Insider Privacy Breach and Trust Restoration: Is the CEO's Gender as Important as the CEO's Response?

Completed Research Paper

Gaurav Bansal
University of Wisconsin – Green Bay
bansalg@uwgb.edu

Abstract

In this study we use Politeness Theory to understand the trust violation and restoration process. The study examines the role of CEO gender, perceived CEO status, and response type (apology vs. denial) on restored trust and trusting beliefs in the case of an insider data breach incident. The data were collected using a scenario based experiment from students studying in a Midwestern University. Data were analyzed using SEM approach with five different models. The study controlled for perceived news seriousness, website reputation and perceived design quality, user's privacy concern, trust propensity and user-gender. The results show that in the case of an insider data breach incident a CEO apology is more effective than a denial. Perceived CEO status helps in restoring trust especially in the case of denial. The study also reveals the hidden gendered biases. Male CEOs are more effective in restoring trust with denial than female CEOs are. Social, managerial and theoretical implications are discussed.

Keywords

Insider privacy breach, trust violation, CEO gender, apology, denial

Introduction

More and more females are rising to the corner offices. Today there are more women CEOs in fortune 500 companies then there ever has been in the past. The Wharton's MBA class for the first time had more than 45% female students in fall 2013. Even though there are more women CEOs now, their number is relatively small – around 4%. As more female students enter business and science fields, there is little doubt that this ratio will only rise. These ratios historically have led to several stereotypes associated with gender and leadership roles. However, there are not many studies guiding the female CEOs about these gender biases and stereotypes as they adjust their managerial and communication styles in this evolving (both socially and technically) and highly digitized business world.

Today's businesses are experiencing an increased threat of a possible data breach. Identity Theft Resource Center (2014) states that 610 data breaches were reported in 2013 which was 30% more than reported in 2012. These data breaches could be caused by external elements such as hackers, however, a significant number of them occur because of negligent or malicious employees (Hatchimonji 2013). These privacy breaches diminish the reputation of the business and lower trust in current and potential customers (Ponemon Institute 2013).

In this study we rely on Politeness Theory to understand the trust violation and restoration process. The study examines the role of CEO status, gender and response (apology vs. denial) on restored trust. We control for several variables such as perceived news seriousness, privacy concern, trust propensity, reputation, design, and user gender.

Literature has ample evidence on antecedents of initial trust, however there are not many studies examining the process of understanding how the trust is violated, and then restored. The issue is of

importance to the MIS community in particular as information technology plays an increasingly important role in causing trust violations (such as data breaches), and often involves businesses which are run solely on the Internet (such as Zappos.com). Not only this, there is little guidance for CEOs in general on how to engineer their response in the event of a data breach crisis. There is increasingly little guidance for female CEOs in particular. The comprehensive examination of several factors in understanding the trust restoration process would help us understand their respective roles, and also provide guidance to business managers and women managers in particular. The findings also shed light on social issues surrounding women stereotypes - which are so finely ingrained in our social structure that most of the time they go unnoticed.

Theory and Hypothesis Development

We examine the trust violation and restoration process through the lens of Politeness Theory (Brown and Levinson 1987) which suggests that in order to maintain social harmony the actors try to minimize damage to another actor's *face* by following appropriate communication strategies. The theory suggests that actors use more polite language when addressing individuals with high status than individuals with equal or low status, when asking for a big favor (big imposition) than a small favor, and when addressing strangers (high social distance) than familiar people (low social distance). In this research we examine the trust violation and restoration for aggregated trust beliefs (Bansal et al. 2010; Gefen et al. 2003) and contrast them with the specific trust beliefs pertaining to ability, integrity and benevolence (Bhattacherjee 2002; Kim et al. 2006).

CEO Response: Apology vs. Denial

Kim et al. (2004) argues that apology consists of two things, admittance of guilt and demonstration of intent to prevent future violations. Denial doesn't admit guilt and fails to provide assurance to prevent future violations. Based on Politeness Theory it could be argued that the breach incident is a face threatening act to the website's users, and by apologizing and being polite the website attempts to lessen the negative feelings of its users. Hence,

Hypothesis 1: Apology vs. denial leads to higher restored (a) trust, and (b) trusting beliefs (integrity, benevolence and ability).
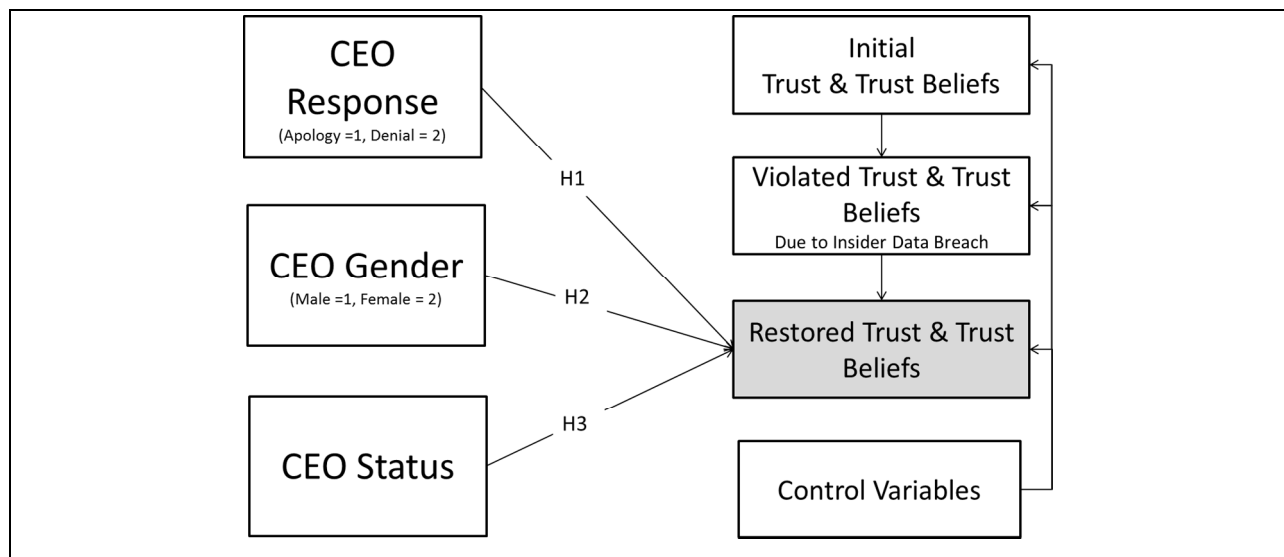

Figure 1. The Research Model

CEO Gender

Historically there have been more male CEOs than female CEOs. This fueled the stereotype that men are more suitable for CEO positions than women are (Lee and James 2007), and contributed to lower social

power of women managers (Walfisch et al. 2013). Politeness theory (Brown and Levinson 1987) suggests that the lower perceived social power of women in a business setting would require women to be nicer than men. Walfisch et al. (2013) showed that a "woman's apology is more expected and less effective" (1455). Similarly, using the Politeness Theory it could be argued that denial from a female CEO would be perceived as rather impolite as well. Hence,

Hypothesis 2: CEO gender (where male=1, female=2) negatively impacts restored (a) trust, and (b) trusting beliefs (integrity, benevolence, and ability).

CEO Status

Many theorists such as Maslow have argued that the desire for higher status is a fundamental driver of human behavior (Eckel et al. 2010). There are several benefits of having a high status such as respect, influence, and social support (Anderson et al. 2012). Moreover, according to Politeness Theory low status actors need to be nicer to relatively high status actors. Conversely, using the Politeness Theory lens it could be argued that relatively high status actors are perceived more favorably. Hence,

Hypothesis 3: Perceived CEO status is positively associated with restored (a) trust, and (b) trusting beliefs (integrity, benevolence and ability).

Control Variables

We control for the following variables which we believe could impact the trust violation and restoration process (i) Prior Trust Level: According to Belief Adjustment Theory when new information is revealed users revise their beliefs according to the negative or positive effect of the new information and the strength of prior beliefs (Hogarth and Einhorn 1992). Recently the theory has been proven to be applicable to trusting beliefs (Zahedi and Song 2008); (ii) Perceived Seriousness of News: Magnitude of the perceived violation is positively associated with the shift in trust (Jones and George 1998). Perceived seriousness of privacy violation news is associated with a drop in trust (Bansal 2012); (iii) Privacy concern, (iv) reputation, (v) design, (vi) user gender, and (vii) trust propensity.

Research Methodology

Operationalization of variables

To ensure construct validity we used items from existing scales wherever possible. We converted the items to semantic differential (0-10) so as to minimize common method variance (CMV) (Chin et al. 2008; Podsakoff et al. 2003; Song and Zahedi 2005), and data was collected in three sequences (before the violation scenario, after the violation scenario and after the social response), which reduced the threat of CMV (Podsakoff et al. 2003).

Code	Construct	Operational Definition	Adapted From
TRPR	Trust Propensity	One's tendency to trust others	Zahedi and Song (2008)
REP	Reputation	Website's perceived reputation which refrains the website from opportunism	Jarvenpaa et al. (2000); Zahedi and Song (2008)
ABL	Ability	The degree to which the website is perceived to be competent in performing the transactions	Zahedi and Song (2008)
BEN	Benevolence	The degree to which the website is perceived to be caring about its users	Zahedi and Song (2008)
INT	Integrity	The degree to which the website is perceived to be faithful and honest	Zahedi and Song (2008)
DES	Design	The degree to which the website design looks professional	Bansal et al. (2008)

PC	Privacy Concern	Privacy concern reflects users' subjective view of fairness within the context of information privacy	Campbell (1997)
SN	Seriousness of News	Perceived seriousness of the privacy violation incidence	Bansal (2012)
STATUS	CEO Status	The degree to which the CEO of the website is perceived to be influential	Self-developed
TR	Trust	Trust in the website	(Bansal et al. 2010); Gefen et al. (2003)

Table 1. Operationalization of Variables

Study Design & Data Analysis

Study design was on online survey based experiment. 280 students were offered and completed responses. The design was full factorial (2 x 2), leading to a total of four scenarios: two CEO genders times two social accounts (apology vs. denial) responses. Every person was asked to browse a website, and their initial trust and trusting beliefs (T1) in the website were measured. Then we shared with the participants a vignette pertaining to an insider data breach incident (refer to vignette 1 in Table 2) which occurred at the website they browsed. We measured the trust and trusting beliefs in the website again at this point (T2). Subsequently one of the following four vignettes (refer to vignettes 2~5 in Table 2) was randomly assigned to the participants. Trust and trusting beliefs in the website were re-measured at this time (T3).

S. No.	Scenario	Description	Remarks
#1	Insider data breach:	The website you saw announced last week that it has come to its attention that some of its own employees were involved in inappropriately accessing customers' personal information from the company's database.	All respondents were assigned to view this vignette (#1).
#2	Male Apology:	The website responded apologetically in a letter sent out individually to the concerned customers. The CEO of the website, Michael Smith, has sincerely apologized for this incident.	Respondents were randomly assigned to one of these four vignettes (#2~#5).
#3	Female Apology:	The website responded apologetically in a letter sent out individually to the concerned customers. The CEO of the website, Mary Jane, has sincerely apologized for this incident.	
#4	Male Denial:	The website's CEO Michael Smith has clearly denied any wrongdoing on the website's part regarding the recent news article.	
#5	Female Denial:	The website's CEO Mary Jane has clearly denied any wrongdoing on the website's part regarding the recent news article.	

Table 2. Vignettes

In order to ensure that the participants seriously participated in the experiment they were asked several questions. This made sure that they have read the scenario well and understood the information presented to them. Those who failed any of these questions were excluded from the analysis. Out of those 280 students, 78 failed at least one of these tests. Thus we have sample size of 202. Table 3 provides descriptive statistics of the respondents' ages.

	Response	N	Min	Max	Mean	Std Dev
Male students	Apology	37	18	44	23.65	5.54
	Denial	53	18	46	23.75	6.38
Female students	Apology	54	18	49	22.74	5.96
	Denial	57	18	51	24.12	8.24

Table 3. Demographics (Age in years)

Test for Common Method Variance (CMV)

To avoid the compounding effect of trust and trust beliefs measured at 3 time intervals we computed trust (Model1) and trusting beliefs (Model2) separately. We found that first factor in model1 and model2 explained 28.91% and 34.83% of the variance respectively. Next we ran the CMV test (for both model1 and model2 separately) as suggested by Jiang et al. (2013). We computed alternate measurement model with an additional single factor that had all the items and constrained that factor to be independent from other factors. We performed this test separately for model1 and model2. We found no significant chi-square difference between the constrained and the original measurement model suggesting that CMV was not a serious threat.

Reliability Check

All CFR values are well above the cutoff value of 0.70, and all AVE values are well above the cutoff value of 0.50 as shown in Table 4, together providing support for the reliability of constructs.

Construct	Time Measured	Trust Model1		Trust Belief Model2	
		CFR	AVE	CFR	AVE
Privacy Concern	T1	0.90	0.75	0.90	0.74
Design	T1	0.86	0.76	0.87	0.78
Reputation	T1	0.78	0.63	0.79	0.65
News Seriousness	T2	0.95	0.91	0.95	0.91
CEO Status	T3	0.86	0.75	0.85	0.74
Trust Propensity	T1	0.86	0.76	0.86	0.77
Trust (TR1)	T1	0.91	0.84	n/a	n/a
Integrity (INT1)	T1	n/a	n/a	0.82	0.69
Benevolence (BEN1)	T1	n/a	n/a	0.78	0.64
Ability (ABL1)	T1	n/a	n/a	0.77	0.63
Trust (TR2)	T2	0.94	0.89	n/a	n/a
Integrity (INT2)	T2	n/a	n/a	0.93	0.87
Benevolence (BEN2)	T2	n/a	n/a	0.88	0.79
Ability (ABL2)	T2	n/a	n/a	0.88	0.78
Trust (TR3)	T3	0.94	0.89	n/a	n/a
Integrity (INT3)	T3	n/a	n/a	0.94	0.89
Benevolence (BEN3)	T3	n/a	n/a	0.94	0.88
Ability (ABL3)	T3	n/a	n/a	0.92	0.85

Table 4. Reliability

Validity Check

We first carried out CFA for both model1 and model2. The factors had high factor loadings as well as high t-values. All indicators in both the models had significant R square values. We compared the square root of AVE with construct correlations. For model1 we found that square root of AVE values are greater than construct correlations thus supporting convergent and divergent validity (Table 5).We could not find a similar pattern for model 2. This could be due to the repeated measures of trust beliefs. A similar issue had been reported earlier in the literature ([Zahedi and Song 2008](#)). To examine discriminant validity for both the models we carried out chi-square test as suggested in the literature ([Gefen et al. 2003](#); [Zahedi and Song 2008](#)). We analyzed every possible combination by collapsing two constructs into one (total 36 and 105 alternate measurement models were computed for model1 and model2 respectively). The alternate models did not provide any significantly different chi-square results. Overall the analysis provides support for the discriminant and convergent validity of the constructs used in model1 and model2.

	UA	T1	DES	REP	SERIOUS	T2	STATUS	T3	TRPR
UA	**0.86**								
T1	-0.30	**0.92**							
DES	-0.05	0.58	**0.87**						
REP	-0.17	0.71	0.69	**0.80**					
SERIOUS	0.13	-0.13	-0.03	-0.17	**0.96**				
T2	-0.18	0.30	0.16	0.40	-0.50	**0.95**			
STATUS	-0.09	0.37	0.29	0.55	-0.14	0.26	**0.87**		
T3	-0.20	0.33	0.17	0.44	-0.42	0.73	0.49	**0.95**	
TRPR	-0.22	0.24	0.06	0.26	-0.15	0.33	0.20	0.36	**0.87**

Table 5. Construct Correlations and Square Root of AVE (Model1)

Note: Diagonal values are square root of AVE

Estimation Model

We estimated the models using MPlus. The fit indices (Table 6) provide support for the model fit.

Fit Index	Measurement Models		Estimation Models		Threshold ([Song and Zahedi 2005](#))
	Trust Model 1	**Trust Beliefs Model 2**	**Trust Model 1**	**Trust Beliefs Model 2**	
Normed χ2	1.74	1.67	1.67	1.93	<3
CFI	.96	.95	.96	.91	>0.90
TLI	.95	.93	.94	.89	>0.90
RMSEA	.06	.06	.06	.07	<0.06
SRMR	.04	.04	.04	.05	<0.10

Table 6. Fit Indices for the Measurement and Estimation Models

Results

Results are shown in figures 2 and 3. Results for *hypothesis 1* indicate that denial as opposed to apology had a significant negative impact on restored trust (sig .001). Response type also seems to have an impact on trusting beliefs. We see the biggest negative impact of denial (as opposed to apology) on benevolence based beliefs (sig .001 level), followed by integrity (sig level .01) and then by ability (sig level .05). The results support the hypothesis that apology, as opposed to denial, appears to be better in restoring trust in the case of insider data breach. Results for *hypothesis 2* from model 1 suggest that responses from male
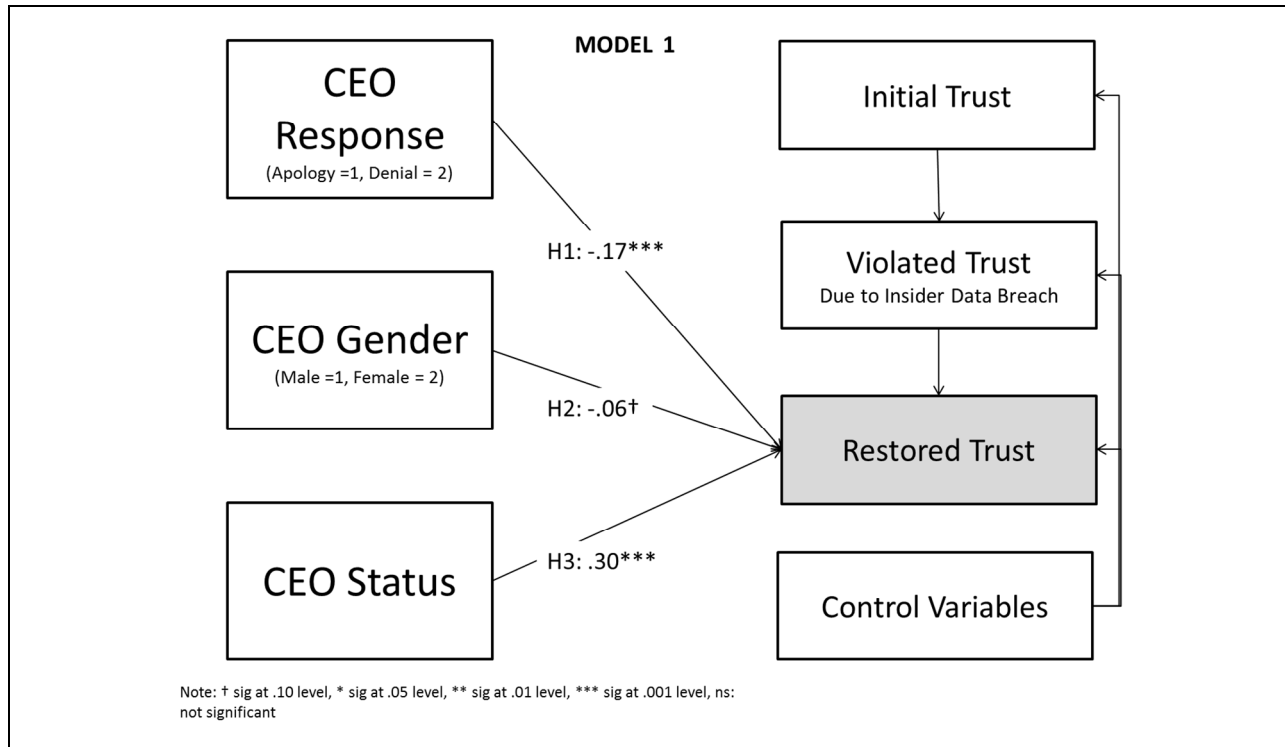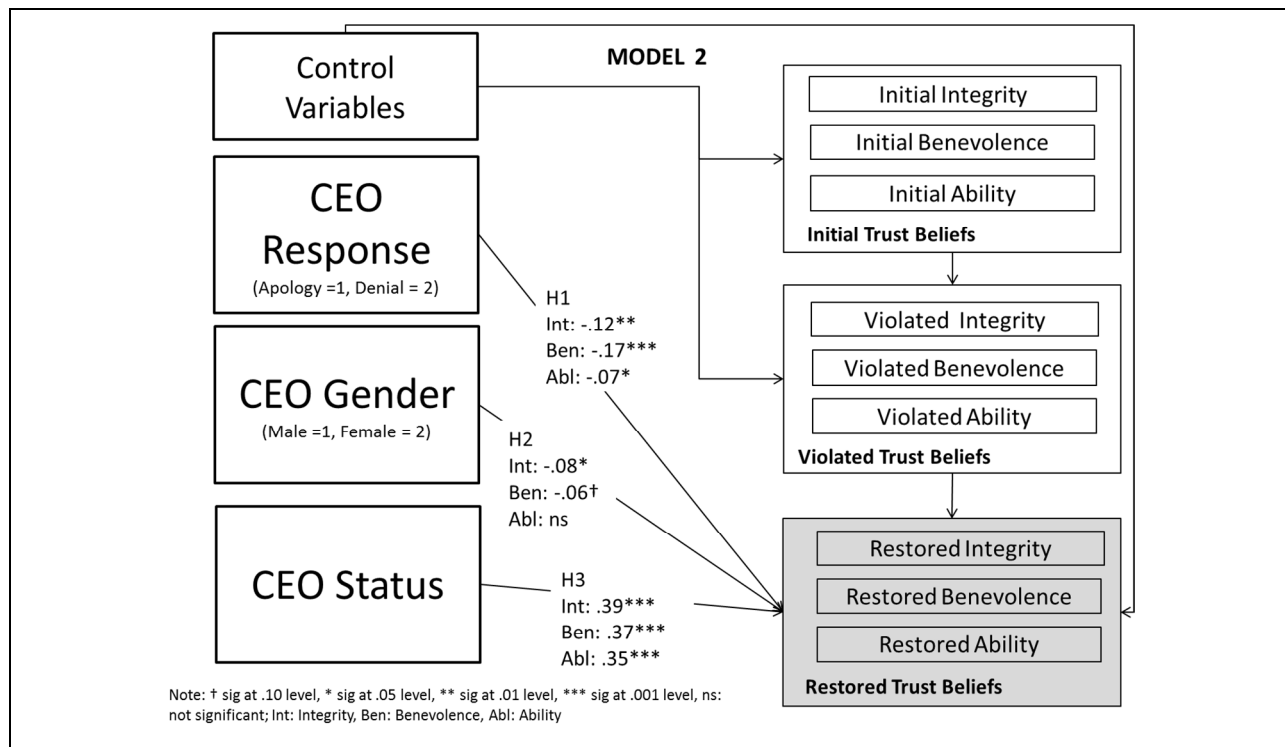
Figure 2. Results (Model1: Trust Model)

Figure 3. Results (Model2: Trust Beliefs Model)

CEOs as opposed to female CEOs had a slightly better impact on restored trust (sig .10). However, the male gender (as opposed to female gender) was associated with higher restored integrity based beliefs (sig .05), and slightly positive restored benevolence based beliefs (sig .10). Male CEOs did not enjoy any

strategic gender advantage when it came to restored ability based trusting beliefs. *Hypothesis 3* was strongly supported for both trust and trusting beliefs (sig .001).

Post hoc Analysis

We carried out the post hoc analysis by splitting the dataset into two groups: Apology and Denial. We carried out analysis for both trust model (Model PH1) and trust belief model (Model PH2). Analysis was carried out using GROUP command in MPlus. R squares for all the indicators were all significant and quite high for almost all the indicators except for trust propensity. Across all the models and subgroups the factor loadings had t values greater than 9.49. The findings are shown in figure 4 and 5 respectively. We trimmed the model in figure 6 and removed trust beliefs at time T1 from the model to lower the model complexity, and re-estimated the model (Model PH-3).

Fit Index	Model PH1	Model PH2	Model PH3	Threshold ([Song and Zahedi 2005](#))
Normed χ2	1.54	1.77	1.69	<3
CFI	.93	.87	.90	>0.90
TLI	.92	.84	.88	>0.90
RMSEA	.07	.09	.09	<0.06
SRMR	.07	.07	.07	<0.10

Table 7. Fit Indices for the Estimated Posthoc Models

Post hoc clearly shows that there is an interaction effect between CEO gender and CEO response such that female CEOs were associated with lower restored trust especially in the case of denial. There was no CEO gender effect in the case of apology. Models PH2 and PH3 reveal that female CEOs were associated with lower integrity, ability, as well as benevolence based trust beliefs – for denial and not for apology. We noticed that female CEOs experienced a lower drop in ability as opposed to benevolence and integrity (the difference is not statistical though). Perceived CEO status is found to assist in restored trust significantly so only in the case of denial and not in the case of apology. In the case of denial the impact of CEO status is felt more positively on restored integrity and benevolence based beliefs than for ability based beliefs.
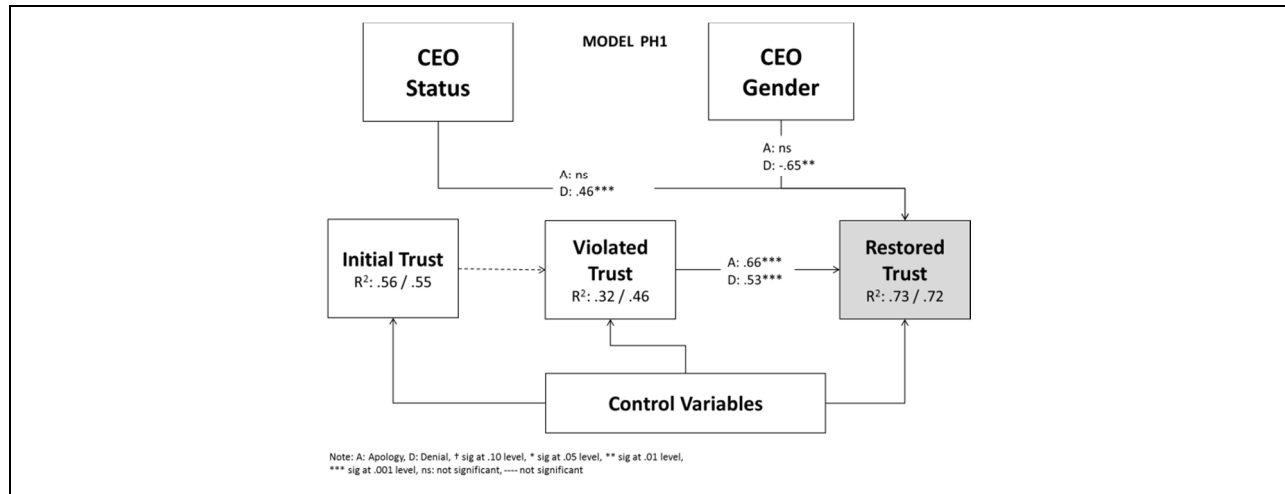

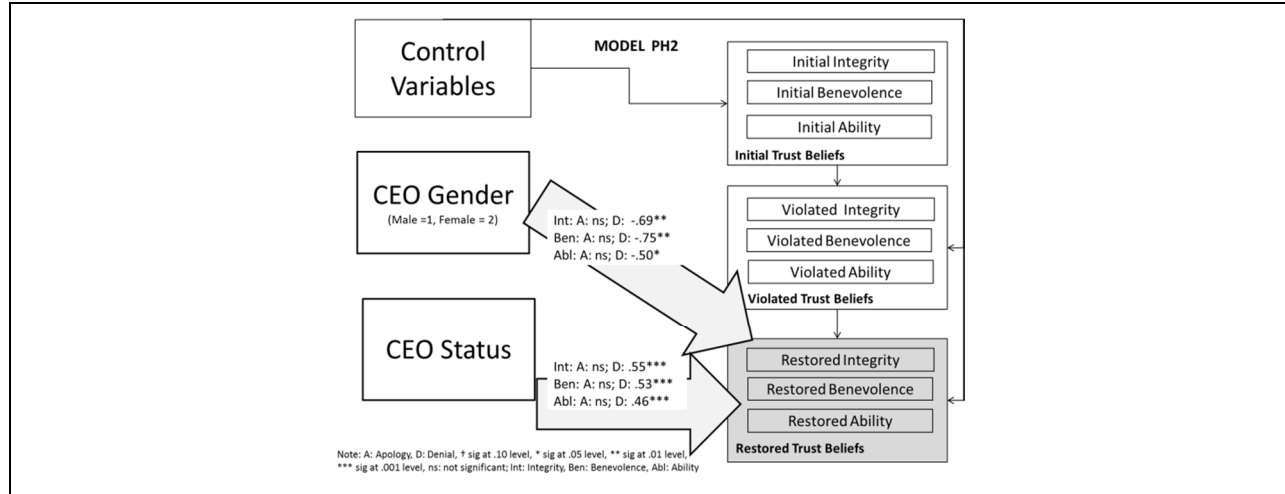**Figure 4. Model PH1: Trust Group Analysis (Apology Vs. Denial)**

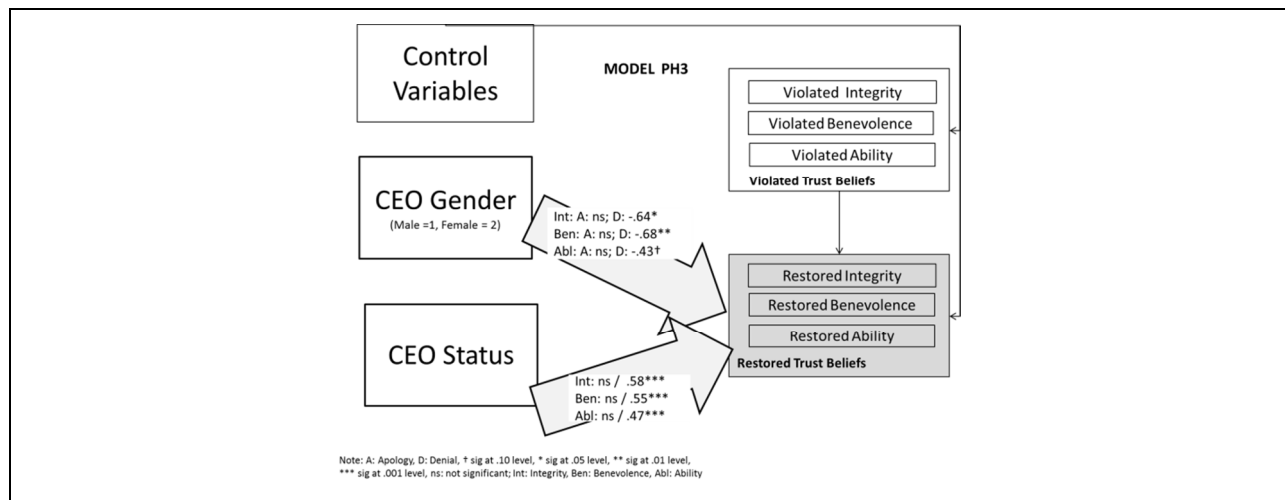**Figure 5. Model PH2: Trusting Beliefs Group Analysis (Apology Vs. Denial)**

Figure 6. Model PH3: Trusting Beliefs Group Analysis (Apology Vs. Denial) (Without Initial Trust)

Control Variables

Here we provide broad analysis on control variables based on the overall trends observed across all the five models (Model1, Model2, PH1, PH2, and PH3). *Trust revision:* There is strong evidence that trust revision is happening from T2 to T3 especially for benevolence and ability and not for integrity – *Privacy concern:* It seems that privacy concern in the form of unauthorized access is negatively impacting initial trust. There is no similar strong support for the negative impact of privacy concern on violated trust and restored trust in this scenario. This needs to be further investigated. *Perceived news seriousness:* The comprehensive analysis suggest that perceived news seriousness does impact violated trust. A similar strong effect was observed for trusting beliefs in PH2 and PH3 as well. The effect of news seriousness was negative on restored trust and trusting beliefs as well, but the effect was not as broadly consistent. *Trust propensity:* Review of all of the five models suggests that trust propensity did cushion the violated trust. *User gender:* In general there was no significant role of user gender in any of the trust and trust belief measurements. Website *Design* had a clear impact on both initial trust and initial trusting beliefs. Design was found to impact neither restored trust nor trusting beliefs. The positive effect was not so pronounced for violated trust and trusting beliefs. *Reputation* had a clear impact at T1 on both trust and trusting beliefs. Reputation didn't have impact on restored trust or restored trusting beliefs. Moreover, the effect of reputation was positive for violated trust, but had less impact on violated trusting beliefs.

Construct	Trust Model (Model)			Trust Belief Model (Model2)								
	T1	T2	T3	T1			T2			T3		
				INT	BEN	ABL	INT	BEN	ABL	INT	BEN	ABL
PC	-**	ns	ns	ns	ns	ns	†	†	†	ns	ns	ns
Rep	***	**	ns	***	***	***	ns	ns	ns	ns	ns	ns
Design	*	ns	ns	*	*	ns	ns	ns	ns	ns	ns	ns
Gender	ns	ns	ns	†	*	ns	ns	ns	ns	-†	ns	ns
TRPR	ns	**	†	-*	-†	ns	*	***	***	†	-†	**
NS		-***	-†				ns	ns	ns	-†	-*	-†
T1 to T2		ns					ns	***	ns			
T2 to T3			***							ns	***	**

Table 8. Estimations for Control Variables (Research Models 1 and 2)

	Model PH1				Model PH2											
Construct			T3		T1			T2			T3					
	T1	T2	A	D	INT	BEN	ABL	INT	BEN	ABL	INT		BEN		ABL	
											A	D	A	D	A	D
PC	-***	Ns	-†	ns	ns	-*	†	†	ns	†	ns	ns	ns	ns	ns	ns
Rep	***	**	ns	ns	**	*	**	-*	-†	-*	ns	ns	ns	ns	ns	ns
Design	**	Ns	-†	ns	***	***	***	**	†	**	ns	ns	ns	ns	ns	ns
Gender	ns	Ns	†	ns	*	**	ns	ns	ns	ns	ns	-†	ns	ns	ns	-†
TRPR	ns	**	ns	**	**	**	**	***	***	***	ns	ns	ns	-†	**	ns
NS		-***	-*	ns				-***	-***	-***	ns	-**	ns	ns	-*	-*
T1 to T2		Ns						-†	***	**						
T2 to T3			***	***							ns	ns	***	***	*	***

Table 9. Estimations for Control Variables in Posthoc Analysis (Models PH1 & PH2)

	Model PH3								
	T2			T3					
Construct	INT	BEN	ABL	INT		BEN		ABL	
				A	D	A	D	A	D
PC	†	ns	†	ns	ns	ns	ns	ns	ns
Rep	-*	-†	ns	ns	ns	ns	ns	ns	ns
Design	**	*	**	ns	ns	ns	ns	ns	ns
Gender	ns	ns	ns	ns	ns	ns	ns	ns	ns
TRPR	***	***	***	ns	†	ns	ns	***	ns
NS	-**	-**	-**	ns	-*	ns	ns	-*	-*
T2 to T3				ns	ns	***	**	**	**

Table 10. Estimations for Control Variables in Posthoc Analysis (Model PH3)

Note to tables 7~9: Shaded cells reflect those relationships which were not measured for theoretical reasons, T1: trust measurement at time1, T2: trust measurement at time 2, T3: trust measurement at time 3, INT: Integrity, BEN: benevolence, ABL: Ability; † sig at .10 level, * sig at .05 level, ** sig at .01 level, *** sig at .001 level, TRPR: trust propensity, NS: perceived news seriousness, PC: privacy concern measured as unauthorized access; Rep: Reputation, Gender: User Gender

Discussion and Conclusion

The results provide a very insightful and comprehensive examination of factors which could impact initial, violated and restored trust and trusting beliefs as well. The overall analysis provides support for all the hypotheses. The results show that in the case of an insider privacy breach incident apology is a more suitable response than denial, and higher perceived CEO status is positively associated with restored trust. More interestingly we learned that female CEOs command equal restored trust in the case of apology, however male CEOs have a better strategic gender advantage in the case of denial. However, the impact of CEO gender in the case of denial is not uniform for all the trusting beliefs. The Post hoc analysis reveals that female CEO denial has the biggest negative impact on restored benevolence, with integrity being a close second. Similarly, the contextual examination of control variables on three belief types at different times (T1, T2 and T3) shows their varied impact on initial, violated and restored trust and trusting beliefs.

The reason for users being more critical of female CEOs when they deny is probably related to gender stereotypes. In the case of *denial* the female CEO is defying several stereotypes – that they are inconsistent with leadership roles, and the ones that see women as people-centered, and the ones that see women with lower social power (Walfisch et al. 2013) and hence more likely to make greater efforts to minimize the damage. With denial – the female CEO exacerbates the bias against women as they are perceived as violating gender-role expectations (Lee and James 2007).

It is interesting to note the perceived CEO status influences restored trust, however only in the case of denial. Status is an integral part of economic decision making, and is no less important than monetary reinforcements. It is important because it influences others' behaviors. Organizational researchers Eckel et al. (2010) showed with the help of a star network research experiment that high-status of a leader *obviates the need for punishment* (p. 741) and makes the status of the leader itself a kind of substitute for punishment. As mentioned earlier, denial has two parts- no wrong doing, and no implied promise for future prevention. In the case of data breach, users probably are more interested in the future preventions than they are in appreciating that the company did nothing wrong. So the punishment for a CEO's denial is meted out in terms of lower restored trust. However, the perceived high status of a CEO provides shields and tends to *obviate the need for punishment.* The status theory could also be used to shed a different light on the negative association of female CEO denial and restored trust. Women are generally associated with lower social power and hence lower status. Apparently gender works as a substitute for status and hence the negative association.

The study's limited generalizability is of course one of the limitations. However, it provides several significant theoretical, social and managerial implications. The examination of a data breach incident with the perspective of Politeness Theory adds to the MIS literature. It adds to our understanding of Politeness Theory as well. The moderating role of response type (apology vs. denial) extends Politeness Theory by suggesting that if power (CEO) and imposition (denial) are held constant then perceived politeness (in the form of trust) might vary as a function of perceived social status (high vs. low). The examination of hidden gendered effects and biases surfaces stereotypes faced by women as they progress to the leadership positions. This awareness would assist as we as a progressive society self-reflect on our practices. There are several managerial implications. One noticeable finding is that when it comes to restoring trust, as in the case of data breach incidents, belief revision from prior trust (i.e. violated trust at T2) serves as a very strong custodian of restored trust. Managers should try to create a social bond with their users so that when such incidents happen the violated trust stays as high as it can, because the higher the trust at T2, the easier it would be for the mangers to restore it eventually. Reputation helps in initial trust (T1) building but may not help in restoring trust directly (T3), however it definitely aids in cushioning the blow to the violated trust (T2). Reputation is an asset which the web businesses must aggressively protect.

With the rise in ubiquitous computing, and the proliferation of newer technologies and storage capabilities such incidents have become more common than ever before. Going forward it is quite likely that such incidents will only rise. With permeating data collection, integration, and accidental and on-purpose data breaches – users are already realizing the reduced privacy paradigm they are in. In such a situation company response becomes very critical. If handled well, customers might forgo the crisis and engage with the website or business in a renewed manner. "The data breach – is one crisis but the response may ignite a series of secondary crises if not handled well" (McNulty 2013). Obviously, the most

important objective for the company's management is to restore the confidence of customers – and "never say never" (McNulty 2013).

Acknowledgement

References

Anderson, C., Brion, S., Moore, D. A., and Kennedy, J. A. 2012. "A status-enhancement account of overconfidence," *Journal of Personality and Social Psychology* (103:4), p. 718.

Bansal, G. 2012. "Unauthorized information sharing vs. hacking: The moderating role of privacy concern on trust found and lost," *Eighteenth Americas Conference on Information Systems,* Seattle, Washington.

Bansal, G., Zahedi, F. M., and Gefen, D. 2008. "The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation," *Twenty Ninth International Conference on Information Systems,* Paris, France.

Bansal, G., Zahedi, F. M., and Gefen, D. 2010. "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online," *Decision Support Systems* (49:2), pp. 138-150.

Bhattacherjee, A. 2002. "Individual trust in online firms: Scale development and initial test," *Journal of Management Information Systems* (19:1), pp. 211-241.

Brown, P., and Levinson, S. C. 1987. *Politeness: Some universals in language usage*, Cambridge University Press: Cambridge, England.

Campbell, A. J. 1997. "Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy," *Direct Marketing* (11:3), pp. 44-57.

Chin, W. W., Johnson, N., and Schwarz, A. 2008. "A fast form approach to measuring technology acceptance and other constructs," *MIS Quarterly* (32:4), pp. 687-703.

Eckel, C., C., Fatas, E., and Wilson, R. 2010. "Cooperation and status in organizations," *Journal of Public Economic Theory* (12:4), pp. 737-762.

Gefen, D., Karahanna, E., and Straub, D. W. 2003. "Trust and TAM in online shopping: An integrated model," *MIS Quarterly* (27:1), pp. 51-90.

Hatchimonji, G. 2013. "Report indicates insider threats leading cause of data breaches in last 12 months," www.csoonline.com, Oct 8.

Hogarth, R. M., and Einhorn, H. J. 1992. " Order effects in belief updating: The belief-adjustment model," *Cognitive Psychology* (24:1), pp. 1-55.

Identity Theft Resource Center. 2014. "2013 Data Breach Category Summary," (http://www.idtheftcenter.org/ITRC-Surveys-Studies/2013-data-breaches.html)

Jarvenpaa, S. L., Tractinsky, N., and Vitale, M. 2000. "Consumer trust in an Internet store," *Information Technology Management* (1), pp. 45-71.

Jones, G. R., and George, J. M. 1998. "The experience and evolution of trust: Implications for cooperation and teamwork," *Academy of Managemenf Review* (23:3), pp. 531-546.

Kim, P. H., Dirks, K. T., Cooper, C. D., and Ferrin, D. L. 2006. "When more blame is better than less: The implications of internal vs external attributions for the repair of trust after a competence- vs integrity-based trust violation," *Organizational Behavior and Human Decision Processes* (99), pp. 49-65.

Kim, P. H., Ferrin, D. L., Cooper, C. D., and Dirks, K. T. 2004. "Removing the shadow of suspicion: The effects of apology versus denial for repairing competence- versus integrity- based trust violations," *Journal of Applied Psychology* (89:1), pp. 104-118.

Lee, P. M., and James, E. H. 2007. "She'-e-os: Gender effects and investor reactions to the announcements of top executive appointments," *Strategic Management Journal* (28:3), pp. 227-241.

McNulty, E. J. 2013. "How to lead during a data breach," (http://blogs.hbr.org/2013/12/how-to-lead-during-a-data-breach/)

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., and Podsakoff, N. P. 2003. "Common method biases in behavioral research: A critical review of the literature and recommended remedies," *Journal of Applied Psychology* (88:5), pp. 879-903.

Ponemon Institute 2013. "2013 Cost of Data Breach Study: Global Analysis."

Song, J., and Zahedi, F. M. 2005. "A theoretical approach to web design in e-commerce: A belief reinforcement model," *Management Science* (51:8), pp. 1219-1235.

Walfisch, T., Dijk, D. V., and Kark, R. 2013. "Do you really expect me to apologize? The impact of status and gender on the effectiveness of an apology in the workplace," *Journal of Applied Social Psychology* (43), pp. 1446-1458.

Zahedi, F. M., and Song, J. 2008. "Dynamics of trust revision: Using health infomediaries," *Journal of Management Information Systems* (24:4), pp. 225-248.