing a hack/data breach (617/60%) and those who have not (419/40%). To insure that there was no bias introduced to the results by parsing the sample, analysis of variance based on the demographic factors listed above was conducted. The results indicated that there were no statistically significant differences between the hacked and non-hacked groups for any demographic factors. Finally, analysis of variance was run for each factor.

Results/Hypotheses Testing

The expectation at the beginning of this study was that those directly impacted by a hack or data breach would experience some degree of trauma. As a result of that trauma, we expected to observe a measurable difference in behaviors. Since it is impossible to accomplish this longitudinally in the real world, we believed that measurement of the two groups would provide a useful surrogate. The primary interest is the impact on trust and distrust since, as per the literature, they influence intentions. The results clearly suggest that there is a statistically significant difference on both constructs as a result of the trauma suffered to the hacked group. Hypothesis 1 posits that with regard to trust those who had direct personal experience with a hack/data breach would have lower levels of trust than their non-hacked counterparts. The mean for the trust construct for the non-hacked group was 4.04 and for the hacked group was 3.18 with a p-value of <.0001. With regard to Hypothesis 2 (levels of distrust will be higher for those

experiencing a hack), our findings also demonstrate a significant difference between the two groups ($p<.0001$). The mean for the hacked group was 5.07 with non-hacked at 4.37.

Our next level of interest related to the antecedents, predicted by the literature, for trust and distrust. The most logical starting point is with disposition to trust or distrust. These two constructs are rooted in an individual's persistent view (glass half full vs. half empty) plus their cumulative lifetime experiences. Hypothesis 3, similar to Hypothesis 1, suggests that we would expect those directly impacted by a hack/data breach to have lower levels of disposition to trust. The mean values for those experiencing a hack where 3.37 compared to 4.22 for the non-hacked group with a p-value of .01. While this finding is statistically significant, it is not as strong as those for trust and distrust. Hypothesis 4 examines the disposition to distrust, suggesting that those who have been hacked will have higher levels of this construct than their non-hacked counterparts. Analysis indicates a mean for the hacked group of 4.92 and 3.96 for the non-hacked (p-value <.0001).

The analysis continued, examining the other antecedents derived from the literature, starting with reputation. Per Hypothesis 5, we expect those in the hacked group's levels to be negatively influenced. The mean for the hacked group is 4.84 and 4.76 with a p-value of <.05. Hypothesis 6 (Environmental scanning) suggests an increase in the factor as a result of the trauma from being hacked. The hacked group showed a statistically significant difference (p – value <.01) between the two groups with means for those hacked of 5.57 and 5.23 for non-hacked. Two additional antecedents, not anchored in the literature, we also examined. Defensive posture, created for this study, demonstrated statistical significance ($p <.0001$) with those in the hacked group experiencing higher levels/activity (hacked 5.24/non-hacked 4.44). The unexpected factor technology (tech) trust was also analyzed although there was no formal hypothesis associated with the construct. Those in the hacked group had lower levels of tech trust (hacked 4.094/non-hacked 4.39) with statistical significance at <.01.

Finally, we examined an individual's behavioral intention. These intentions could manifest themselves in a future action to continue a relationship with a business or organization that the participant's information had been compromised as a result of a data breach/hack. These actions could include future purchase intent, future purchase intent using a credit card, or simply providing their personal information to the organization. As expected, the analysis demonstrated statistical significance at the <.0001 level with the non-hacked group showing higher future intentions (non-hacked 5.62/hacked 3.61).

Insert Table 1 – about here

DISCUSSION

The primary objective of this study was to derive an understanding of data breach/hack induced trauma on consumer behaviors and influences of those behaviors in high data theft environments. The findings of this exploratory study are not surprising and do provide some interesting insights into the phenomena of trust and distrust while deepening our understanding of the impacts of data breaches/hacks. From a research perspective our exploratory factor analysis cleanly resolved trust and distrust as distinct constructs, not two ends of the same continuum. This supports the notion (at least in this study's context) that an individual can both trust and distrust simultaneously, a decades old debate. The factor analysis further resolved unique antecedents of trust and distrust as predicted by the literature as well as providing two new antecedents.

All of the hypotheses was proven valid at statistically significant levels although some more strongly than others (see Table 1 for a full review). As expected those who had not experienced a data breach/hack had higher levels of trust and those that had had higher levels of distrust. While both are statistically significant, the magnitude of the results provides some insights. The overall levels of distrust are much stronger than those for trust. The literature suggests that negative events create much stronger 'emotions' than positive events. If we assume that data breaches/hacks actually do create trauma-like reactions in individuals, the overall higher levels of distrust would support that belief. Practitioners – retailers, businesses, organizations – should be very cognizant of this finding. If negative events (hacks) occur in an organization and their constituents are affected (yielding traumatic outcomes), the creation of distrust could have serious implications for continued business relationships.

The antecedents, disposition to trust/distrust were statistically significant in the directions expected. At the onset of the research we wondered if this would be the case as predisposition is composed in part of pervasive views of the world. It seems that the environmental component of these factors has a very strong impact. An interesting extension for behavioral researchers might be to track an individual over time – post traumatic incident – to determine the duration of these affects, with the assumption that those who are predisposed to trust would recover quicker. Similar to the finding for trust and distrust, we see the magnitude of predisposition of distrust to be stronger than for predisposition to trust. We can assume that as suggested above, the trauma of negative events weigh more heavily on individuals, another potential avenue for future study.

Reputation appears to be a more enduring construct than those examined so far. While still statistically significant, it was the weakest of the analysis. Since reputation has long been regarded as a valued corporate asset, individuals who hold an organization in high regard might be 'more forgiving' of negative events related to that organization. This could be a positive factor for organizations that are held in high esteem by their customers if they do experience a data breach/hack. One might exercise caution however, since the marketing literature suggests

that reputation can be quickly lost, so overreliance could prove dangerous. A longitudinal study of this factor and the extent of its duration could provide interesting insights. Environmental scanning, while significant, was also weaker than expected. We had assumed that those who experienced a hack/data loss would be more proactive in their behavior. Overall, levels for this construct were quite high (hacked 5.57/non 5.23). The prevalence of stories and the magnitude of data breaches have perhaps raised the awareness of all individuals. We do not find this surprising and expect this behavior to increase into the future as all individuals seek to protect themselves.

Defensive posture also provided strong differences between the groups. It comes as no surprise that those who have experienced the trauma of a data breach would take actions to protect themselves from further harm. This suggests that the market for credit monitoring and prevention/repair from identity theft should be robust in the future. Organizations might consider proactive steps to partner with consumers to prevent identity theft. This is becoming more common as banks and other business send texts to customers if usual activity takes place on their accounts. One would believe that this is viewed positively by individuals and could increase their trust in those organizations. The unexpected factor, tech trust, behaved exactly as expected. Those individuals who had experienced a breach were significantly less trusting than their non-hacked counterparts. We have no way of knowing what that level of technology trust might have been before this study and again we suggest that a longitudinal study would provide insights.

Finally, intention or the individual's future intent was statistically significant (<.0001). This finding suggests that those who have experienced the trauma of a breach would alter their future behaviors. The result supports the trauma-based literature and suggests that loss of information - including identity theft – is traumatic (to some extent) for individuals. The result has very serious implications for organizations/businesses where individuals have the option to continue a relationship or conduct purchases. Consumers could elect not to conduct business with an entity altogether or they could modify their behavior such as only using cash to make their purchases. Antidotal evidence shows that consumers do change behaviors as a result of data breaches but surprisingly also shows a number of consumers electing not to change any behavior what so ever (as with the Target hack). If the latter is the case (contrary to our findings), it might suggest that data breaches/hacks are becoming the new norm and that consumers have 'adjusted' to the potential risk. What is less clear and harder to measure is the potential impact of interactions that are not optional. There is no option for individuals to elect not provide their personal information in many cases, the OPM, IRS, and at physician offices for example. Individuals who were compromised on those occasions were offered a degree of credit monitoring (common in many situations) but given the researcher's personal experience, these remedies offer minimal assurance or protection.

Future Research

This was an exploratory study and was undertaken in part because both researchers had their information compromised during data breaches. While shedding light on a new phenomenon, the study created as many questions as it provided answers. Since this study was a snapshot in time a follow-up study of a longitudinal nature would be very interesting to understand the lasting impacts of data breach induced trauma and its implications. Additionally, this study did not measure the degree of trauma suffered by any participant, only if the participants had been directly exposed to a data breach. Clearly the magnitude of the incident would create higher levels of trauma, leading to stronger behavioral modifications. Again, since this was an exploratory study, we suggest a more in depth look at individuals in this category.

The subject material of this research is of interest to both academics and practitioners. Future studies from an academic standpoint should extend this work while attempting to understand the relationships amongst trust and distrust and their antecedents. Those relationships and their strengths, in future studies, could assist in the understanding of how changes in one factor impact a consumer's behaviors and intentions. This in turn could assist organizations in developing remedies that go beyond 'locking down' a system. Trust and distrust were historically believed to be opposite ends of the same continuum. The belief that they are distinct constructs with unique antecedents was introduced by Lewiciki et al (1989) and is still widely argued. Using a large sample of real-world participants, as opposed to students, we lay the groundwork for additional research in this area. Further, while not emphasized in this study, our sample was drawn from a global population (although predominately USA). We did not differentiate on national or cultural origin but it would be interesting to understand any cultural implications that future studies might derive. We believe that practitioners would also find insights in this and future work. If tech trust and reputation are predictors into consumer behavior than it is possible for them to take appropriate actions to improve their technology (safeguards) while enhancing their reputation.

CONCLUSION

All investigations and reports suggest that data breaches and loss of data will continue to increase and that the magnitude of the losses will expand correspondingly. This exploratory study examined the impact from the trauma of data breaches/hacks on trust, distrust, their antecedents, and intentions. Findings indicate that there is a statistically significant difference between those would have directly experienced a hack on all studied factors including future intention. The study further demonstrates that, within this context, trust and distrust are distinct constructs.

REFERENCES

___ 2015 Data Breach Investigation Report. Verizon. http://verizonenterprise.com

____ 2014 The Impact of Target's Data Breach on Consumer Trust. Bizrate Insights. May 12, 2014. http://connexity.com/blog/2014/05/the-impact-of-targets-data-breach-on-consumer-trust/

___ 2015. $16 Billion Stolen from 12.7 Million Identity Fraud Victims in 2014. Javelin Strategy & Research. https://www.javelinstrategy.com/news/1556/92/16-Billion-Stolen-from-12-7-Million-Identity-Fraud-Victims-in-2014-According-to-Javelin-Strategy-Research/d,pressRoomDetail.

Alba, J.W. and Hutchinson, J.W. 1987. Dimensions of Consumer Expertise. Journal of Consumer Research, 411–454.

Abimbola and Vallaster. 2007. Brand, Organization Identity and Reputation: SMEs as Expressive Organizations. *Qualitative Market Research: An International Journal,* 10:4, 416-430.

Albarracin, D. and Wyer, R.S. 2000. The Cognitive Impact of Past Behavior: Influences on Beliefs, Attitudes, and Future Behavioral Decisions. Journal of Personality and Social Psychology, 79:1, 5-22.

Bloom, H.S. and Price, H.D. 1975. Voter Response to Short-Run Economic Conditions: The Asymmetric Effect of Prosperity and Recession. American Political Science Review, 64:4, 1240-1254.

Ba, S. and Pavlou, P.A. 2002. Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior. MIS Quarterly, 26:3, 243-268.

Barber, N., Taylor, C., and Strick, S. 2009. Wine Consumers' Environmental Knowledge and Attitudes: Influence on Willingness to Purchase. International Journal of Wine Research, 1:1, 59–72.

Benamati, J. and Serva, M.A. 2007. Trust and Distrust in Online Banking: Their Role in Developing Countries, 13:2, 161-175.

Benamati, J., Serva, M.A., and Fuller, M.A. 2010. The Productive Tension of Trust and Distrust: The Coexistence and Relative Role of Trust and Distrust in Online Banking. Journal of Organizational Computing and Electronic Commerce, 20, 328-346.

Bettman, J.R., & Park, C.W. 1980. Effects of Prior Knowledge and Experience and Phase of the Choice Process on Consumer Decision Processes: A Protocol Analysis. *Journal of Consumer Research,* 7:3, 234-248.

Bhattacherjee, A. 2002. Individual Trust in Online Firms: Scale Development and Initial Test. Journal of Management Information Systems, 19:1, 211-241.

Brucks, M. 1985. The Effects of Product Class Knowledge on Information Search Behavior. *Journal of Consumer Research,* 12:1, 1-16.

Cave, J. 2005. The Economics of Cyber Trust Between Cyber Partners. Trust and Crime in Information Societies. (Chelteham:Edward Elgar), 380-427.

Chau, P.Y., Ho, S.Y., Ho, K.K., and Yao, Y. 2013. Examining the Effects of Malfunctioning Personalized Services on Online Users' Distrust and Behaviors, 56, 180-191.

Conlon, E.J. and Mayer, R.C. 1994. The Effect of Trust on Principal-Agent Dyads: An Empirical Investigation of Stewardship and Agency. Academy of Management Presentation, Dallas, TX.

Connelly, B.L., Miller, T, and Devers, C.E. 2012. Under A Cloud of Suspicion: Trust, Distrust, and Their Interactive Effect in Interorganizational Contracting. Strategic Management Journal, 33, 820-833.

Court, D., Elzinga, D., Mulden, S., and O. J. Vetvik.O.J. 2009 The Consumer Decision Journey. *The McKinsey Quarterly*, June.

Daft, R. L., Sormunen, J., and Parks, D. 1988. Chief Executive Scanning, Environmental Characteristics, and Company Performance: An Empirical Study. Strategic Management Journal, 9:2, 123-139.

Dirks, K.T. and Ferrin, D.L. 2001. The Role of Trust in Organizational Settings. Organizational Science, 12:4, 450-467.

Elenkov, D.S. 1997. Strategic Uncertainty and Environmental Scanning: The Case for Institutional Influences on Scanning Behavior. Strategic Management Journal, 18:4, 287-302.

Fein, S. 1996. Effects of Suspicion on Attributional Thinking and the Corresponding Bias. Journal of Personality and Social Psychology, 70, 1164-1184.

Fogg, B. 2002. Persuasive Technology: Using Computers to Change What We Think and Do.

Fombrun, C. and Rindova, V. P. 2000. The Road to transparency: Reputation Management at Royal Dutch/Shell. *The Expressive Organization*. Oxford University Press, Oxford, U.K.

Fombrun, C. 2005. The Leadership Challenge of Building Resilient Corporate Reputations. *Handbook on Responsible Leadership and Governance in Global Business*. Edward Elgar, Northampton, MA.

Gambetta, D.G. 1988. Can we Trust Trust? In Trust, 213-237. (New York: Blackwell).

Ganesan, S. 1998. Determinants of Long-Term Orientation in Buyer-Seller Relationships. Journal of Marketing, 58:2, 1-19.

Garbarino, E. and Johnson, M. S. 1999. The Different Roles of Satisfaction, Trust and Commitment in Customer Relationships. *Journal of Marketing*, 63:2, 70-87.

Gefen, D. 2000. E-Commerce: The Role of Familiarity and Trust. Omega: The International Journal of Management Science, 28, 725-737.

Gefen, D., Karahanna, E., and Straub, D.W. 2003. Trust and TAM in Online Shopping: An Integrated Model. MIS Quarterly, 27:1, 51-90.

Gefen, D. 2004. What Makes an ERP Implementation Relationship Worthwhile: Linking Trust Mechanisms and ERP Usefulness. Journal of Management Information Systems, 21:1, 263-288.

Hadar, L., Sood, S. and Fox, C. , (2013) Subjective Knowledge in Consumer Financial Decisions. *Journal of Marketing Research*, 50:3, 303-316.

Hall, R. 1993. A Framework Linking Intangible Resources and Capabilities to Sustainable Competitive Advantage. *Strategic Management Journal*, 14:8, 607- 618

Hennig-Thurau, T., Gwinnet, R. P and Gremier, D. D. 2002. Understand Relationship Marketing Outcomes: An Integration of Relational Benefits and Relationship Quality. *Journal of Science Research*, 4:3, 230- 247.

Ho, S.Y. and Chau, P.Y. 2013. The Effects of Location Personalization on Integrity Trust and Integrity Distrust in Mobile Merchants. International Journal of Electronic Commerce, 17:4, 39-71.

Hoffman, D.L., Novak, T.P., and Peralta, M. 1999. Building Consumer Trust Online. Communications of the ACM, 42:4, 80-85.

Jarvenpaa, S.L. and Tractinsky, N. 1999. Consumer Trust in an Internet Store: A Cross-Cultural Validation. Journal of Computer-Mediated Communication, 5:2.

Jarvenpaa, S.L., Tractinsky, N., and Vitale, M. 2000. Consumer Trust in an Internet Store. Information Technology and Management, 1:12, 45-71.

Jeng, J., & Fesenmaier, D.R. 2002. Conceptualizing the Travel Decision-Making Hierarchy: A Review of Recent Developments. *Tourism Analysis*, 7:1, 15-32.

Johnson, D. S. 2007. Achieving Customer Value From Electronic Channels Through Identity Commitment, and Trust in Technology. Journal of Interactive Marketing, 21:4, 2-22.

Johnson, E.J., & Russo, J.E. 1984. Product Familiarity and Learning New Information. *Journal of Consumer Research,* 11:1, 542-550.

Jogartnam, G. and Wong, K.F. 2009. Environmental Uncertainty and Scanning Behavior: An Assessment of Top-Level Hotel Executives. International Journal of Hospitality and Tourism Administration, 10, 44-67.

Keen, P.G. 2000. Ensuring e-trust. Computerworld, 34:11, 46.

Kim, E. and Tadisina, S. 2007. A Model of Customers' Trust in E-Business: Micro-Level Inter-Party Trust Formation. Journal of Computing Information Systems, 48:1, 88-104.

Kim, H.W., Xu, Y., and Koh, J. 2004. A Comparison of Online Trust Building Factors between Potential Customers and Repeat Customers. Journal of the Association for Information Systems, 5:10, 392-420.

Kim, J.B. 2012. An Empirical Study on Consumer First Purchase Intention in Online Shopping: Integrating Initial Trust and TAM. Electronic Consumer Research, 12, 125-150.

Klink, R. R. and Smith, D.C. 2001. Threats to the External Validity of Brand Extension Research. Journal of Marketing Research, 38, 326-335.

Komiak, S.Y. and Benbassat, I. 2008. A Two-Process View of Trust and Distrust Building in Recommendation Agents: A Process-Tracing Study. Journal of the Association for Information Systems, 9:12, 727-747.

Kramer, R.M. 1999. Trust and Distrust in Organizations: Emerging Perspectives, Enduring Questions. Annual Review of Psychology, 50:1, 569-598.

Lee, M.K. and Turban, E. 2001. A Trust Model for Consumer Internet Shopping. International Journal of Electronic Commerce, 6:1, 75-92.

Lewicki, R.J., McAllister, D.J, and Bies, R.J. 1998. Trust and Distrust: New Relationships and Realities. Academy of Management Review, 23:3, 438-458.

Liu, C.T., Marchewka, J., and Yu, C. 2005. Beyond concern: A privacy trust-behavioral intention model of electronic commerce. Information and Management, 42:2, 289-304.

Luhmann, N. 1979. Trust and Power, (Chichester: John Wiley and sons).

Macintosh, G. and Lockshin, L.S. 1997. Retail relationships and store loyalty: A multi-level perspective. International Journal of Research in Marketing, 14:5, 478-497.

Maheswaran D., Sternthal B., and Zeynap, G. 1996. Acquisition and Impact of Consumer Expertise. Journal of Consumer Psychology, 5:2, 115-133.

Malhotra, N.K. 1983. On Individual Differences in Search Behavior for a Nondurable. Journal of Consumer Research 10, 125–131.

Mayer, R.C., Davis, J. H., Schoorman, F. D. 1995. An Integrative Model of Organizational Trust. The Academy of Management Review, 20:3, 709-734.

McKnight. D.H., Cummings, L.L., and Chervany, N.L. 1998. Initial Trust Formation in New organizational Relationships. Academy of Management Review, 23:3, 437-490.

McKnight. D.H. and Chervany, N.L. 2001-2002. What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology. International Journal of Electronic Commerce, 6:2, 35-59.

McKnight, D.H., Choudhury, V., and Kacmar, C. 2002. Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. Information Systems Research, 13:3, 334-359.

McKnight, D.H., Kacmar, C., Choudhury, V. 2004. Dispositional Trust and Distrust Distinctions in Predicting High- and Low-Risk Internet Expert Advice Site Expectations. E-Service Journal, 35-58.

Merritt, S.M. and Ilgen, D.R. 2008. Not all Trust is Created Equal: Dispositional and History-Based Trust in Human-Automation Interactions. Human Factors, 50:2, 194-210.

Merritt, S.M., Heimbaught, H., LaChapell, J, and Lee, D. 2013. I Trust It, but I Don't Know Why: Effects of Implicit Attitudes Toward Automation on Trust in an Automated System. Human Factors, 55:3, 520-534.

Mitchell, A. A. and Dacin, P.A. 1996. The Assessment of Alternative Measures of Consumer Expertise. Journal of Consumer Research, 23 (December), 219-239.

Moody, G.D., Galletta, D.F., and Lowry, P.B. 2014. When Trust and Distrust Collide Online: The Engenderment and Role of Consumer Ambivalence in Online Consumer Behavior. Electronic Commerce Research and Applications, 13, 266-282.

Ou, C.X., and Sia, C.L. 2010. Consumer Trust and Distrust: An Issue of Website Design. International Journal of Human-Computer Studies, 68, 913-934.

Park, C.W., and Moon, B.J. 2003. The Relationship Between Product Involvement and Product Knowledge: Moderating Roles of Product Type and Product Knowledge Type. *Psychology and Marketing*, 20:11, 977-997.

Pavlou, P.A. 2003. Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. International Journal of Electronic Commerce, 7:3, 101-134.

Pavlou, P.A. and Gefen, D. 2005. Psychological Contract Violation in Online Marketplaces: Antecedents, Consequences, and Moderating Role. Information Systems Research, 16:4, 372-399.

Ratchford, B.T. 2001. The Economics of Consumer Knowledge. *The Journal of Consumer Research,* 27:4, 397-411

Riegelsberger, J., Sasse, M.A., and McCarthy, J.D. 2005. The Mechanics of Trust: A Framework for Research and Design. International Journal of Human-Computer Studies, 62:3, 381-422.

Rotter, J.B. 1971. Generalized Expectancies for Interpersonal Trust. American Psychology, 26:5, 443-452.

Rousseau, D.M., Sitkin, S.B., Burt, R.S., Camerer, C. 1998. Not so Different After All: A Cross-Discipline View of Trust. Academy of Management Review, 23:3, 393-404.

Schmidt, J.B., and Spreng, R.A. 1966. A Proposed Model of External Consumer Information Search. Journal of the Academy of Marketing Science 24, 246–256.

Schoorman, F.D., Mayer, R.C., and Davis, J.H. 2007. An Integrative Model of Organizational Trust: Past, Present, and Future. Academy of Management Review, 32:2, 344-354.

Schul, Y., Mayo, R. and Burnstein, E. 2004. Encoding Under Trust and Distrust: The Spontaneous Activation of Incongruent Cognitions. Journal of Personality and Social Psychology, 86:5, 668-679.

Seckler, M., Heinz, S., Forde, S., Tuch, A.N., Opwis, K. 2015. Trust and Distrust on the Web: User Experiences and Website Characteristics. Computers in Human Behavior, 45, 39-50.

Selnes, F. and Howell, R. 1999. The Effect of Product Expertise on Decision Making and Search for Written and Sensory Information. Advances in Consumer Research, 26:1, 80-89.

Shapiro, S.P. 1987. The Social Control of Interpersonal Trust. American Journal of Sociology, 93:3, 623-658.

Sitkin, S.B. and Roth, N. 1993. Explaining the Limited Effectiveness of Legalistic Remedies for Trust/Distrust. Organizational Science 4:3, 367-392.

Slovic, P. 1993. Perceived Risk, Trust, and Democracy. Risk Analysis, 13:6, 675-682.

Sujan, M. 1985. Consumer Knowledge: Effects on Evaluation Strategies Mediating Consumer Judgments. *Journal of Consumer Research,* 12:1, 31-46.

Thornhill, T. 2014. Nearly half of South Koreans have their bank details stolen (including the President) as anti-fraud worker arrested. Daily Mail. January 21, 2014. http://www.dailymail.co.uk/news/article-2543167/Data-100MILLION-South-Korean-

credit-cards-stolen-scam-affecting-40-population-including-President-Park-Geun-hye.html#ixzz3ge2rKCmY

Vogt, C.A., and Fesenmaier, D.R. 1998. Expanding the Functional Information Search Model. *Annals of Tourism Research, 25:*3, 551-578.

Williamson, O.E. 1985. The Economic Institutions of Capitalism. (New York: Free Press).

Winn, J. and Jondet, N. 2008. A "New Approach" to Standards and Consumer Protection. Journal of Consumer Policy, 31:4, 459-472.

Wu, J.J. and Tsang, A.S. 2008. Factors affecting members' trust belief and behavior intention in virtual communities. Behaviour & Information Technology, 27:2, 115-125.

Zhou, M. and Tian, D. 2010. An Integrated Model of Influential Antecedents of Online Shopping Initial Trust: Empirical Evidence in a Low-Trust Environment. Journal of International Consumer Marketing, 22, 147-167.

Zucker, L.G. 1986. Production of Trust: Institutional Sources of Economics Structure, 1840-1920. In Research in Organizational Behavior. (Greenwich: JAI Press).

Table 1
Recap and findings

FACTOR	HYPOTHESIS	CRONBACH'S ALPHA	STRENGTH
TRUST	*Levels of trust will be negatively influenced as a result of personal experience with data breaches.*	.98	<.0001
DISTRUST	*Distrust will be positively influenced as a result of personal experience with data breaches.*	.98	<.0001
DISPOSITION TO TRUST	*Disposition to trust will be negatively influenced as a result of personal experience with data breaches.*	.86	<.01
DISPOSITION TO DISTRUST	*Disposition to distrust positively influenced as a result of personal experience with data breaches.*	.93	<.0001
REPUTATION	*Reputation will be negatively influenced as a result of personal experience with data breaches.*	.95	<.05
ENVIRONMENTAL SCANNING	*Environmental scanning will be positively influenced as a result of personal experience with data breaches.*	.84	<.01
DEFENSIVE POSTURE	*Defensive posture will positively influenced as a result of personal experience with data breaches.*	.89	<.0001
TECHNOLOGY TRUST	No formal hypothesis: *expected to be negatively influenced by experience with data breaches.*	.92	<.01
INTENTIONS	No formal hypothesis: *expected to be negatively influenced by experience with data breaches.*	.92	<.0001