Aug 10th, 12:00 AM

The Role of Cybersecurity Risk Disclosures in Influencing Stakeholder Intentions and the Moderating Role of Privacy Concern

Zhuoli Axelton
University of Wisconsin - Green Bay, axeltonz@uwgb.edu

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

The Role of Cybersecurity Risk Disclosures in Influencing Stakeholder Intentions and the Moderating Role of Privacy Concern

Completed Research

Zhuoli Axelton*
University of Wisconsin – Green Bay
axeltonz@uwgb.edu

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

** authors are listed in alphabetical order; both authors contributed equally to the paper*

Introduction and Background

Cybersecurity threats such as data breaches pose severe risks to users' privacy and impact customers' trust, as well as investors' and employees' confidence. A company that suffers a data breach has to deal with the loss of trust and confidence from not only users (Burt, 2019) but also investors (Ali et al., 2021; Cheng and Walton, 2019; Kelton and Pennington, 2020; SEC, 2018), and employees (Adams, 2020; Sanders, 2019). Data breaches are known to undermine trust in the ability of a company (Bansal and Warkentin, 2021) or even government (Farrell, 2017) to protect users' data.

Risk communication is part of a business strategy to restore credible, trusting relationships with the stakeholders, including investors (Coombs, 2014; Spence, 2020). Given the increased frequency of data breach and their relative magnitude in recent years, regulators (such as SEC) have urged companies to enhance cybersecurity risk disclosures in their financial statements (SEC, 2018). However, the informativeness of cybersecurity risk disclosures varies significantly across companies (Bansal et al., 2015). Further, little is known about *how* cybersecurity risk disclosures may influence various stakeholders' attitudes and behavior following a data breach. Hence, building on the belief reinforcement model (BRM) (Song and Zahedi, 2005), we examine how the perceived presence of disclosure specificity impacts the behavioral intentions of different stakeholders – users, investors, and employees.

Building on the belief reinforcement model (Song and Zahedi, 2005), we examine how the perceived presence of disclosure specificity and belief about the verifiability of specific disclosure elements impact the behavioral intentions of different stakeholders – users, investors, and employees, through beliefs and attitudes. This research focuses on ability-based trust since a data breach could be considered an ability-based violation when viewed as management's inability to effectively manage the data protection processes (Bansal and Warkentin, 2021).

Prior research suggests that disclosures with high specificity and verifiability will convey management credibility and restore higher trust than general or no disclosure (Cannon, 2021; Rosenthal, 1971). Consistent with this notion, Hope et al. (2016) document that higher specificity (as measured by name, location, date, and quantitative value, among others) of risk disclosures benefits financial statement users more. However, no research examines *how* disclosures' perceived specificity and verifiability can mitigate the drop in ability-based trust and thus influence stakeholder intentions (Spence, 2020). The Belief Reinforcement Model (BRM) suggests that the saliency of beliefs is specific to the individuals' behavior under investigation (Song and Zahedi, 2005). Drawing on BRM, we hypothesize that the perceived presence of specific disclosure elements directly impacts the beliefs about disclosure specificity. In turn, the beliefs about disclosure specificity and verifiability mitigate the drop in ability-based trust and thus influence stakeholder behavioral intentions following a data breach.

Privacy concern (PC) is a pivotal trait that impacts the users' trust violation and rebuilding following a data breach (Bansal and Zahedi, 2015). Thus, we investigate the role of PC in moderating the relationship

between the perceived disclosure specificity, verifiability, trust violation, and stakeholder intentions using the ELM lens (Petty et al., 1981) in the context of a data breach. Prior research suggests that individuals with high PC are more involved and motivated to scrutinize and process the information (Bansal et al., 2015). In other words, high PC individuals rely more on the central route, i.e., quality of the argument, while low PC individuals rely more on peripheral cues. In our setting, disclosures specificity are easy to process and thus can be treated as peripheral cues. In contrast, verifiability of specific disclosure elements requires more cognitive effort to process and thus can be treated as a central route. Overall, we posit that the indirect effect of perceived disclosure specificity and verifiability on stakeholder intentions will differ conditional on the level of individuals' PC.

Thus, we have the following two research questions. First, we examine if disclosures' perceived specificity and belief about verifiability can help lower the drop in ability-based trust and thus influence stakeholder intentions for continuing business after a data breach. Second, we examine the moderating role of PC on the perceived specificity and verifiability on trust violation and stakeholder intentions. The research questions were examined using an experimental survey. Participants were first shown a fictitious e-commerce website and asked to rate the perceived familiarity, design, and reputation on a scale of 1 to 7. Ability-based trust dimensions were measured next. Participants then viewed one of the three scenarios designed with varying specificity of risk disclosures about the data breach (including date, size of the breach, type of information stolen, and business location). The perceived seriousness of the breach news and the perceived presence of the specific elements were measured next. We then measured the violated ability-based trust. The drop in the ability-based trust (DAT) was computed by taking a difference between the initial and the violated ability-based trust ratings. We then measured the behavioral intentions for three different stakeholder groups – users, investors, and employees. PC, trust propensity, and demographics were measured at the end. We intercepted several attention checks throughout the survey to ensure the participants were attentive to the scenario and the items asked.

The findings show that the perceived presence of specific disclosure elements reinforces belief about disclosure specificity. The belief about disclosure specificity is negatively associated with the drop in ability-based trust in protecting data. Similarly, beliefs about the verifiability of the specific disclosure elements are also negatively associated with the drop in ability-based trust (DAT) in protecting data. Consistent with our hypothesis, the drop in ability-based trust in protecting data is negatively associated with stakeholder intentions for all three groups - users, investors, and employees. Similarly, aligned with the ELM, the indirect effect of perceived specificity (akin to a peripheral cue) matters more for low-PC individuals, and the indirect effect of beliefs about verifiability (akin to the central route) matters more for high-PC individuals.

The study contributes to research and practice in cybersecurity and trust rebuilding following a data breach. We contribute to the disclosure and trust literature by providing additional insight on how the perceived presence of disclosure specificity and verifiability mitigate trust violations following a data breach differently for high and low PC individuals. Our findings suggest that the informativeness of cybersecurity risk disclosures matters to various stakeholders. However, high- vs. low- PC individuals may place different weights on the beliefs about disclosure specificity vs. verifiability when they process the information in cybersecurity risk disclosures after a data breach. Thus our findings inform ELM literature as well.

Research Model and Hypotheses

Perceived presence of specific risk disclosure elements. The belief reinforcement theory suggests that "the mere presence of elements in a Web-design category is not adequate for influencing a Web customer; its presence must be perceived to create any possible impact on the Web customer's belief (Song and Zahedi, 2005)." Further, the saliency of beliefs is specific to the individuals' behavior under investigation. In the context of cybersecurity risk disclosures following a data breach, we argue that the perceived presence (and not actual presence) of specific disclosure elements directly impacts the underlying individual's beliefs about the disclosure specificity.

H1: The perceived presence of specific disclosure elements (date, size of the breach, type of information stolen, and business location) is positively associated with belief about the disclosure specificity.

Belief about the specificity of risk disclosure. Disclosures with higher specificity present a complete and clear representation of reality and help deliver persuasive communication (Rosenthal, 1971). Further, the belief that risk disclosures are specific and complete would build trust that the disclosing party will behave dependable, ethical, and in a socially appropriate manner (Gefen et al., 2003). Such beliefs would enable the trust that will help mitigate the perceived violation following a data breach, a trust-impairing event.

Belief about the verifiability of specific risk disclosure elements. The verifiability of disclosures also plays an important role in delivering persuasive communication (Rosenthal, 1971). Prior market research suggests that perceived verifiability can become a pivotal signal to build credibility and trust (Collins and Martinez-Moreno, 2021). Further, when specific disclosure elements can be verified through an independent third party, the credibility of the disclosures can be optimized and strengthened (Rosenthal, 1971).

Data breaches have been shown to erode all three trust beliefs – ability, benevolence, and integrity (Bansal and Zahedi, 2015). However, a data breach could be considered an ability-based trust violation primarily because it could be viewed as management's inability to effectively manage the data protection processes (Bansal and Warkentin, 2021). Thus, in this research, we focus on trust violations about ability-based trust. Ability-based trust is contextual because the ability is task and situation-specific (Mayer et al., 1995). Ability-based trust in an online business is conventionally measured as the degree of one's belief that the company is competent in conducting the transactions (Bhattacherjee, 2002). In the context of cybersecurity risk disclosures following a data breach, we argue that ability-based trust in protecting data is a separate construct from ability-based trust in conducting transactions. Thus, we hypothesize that beliefs about the disclosure specificity will mitigate the negative impact of ability-based trust violation following a data breach, focusing on the ability-based trust in protecting data.

H2: Following a data breach, belief about disclosure specificity will mitigate the drop in ability-based trust in protecting data.

H3: Following a data breach, belief about the verifiability of specific disclosure elements will mitigate the drop in ability-based trust in protecting data.

Trust and user intentions. Trust is an expectation that others one chooses to trust will not behave opportunistically by taking advantage of the situation. Such behaviors include privacy violations and unauthorized use of data from users (Gefen et al., 2003; Mayer et al., 1995). Trust is particularly important in online transactions because of the risk of information asymmetry between users and the business. In addition, the risks may arise from the absence of proven guarantees that the company will not engage in harmful opportunistic behaviors. Thus, building trust is a critical aspect of e-commerce.

From a user standpoint, higher trust is associated with a higher likelihood of engaging with the company. In the information age, stakeholders are increasingly interconnected. A company's actions toward users are visible to other stakeholders, such as employees and investors, and thus impact the trustworthiness of different stakeholders. In turn, a company's trustworthiness will determine to what degree other stakeholders will assume vulnerability and engage in future exchange relationships (Crane, 2020). Therefore, a company that suffers a data breach has to deal with the loss of trust and confidence of different stakeholders, including users (Curtis et al., 2018), investors (Ali et al., 2021), as well as employees (Adams, 2020; Sanders, 2019)

Hence, in the context of cybersecurity risk disclosures following a data breach, we argue that a drop in the ability-based trust will negatively impact all three stakeholder intentions: users, investors, and employees.

H4: Drop in ability-based trust in protecting data is negatively associated with (a) user intentions, (b) investor intentions, and (c) employee intentions.

Information processing for high- vs. low- PC individuals. Several studies have demonstrated that the PC level could be used to demonstrate the level of involvement regarding attitude and intentions (Angst and Agarwal, 2009; Bansal et al., 2015; Gu et al., 2017; Lowry et al., 2012; Zhou, 2017). The elaboration likelihood model (ELM) suggests that highly involved users engage in extensive elaboration to shape their attitudes and intentions, whereas those less involved rely more on peripheral cues (Petty et al., 1981). In other words, ELM postulates that highly involved users develop their attitude change through the central route instead of the peripheral cues (Petty et al., 1981). The central route entails more effort as it requires the users to carefully scrutinize arguments to form their judgment (Petty et al., 1981). Using ELM theory,

Bansal et al. (2015) showed that high PC individuals have a stronger motivation for careful elaboration and rely more on the central route, such as the quality of the arguments, whereas low PC individuals rely on peripheral cues such as availability of company information.

Perceived presence of disclosure specificity as peripheral cues. We argue that the *perceived* presence, as opposed to the absolute presence of specific disclosure elements, forms a salient peripheral cue, as the presence of the elements must be perceived to be registered (Song and Zahedi, 2005). Further, similar to website surface elements, those disclosure attributes require little cognitive energy and are more easily recognized and processed (Bansal et al., 2015; Wells et al., 2011). Thus, the perceived presence of specific disclosure specific elements can be termed as peripheral cues. In turn, low PC individuals rely on peripheral cues such as the perceived presence of specific disclosure elements to impact their attitude and intentions.

Belief about disclosure verifiability as a central route. Verifiability of a message is associated with the argument quality (Petty et al., 1981) and the persuasive power of the message and thus impacts attitude change through the central route. Verifiability is among persuasion techniques that influence the "cognitive thinking of the users and thus require deep consideration to avoid unintended results" (Ibrahim et al., 2013, p. 424). The central route to persuasion is when people elaborate on a persuasive argument – carefully and effortfully, thinking about the logic behind the message; and the thought process is active, creative, and alert and includes scrutiny of the message, including verifying its credibility (Petty et al., 1981; Racherla et al., 2012). Thus we argue that the verifiability of specific disclosure elements positively reinforces the argument quality and thus can be treated as a central route in our setting. A message with higher argument quality influences the cognitive thinking of the users and therefore requires deep consideration to avoid unintended results (Conger, 1998; Ibrahim et al., 2013). Individuals with high involvement rely more on the central route, which requires deep consideration in building trust (Petty et al., 1981). Similarly, high-PC individuals are likely to rely more on central routes, such as belief about disclosure verifiability, when processing the information from cybersecurity risk disclosure.

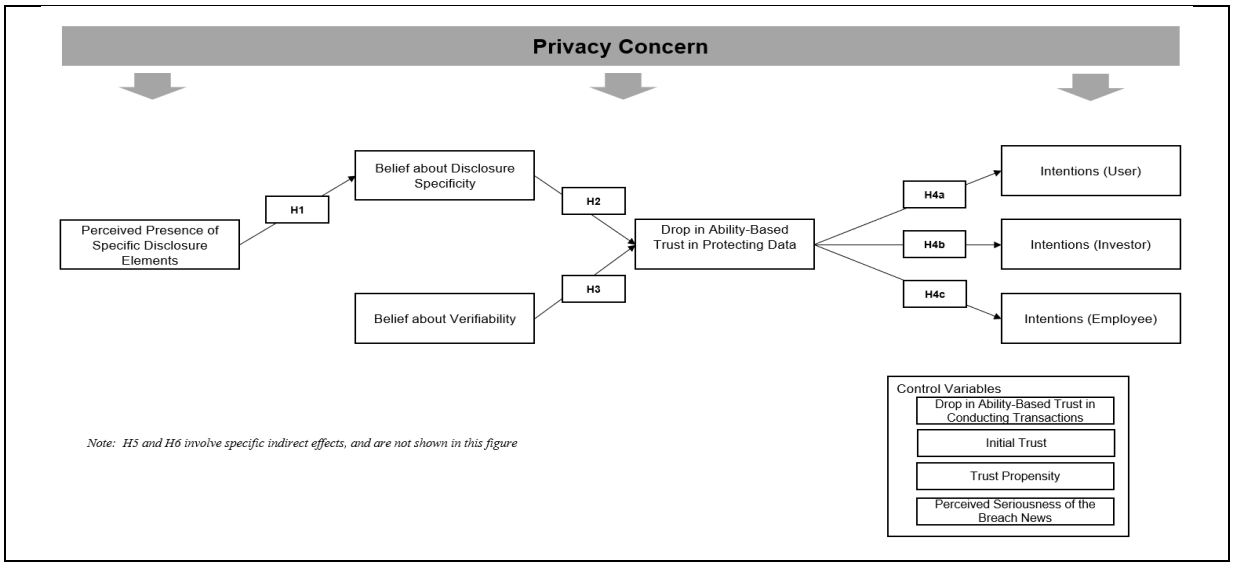

Figure 1. Research Model

The perceived presence of specific disclosure elements and beliefs about disclosure verifiability are trust-generating attributes and thus influence stakeholder intentions (Cannon, 2021; Rosenthal, 1971). However, the effects of those two attributes differ conditional on high- vs. low- PC individuals. On the one hand, the perceived presence of disclosure-specific elements influences trust and intentions as peripheral cues. Low PC individuals rely more on peripheral cues; we posit that the perceived presence of specific disclosure and ensuing beliefs impact attitude change more for low PC users than for high PC users. On the other hand, perceived verifiability influences trust through a central route. High PC individuals rely more on the central route; we predict that perceived verifiability impacts attitude change more for high PC users than low PC

users. In other words, we argue that perceived specificity (perceived verifiability) of such disclosure would matter more for low (high) PC individuals in mitigating trust violation and thus influence stakeholder intentions. Thus, we have the following two hypotheses.

H5: The specific indirect effect of the *perceived presence of specific disclosure elements -> belief about disclosure specificity -> drop in ability-based trust in protecting data -> intentions* is significantly more important for low PC individuals than high PC individuals for all three stakeholder groups – users, investors and employees.

H6: The specific indirect effect of *belief about the verifiability of specific disclosure elements -> drop in ability-based trust in protecting data -> intentions* is significantly more important for high PC individuals than for low PC individuals for all three stakeholder groups – users, investors, and employees.

Experiment

A survey instrument was developed in Qualtrics. We developed the scale for perceived presence and beliefs related to specific disclosure items based on Rosenthal (1971) and Song and Zahedi (2005). Intention items were adapted from Alniacik et al. (2011) and Rana et al. (2017). Perceived seriousness of news, trust propensity and ability-based trust beliefs, and overall trust items were adapted from Bansal and Zahedi (2015). Privacy concern items were adapted from (Malhotra et al., 2004). We identified four specific disclosure elements: date, time, location, and entity, based on suggestions made by Rosenthal (1971) and (Hope et al., 2016). The study was conducted online, and data was gathered from subjects solicited through Amazon Mechanical Turk (MTurk). Data collected through MTurk has been shown to possess high reliability and validity (Hibbeln et al., 2017). After removing incomplete and respondents who failed attention checks, we had three hundred and nine usable responses. There were 193 males and 115 females in the final sample. One person chose the other as gender. The average age of the respondents is shown in Table 1 below. We examined the discriminant and convergent validity (see Table A1 in Appendix) and reliability and found no major issues. VIF for the combined high and low PC data was less than 3, indicating common method variance is probably not a concern. The data were analyzed using Smart PLS (Ringle et al., 2015).

Gender	Average age	Std dev	N
Male	37.326	10.703	193
Female	39.417	12.335	115
Other	26.000	-	1

Table 1. Demographics

We examined H1~H4 using pooled data (combined data from high and low PC groups). In contrast, for analyzing moderating hypotheses H5 and H6, we partitioned our data into two groups – high and low PC using the median approach. We computed the median of the PC construct by first summing the four PC items from each subdimension collection, secondary use, unauthorized access, and error. The moderating hypotheses (H5 and H6) were then examined using a multi-group analysis approach in SmartPLS.

Results

All the hypotheses were examined using the bootstrap algorithm in SmartPLS, H1~H4 were examined using direct paths, while H5 and H6 were examined using multi-group analysis of the specific-indirect paths. The perceived presence of specific disclosure elements explains 17.9% of the variance in belief about the perceived specificity of disclosure. The model explains 17.8% of the variance in the drop-in ability-based trust in protecting data. R square for intentions is 49.3%, 49.3%, and 48.7% for users, investors, and

employee groups. The results of H1~H4 are shown in Figure 2, while the results of H5 and H6 are shown in Table 3 and discussed below. All the direct hypotheses H1~H4 and moderation hypotheses H5 and H6 were supported. Direct hypotheses H1~H4 had strong support, as shown in Figure 3 below. The moderation hypothesis H5 had partial support as it was supported only by structural moderation, where the path is significant in one group and not significant in the other. In contrast, the second moderation hypothesis H6 was supported by both structural moderation and stringent multi-group moderation (see Table 2 below).

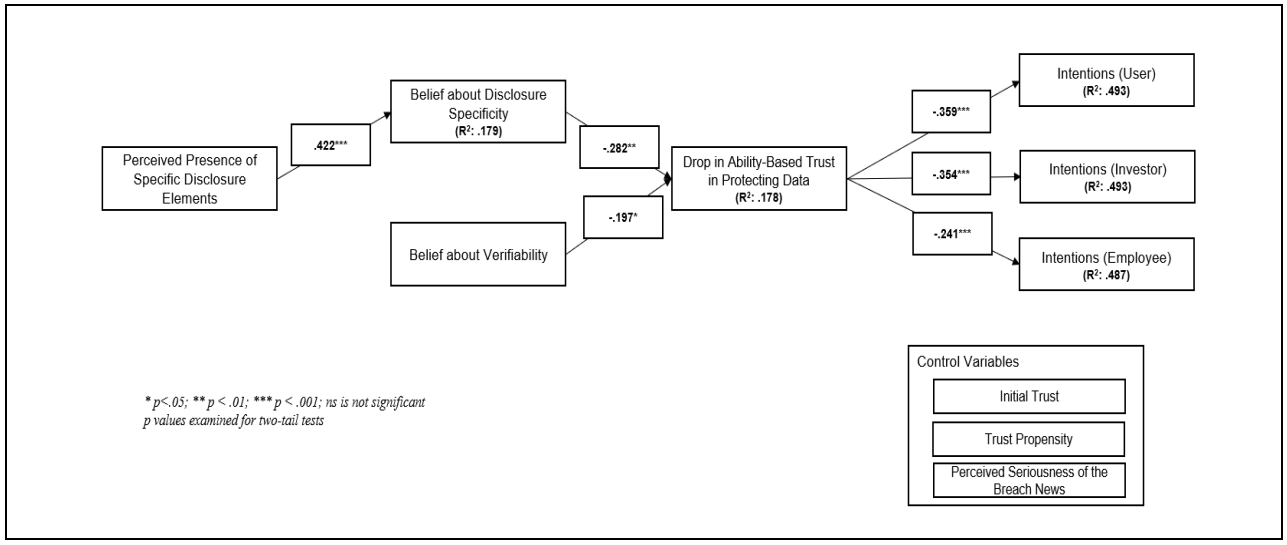

Figure 2. Results for H1~H4

Figure 3 helps explain the H5 and H6 results better and shows that DAT to intentions path is significant for high and low PC stakeholders. However, the relationship between BDS, VRF, and DAT is moderated by the degree of PC. High PC individuals are influenced by beliefs about verifiability, whereas low PC individuals are impacted more by BDS. The analysis of the control variables and paths shows a very interesting pattern. Figure 3 shows that the impact of verifiability on DAT is moderated by PC. However, irrespective of PC level, verifiability impacts intentions for all three stakeholder groups – users, investors, and employees (see Table 3) equally.

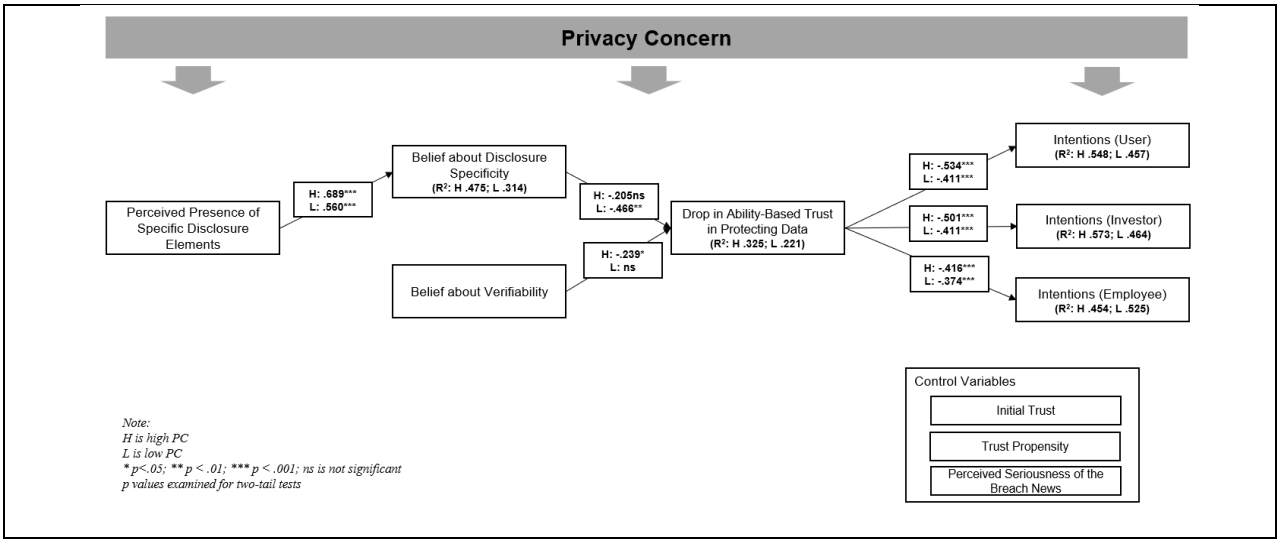

Figure 3. Post hoc Results in Support for H5 and H6

Hyp #	Indirect path	High PC			Low PC			Remarks
		Path	T	Sig	Path	T	Sig	
H5	PE -> BPSD -> DAT -> USRINT	.076	1.66	.097 (ns)	.11	**1.91**†	.056	Structural moderation supported (two-tail p values)
	PE -> BPSD -> DAT -> INVINT	.071	1.65	.100 (ns)	.10	**1.95**†	.052	
	PE -> BPSD -> DAT -> EMPINT	.059	1.69	.092 (ns)	.10	**2.03***	.043	
H6	VRF -> DAT -> USRINT	.128	**2.27***	.024	-.07	.82 (ns)	.415	Structural moderation supported for all three stakeholder groups; whereas multi-group comparison p values for different stakeholder groups are- users: .038*; investors: .041*, and employees: .056† (two-tail p values)
	VRF -> DAT -> INVINT	.120	**2.14***	.033	-.07	.85 (ns)	.398	
	VRF -> DAT -> EMPINT	.100	**2.16***	.032	-.07	.87 (ns)	.384	

Table 2. Results of PC Moderation for H5 and H6

Note: DAT is drop in ability-based trust in protecting data; EMPINT: intentions (employees); USERINT: intentions (users); INVINT: intentions (investors); PC: privacy concern; PE: the perceived presence of specific disclosure elements; BDS: belief about disclosure specificity; VRF: belief about verifiability; † p < .10; * *p< .05; ** p < .01; *** p < .001; ns: not significant; significant paths are highlighted in bold (two tail p-values were examined).*

Path	High PC			Low PC		
	Path Coeff.	T stat.	Sig.	Path Coeff.	T stat.	Sig.
Trust1 -> DAT	0.155	1.396	'ns	-0.011	0.078	'ns
Serious -> DAT	0.232	1.066	'ns	0.340	2.539	*
TRPR -> DAT	-0.306	2.761	**	-0.132	0.923	'ns
VRF -> USRINT	0.357	5.012	***	0.515	5.594	***
VRF -> INVINT	0.417	5.552	***	0.532	6.838	***
VRF -> EMPINT	0.402	4.274	***	0.601	11.087	***

Table 3. Control Variables (two-tail p-value were examined)

Note: DAT is drop in ability-based trust in protecting data; EMPINT: intentions (employees); USERINT: intentions (users); INVINT: intentions (investors); VRF: belief about verifiability; Trust1: Initial Overall Trust; † p < .10* *p< .05; ** p < .01; *** p < .001;* ns: not significant (*two tail p-values were examined).*

Discussion and Conclusion

The results confirm the hypotheses and provide several theoretical and practical implications. This research has four significant theoretical implications. First, a significant contribution of this research has been to demonstrate that in the context of a data breach, the trust violation negatively impacts the behavioral intentions for all three stakeholders – users, investors, and employees. The findings align with the argument that in the information age, stakeholders are increasingly interconnected, where a company's actions toward one stakeholder can impact members of the stakeholder ecosystem (Crane, 2020). Second, our conceptual model and supporting results help reestablish PC as the 'involvement' factor that shapes the elaboration likelihood in the context of rebuilding trust after a data breach. The findings show that beliefs about perceived specificity of disclosure elements and verifiability have a differential effect on trusting beliefs and intentions, moderated by one's degree of PC. The findings (H6) show that high PC individuals rely on verifiability, whereas low PC individuals rely on belief about perceived specificity of disclosure elements to develop trusting attitudes and intentions. And these findings hold for all three stakeholder groups – users, investors, and employees. Thus, this research makes novel contributions by extending ELM and showing that verifiability can work as a *central argument*, and beliefs about perceived specificity of disclosure elements can work as *peripheral cues*. Third, our findings also add to disclosure literature by demonstrating that the role of verifiability and specific disclosure in generating trust or credibility is dependent on individual traits of PC. Fourth, the research findings also contribute to the trust and disclosure literature. The findings provide evidence that the *perceived presence* of specificity of risk disclosure elements (namely, date, size of the breach, type of information stolen, and business location) is important in developing beliefs regarding the perceived specificity of the disclosures. Future research can apply these findings in other contexts and other types of information and specific disclosures.

The study supports the SEC's call to promote quality cybersecurity risk disclosures to restore credibility and trust by increasing transparency following a data breach. The study guides website managers by giving them practical guidance about the importance of being transparent and providing verifiable specific disclosure – as the presence of specific disclosure elements will help low PC stakeholders more. In contrast, the verifiability of the specific disclosure elements will help mitigate trust violations with high PC stakeholders more. It also shows how the websites handle the user information matters not only for users but also for investors and, more importantly, for employees.

References

Adams, D. 2020. "Data Breaches Cause Stress for Employees at Affected Companies," available at https://www.techrepublic.com/article/data-breaches-cause-stress-for-employees-at-affected-companies/ (last accesssed Feb 6, 2022).

Ali, S. E. A., Lai, F.-W., Hassan, R., and Shad, M. K. 2021. "The Long-Run Impact of Information Security Breach Announcements on Investors' Confidence: The Context of Efficient Market Hypothesis," *Sustainability* (13), pp. 1-27.

Alniacik, U., Alniacik, E., and Genc, N. 2011. "How Corporate Social Responsibility Information Influences Stakeholders' Intentions," *Corporate Social Responsibility and Environmental Management* (18:4), pp. 234-245.

Angst, C., and Agarwal, R. 2009. "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion," *MIS Quarterly* (33:2), pp. 339-370.

Bansal, G., and Warkentin, M. 2021. "Do You Still Trust?: The Role of Age, Gender, and Privacy Concern on Trust after Insider Data Breaches," *The DATA BASE for Advances in Information Systems* (52:4), pp. 9-44.

Bansal, G., Zahedi, F., and Gefen, D. 2015. "The Role of Privacy Assurance Mechanisms in Building Trust and the Moderating Role of Privacy Concern," *European Journal of Information Systems* (24:6), pp. 624-644.

Bansal, G., and Zahedi, F. M. 2015. "Trust Violation and Repair: The Information Privacy Perspective," *Decision Support Systems* (71), pp. 62-77.

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

Burt, A. 2019. "Cybersecurity Is Putting Customer Trust at the Center of Competition " *Harvard Business Review*, available at https://hbr.org/2019/03/cybersecurity-is-putting-customer-trust-at-the-center-of-competition (last accessed Feb 5, 2022).

Cannon, J. N., Denison, C. A., & Watanabe, O. V. 2021. "Do Detail and Its Verifiability Serve as Indicators of Strategy Effectiveness and as Sources of Credibility in Voluntary Qualitative Disclosure?," *Journal of Accounting, Auditing & Finance* (36:3), pp. 557-584.

Cheng, X., and Walton, S. 2019. "Do Nonprofessional Investors Care About How and When Data Breaches Are Disclosed?," *Journal of Information Systems* (33:3), pp. 163-182.

Collins, C. J., and Martinez-Moreno, J. E. 2021. "Recruitment Brand Equity for Unknown Employers: Examining the Effects of Recruitment Message Claim Verifiability and Credibility on Job Pursuit Intentions," *Human Resource Management*, pp. 1-13.

Conger, J. A. 1998. "The Necessary Art of Persuasion," *Harvard Business Review* (76), pp. 84-97.

Coombs, W. T. 2014. "State of Crisis Communication: Evidence and the Bleeding Edge," *Research Journal of the Institute for Public Relations* (1:1), pp. 1-12.

Crane, B. 2020. "Revisiting Who, When, and Why Stakeholders Matter: Trust and Stakeholder Connectedness," *Business & Society* (59:2), pp. 263-286.

Curtis, S. R., Carre, J. R., and Jones, D. N. 2018. "Consumer Security Behaviors and Trust Following a Data Breach," *Managerial Auditing Journal* (33:4), pp. 425-435.

Farrell, P. 2017. "Data Breaches Undermine Trust in Government's Ability to Protect Our Information," available at https://www.theguardian.com/australia-news/2017/jul/08/data-breaches-undermine-trust-in-governments-ability-to-protect-our-information (last accessed Feb 5, 2022).

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.

Gu, J., Xu, Y. C., Xu, H., Zhang, C., and Ling, H. 2017. "Privacy Concerns for Mobile App Download: An Elaboration Likelihood Model Perspective," *Decision Support Systems* (94), pp. 19-28.

Hibbeln, M., Jenkins, J. L., Schneider, C., Valacich, J. S., and Weinmann, M. 2017. "How Is Your User Feeling? Inferring Emotion through Human-Computer Interaction Devices," *MIS Quarterly* (41:1), pp. 1-21.

Hope, O.-K., Hu, D., and Lu, H. 2016. "The Benefits of Specific Risk-Factor Disclosures," *Review of Accounting Studies* (21:4), pp. 1005-1045.

Ibrahim, N., Shiratuddin, M. F., and Wong, K. W. 2013. "A Dual-Route Concept of Persuasive User Interface (UI) Design," *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*: IEEE, pp. 422-427.

Kelton, A. S., and Pennington, R. R. 2020. "If You Tweet, They Will Follow: CEO Tweets, Social Capital, and Investor Say-on-Pay Judgments," *Journal of Information Systems* (34:1), pp. 105-122.

Lowry, P. B., Moody, G., Vance, A., Jensen, M., Jenkins, J., and Wells, T. 2012. "Using an Elaboration Likelihood Approach to Better Understand the Persuasiveness of Website Privacy Assurance Cues for Online Consumers," *Journal of the American Society for Information Science and Technology* (63:4), pp. 755-776.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Internet Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336-355.

Mayer, R. C., Davis, J. H., and Schoorman, F. D. 1995. "An Integrative Model of Organizational Trust," *Academy of Management Review* (20:3), pp. 709-734.

Petty, R. E., Cocioppo, J. T., and Goldman, R. 1981. "Personal Inolvement as a Determinant of Argument-Based Persuasion," *Journal of Personality and Social Psychology* (41:5), pp. 847-855.

Racherla, P., Mandviwalla, M., and Connolly, D. J. 2012. "Factors Affecting Consumers' Trust in Online Product Reviews," *Journal of Consumer Behaviour* (11:2), pp. 94-104.

Rana, N. P., Dwivedi, Y. K., Lal, B., Williams, M. D., and Clement, M. 2017. "Citizens' Adoption of an Electronic Government System: Towards a Unified View," *Information Systems Frontiers* (19:3), pp. 549-568.

Ringle, C. M., Wende, S., and Becker, J. 2015. *Smartpls 3*. SmartPLS GmbH, Bönningstedt, Germany.

Rosenthal, P. I. 1971. "Specificity, Verifiability, and Message Credibility," *Quarterly Journal of Speech* (57:4), pp. 393-401.

Sanders, J. 2019. "33% of Executives Don't Trust Their Organization to Protect Employee Data," available at https://www.techrepublic.com/article/33-of-executives-dont-trust-their-organization-to-protect-employee-data/ (last accesssed Feb 6, 2022).

SEC. 2018. "Commission Statement and Guidance on Public Company Cybersecurity Disclosures," available at https://www.sec.gov/rules/interp/2018/33-10459.pdf (last accesssed Feb 6, 2022).

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.

Spence, P. R., Lin, X., Lachlan, K. A., & Hutter, E. . 2020. "Listen up, I've Done This Before: The Impact of Self-Disclosure on Source Credibility and Risk Message Responses," *Progress in Disaster Science* (7), pp. 1-6.

Wells, J. D., Valacich, J. S., and Hess, T. J. 2011. "What Signal Are You Sending? How Website Quality Influences Perceptions of Product Quality and Purchase Intentions," *MIS Quarterly* (35:2), pp. 373-396.

Zhou, T. 2017. "Understanding Location-Based Services Users' Privacy Concern: An Elaboration Likelihood Model Perspective," *Internet Research* (27:3), pp. 506-519.

Appendix

	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.
1. DAT	0.68										
2. EMPINT	-0.35	0.82									
3. USERINT	-0.46	0.85	0.86								
4. INVINT	-0.45	0.82	0.92	0.87							
5. PC	0.11	0.19	0.14	0.13	0.76						
6. PE	-0.14	0.30	0.35	0.33	0.08	0.65					
7. Trust	-0.04	0.47	0.42	0.40	0.17	0.15	0.60				
8. BPSD	-0.19	0.67	0.66	0.64	0.37	0.42	0.40	0.83			
9. Serious	0.16	0.36	0.23	0.20	0.46	0.09	0.34	0.57	0.74		
10. TRPR	-0.16	0.70	0.65	0.63	0.33	0.28	0.42	0.62	0.46	0.77	
11. VRF	-0.18	0.66	0.61	0.61	0.32	0.20	0.43	0.67	0.54	0.61	0.76

Table A1. Construct Correlations and Square-root of AVE

Note: DAT: drop in ability-based trust in protecting data; EMPINT: intentions (employees); USERINT: intentions (users); INVINT: intentions (investors); PE: the perceived presence of specific disclosure elements; Trust: initial trust; BDS: belief about disclosure specificity; Serious: perceived seriousness of breach news; TRPR: trust propensity; VRF: belief about verifiability. Cells highlighted in gray: Constructs are parallel dependent constructs, and hence high correlations are acceptable.