SECURITY BREACHES AND ORGANIZATION RESPONSE STRATEGY: EXPLORING CONSUMERS' THREAT AND COPING APPRAISALS

ABSTRACT

We address a long-standing lacuna in the Information Management literature on the relationships among security breaches, organization response strategy as well as consumers' threat and coping appraisal. Security breaches can involve the leak of sensitive data, and potentially lead to negative consumer reactions. It is, thus, timely and critical to theorize and empirically investigate the ways in which organization can respond effectively to security breaches and how consumers' threat and coping appraisals vary according to the different response strategies. Our study addresses this lacuna by developing a conceptual model of i) security breach, ii) organization response strategies, and iii) consumer appraisal, grounded on the risk theory and protection motivation theory. We use the principal and agent perspectives to portray the breached organization as the agent providing the coping strategy, and consumers as the principal actors who evaluate the strategy. We incorporated a vignette-based survey to test the model with empirical data. We identify that the variations in the response strategy of organization after a security breach can lead to significantly different consumers' reactions. We discuss the implications of our findings for theory and practice and delineate an agenda for future research.

Keywords: *security breach, organization response strategy (ORS), protection motivation theory (PMT), perceived risk, corporate reputation, intention to re-transact*

1. Introduction

The exposure of confidential information or privacy-sensitive data during security breach incidents can result in serious losses to both consumers (e.g., Ayaburi & Treku, 2020; Ioannou et al., 2020) and organizations (e.g., Ioannou et al., 2020). Organizations exposed to breach incidents usually take different actions against the incidents with the aim to recover from and to control damages of the breach incidents (Gwebu et al., 2018). In line with the recent trend of information management (IM) research on privacy and security (e.g., Angelopoulos et al., 2021; Stacey et al., 2021), scholars increasingly show interest in investigating organizations' effective post-breach recovery or damage control strategies since complete security breach prevention is practically infeasible (Gwebu et al., 2018). Whereas previous studies on organizations' post-breach actions have recognized that organization response strategy (ORS) matters in general (Bansal and Zahedi, 2015; Choi et al., 2016), the ways in which an ORS and consumers' perceptions regarding a focal security breach incident jointly affect consumers' post-breach reactions remains a black box. Thus, we aim to contribute to the literature on organizations' post-breach response strategies by theorizing and empirically investigating the ways in which organizations can effectively respond to security breach incidents, as well as how consumers' threat and coping appraisals vary according to these different response strategies.

The literature on individuals' volitional coping behaviors when facing IT security threats demonstrates that the threat appraisal and coping appraisal responses emerge automatically (Liang et al., 2019). The threat appraisal itself motivates individuals to take actions against the security threat (Chakraborty et al., 2016; Rogers, 1975). Combining the literature on individuals' volitional coping behaviors against IT security threats with the research on organizations' post-breach response strategies, we maintain that consumers' post-breach reactions are likely to be a function of both the attributes of ORS and consumers' threat

and coping appraisals against the security breach incidents. However, such integration, to the best of our knowledge, has not been sufficiently theorized. To fill this research gap, we aim to answer the following research question: *How do organizations' post-breach response strategy and security breach incidents jointly affect consumers' threat and coping appraisals and thus their post-breach reactions, such as the re-transaction intentions?*

We ground our work on the protection motivation theory (PMT). PMT is widely used to understand threat appeals, and how an individual copes with them (Rogers, 1983). PMT theorizes individuals' cognitive and behavioral processes to manage a focal threat. The PMT model consists of two cognitive mediating processes: the threat appraisal and the coping appraisal (Anderson & Agarwal, 2010; Floyd et al., 2000; Li et al., 2019; Rogers, 1983). The PMT model has been widely used in studies on individuals' volitional coping behaviors against the IT security threats (Li et al., 2019; Liang et al., 2019; Menard et al., 2017; Vedadi & Warkentin, 2020). However, its usage in the literature on organizations' post-breach response strategies is still rare, though highly relevant. By answering our research question, we also attempt to theoretically extend the PMT model in two ways: i) focusing on the perceived vulnerability in the threat appraisal process, in which a threat leads to various risks with some risk dimensions that might be more relevant to a security breach than others and thus perceived vulnerability should be formally conceptualized and operationalized as a multidimensional construct associating with different types of risks; ii) focusing on the response efficacy in the coping appraisal process, we argue that actors who appraise the threats may evaluate the response efficacy of the coping mechanisms taken by the external agents, especially when such mechanisms are critical yet unavailable to the actors. In our context, that means consumers (i.e., consumers as the principal) implicitly delegate to the agent (i.e., the breached organization) the duty to protect them from further losses due to the focal and any potential security breach events (Poddar et al., 2009). Thus, consumers evaluate the response efficacy of

coping actions taken by the breached organization, forming a typical principal-agent perspective (Pavlou, et al., 2007). We argue that these two appraisal processes ultimately affect customers' re-transaction intention with the breached web shop. To validate the proposed conceptual model, we incorporate a vignette-based approach with variations of security breach types and organizations' response strategies and collect survey data from Amazon Mechanical Turk (AMT) for the empirical tests.

Our findings demonstrate how the response strategies of organizations following a security breach incident affect consumers' evaluation of the situation, the way organizations conduct business, and the potential ramifications for failing to adequately protect sensitive data. By conceptualizing the impact of security breach incidents and the ORS on consumers' evaluation of risk severity, and response efficacy, and subsequently their intention to re-transact with the breached organization, we identify that the variations in the response strategy of organizations after a security breach incident can lead to different reactions from consumers. We show that only the financial and privacy risks are influential determinants of consumers' intention to re-transact after a security breach incident, which provides for interesting explanations that deviate from the existing literature and suggest that consumers do not give equal weight to the risk dimensions. Furthermore, using the principal-agent perspective of the PMT model to conceptualize the overall threats and coping appraisal open the black box of consumers' assessment of security breach and organizations' response strategies. Our study, therefore, brings novel insights on the topic, has important implications for both theory and practice, and can provide a springboard for future investigation in this domain, and broadly contribute to IM research (c.f. Struijk et al., 2022) on the implications of technology, security and privacy to organizations and users.

The rest of this paper is organized as follows. In the next section, we provide the theoretical background of our study on security breaches and consumer perceptions of risk in

e-commerce. This is followed by the hypothesis development section, where we introduce our models and hypotheses based on PMT. After that, we describe the vignette and survey methodology of our study, followed by the data analysis. Finally, we discuss our key findings, implications, and contributions, and delineate an agenda for future research on the topic.

2. Theoretical Background

Our literature review focused on the relevant academic outlets in the field, specifically the *International Journal of Information Management* and the "senior scholars' basket of eight" journals from the Association for Information Systems'.[1] The choice of these nine journals is attributed to their well-recognized leadership role in the IS/IM field with leading impact factors and article influence scores. These journals also have the reputation for topical, methodological, and geographical diversity and more importantly intellectual depth. As a result, the theoretical and practical rigor and relevance of articles published in these nine journals provide a solid foundation for us to conduct the literature review. Procedurally, we first identified within these 9 journals all papers with the keywords "security", "breach" or "security breach", coming up with 362 papers. Subsequently, each paper was manually scanned with a focus on its research topic and theory by two of the authors independently, and all papers were labelled as either relevant or irrelevant to our study. For example, papers that focused on asset security rather than cyber security were labelled as irrelevant. Finally, 65 papers were identified as relevant to our study and were further examined.[2]

2.1 Security Breach and Information Security Management

Whilst leveraging information systems can facilitate the exchange of enormous amounts of information, products, and services (Dwivedi et al., 2020), it increasingly exposes

[1] MIS Quarterly, Information Systems Research, Journal of Management Information Systems, Journal of Strategic Information Systems, Journal of AIS, European Journal of Information Systems, Journal of Information Technology, and Information Systems Journal.

[2] These papers are listed in Supplementary Material I for review.

organizations to risks that their information systems fail to protect themselves against different kinds of damages or losses due to security breaches (Straub & Welke, 1998; Chan & Janjarasjit, 2019). Security breaches, caused by either insiders (e.g., employees) or outsiders (e.g., hackers), can lead to the leakage of sensitive data such as corporate secrets or confidential consumer information and can negatively affect both the organization and its consumers (Angelopoulos et al., 2021). Software source code can be modified, services can be purposefully interrupted, and data can be deleted or stolen. When hackers obtain personal data, organizations may face lawsuits, governmental sanctions, and potential loss of their competitive position (Choi et al., 2016; Ioannou et al., 2020).

Security breaches can vary, but the most common categories include the distributed denial-of-service (DoS) attack, virus attack, and theft of information (Table 1) any of which can result in significant losses to organizations and users (Kumar et al., 2008; Yayla & Hu 2011). Among the types of security breaches, DoS attacks have the greatest impact on organizations that conduct business over the Internet (Ettredge & Richardson, 2002). While DoS attacks can significantly influence the cumulative abnormal returns of organizations in the stock market, unauthorized access, and other security attacks such as virus attacks have no influence (Hovav & D'Arcy 2003; Yayla & Hu, 2011).

Security Breach Category	**Descriptions**
Denial of service (DoS)	In DoS attacks, the attacker sends large number of information requests to the web servers of the target organization. The purpose of this attack is to overload the web servers and make the websites unavailable for legitimate use.
Virus attack	In these attacks, the attacker gains access to the host program via a program. When the program is executed, the attacker can alter the website with a message, logo or inappropriate material, or delete all the files and completely shut down the website.
Theft of Information	In these attacks, unauthorized individuals gain access to customer data. Depending on the target organization, the customer data can be names, addresses, birthdates, credit card details, social security numbers, medical records, online purchasing behavior, etc. These types of attacks are mostly considered as breach of confidentiality.

Table 1. Most Common Security Breaches Based on Yayla & Hu (2011) and Kumar et al. (2008)

Multiple studies have explored the financial impact of security breach announcements on the stock market to provide policy makers and risk managers with accurate measures of the financial impact of security breaches but returned with mixed results (Appendix 1). Along with these studies on the stock market reactions towards the security breach events, how to systematically manage the information security has aroused the interest of many information systems scholars. Nowadays, the information security management has become one of the most extensively investigated topics in information system control literature (Cram et al., 2016). Scholars have studied various aspects in information security management (Sommro et al., 2016), such as developing and implementing an information security policy, human aspects of information security management, and post-breach management.

2.2 Organizations' Post-Breach Response Strategies

Partly because of the difficulties in developing, implementing, and executing effective information security policies, and partly because of the inevitable "unforeseen holes" (Choi et al., 2016, p.905) in daily information security management, complete security breach prevention is practically infeasible (Gwebu et al., 2018). Therefore, the other stream of literature pays the attention to investigate organizations' effective post-breach recovery or damage control strategies.

Focusing on what attributes good response strategies should have, on the one hand, some studies adopt the lens of justice and argue that the perceived fairness of organizations' post-breach responses could recover service failure (Bansal and Zahedi, 2015; Choi et al., 2016). For example, one study suggests that response strategies that facilitate distributive, procedural and interactional justice positively affect consumers' word of mouth and likelihood of switching (Choi et al., 2016). On the other hand, some studies maintain that effective response strategies help consumers reduce their cognitive dissonance based on the argument that individuals avoid the cognitive dissonance (Goode et al., 2017; Gwebu et al., 2018). In

terms of the compensation as a post-breach recovery tool, any discrepancy between consumers' expected compensation and experienced compensation will negatively affect consumer repurchase intentions (Goode et al., 2017). Considering that corporate reputation (CR) and negative opinions towards a security breach event create a natural cognitive dissonance, it is found that response strategies' effectiveness vary depending on CR (Gwebu et al., 2018). Specifically, if organizations have high reputation, response strategies can appear less relevant to their post-breach stock market performance. On the contrary, for less reputable organizations, moderate response strategies and image renewal response strategies can effectively alleviate the negative post-breach stock market reactions (ibid.).

Whereas studies on organizations' post-breach response strategies have made admirable efforts in investigating the desired attributes good response strategies should have, consumers' threat appraisal and coping appraisal regarding the security breach event itself are largely overlooked. On the contrary, the literature on individuals' volitional coping behaviors against the IT security threats emphasizes that facing an unpleasant situation, individuals' threat appraisal and coping appraisal against the situation emerge automatically (Liang et al., 2019), and that the threat appraisal itself will motivate individuals to take actions against the situation (Rogers, 1975; Chakraborty et al., 2016).

Combining the literature on individuals' volitional coping behaviors against the IT security threats with the literature on organizations' post-breach response strategies, we argue that consumers' post-breach reactions are likely to be a function of both the attributes of ORS and consumers' appraisals regarding the security breach event itself. However, such integration, to the best of our knowledge, has not been sufficiently theorized despite its both conceptual and practical importance in the IT security breach domain. To fill this research gap, we aim to study how organizations' post-breach responses and security breach incidents jointly affect consumers' appraisals, which, in turn, affect consumers' post-breach reactions, such as

the re-transaction intentions. To achieve our purpose, we extend the PMT in two ways, as explained below.

2.3 Protective Motivation Theory (PMT)

PMT theorizes individuals' cognitive and behavioral processes to manage a focal threat (Rogers, 1983). The model consists of two cognitive mediating processes: the threat appraisal and the coping appraisal (Rogers, 1983; Floyd et al., 2000; Anderson & Agarwal, 2010; Li et al., 2019). Whereas the threat appraisal process stresses that the perceived threat and a desire to avoid the potential losses associated with the threat trigger the motivation toward protection (Menard et al., 2017), the coping appraisal refers to individuals' assessment over the available coping mechanisms against the focal threat. Specifically, the threat appraisal includes perceived vulnerability and perceived severity when individuals face a certain threat. Perceived vulnerability refers to one's likelihood of being exposed to a threat. Perceived severity stresses the impact of the potential consequences related to the threat, stressing the level of the threat. Together, the two factors drive individuals to take actions to cope with the perceived threat (Vance et al., 2014). In the coping appraisal, three more factors to consider are response efficacy, response costs and self-efficacy. Whereas response efficacy refers to individuals' evaluation on the effectiveness of the coping mechanism, self-efficacy reflects individuals' perceived ability to conduct the available coping mechanism. Together, the perceived efficacy will increase the likelihood of adopting the available coping mechanism. However, the perceived extrinsic or intrinsic personal costs of performing the coping mechanism (i.e., response costs) will decrease the likelihood of adopting the available coping mechanism (Lee & Larsen, 2009).

The threat appraisal and the coping appraisal together determine individuals' behavioral intention, which is the typical dependent variable in PMT research. Underlying the threat appraisal is the trade-off between rewards associated with undertaking the protection activities

and the potential losses of not doing so. The coping appraisal is associated with the cost-benefit analysis of taking certain coping mechanisms (Vedadi & Warkentin, 2020). Thus, PMT provides a good framework to understand individuals' behavioral intention or to persuade individuals to follow certain recommendations (Floyd et al., 2000). In the literature on individuals' volitional coping behaviors against IT security threats, PMT has been used to understand employees' information security policy (ISP) compliance (Herath & Rao, 2009; Menard et al., 2017; Johnston et al., 2015; Li et al., 2019), ISP violations (D'Arcy et al., 2014; Johnston et al., 2016), executives' decision of anti-malware software adoption (Lee & Larsen, 2009), individuals' continuance intention of using certain security solution (Vedadi & Warkentin, 2020), and computer users' security behaviors (Anderson & Agarwal, 2010; Liang et al., 2019).

Before utilizing PMT to understand how security breaches and ORS jointly affect consumers' threat and coping appraisal toward the re-transaction intention, it is important to extend the original PMT model in two ways. Firstly, focusing on the perceived vulnerability in the threat appraisal of the PMT model, previous studies typically argue the perceived vulnerability as reflecting one's perceived likelihood of exposing to a focal threat, e.g., password being breached (Menard et al., 2017). However, the security breach may lead to different types of losses and thus is associated with various risks. Inspired by the risk literature, we argue that the perceived vulnerability suits to be formally conceptualized and operationalized as a multidimensional construct associating with different types of risks. Specifically, in line with previous risk studies, we focus on financial risk, performance risk, social risk, time risk, psychological risk, and privacy risk (Almousa, 2011; Bertea, 2015; Ariffin et al, 2018). We explain the key concepts in Table 2 and more details in Appendix 2.

Risk Dimensions	Descriptions
Financial risk	Financial risk is "the potential monetary outlay associated with the initial purchase price as well as the subsequent maintenance cost of the product" (Grewal *et al*., 1994). This definition is currently expanded with financial loss occurring due to fraud (Featherman & Pavlou, 2003). So, financial risk is the potential monetary loss consumers may experience after buying a product or service.
Privacy risk	Privacy risk is the probable loss of control over personal information, for instance when data is used without data subject's awareness or approval. Identity theft in general is a severe example of privacy loss where criminals use the victim's identity to perform fraudulent transactions. Privacy was found relevant by Featherman and Pavlou (2003) and Jarvenpaa and Todd (1997).
Performance risk	Performance risk is the potential loss that will occur due to the failure of a product to perform as expected (Mitchell, 1999). Performance risk addresses the circumstance of the product to be bought and 'the possibility of the product malfunctioning and not performing as it was designed and advertised and therefore failing to deliver the desired benefits' (Grewal *et al*., 1994).
Time risk	Time risk is defined as the time that consumers face losing when making a bad purchase decision by wasting time on searching and making the purchase, learning how a product works or needing to use support when the product does not function as predicted (Featherman & Pavlou, 2003).
Psychological risk	Psychological risk is the risk that the consumer's peace of mind or self-perception will be disturbed negatively by the performance of the e-commerce merchant or the product (Mitchell, 1999). It is the potential loss of self-esteem stemming from the failure to not achieve the buying of the intentioned product or service. Psychological risk captures the chance that the selected product will not match with the buyers' self-image.
Social risk	Social risk is the final aspect of risk (Cunningham, 1967) and constitutes the potential risk of losing a certain status in one's social group as a result of buying a product or service (Featherman & Pavlou, 2003). So social risk is associated with perceptions that others have towards the product that is bought. For instance, it could make the buyer look foolish or untrendy.

Table 2. A Summary of Risk Dimensions Based on the Literature

Secondly, focusing on the response efficacy in the coping appraisal of the PMT, the original model assumes that actors who appraise the threats evaluate their response efficacy on the coping actions available to them (Rogers, 1975; Vishwanath et al., 2018). We term this as the unitary actor perspective. Facing a security breach event, individuals can certainly take some problem-focused coping actions against the security breach event. For example, studies show that individuals may alleviate their concerns over the security breach by actively monitoring their bank transactions (Chakraborty et al., 2016; Aivazpour et al., 2018). However, systematic post-breach management is critical in preventing the organization from future possible security breach events. Such complex coping actions can only be taken by the organization rather than individuals such as consumers (Gwebu et al., 2018). Organizations may take different coping actions and these coping actions are typically reflected by their post-

breach response strategies. Focusing on varied ORS, in our study, we argue that consumers implicitly delegate an organization the duties to protect them from further losses due to the focal and any potential security breach events (Poddar et al., 2009). Losses include such as losses of personal or monetary information (in the case of theft of information security breach) or service failure (in the case of DoS security breach). Following Pavlou et al. (2007), we label this understanding as the *principal-agent perspective* of PMT, proposing that in the coping appraisal processes, individuals evaluate the response efficacy of the coping mechanisms taken by the external agents, especially when such mechanisms are critical yet unavailable to the individuals. The understanding is in line with the psychological contract theory, "specifically, the psychological contract perspective posits that social exchange partners establish a contract, which can be developed explicitly or implicitly, to delineate obligations between partners in the exchange (Choi et al., 2016, p.910)". Below we use this principal-agent perspective of PMT to further develop the hypotheses.

3. Hypothesis Development

PMT allows us to model the individual's responses to threat and protective actions via a threat appraisal and coping appraisal process (Floyd et al., 2000; Anderson & Agarwal, 2010). Whereas the PMT model is widely used in studies on individuals' volitional coping behaviors against the IT security threats, we apply the PMT model to study how security breach incidents and organizations' post-breach response strategies jointly affect consumers' threat and coping appraisals, which, in turn, affect consumers' post-breach reactions, such as the re-transaction intentions. To achieve this purpose, we theoretically extend the original PMT model in two ways. Firstly, by focusing on the perceived vulnerability in the threat appraisal process, we argue that a threat leads to various risks with some risk dimensions that might be more relevant to a security breach than others. As a result, perceived vulnerability should be formally conceptualized and operationalized as a multidimensional construct associated with different

types of risks. Secondly, focusing on the response efficacy in the coping appraisal process, we argue that actors who appraise the threats may evaluate the response efficacy of the coping mechanisms taken by the external agents, especially when such mechanisms are critical yet unavailable to the actors.

In our study, while the focal threat is security breach, covering DoS, virus attack and theft of information (Yayla & Hu, 2011), it may lead to different types of losses and thus is associated with various risks, namely the financial risk, performance risk, social risk, time risk, psychological risk, and privacy risk (Almousa, 2011; Bertea, 2015; Ariffin et al, 2018). We assume that consumers implicitly delegate the organization the duty to protect them from further losses due to the focal and any potential security breach incidents (Poddar et al., 2009) as systematic coping mechanisms against a security breach incident are unavailable to consumers (Gwebu et al., 2018). In our research design, consumers learn the information about the security breach together with the ORS, ranging from defensive strategy, moderate strategy accommodating strategy, and image renewal strategy (Gwebu et al. 2018), supplemented with a fifth baseline strategy, "no response". After that the threat appraisal and coping appraisal are practiced and depending on the security breach types and different response strategies, consumers will react differently in terms of their threat and coping appraisals. We further argue that these PMT constructs are directly relevant to consumers' intention to re-transact after a security breach announcement. Figure 1 captures the proposed model. We justify each of the hypotheses below, starting from the PMT in the theoretical development.

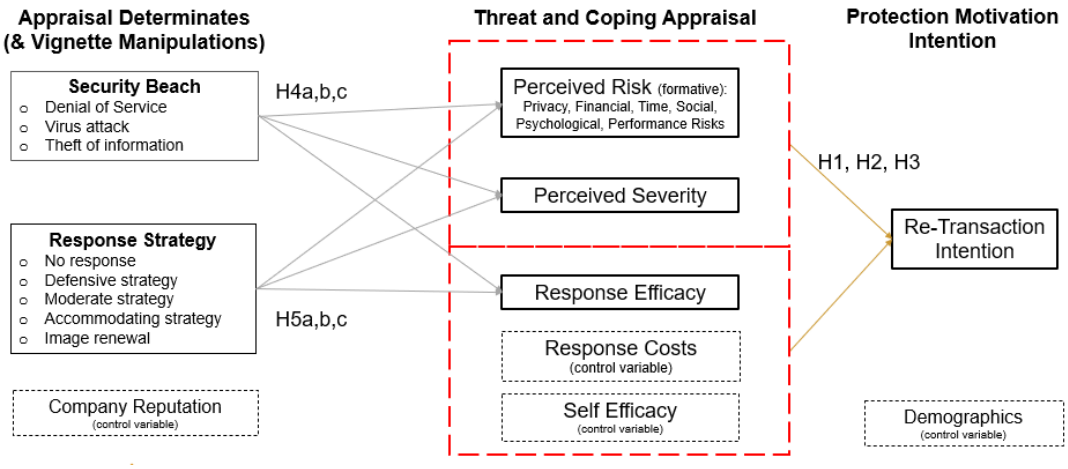

Figure 1. The Proposed Model Based on the PMT

The threat appraisal process includes the evaluation of perceived vulnerability and perceived severity. Perceived vulnerability is one's assessment of the probability of being exposed to a threat, or the perception of experiencing possible negative consequences from performing a risky behaviour (ibid.). In our study, a security breach event represents the focal threat. The threat potentially leads to different losses and thus various risks. Thus, we formally conceptualize the perceived vulnerability as the *perceived risk* (Pavlou, 2003) with some risk dimensions that might be more relevant to a security breach. Individuals who perceive vulnerability (i.e., the perceived risks in our contexts) will likely cope with the breach threat and adapt their behaviour accordingly (Rogers, 1983). Previous studies have related perceived risk to different information security protective actions in organizations (Menard et al., 2017). In our context, we argue that not to further transact with the breached organization is a reasonable reaction of a consumer to deal with the potential threat in information leakage and virus attacks. As we argue below, consumers' threat appraisals also depend on ORS. If all else is equal, in line with the above logic, we argue that a security breach incident, exhibiting various types of risk, can significantly affect consumers' intention to re-transact with the breached organization. Hence, we propose:

H1: *There is a negative relationship between consumers' risk evaluation of an online merchant with a security breach and their intention to re-transact with the breached merchant.*

The second factor in the threat appraisal process is the perceived severity of the breach. The significance of a threat affects individuals' willingness to cope with it and adapt their behaviour accordingly (Rogers, 1983). Whereas perceived risks underscore a consumer's expectancy of exposure of a threat, perceived severity refers to one's fear about the impact of the potential consequences related to a threat, stressing the level of the threat in the focal context. Similar to the aforementioned logic that no remedies means no actions, if a consumer deems the perceived risks to be nothing serious, the consumer will not take any actions against the threat (Rogers, 1983). All else being equal, given various risks potentially associated with a security breach, we argue that as the perceived severity increases, a consumer's intention to re-transact with the breached organization decreases. Therefore, we propose:

H2: *There is a negative relationship between consumers' evaluation of severity of a security breach and their intention to re-transact with the breached merchant.*

In most security breaches, the organization also announces the actions taken against the breaches. As argued above on the principal-agent perspective of PMT, *response efficacy* in this context is the degree to which the individual consumer's belief that the actions taken by the breached organization are effective in alleviating the associating problems. Given the security breach incident and breached ORS, they evaluate whether the response sufficiently mitigates, controls, or compensates for the perceived damage associating with the security breach incident (Anderson & Agarwal, 2010). Suggested by PMT related studies, the efficacy of the focal coping mechanism has a significant positive relationship with the intention to practice proactive behaviours (e.g., Goode et al., 2017; Gwebu et al., 2018), and if the actions taken can address the potential risks associating with the security breach incident, consumers will have a higher chance to restore their confidence to the breached organization. Thus, we argue that all

else being equal, higher perceived response efficacy is associated with higher consumers' intention to re-transact with the breached merchant. In our exploration of how consumers appraise the response strategy of organizations after a security breach, we treat the response costs and self-efficacy as control variables, while we hypothesize that:

H3: *Consumers' positive appraisal of the organization's response efficacy has a positive effect on their intention to re-transact with the breached merchant.*

As mentioned above, we deem the perceived risk as a multidimensional construct with some risk dimensions that might be more relevant to a security breach. The construct includes six dimensions, viz., financial risk, performance risk, social risk, time risk, psychological risk and privacy risk (Almousa, 2011; Bertea, 2015; Ariffin et al, 2018). After a security breach, consumers may be concerned that their personal information (e.g., credit card or bank account data) will be leaked resulting in financial consequences. Also, security breaches might lead to service downtime, and time risk increases when consumers want to shop from an online merchant that is not available. They might search for the product elsewhere or wait until the web shop is back online, which might lead to increased time risk, or the performance of web shop may not match the expected standard. The psychological risk, defined as a consumer's dissatisfaction in choosing a poor service despite having a huge array of choices (Mitchell, 1999), can take place when a shopping goal is not attained (Ariffin et al., 2018) due to the security breach. Consumers might also be concerned about the potential loss of reputation in their social groups (i.e., social risk) due to dissatisfaction of using the breached shopping channel (c.f., Stone & Grønhaug, 1993). Broadly speaking, whereas DoS and virus attacks usually target at damaging organizations' service level, the theft of information aims at organizations' or customers' confidential data. Arguably, depending on their purposes, different types of security breach can lead to different risks. Accordingly, consumers' appraisal of the risk will vary with types of security breach. We thus hypothesize:

H4a: *The type of security breach determines a consumer's appraisal of the risk.*

Although each type of security breach can have different consequences, DoS and virus attacks have a strong negative impact on the presence of web shops (Yayla and Hu, 2011), leading to system outages, and decreased service availability. Such attacks, however, rarely result in loss of confidential data (Yayla & Hu, 2011). Theft of information is often categorized as a breach of confidential information and may result in both intangible and tangible costs. Comparing to DoS and virus attacks, we argue that the theft of information breach triggers consumers to feel the damage is greater (i.e., higher perceived severity) because such information breaches can cause direct losses for consumers. As a result, our next hypothesis is:

H4b: *The type of security breach determines a consumer's appraisal of the severity.*

Whereas in hypothesis 3, we argue that the response efficacy of ORS is positively associated with consumers' re-transaction intention, the level of response efficacy of a specific response strategy perceived by consumers arguably depends on the type of security breach incident as well. For example, no response could be more harmful in the case of the theft of information rather than the case of the DoS. Besides, a perceived proactive and more protective response strategy could be typically seen as more effective. Furthermore, for bigger security breaches, consumers will demand a more effective response from the focal organization and hence, assuming everything else to be equal, more serious, or bigger security breaches will dilute the efficacy of organizations' responses. So, we derive the following hypothesis:

H4c: *The type of security breach determines a consumer's appraisal of the breached organization's response efficacy.*

Returning to organizations' post-breach response strategies, in general, acknowledging a security breach is more effective than denial or no response (Bansal & Zahedi, 2015) in rebuilding consumers' trust. A taxonomy of ORS is outlined by Gwebu et al. (2018), including

defensive, moderate, accommodating, and image renewal. The efficacy of such strategies on stock market performance was examined via an event study. The moderate and image renewal strategies seemed to be more effective than the defensive or accommodating ones, but their effectiveness is subject to CR. We speculate that the accommodating and image renewal strategies are more effective in reducing consumers' concerns and contribute to their appraisal. To the extent that a response strategy suggests the risk mitigation mechanisms (such as files are protected, security measures are used, etc.), consumers' feeling of risks will be reduced because of these security measures are provided by the organization. Consequently, we propose our hypothesis as:

H5a: *An organization's response strategy to handle the security breach determines a consumer's appraisal of the risk.*

Similarly, security measures taken by the organization may also reduce consumers' perception of severity regarding the risks. For example, if the files are protected, consumers may perceive the theft of information attack to be less severe. If the security breach is announced as one single incident where consumers are protected, the perception of the seriousness of the incidents can be managed at a reduced level (c.f. Gwebu et al., 2018). Given a focal security breach, different response strategies signal different capabilities or willingness of organizations to deal with the breach event. We thus argue:

H5b: *An organization's response strategy to handle the security breach determines a consumer's appraisal of the severity.*

Overall, more protective strategies can demonstrate better the efforts of the breached organization, its willingness to invest in handling the security breach incident, its commitment and sincerity to rebuild stakeholder's confidence, and its pledge to avoid similar security breach incidents from happening in the future. Depending on different types of response strategies and

the experienced security breach incident, arguably one's evaluation over the response efficacy also vary. Thus, we have:

H5c: *An organization's response strategy to handle the security breach determines a consumer's appraisal of the breached organization's response efficacy.*

4. Methodology

4.1 Research Design and Measurement

We conducted a vignette-based survey to collect empirical data to test our conceptual model. Vignettes represent simulations of real-life situations (Gould, 1996) in the form of "stories about individuals, situations and structures which can make reference to important points in the study of perceptions, beliefs, and attitudes" (Hughes, 1998; p. 381), where participants are presented with a hypothetical situation and are questioned about their beliefs and perceptions (e.g., Daft et al., 1987; El-Shinnawy & Markus, 1992; Russ et al., 1990). Whilst vignettes are not commonly used in IS studies (but see Couger, 1989; Dennis et al., 2012; Gattiker & Kelley, 1999; Harrington, 1996; Jarvenpaa & Staples 2000; Robert et al., 2009 for exceptions), they can be particularly useful for the investigation of perceptions, beliefs, and attitudes (Hughes, 1998, Murphy et al., 1986, Pierce et al., 2000), while prior research has also incorporated vignettes for the study of trust (Buskens & Raub 2002; Dennis et al., 2012; Elsbach & Elofson, 2000; Nakayachi & Watabe, 2005; Robert et al., 2009).

We focus on five ORS and investigate their efficacy to deal with the three types of security breaches. As a result, 5*3 scenarios are used in this study. We relied on examples from databreachtoday.com and the literature to design our vignettes. Specifically, three types of security breaches (DoS attack, virus attack and theft of information) are derived from Yayla and Hu (2011). The five ORS include the defensive, moderate, accommodating, and image

renewal strategies from Gwebu et al. (2018), supplemented with a fifth response strategy of no response. The details of the scenarios are listed in Appendix 3.

During the data collection, the participants were first asked to provide the name of a web shop they had visited recently and to evaluate the CR. Then they were presented with one of three vignettes describing the security breach, followed by one of five vignettes describing the ORS. Participants were randomly assigned to one of these fifteen scenarios (3*5). After that, they answered questions regarding the perceived risks (six dimensions), perceived severity, response efficacy, and intention to re-transact with the breached organization, as well as other control variables (response costs, self-efficacy, and demographic data).

To establish the survey questions, we adapted all measures from prior studies. Appendix 4 lists the items we adopted to measure the principal constructs and key control variables, which, apart from the security breach announcement, are all measured with the use of a seven-point Likert scale from strong disagreement to strong agreement. To increase validity, some Likert scale items were reversed. Before launching the large-scale data collection, a pre-test with a small group of fifteen respondents was organized to check for consistency and improve the clarity of the questionnaire for each of the two studies.

4.2 Data Collection, Manipulation and Collinearity Checks

We used Amazon Mechanical Turk (AMT) to collect the empirical data between June and July 2021. AMT is increasingly considered as a valuable source to support research in information systems (IS) (Mamonov & Koufaris, 2020; Windasari et al., 2021) and is well recognized by IS scholars (Lowry et al., 2016). To obtain sufficient survey respondents and to avoid potential cross-cultural effects, we have limited the AMT survey participants to those living in the United States. To encourage participation commitment, we pay for each valid response at the market's hourly rate of US$6. We conducted two rounds of data collection. We first explored

the validity of the survey responses with 100 responses in June 2021. We then proceeded with the rest of data collection at AMT in July 2021. After three weeks of data collection, we obtained 964 responses. After checking the answering time and removing the duplicated IP address, 573 responses were confirmed as valid data to proceed with the further data analysis. Table 3 summarizes the demographics and Table 4 shows the distributions of survey responses to each vignette scenario.

Gender	***Percentage***	***Education***	***Percentage***	***Work experience***	***Percentage***
Female	46.6%	high school or below	25%	>= 5 years	15%
Male	52.7%			6-10 years	15%
Others	0.6%	bachelor	50.3%	11-20 years	25.6%
		master	23%	21-30 years	20.3%
		doctorate	1.7%	30-40 years	14.7%
				30 years or above	9.6%
Annual income	***Percentage***	***Age***	***Percentage***	***Online purchases in the past one year (times)***	***Percentage***
$9,999 and below	14.2%	Under 20	0.2%		
$10,000-29,999	24.6%	20-29	13.3%		
$30,000-49,999	26.5%	30-39	26.5%		
$50,000-69,999	14.5%	40-49	24.1%	1-10	29.3%
$70,000-89,999	10.8%	50-59	17.8%	11-20	22.7%
$90,000 and above	9.4%	60-69	14.3%	21-30	15.7%
		70 or above	3.8%	31-40	5.9%
				41-50	15.7%
				51 or above	13.4%
Web shop category		***Percentage***	***Web shop category***		***Percentage***
Fashion, Clothing and Accessories		25.8%	Groceries, Food and Drink		9.1%
Health and Beauty		8.4%	Technology (including Phones and Computers)		15.2%
Toys and Baby Equipment		0.9%			
Books, CDs, and Other Physical Media		6.6%	Home and Furniture		5.2%
			Flowers and Gifts		0.2%
			Others		28.6%

Table 3. Demographics of Participants (n=573)

Survey Responses		**Company Response Strategy**					
		No response	Defensive strategy	Moderate strategy	Accommodating strategy	Image renewal	**Total**
Security Breach Type	1 Denial of service	45	42	42	37	37	203
	2 Virus Attack	31	32	35	35	40	173
	3 Theft of Information	35	40	43	45	34	197
Total		111	114	120	117	111	**573**

Table 4. Distributions of 573 Valid Responses across Different Scenarios (3*5)

5. Data Analysis

5.1 Manipulation checks, construct validity and reliability

As the vignette contains two manipulations, we first conducted manipulation checks. For the three security breach types, we ask the respondents to rate the damage level after reading one of the three randomized security breach announcements. Then we ran an ANOVA test as a manipulation check to examine whether the damage level (1~7) varies across the three security breach types. The ANOVA result confirms the significant between-group difference ($F=30.742$, $p<0.01$), with low to high damage (1~7) ranging from DoS attack, virus attack, and to theft of information. For the manipulation of ORS, we asked survey respondents to rate the protective level (1~5) after reading one of the five randomized ORS. The manipulation check for ORS also suggests a significant between-group difference ($F=149.206$, $p<0.01$), ranging from no response, defensive, moderate, accommodating, and image renewal response strategies. These two manipulation checks suggest our vignette setting is valid initially.

We next used PLS-SEM for further data analysis considering the predictive nature of our study and the explanations of the target constructs (Hair et al., 2011). We conducted the analysis on Smart-PLS (v.3.3.3). Table 5 shows the construct reliability and validity analysis, with all Cronbach's Alphas above 0.82, composite reliability higher than 0.83, and the average variance extracted above 0.71. We tested for potential common method bias. Our principal components factor analysis, as shown in online supplementary materials II, indicated each factor explains roughly equal variance (6.229%~8.296%), with all eigenvalues larger than 1, suggesting the lack of serious common method bias (Podsakoff & Organ, 1986). Furthermore, the correlation matrix (Table 5) shows that the highest inter-construct correlations are below 0.67, while common method bias is usually evidenced by extremely high correlations ($r>0.90$) (Bagozzi et al., 1991; Hong & Pavlou, 2014). Collinearity is not an issue as all Variance Inflation Factors (VIF) are smaller than 3.0 (Hair et al., 1995). The discriminant validity is confirmed by the exploratory and confirmatory factor analysis, with all the self-loading scores

being much higher than the cross-loading scores (as detailed in the online supplementary material II), and each AVE is larger than the latent variable correlations.

	CR	FR	PR	PER	PSR	SR	SEV	RE	RC	SE	IR
Corporate Reputation (CR)	**0.758**										
Financial Risk (FR)	-0.158	**0.890**									
Privacy Risk (PR)	-0.225	0.325	**0.894**								
Performance Rick (PER)	-0.173	0.662	0.210	**0.832**							
Psychology Risk (PSR)	-0.013	0.599	0.301	0.517	**0.749**						
Social Risk (SR)	0.048	0.375	-0.213	0.497	0.224	**0.707**					
Severity (SEV)	0.080	0.474	0.197	0.330	0.466	0.182	**0.739**				
Response Efficacy (RE)	0.203	-0.047	-0.578	-0.005	-0.059	0.306	-0.033	**0.883**			
Response Costs (RC)	-0.091	0.543	-0.020	0.559	0.306	0.475	0.386	0.075	**0.785**		
Self-Efficacy (SE)	0.047	0.108	-0.477	0.217	-0.067	0.431	-0.017	0.438	0.323	**0.762**	
Intention to Re-transact (IR)	0.186	-0.431	-0.670	-0.312	-0.338	0.044	-0.294	0.430	-0.153	0.294	**0.916**
Cronbach's Alpha	0.894	0.877	0.941	0.901	0.841	0.930	0.824	0.934	0.912	0.854	0.954
Composite Reliability	0.926	0.942	0.962	0.937	0.899	0.825	0.895	0.958	0.936	0.906	0.970

Table 5. Construct Validity and Reliability

Note: Diagonal elements are the Average Variance Extracted (AVE) value from their indicators. Off-diagonal elements are correlations between constructs.

5.2 Structural Models

After confirming the reliability and validity of the construct measures, we examine the research model in a two-stage analysis in Smart-PLS v3.3.3. We first analysed the model related to PMT, by including the six dimensions of risk, severity, response efficacy, response costs and self-efficacy, intention to re-transact in the statistical model. The results of the statistical model shown in Table 6 indicates that only financial risk, privacy risk, severity and response efficacy assert significant impacts on intention to re-transact. The insignificant effects of time risk, performance risk, psychology risk and social risk are consistent with our speculations and findings in our pilot study.

Path Coefficients	**DV: Intention to Re-transact**
Financial Risk	-0.180**
Privacy Risk	-0.494**
Performance Risk	-0.060 (ns)
Psychological Risk	0.004 (ns)
Social Risk	0.009 (ns)
Severity	-0.082*
Response Efficacy	0.109*
Response Costs	-0.027 (ns)
Self-Efficacy	0.046 (ns)
R Square Adjusted	**0.509**
Model_Fit (Estimated Model):	Chi-Square: 5139.338
SRMR: 0.236	d_ULS: 31.286
NFI: 0.687	d_G: 1.696

Table 6. The Statistical Model of PMT
Note: **p<0.01; *0.01<p<0.05; ns: not significant, p>0.05

Considering self-efficacy and response costs are not the focus of the current study and the current model fit index in Table 6 is low (SRMR=0.236; NFI=0.687), we excluded these factors from the statistical models to examine the model fit again. When financial risk, privacy risk, severity, and response efficacy are included as the determinants of intention to re-transact, the model fit indicators (SRMR=0.039; NFI=0.886) became satisfactory (Bagozzi and Yi, 1988; Hair et al., 2021). Therefore, we focus on our research hypotheses with the better-fit model as shown in Table 7 to statistically examine the relationships among three types of security breaches, five types of responses, CR and PMT.

Path Coefficients	**DV: Intention to Re-transact**
Financial Risk	-0.217**
Privacy Risk	-0.513**
Severity	-0.087*
Response Efficacy	0.120**
R Square Adjusted	**0.511**
Model_Fit (Estimated Model)	Chi-Square: 804.364
SRMR: 0.039	d_ULS: 0.156
NFI: 0.886	d_G: 0.217

Table 7. The Statistical Model of PMT with A Better Fit

Although the fifteen (3*5) scenarios are designed as manipulations, it is practically infeasible to compare fifteen models. We thus take the following two steps for the analyses.

5.2.1 Step 1: Binary Dummy Variables and Separate Regressions

We first explore the impacts of each security breach type and each response strategy on consumers' threat and coping appraisal. To make the whole statistical model manageable, we created a second-order construct of perceived risk, by including the two significant risk dimensions as the two formative measures of perceived risk with significant loadings of financial risk (weights of 0.348, $p<0.01$) and privacy risk (weights of 0.839, $p<0.01$) in the formative measured construct. Then in each of the regression test, we created binary dummy variables for three security breach types and five response strategies. Each binary dummy variable represents one category of the explanatory variable and is coded with 1 if the case falls in the category and with 0 if not. For example, in the binary dummy variable DoS attack, all cases in which the respondent sees the DoS attack scenario are coded as 1, and all other cases, in which the respondent doesn't see the DoS attack scenario, are coded as 0. The same is done in the Virus attack and Theft of Information attack, as well as for each of the five types of ORS. As a result, we created three binary dummy variables for security breach and another five binary dummy variables for ORS. This allows us to enter in the security breach type values and ORS as numerical (i.e., either 0 or 1), which is meaningful and feasible.[3] Meanwhile, to avoid the dummy variable trap (i.e., a case of perfect multicollinearity),[4] we take DoS Attack and No Response as the base lines and pool the other six binary dummy variables into three separate regressions to explore the respective impacts of each security breach type and each

[3] See https://www.southampton.ac.uk/passs/confidence_in_the_police/multivariate_analysis/linear_regression.pagethe.

[4] See https://www.jigsawacademy.com/understanding-dummy-variable-traps-regression/.

response strategy on consumers' threat and coping appraisal in three separate models. Below it is one example formula.

$$\textit{Perceived Risk} = a + b_1 \text{ Virus Attack} + b_2 \text{ Theft of Information} + b_3 \text{ Defensive Response} + b_4 \text{ Accommodating Response} + b_5 \text{ Moderate Response} + b_6 \text{ Image Renewal} + b_7 \text{ Corporate Reputation} \quad \text{(model 1)}$$

From the coefficients summarized in Table 8, theft of information has much bigger impacts on consumers' risk perception and severity evaluation. Meanwhile, when facing security breach, organizations' response efficacy ranges from no response (baseline), defensive response, moderate response, accommodating to image renewal strategy with increasing positive effects in consumers' coping appraisal. These separate regression results provide a good foundation to code security breach as an ordinal variable, and ORS as the other ordinal variable in the structural model, as further explained in the second step below.

IVs	**Model 1: DV= Perceived Risk**	**Model 2: DV= Severity**	**Model 3: DV= Response Efficacy**
Virus Attack	0.012(ns)	-0.002(ns)	0.075(ns)
Theft of Information	**0.172****	**0.356****	-0.051(ns)
Defensive Response	-0.085(ns)	-0.074(ns)	**0.154***
Moderate Response	**-0.284****	**-0.189****	**0.420****
Accommodating Response	**-0.268****	-0.061(ns)	**0.468****
Image Renewal	**-0.239****	0.021(ns)	**0.535****
Corporate Reputation	**-0.228****	**0.073***	**0.176****
Adjusted R Square	**15.0%**	**15.1%**	**30.3%**

Table 8. Coefficients in the Regressions of Binary Dummy and Control Variables
Baseline: DoS Attack and No Response

5.2.2 Step 2: The Overall Structural Model

Consistent with the empirical results in the first step, types of security breach can be conceptualized and operationalized as the level of breach, while types of ORS can be conceptualized as the extent of organizational efforts to provide explanations and taking the responsibility and actions (c.f. Bansal & Zahedi, 2015). With this conceptualization and

according to the results of those dummy variable regressions in the first step, we code security breach as an ordinal variable (1-denial of service; 2-virus attack; 3-theft of information) and similarly for ORS (1-no response, 2-defensive strategy, 3-moderate strategy, 4-accomodating strategy, and 5-image renewal strategy). Then we include these two ordinal variables, i.e., security breach and ORS, together with CR, into the full model for the data analysis of the overall structural model at Smart-PLS.

As shown in Table 9, the overall structural model is largely supported by the empirical data. Consistent with the PMT model tested earlier, perceived risk (β=-0.606, $p<0.01$), severity (β=-0.069, $0.01<p<0.05$) and response efficacy (β=0.118, $p<0.01$) have significant impacts on the intention to re-transact, supporting H1, H2 and H3. The control variables response costs (β=-0.033, $p>0.50$), self-efficacy (β=0.049, $p>0.50$), and the demographics variables assert no significant influence on consumers' intention to re-transact. Security breach has a significant direct effect on perceived risk (β=0.142, $p<0.01$) and severity (β=0.306, $p<0.01$), but not response efficacy (β=-0.040, $p>0.50$), thus supporting H4a and H4b, but rejecting H4c. ORS can influence consumers' risk perception (β=-0.241, $p<0.01$) and response efficacy (β=0.494, $p<0.01$), but not severity (β=0.010, $p>0.50$), thus supporting H5a and H5c, while rejecting H5b. We have also included the key control variable CR in the model and found it significant in determining perceived risk (β=-0.230, $p<0.01$), severity (β=0.080, $0.01<p<0.05$), and response efficacy (β=0.177, $p<0.01$). We also tested the interaction effects of ORS with security breach, as well as CR, but found that they have no significant effects on the model. The total variance explained for perceived risk, severity, response efficacy, and intention to re-transact are 12.7%, 9.4%, 28.1%, and 51.2%, respectively.

Path Coefficients	Perceived Risk	Severity	Response Efficacy	Intention to Re-transact
Corporate Reputation (CR)	-0.230**	0.080*	0.177**	
Security Breach (SB)	0.142**	0.306**	-0.040(ns)	
Organizational Response Strategy (ORS)	-0.241**	0.010(ns)	0.494**	
ORS*CR	-0.016(ns)	0.030(ns)	0.016(ns)	
ORS*SB	0.012(ns)	0.021(ns)	0.049(ns)	
Perceive Risk				-0.606**
Severity				-0.069*
Response Efficacy				0.118**
Response Costs				-0.033(ns)
Self-Efficacy				0.049(ns)
Demographics control variables				ns
R Square Adjusted	**12.7%**	**9.4%**	**28.1%**	**51.2%**

Table 9. Statistics of The Overall Structural Model

5.3 Mediation tests

The current research focuses on the role of ORS in handling security breach to decide consumers' intention to re-transact. We further examined the mediating role of key constructs of PMT (i.e., perceived risk, severity, and response efficacy) in the proposed path between ORS and intention to re-transact. Following Zhao et al. (2010), we conducted mediation tests using the classical bootstrapping method (Preacher and Heyer, 2008). The test results, as detailed in Appendix 5, indicate the mediation effect of perceived risk (β=-0.9128, $p<0.01$), severity (β=-0.1109, $p<0.01$), and response efficacy (β=0.0862, $p<0.01$) exists, but ORS has no direct effect (β=0.0368, $p>0.05$) on intention to re-transact. We discuss the key findings and implications below.

6. Discussion

6.1 Key findings

We set out to enhance our understanding on the impacts of security breaches and ORS on consumers' threat and coping appraisals. By integrating the existing risk theories in e-commerce (Featherman & Pavlou, 2003; Forsythe *et al*., 2006; Forsythe & Shi, 2003; Nepomuceno *et al*., 2014), we extend PMT (Rogers, 1983) to the security breach context.

Several important findings can be observed from our empirical analysis. First, the proposed overall model was largely supported. Within the PTM, perceived risk, severity and response efficacy are identified as the major influential determinants of consumers' security threat and coping appraisal process, while response costs and self-efficacy are not the focus of consumers in reacting to the security breach. Specifically in the threat appraisal, six risk dimensions are identified in the literature (see Table 2 and Appendix 2). Our empirical analysis suggested that only financial risk and privacy risk were influential in determining consumers' intention to re-transact with the focal organization after the incident of a security breach. This finding provides interesting explanations that differ from the existing risk literature in the e-commerce domain (e.g., Aghekyan-Simonian et al., 2012; Featherman & Pavlou, 2003; Forsythe et al., 2006; Forsythe & Shi, 2003; Nepomuceno et al., 2014; Almousa; 2011; Ariffin et al. 2018) and suggests consumers do not give equal weight to risk dimensions. Appendix 2 has suggested that financial risk, privacy risk, performance risk and time risk are the most relevant risks investigated in the literature, as also indicated by Nepomuceno et al. (2014). Our empirical data further demonstrated in the online shopping contexts privacy and financial consequences are the two major concerns hindering consumers to repurchase, while making use of the explanations from Parks et al. (2017), consumers are less sensitive to the other consequences of security breaches because of deindividuation (i.e., as an individual they feel it is irrelevant to them) such as in our context for social risk and psychological risk or apathy (i.e., there is nothing they can do about it) such as in our context for time risk and performance risk also because consumers can easily find a replacement website to shop online.

Regarding the security breach, ORS and CR, our data analysis also demonstrated important findings. Consumers consider theft of information having the most negative effects in their appraisal of the security breach situation and hence a security breach requires a more sophisticated and nuanced handling process. The announcement of a security breach alone did

increase consumers' concerns of financial and privacy consequences, as well as severity, but understandably not directly response efficacy as the security breach itself has not yet touched upon on organization's response and the breach management. Furthermore, our empirical data also suggests when evaluating response efficacy, ORS dominates the appraisal result, hence further explaining the unsupported H4c. Specifically, our study suggests an organization can choose among no response, defensive, moderate, accommodating and image renewal strategies. When a more protective ORS is included, consumers' risk perception can be effectively reduced, and consumers' appraisal of a breached organization's response efficacy can be very positive. However, the proposed influence from ORS on perceived severity (H5b) was not supported by our empirical data. We speculate the insignificant effect is first because the direct overwhelming impacts from security beach on consumers' severity evaluation (β=0.306, $p<0.01$). Also, the announcement of security beach might have already introduced some anchoring effects on consumers' evaluation of how serious of the security incident.

We deliberately collected the data of CR prior to the security breach announcement. It is interesting to observe that CR can assert a persistent and significant impact on consumers' security threat and coping appraisal. This implies that CR, as based on historical performance and past transaction experience, can play a major role in risk mitigation, and serve as a quality signalling mechanism to consumers when organizations are faced with a security breach. The findings of our study demonstrate the competing effects of one-time events such as a security breach versus the long-standing impact of organizational image on consumers' security threat and coping appraisal. Furthermore, our mediation tests (as shown in Appendix 5) demonstrate that consumers' security threat and coping appraisal fully mediates the direct effect of ORS on consumers' intention to repurchase from the breached organization. We discuss the corresponding theoretical and practical implications below.

6.2 Theoretical implications

Our work fills the research gap on security breach, ORS and consumers' appraisal of threat and coping. Consumers are the important stakeholders and affected by the security breach. It is critical to understand consumers' threat and coping appraisal of ORS to handle the security breach incidents. Our study is among the first research to extend PMT in the security breach context. The conceptualizations of security breach and ORS, as well as the principal and agent perspectives, in the current PMT model provides researchers with a conceptual opportunity to further investigate PMT and its determinants. Specifically, we extend the PMT model in two ways. On the one hand, we integrate PMT with the theory of consumer risk in e-commerce. We recognize that the perceived vulnerability should be operationalized as a multi-dimensional construct as the security breach incidents may lead to different types of losses. On the other hand, we challenge the long-standing presumption that coping mechanisms against a threat are always available to actors who evaluate the threat. We synergize the principal-agent perspective (following Pavlou et al., 2007) in the adapted PMT in which the breached organization is the agent who provides the coping strategy, while consumers are the principal actors who evaluate the breached organization's coping strategy. We argue that actors who appraise the threats may evaluate the response efficacy of the coping mechanisms taken by the external agents, especially when such mechanisms are critical yet unavailable to the actors. Focusing on varied organizations' response strategies, we argue that consumers implicitly delegate an organization the duties to protect them from further losses due to the focal and any potential security breach events. We label this understanding as the principal-agent perspective of PMT, proposing that in the coping appraisal processes, individuals evaluate the response efficacy of the coping mechanisms taken by the external agents, especially when such mechanisms are critical yet unavailable to the individuals.

Furthermore, our study also sheds light on the theoretical applicability of PMT in the security breach context and implies response costs and self-efficacy are not the major concern

in consumers' security threat and coping appraisal. Our conceptualization demonstrates that PMT is an effective theoretical lens to explain the phenomenon of security breach and ORS. Our mediation tests further imply consumers' threat and coping appraisal is the necessary and critical process for ORS to make effects to mitigate the damaging effects of security breach in consumers' perceptions and intentions. These findings provide a good theoretical starting point to a fine-grained enhancement of PMT in security breach research.

More specifically, the proposed model (and the empirical data) implies that risk cannot be regarded as one single-dimensional construct. Different types of risk can render a distinct influence on consumers' perceptions and can lead to different judgements as to whether to transact with the organization in the future. More importantly, this study is among the first to deploy the current risk theories to the context of security breaches and to conceptualize the theoretical relationship between security breaches, ORS, and risk evaluation in e-commerce. CR is incorporated based on the risk literature, serving as the risk mitigation mechanism in the proposed theoretical model. Overall, we offer fresh insights about the competing impacts of one-time security breaches and ORS, as well as long-standing CR, in determining consumers' security threat and coping appraisal associated with online transactions.

6.3 Practical Implications

Along with the aforementioned novel contributions to the extant IM theory, our study also brings a number of implications at the level of both the organization itself and the consumers who avail themselves of the services of the organization. There are also policy implications.

When it comes to the consumer implications of our study, our empirical findings indicate that a sense of risk occurs when personal data is stolen during a security breach, along with a sense of fear that a breach will result in significant concerns about financial and privacy

loss. The concerns raised by the security breach announcement and ORS vary significantly across different scenarios. Among different types of security breaches, theft of information is evaluated by consumers as the most serious incident. Consumer's risk perception is salient; however, to some extent it can be compensated by one-time ORS and a long-standing CR based on historical records and brand image.

It is important, therefore, to highlight that more proactive, long-term visioned ORS are much more effective in managing consumers' perception of damage. This suggests that to mitigate potential damage to consumer confidence in the short run, breached organizations could publicly announce the occurrence of a security breach by emphasizing that it is a rare, one-off event and by further highlighting the long-term outstanding CR. This is in effect a form of crisis communication (Zheng et al., 2018) and the intention would be to help the consumers to trust that they will not suffer any financial or privacy losses due to possible future security breaches with these organizations. In the long run, however, organizations cannot risk damaging their reputation because a breach is a major source of negative evaluation when consumers consider the risk levels of engaging in transactions with the organizations. Organizations, thus, should take seriously the occurrence of any types of security breaches, and ensure that such incidents are indeed rare and one-off.

Concurrently, the implications of our findings provide nuanced expositions for legislative as well as policy-making processes. The ongoing pandemic has accentuated that the internet and e-commerce are essential elements of our lives, especially in times of crisis, and therefore legislative efforts related to security breach announcements are increasingly critical. The legislation to mandate the announcement of security breaches, at least for publicly listed organizations, will bring needed transparency to the public, and increase the trust of consumers towards organizations that take privacy and security issues seriously. The effect of a security breach announcement, however, can be compensated by the ORS in handling the security

breach and the long-standing CR. Therefore, legislators and policymakers should engage security experts from the industry and academia, who could help by incorporating measures that ensure privacy and security, as well as processes on promptly announcing security breaches. These measures may extend or augment current privacy legislation (such as GDPR) if it is in place. Such teams of experts will be able to appreciate the timeliness and importance of the topic, and the adverse implications that security breaches can have. Consequently, these changes may further strengthen the confidence of consumers.

6.4 Limitations and Future Research

Our work has limitations that open avenues for further research. First, due to the design of a cross-sectional survey, we only examine consumers' re-transaction intention. Future research can use the combination of objective data (such as transaction records) and subjective data (such as survey questions) to scrutinize the differences in consumer behaviour before and after an actual security breach. For instance, we collected the data about CR before a security breach. Future research can focus on how security breach announcements can affect CR over time. A longitudinal design can also help address the potential common method bias associated with the current cross-sectional study.

Second, we only collected data from a sample population of the United States through AMT, despite the fact that the security breach has attracted much interest in wider population from research in the field. We, thus, invite future researchers in the field to conduct cross-country studies and consider constructs like uncertainty avoidance and other cultural dimensions (Hofstede et al., 2005) to further investigate and validate our findings.

Thirdly, while we incorporated a vignette-based approach, the participants might respond differently when presented with a vignette instead of a real context (Greenberg & Eskew, 1993). Studies in general have demonstrated that vignettes can reach the same

conclusions as other research approaches (de Cremer et al., 2007; Shaw et al., 2003), supporting the view that individuals respond in a similar way regardless of whether they are presented with a vignette or a more realistic setting. While our findings are statistically significant, vignettes represent a more subtle arrangement of different scenarios and might not be strong enough to induce the genuine thoughts and behaviours of participants, so treatments are more likely to fail in vignette studies, resulting in non-significant results (Hughes & Huby, 2002). Future research should investigate further our model in a more realistic setting.

Last, the world is now focused on security breaches, perhaps more so than previous cybersecurity threats. In June 2021,[5] McDonald's security breach announcement exposed Korean and Taiwanese customers' personal data taken from the delivery system. In the same month, Volkswagen and Audi notified 3.3 million people in the U.S. and Canada of a breach of personal information including driver's license numbers, and a smaller number within that group may also have had their birth dates, social security or social insurance numbers, account or loan numbers and tax identification numbers leaked. A security breach represents a real concern for businesses of all sizes. It is worthwhile to study and scrutinize the evolving attitudes of consumers regarding these security breaches, the determination of organizations to prevent future security issues, as well as the associated legislative developments.

7. Conclusion

Our study sheds light on the interwoven relationship among security breaches, ORS, CR, consumers' security threat and coping appraisal, and consumers' intention to re-transact with a breached web shop. Nowadays, organizations and institutions are managing a huge volume of sensitive data about their customers (Angelopoulos et al., 2021). Data security and privacy

[5] https://www.databreachtoday.com/

are paramount concerns for both consumers and organizations (Lowry et al., 2017). As consumers continue to share data for online transactions and organizations become more dependent to store data on the cloud, the concerns of potential security breaches and the demand for data protection will continue to grow. Our work demonstrates how security breaches and ORS may affect consumers' evaluation of the situation, the way an organization conducts business, and the potential ramifications for failing to adequately protect sensitive data. This study provides a springboard for future investigation in this domain. We, thus, call on IM scholars to further focus on security breach, data privacy, risk management, and ORS.

8. References

Aghekyan-Simonian, M., Forsythe, S., Kwon, W. S., & Chattaraman, V. (2012). The role of product brand image and online store image on perceived risks and online purchase intentions for apparel. *Journal of Retailing and Consumer Services*, 19(3), 325-331.

Aivazpour, Z., Valecha, R. & Chakraborty, R. (2018). The impact of data breach severity on post-breach online shopping intention." *Thirty Ninth International Conference on Information Systems (ICIS)*, San Francisco, U.S.

Almousa, M. (2011). Perceived risk in apparel online shopping: A multi dimensional perspective. *Canadian Social Science*, 7(2), pp. 23-31.

Angelopoulos, S., Brown, M., McAuley, D., Merali, Y., Mortier, R. & Price, D. (2021). Stewardship of personal data on social networking sites, *International Journal of Information Management, 56*, 102208.

Ariffin, S. K., Mohan, T., & Goh, Y. N. (2018). Influence of consumers' perceived risk on consumers' online purchase intention. *Journal of Research in Interactive Marketing*, 12(3), 309-327.

Ayaburi, E. W., & Treku, D. N. (2020). Effect of penitence on social media trust and privacy concerns: The case of Facebook. *International Journal of Information Management, 50*, 171-181.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, 16(1), 74-94.

Bagozzi, R. P., Yi, Y., & Phillips, L.W. (1991). Assessing construct validity in organizational research, *Administrative Science Quarterly 36*, 421–458.

Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. *Decision Support Systems, 71*, 62-77.

Bertea, P. E. (2015). From fearful to trustful - How perceived risk dimensions in e-commerce differentiate between consumers. *Review of Economic and Business Studies, 8* (1), 47-54.

Buskens, V., & Raub, W. (2002). Embedded trust: Control and learning. *Advances in Group Processes, 19*(2002), 167-202.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security, 11*, 431-448.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. *International Journal of Electronic Commerce, 9(*1), 69-104.

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S. & Rao, H.R. (2016). Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decision Support Systems*, 83, 47-56.

Chan, S. H., & Janjarasjit, S. (2019). Insight into hackers' reaction toward information security breach. *International Journal of Information Management, 49*, 388-396.

Choi, B. C., Kim, S. S., & Jiang, Z. (2016). Influence of firm's recovery endeavors upon privacy breach on online customer behavior. *Journal of Management Information Systems, 33(*3), 904-933.

Couger, J. D. (1989). Preparing IS students to deal with ethical issues. *MIS Quarterly, 13*(2), 211-218.

Crespo, A. H., del Bosque, I. R., & de los Salmones Sanchez, M. G. (2009). The influence of perceived risk on Internet shopping behavior: A multidimensional perspective. *Journal of Risk Research, 12(*2), 259-277.

Cunningham, S. M. (1967). *The major dimensions of perceived risk, Risk Taking and Information Handling in Consumer Behavior*, Cambridge, MA: Harvard University Press.

Daft, R. L., Lengel, R. H., & Trevino, L. K. (1987). Message equivocality, media selection, and manager performance: Implications for information systems. *MIS Quarterly, 11*(3), 355-366.

de Cremer, D., Van Dijke, M., & Bos, A. E. (2007). When leaders are seen as Transformational: the effects of organizational justice. *Journal of Applied Social Psychology, 37*(8), 1797-1816.

Dennis, A. R., Robert, L. P., Curtis, A. M., Kowalczyk, S. T., & Hasty, B. K. (2012). Research note—trust is in the eye of the beholder: A vignette study of postevent behavioral controls' effects on individual trust in virtual teams. *Information Systems Research, 23*(2), 546-558.

Dwivedi, Y. K., Ismagilova, E., Hughes, D. L., Carlson, J., Filieri, R., Jacobson, J., Jain, V., Karjaluoto, H., Kefi, H., Krishen, A. S. & Kumar, V. (2020). Setting the future of digital

and social media marketing research: Perspectives and research propositions, *International Journal of Information Management*, 102168.

Elsbach, K. D., & Elofson, G. (2000). How the packaging of decision explanations affects perceptions of trustworthiness. *Academy of Management Journal*, *43*(1), 80-89.

Ettredge, M., & Richardson, V. J. (2002). Assessing the risk in e-commerce. *Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HCISS)*, Big Island, Hawaii.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies*, 59(4), 451-474.

Forsythe, S. M, & Shi, B. (2003). Consumer patronage and risk perceptions in Internet shopping. *Journal of Business Research*, *56*(11), 867-875.

Forsythe, S., Liu, C., Shannon, D., & Gardner, L. C. (2006). Development of a scale to measure the perceived benefits and risks of online shopping. *Journal of Interactive Marketing*, *20*(2), 55-75.

Garg, A., Curtis, J., & Halper, H. (2003). The financial impact of IT security breaches: What do investors think?. *Information Systems Security*, *12*(1), 22-33.

Gattiker, U. E., & Kelley, H. (1999). Morality and computers: Attitudes and differences in moral judgments. *Information Systems Research*, *10*(3), 233-254.

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*, *46*(7), 404-410.

Gordon, L., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs?. *Journal of Computer Security*, *19*(1), 33-56.

Gould, D. (1996). Using vignettes to collect data for nursing research studies: How valid are the findings?. *Journal of Clinical Nursing*, *5*(4), 207-212.

Greenberg, J., & Eskew, D. E. (1993). The role of role playing in organizational research. *Journal of Management*, *19*(2), 221-241.

Grewal, D., Gotlieb, J., & Marmorstein, H. (1994). The moderating effects of message framing and source credibility on the price-perceived risk relationship. *Journal of Consumer Research*, *21*(1), 145-153.

Gwebu, K.L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, *35*(2), 683-714.

Hair Jr, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2021). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM).* Sage publications.

Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1995). *Multivariate Data Analyses: With Readings*. Englewood Cliffs, NJ: Prentice Hall.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139-152.

Hanafizadeh, P., & Khedmatgozar, H. R. (2012). The mediating role of the dimensions of the perceived risk in the effect of customers' awareness on the adoption of Internet banking in Iran. *Electronic Commerce Research, 12*(2), 151-175.

Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly, 20*(3), 257-278.

Hassan, A. M., Kunz, M. B., Pearson, A. W., & Mohamed, F. A. (2006). Conceptualization and measurement of perceived risk in online shopping. *Marketing Management Journal, 16*(1), 138-147.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

Hofstede, G., Hofstede, G. J., & Minkov, M. (2005). *Cultures and Organizations: Software of the Mind*. Vol. 2. New York, NY: McGraw-Hill.

Hong, Y., & Pavlou, P. A. (2014). Product fit uncertainty in online markets: Nature, effects, and antecedents. *Information Systems Research, 25*(2), 328–344.

Hovav, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review, 6*(2), 97-121.

Hovav, A., & D'Arcy, J. (2004). The impact of virus attack announcements on the market value of firms. *Information Systems Security, 13(*3), 32-40.

Hughes, R. (1998). Considering the vignette technique and its application to a study of drug injecting and HIV risk and safer behaviour. *Sociology of Health & Illness, 20*(3), 381-400.

Hughes, R., & Huby, M. (2002). The application of vignettes in social and nursing research. *Journal of Advanced Nursing, 37*(4), 382-386.

IBM / Ponemon Institute (2020). *Cost of a Data Breach Report 2020,* Available at: https://www.ibm.com/security/data-breach

Ioannou, A., Tussyadiah, I., & Lu, Y. (2020). Privacy concerns and disclosure of biometric and behavioral data for travel. *International Journal of Information Management, 54*, 102122.

Isaac, M. (2014). *Despite Security Breach, eBay Posts Profit and Sees Steady Growth*. The New York Times. https://goo.gl/j7yGug.

Jarvenpaa, S. L., & Staples, D. S. (2000). The use of collaborative electronic media for information sharing: An exploratory study of determinants. *The Journal of Strategic Information Systems, 9*(2-3), 129-154.

Jarvenpaa, S. L., & Todd, P. A. (1997). Is there a future for retailing on the Internet. In Peterson, R.A. (Ed). *Electronic Marketing and the Consumer,* 139-154.

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer trust in an internet store. *Journal of Computer-Mediated Communication, 5*(2), https://doi.org/10.1111/j.1083-6101.1999.tb00337.

Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management, 28*(5), 413-422.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework. *MIS Quarterly, 39*(1), 113-134.

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems, 25*(3), 231-251.

Kim, W., Jeong, O. R., Kim, C., & So, J. (2011). The dark side of the Internet: Attacks, costs and responses. *Information Systems, 36*(3), 675-705.

Ko, M., & Dorantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: An empirical investigation. *Journal of Information Technology Management, 17*(2), 13-22.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177-187.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13-24.

Littler, D., & Melanthiou, D. (2006). Consumer perceptions of risk and uncertainty and the implications for behaviour towards innovative retail services: The case of internet banking. *Journal of Retailing and Consumer Services, 13*(6), 431-443.

Lowry, P. B., D'Arcy, J., Hammer, B., & Moody, G. D. (2016). "Cargo Cult" science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels. *The Journal of Strategic Information Systems, 25*(3), 232–240.

Lowry, P. B., Dinev, T., & Willison, R. (2017). Why security and privacy research lies at the centre of the information systems (IS). artefact: Proposing a bold research agenda. *European Journal of Information Systems, 26*(6), 546-563.

Mamonov, S., & Koufaris, M. (2020). Fulfilment of higher-order psychological needs through technology: The case of smart thermostats. *International Journal of Information Management, 52*, 102091.

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems, 34*(4), 1203-1230.

Mitchell, V. (1999). Consumer perceived risk: Conceptualisations and models. *European Journal of Marketing, 33*(1/2), 163-195.

Miyazaki, A. D., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer Affairs*, *35*(1), 27-44.

Molok, N. N. A., Ahmad, A., & Chang, S. (2018). A case analysis of securing organisations against information leakage through online social networking. *International Journal of Information Management*, *43*, 351-356.

Murphy, K. R., Herr, B. M., Lockhart, M. C., & Maguire, E. (1986). Evaluating the performance of paper people. *Journal of Applied Psychology*, *71*(4), 654.

Nakayachi, K., & Watabe, M. (2005). Restoring trustworthiness after adverse events: The signaling effects of voluntary "hostage posting" on trust. *Organizational Behavior and Human Decision Processes*, *97*(1), 1-17.

Nepomuceno, M. V., Laroche, M., & Richard, M. O. (2014). How to reduce perceived risk when buying online: The interactions between intangibility, product knowledge, brand familiarity, privacy and security concerns. *Journal of Retailing and Consumer Services*, *21*(4), 619-629.

Park, J., Gunn, F., & Han, S. L. (2012). Multidimensional trust building in e-retailing: Cross-cultural differences in trust formation and implications for perceived risk. *Journal of Retailing and Consumer Services*, *19*(3), 304-312.

Podsakoff, P.M. & Organ, D.W. (1986) Self-reports in organizational research: Problems and prospects, *Journal of Management Information Systems, 12*, 531–544.

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., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly*, *31*(1), 105-136.

Pierce, C. A., Aguinis, H., & Adams, S. K. (2000). Effects of a dissolved workplace romance and rater characteristics on responses to a sexual harassment accusation. *Academy of Management Journal*, *43*(5), 869-880.

Preacher, K. J., & Hayes, A. F. (2008). *Assessing Mediation in Communication Research* (pp. 13-54). London: The Sage Sourcebook of Advanced Data Analysis Methods for Communication Research.

Ratnasingham, P. (1999). Implicit trust in the risk assessment process of EDI. *Computers & Security*, *18(*4), 317-321.

Robert, L. P., Dennis, A. R., & Hung, Y. T. C. (2009). Individual swift trust and knowledge-based trust in face-to-face and virtual team members. *Journal of Management Information Systems*, *26*(2), 241-279.

Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social Psychophysiology: A Sourcebook*, 153-176.

Rosati, P., Cummins, M., Deeney, P., Gogolin, F., van der Werff, L., & Lynn, T. (2017). The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. *International Review of Financial Analysis*, *49*, 146-154.

Rosati, P., Deeney, P., Cummins, M., Van der Werff, L., & Lynn, T. (2019). Social media and stock price reaction to data breach announcements: Evidence from US listed companies. *Research in International Business and Finance*, *47*, 458-469.

Roumani, Y., Nwankpa, J. K., & Roumani, Y. F. (2016). Examining the relationship between firm's financial records and security vulnerabilities. *International Journal of Information Management*, *36*(6), 987-994.

Russ, G. S., Daft, R. L., & Lengel, R. H. (1990). Media selection and managerial characteristics in organizational communications. *Management Communication Quarterly*, *4*(2), 151-175.

Shaw, J. C., Wild, E., & Colquitt, J. A. (2003). To justify or excuse?: A meta-analytic review of the effects of explanations. *Journal of Applied Psychology*, *88*(3), 444.

Stone, R.N. & Grønhaug, K. (1993), Perceived risk: further considerations for the marketing discipline, *European Journal of Marketing*, *27*(3), 39-50.

Struijk, M., Ou, C. X.J., Davison, R. M., & Angelopoulos, S. (2022). Putting the IS back into IS research. *Information Systems Journal*. 32, 3, Pre-print, https://doi.org/10.1111/isj.12368.

Suh, B., & Han, I. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of Electronic Commerce*, *7(*3), 135-161.

Telang, R., & Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software Engineering*, *33(*8), 544-557.

Vedadi, A., & Warkentin, M. (2020). Can secure behaviors be contagious? A two-stage investigation of the influence of herd behavior on security decisions. *Journal of the Association for Information Systems*, *21*(2), 428-459.

Verhagen, T., Meents, S., & Tan, Y. H. (2006). Perceived risk and trust associated with purchasing at electronic marketplaces. *European Journal of Information Systems*, *15*(6), 542-555.

Wang, X., Lin, X., & Spencer, M. K. (2019). Exploring the effects of extrinsic motivation on consumer behaviors in social commerce: Revealing consumers' perceptions of social commerce benefits. *International Journal of Information Management*, *45*, 163-175.

Wang, Y., & Herrando, C. (2019). Does privacy assurance on social commerce sites matter to millennials?. *International Journal of Information Management*, *44*, 164-177.

Windasari, N. A., Lin, F. R., & Kato-Lin, Y. C. (2021). Continued use of wearable fitness technology: A value co-creation perspective. *International Journal of Information Management*, 57, 102292.

Yang, Y., Gong, Y., Land, L. P. W., & Chesney, T. (2020a). Understanding the effects of physical experience and information integration on consumer use of online to offline commerce. *International Journal of Information Management*, *51*, 102046.

Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology*, *26(*1), 60-77.

Zhao, A. L., Hanmer-Lloyd, S., Ward, P., & Goode, M. M. (2008). Perceived risk and Chinese consumers' internet banking services adoption. *International Journal of Bank Marketing*, *26*(7), 505-525.

Zhao, X., Lynch, J.G. & Chen, Q. (2010). Reconsidering Baron and Kenny: Myths and truths about mediation analysis. *Journal of Consumer Research*, *37*(2), 197-206.

Zheng, B.W., Liu, H.F. & Davison, R.M. (2018). Exploring the Relationship between Corporate Reputation and the Public's Crisis Communication on Social Media, *Public Relations Review* 44, 1, 56-64.

Appendix 1. Overview of Security Breach Literature Related to Stock Market

Study	# of Breach Events	Impacts on Stock Performance	Additional Findings
Goel & Shawky, 2009	168	-1% SM*	
Cavusoglu et al., 2004	66	-2.1% SM*	
Campbell et al., 2003	43 attacks, 38 firms	Yes	Confidential breaches impacted the financial performance significantly, whereas non-confidential breaches did not.
Telang & Wattal, 2007	147 incidents, 18 firms	-0.63% SM*	Greater loss if the business is small. Greater loss if the market is highly competitive. Change in stock price is greater when the breach is not fixed by the time the announcement is made. Greater loss if the security flaw is perceived to be more severe.
Ko & Dorantes, 2006	19		No long-term impact could be found.
Garg et al., 2003	22	-0.5%-1.0% AR**	
Hovav & D'Arcy, 2003	20		Only focuses on DoS (Denial of Service) attacks. Losses shown when the Websites were a component of the core sources of income.
Hovav & D'Arcy, 2004	186		The market does not penalize companies that are faced with a virus attack.
Yayla & Hu, 2011	104-123	-0.9% SM*	Pure E-commerce businesses are more heavily influenced than conventional brick and mortar stores. DoS attacks have a greater impact than other types of security breaches. Time period around the days of the breach influences the degree of impact. Results from event year show that breaches had a significant impact around 1994-2000, but not in the period of 2001-2006, indicating a change in attitude towards security breaches.
Gordon et al., 2011	121 incidents, 85 firms		Breaches related to availability had a significant impact on financial performance, but impact has shifted from significant of the major security incident to insignificant over time.

*SM: Stock Market; **AR: Annual Revenue

Appendix 2. Overview of Studies on Perceived Risk Dimensions

Risk Dimension / Study	Featherman & Pavlou, 2003	Crespo et al., 2009	Nepomuceno et al., 2014	Hassan et al., 2006	Pavlou, 2003	Forsythe et al., 2006	Bertea, 2015	Almousa, 2011	Ariffin et al, 2018
Financial	*	*	*	*	*	*	*	*	*
Privacy	*	*		*	*		*	*	*
Product / Performance	*	*	*	*	*	*		*	*
Time / Convenience	*	*	*	*		*		*	*
Psychological	*	*		*			*	*	*
Social	*	*		*			*	*	*
Physical				*	*				
Overall	*								

Note: * The risk dimension is investigated in the corresponding study.

Appendix 3. Survey Setup and the Vignettes

Before answering this questionnaire, please read the story on the next page carefully. Then keep this story in mind while responding to the questions following this story. This test takes about 15 minutes and is completely **anonymous**. Thank you for your participation.

Story for questionnaire (3*5 vignettes)

Consider the most recent web shop where you have purchased something. Any web shop may be chosen, but it must be a purchase that you have completed over the internet. During this purchase you have entered some details that were needed to complete the transaction. This data included your name, email address, password, home address, your telephone numbers, and also your bank or credit card number(s).

Now imagine that a few months after your purchase, the web shop is affected by a security breach.

[Then survey response will see one of the three types of security breaches, followed by one of the five organizational response strategies]

1. Vignettes for three types of security breaches (SB)

SB1 - Denial of Service

Specifically, the web shop experienced a Denial of Service (DoS) attack. The DoS attack is a cyber-attack that the attacker seeks to make the target services (i.e., services of web store in this case) unavailable to its legitimated users by temporarily or indefinitely disrupting services of the target. Though the web shop can limit the concurrent connections to its web store, the countermeasure is often prone to high degree of false-positives. That means that you, as a legitimated user, probably cannot access its web store either. In fact, indeed, if you visit its web store right now, you cannot access the store. You don't know when the attack will be over.

SB2 - Virus Attack

Specifically, the web shop experienced a malicious virus attack. Though it is not uncommon that web shops have anti-virus software to prevent such virus attacks, the virus apparently found its way to self-replicate in the web shop's computer system. As a result, at least some files and data, stored and recorded in the systems of the web shop were destroyed. That may include your personal information. In that case, you may need to retype the information again in your next shopping in this web shop. In any cases, the web shop needs to install patches to repair the damaged files and data. The repairs may lead to system downtime.

SB3 - Theft of information

Specifically, the web shop experienced an attack of theft of information. This means that privacy-sensitive data, recorded and stored in the web shop during your purchase transaction, was acquired by hackers. It is not uncommon that hackers publish data online or sell sensitive data to another party. This may grant other people access to your data. You may thus, for example, receive spam or malicious messages. Strange bank account transactions may also occur because your credit card data was sold. The combination of your email address and password may give others the opportunity to login to your accounts including your social media accounts, online bank accounts and email accounts.

2. Vignettes for five organizational response strategies (ORS)

CRS1 – No Response

[Message empty]

CRS2 - Defensive Strategy

You also learn that the web shop claims the breach occurred due to their security provider's negligence. The web shop itself only has limited or even no responsibilities.

CRS3 – Moderate Strategy

You also learn that the web shop states it has a strong history of data privacy. The web shop values the relationship with its customers and other stakeholders. The breach is rather an isolated act.

- For SB1: The web shop also claims that it believes the breach won't affect customers after the breach is fixed.
- For SB2: The web shop also claims that the lost data were encrypted and password protected.
- For SB3: The web shop also claims that it believes the breach won't affect customers after the breach is fixed. The web shop also claims that the lost data were encrypted and password protected.

CRS4 – Accommodating Strategy

You also learn that the web shop explicitly apologized for the occurrence of the security breach. The web shop also takes steps to repair and control the damage. Financial compensations are possible if customers experience damages during the attack.

CRS5 – Image Renewal

You also learn that the web shop claims it has implemented security measures to prevent a recurrence of such an attack. The web shop will, in any cases, help customers and other stakeholders. The web shop values stakeholders' privacy. It claims that safeguarding the privacy data is a top priority and that it committed to protect stakeholder data.

Appendix 4. Survey Items for Principal Constructs

Scale: Strongly disagree (1) ~ Strongly agree (7)

Perceived Financial Risk (Nepomuceno et al., 2014) o If I bought an item for myself within the next twelve months, I would be concerned that the decision to spend money on the item would not be wise. o Purchasing this item could involve important financial losses. o If I bought this item for myself within the next twelve months, I would be concerned that I would not get my money's worth.
Perceived Privacy Risk (Nepomuceno et al., 2014) o I feel my personal privacy is protected when shopping at this web shop. (Reverse coded) o I feel safe in my transactions when shopping at this web shop. (Reverse coded) o This web shop has adequate security features. (Reverse coded)
Perceived Time Risk (Nepomuceno et al., 2014) o Purchasing an item at this web shop could lead to an inefficient use of my time. o Purchasing an item at this web shop could involve important time losses. o Purchasing an item on this web shop wastes my time.
Perceived Performance Risk (Nepomuceno et al., 2014) o If I were to purchase an item within the next twelve months, I would become concerned that the item will not provide the level of benefits that I would be expecting. o As I consider the purchase of an item soon, I worry about whether it will really "perform" as well as it is supposed to. o The thought of purchasing an item at this web shop causes me to be concerned for how reliable that product will be.
Psychological Risk (Littler & Melanthiou, 2006; Zhao et al., 2008) o I would feel annoyed with myself in case I decided to use the web shop again and something went wrong in the transaction, since I would think I made the wrong decision to use the web shop. o If something went wrong with the web shop, I would feel frustrated. o If something went wrong with the web shop, I would feel concerned.
Social Risk (Hanafizadeh & Khedmatgozar, 2012; Featherman & Pavlou, 2003) o I am sure that if I decide to use the web shop again and mistakes or fraud happen in my transactions, I will lose my good position among my friends, family, and colleagues. o Using the web shop will negatively affect the way others think of me.
Severity (Herath & Rao, 2009) o The security breach affects me directly. o The security breach is severe. o I think security breach is serious and needs attention. o The security breach is exaggerated (Reverse coded).
Response efficacy (Li et al., 2019) o The organization's response will keep security breaches down. o Based on the organization's response, the chance of information security breaches occurring will be reduced. o The organization's response helps to solve the security problems
Intention to Re-transact (Pavlou, 2003) o When given the possibility I intend to use this web shop, knowing that it has been breached. o When given the possibility I predict that I should use this web shop in the future.

o It's likely that I will transact with this web shop in the near future.
Key Control Variable: Corporate reputation (Jarvenpaa et al., 1999; Park et al., 2012) o I believe that the web shop has a reputation for being fair. o The web shop is well respected. o This web shop has a reputation for being honest.
Key Control Variable: Response costs (Menard et al. 2017) o The organization's response is burdensome for me. o The organization's response would require too much from me. o The organization's response is not worth it.
Key Control Variable: Self-Efficacy (Lee & Larsen 2009) o It is easy for me to address this security breach issue. o I can fix the security breach problem by myself. o I have the capability to solve possible security beach errors or problems.

Appendix 5. Mediation Tests

```
Run MATRIX procedure:

***************** PROCESS Procedure for SPSS Version 4.0 *****************

          Written by Andrew F. Hayes, Ph.D.       www.afhayes.com
    Documentation available in Hayes (2022). www.guilford.com/p/hayes3

**************************************************************************
Model  : 4
    Y  : DV           (note: Y=DV=Intention to Re-Transact)
    X  : ORS          (note: X=IV=Organization Response Strategy)
   M1  : Risk         (note: Risk=Perceived Risk)
   M2  : Severity
   M3  : REffi        (note: REffi=Response Efficacy)

Sample
Size:  573

**************************************************************************
OUTCOME VARIABLE:
 RISK

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .2509      .0630      .9404    38.3629     1.0000   571.0000      .0000

Model
              coeff         se          t          p       LLCI       ULCI
constant      .5398      .0961     5.6181      .0000      .3511      .7285
ORS          -.1796      .0290    -6.1938      .0000     -.2365     -.1226

**************************************************************************
OUTCOME VARIABLE:
 Severity

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .0255      .0007     1.3588      .3716     1.0000   571.0000      .5424
```

```
Model
              coeff         se          t          p       LLCI       ULCI
constant     5.3463      .1155    46.2908      .0000     5.1194     5.5731
ORS           .0212      .0348      .6096      .5424     -.0472      .0897

************************************************************************
OUTCOME VARIABLE:
 REffi

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .5012      .2512     2.1414   191.5300     1.0000   571.0000      .0000

Model
              coeff         se          t          p       LLCI       ULCI
constant     2.3644      .1450    16.3081      .0000     2.0796     2.6492
ORS           .6054      .0437    13.8394      .0000      .5195      .6913

************************************************************************
OUTCOME VARIABLE:
 DV

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .7170      .5142     1.0635   150.2750     4.0000   568.0000      .0000

Model
              coeff         se          t          p       LLCI       ULCI
constant     4.9020      .2369    20.6929      .0000     4.4367     5.3673
ORS           .0368      .0357     1.0310      .3030     -.0333      .1068
RISK         -.9128      .0533   -17.1113      .0000    -1.0176     -.8081
Severity     -.1109      .0397    -2.7914      .0054     -.1889     -.0329
REffi         .0862      .0332     2.5946      .0097      .0210      .1515

****************** DIRECT AND INDIRECT EFFECTS OF X ON Y *****************

Direct effect of X on Y
     Effect         se          t          p       LLCI       ULCI
      .0368      .0357     1.0310      .3030     -.0333      .1068

Indirect effect(s) of X on Y:
            Effect     BootSE   BootLLCI   BootULCI
TOTAL         .2138      .0369      .1398      .2874
RISK          .1639      .0289      .1095      .2239
Severity     -.0024      .0039     -.0111      .0052
REffi         .0522      .0246      .0052      .1008

*********************** ANALYSIS NOTES AND ERRORS ************************

Level of confidence for all confidence intervals in output:
  95.0000

Number of bootstrap samples for percentile bootstrap confidence intervals:
  5000

------ END MATRIX -----
```

Online Supplementary Material I: Research Relevant to Security Breach Published at IJIM and AIS Senior Scholars' Basket of Eight Journals

Alkhowaiter, W. A. (2020). Digital payment and banking adoption research in Gulf countries: A systematic literature review. *International Journal of Information Management*, 53, 102102.

Al-Natour, S., Cavusoglu, H., Benbasat, I., & Aleem, U. (2020). An Empirical Investigation of the Antecedents and Consequences of Privacy Uncertainty in the Context of Mobile Apps. *Information Systems Research*, 31(4), 1037-1063.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3), 613-643.

Ayaburi, E. W., & Treku, D. N. (2020). Effect of penitence on social media trust and privacy concerns: The case of Facebook. *International Journal of Information Management*, 50, 171-181.

Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management*, 52, 102063.

Bang, Y., Lee, D. J., Bae, Y. S., & Ahn, J. H. (2012). Improving information security management: An analysis of ID–password usage and a new login vulnerability measure. *International Journal of Information Management*, 32(5), 409-418.

Bose, I., & Leung, A. C. M. (2019). Adoption of identity theft countermeasures and its short-and long-term impact on firm value. *MIS Quarterly*, 43(1), 313-327.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39(4), 837-864.

Breward, M., Hassanein, K., & Head, M. (2017). Understanding consumers' attitudes toward controversial information technologies: A contextualization approach. *Information Systems Research*, 28(4), 760-774.

Buckman, J. R., Bockstedt, J. C., & Hashim, M. J. (2019). Relative privacy valuations under varying disclosure characteristics. *Information Systems Research*, 30(2), 375-388.

Choi, B. C., Kim, S. S., & Jiang, Z. (2016). Influence of firm's recovery endeavors upon privacy breach on online customer behavior. *Journal of Management Information Systems*, 33(3), 904-933.

Crossler, R., & Posey, C. (2017). Robbing Peter to pay Paul: Surrendering privacy for security's sake in an identity ecosystem. *Journal of the Association for Information Systems*, 18(7), 2.

Culnan, M. J. (1993). "How did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly*, 17(3), 341-363.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, 31(2), 285-318.

de Gusmão, A. P. H., Silva, M. M., Poleto, T., e Silva, L. C., & Costa, A. P. C. S. (2018). Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. *International Journal of Information Management*, 43, 248-260.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61-80.

Donalds, C., & Osei-Bryson, K. M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*, 51, 102056.

Goldstein, J., Chernobai, A., & Benaroch, M. (2011). An event study analysis of the economic impact of IT operational risk and its subcategories. *Journal of the Association for Information Systems*, 12(9), 606-631.

Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action: An investigation of the Sony PlayStation network breach. *MIS Quarterly*, 41(3), 703-727.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly*, 34(3), 567-594.

Gwebu, K. L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, 35(2), 683-714.

Hoehle, H., Aloysius, J. A., Goodarzi, S., & Venkatesh, V. (2019). A nomological network of customers' privacy perceptions: linking artifact design to shopping efficiency. *European Journal of Information Systems*, 28(1), 91-113.

Hong, I. B., & Cha, H. S. (2013). The mediating role of consumer trust in an online merchant in predicting purchase intention. *International Journal of Information Management*, 33(6), 927-939.

Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly*, 37(1), 275-298.

Ioannou, A., Tussyadiah, I., & Lu, Y. (2020). Privacy concerns and disclosure of biometric and behavioral data for travel. *International Journal of Information Management*, 54, 102122.

Jung, Y., & Park, J. (2018). An investigation of relationships among privacy concerns, affective responses, and coping behaviors in location-based services. *International Journal of Information Management*, 43, 15-24.

Kumar, R. L., Park, S., & Subramaniam, C. (2008). Understanding the value of countermeasure portfolios in information systems security. *Journal of Management Information Systems*, 25(2), 241-280.

Lankton, N., McKnight, D. H., & Thatcher, J. B. (2014). Incorporating trust-in-technology into Expectation Disconfirmation Theory. *The Journal of Strategic Information Systems*, 23(2), 128-145.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45, 13-24.

Liang, H., Xue, Y., Pinsonneault, A., & Wu, Y. (2019). What users do besides problem-focused coping when facing it security threats: An emotion-focused coping perspective. *MIS Quarterly*, 43(2), 373-394.

Lin, T. C., Huang, S. L., & Chiang, S. C. (2018). User resistance to the implementation of information systems: A psychological contract breach perspective. *Journal of the Association for Information Systems*, 19(4), 306-332.

Luo, M. M., & Chea, S. (2018). Cognitive appraisal of incident handling, affects, and post-adoption behaviors: A test of affective events theory. *International Journal of Information Management*, 40, 120-131.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336-355.

Marakas, G. M., Yi, M. Y., & Johnson, R. D. (1998). The multilevel and multifaceted character of computer self-efficacy: Toward clarification of the construct and an integrative framework for research. *Information Systems Research*, 9(2), 126-163.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3), 334-359.

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, 34(4), 1203-1230.

Najjar, M. S., Kettinger, W. J., & Kettinger, L. D. (2021). IS incident recovery and service value: A service-dominant logic view. *European Journal of Information Systems*, 1-33, https://doi.org/10.1080/0960085X.2020.1869915.

Park, I., Sharman, R., & Rao, H. R. (2015). Disaster Experience and Hospital Information Systems. *MIS Quarterly*, 39(2), 317-344.

Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research*, 15(1), 37-59.

Pavlou, P. A., & Gefen, D. (2005). Psychological contract violation in online marketplaces: Antecedents, consequences, and moderating role. *Information Systems Research*, 16(4), 372-399.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly*, 31(1), 105-136.

Png, I. P., & Wang, Q. H. (2009). Information security: Facilitating user precautions vis-à-vis enforcement against attackers. *Journal of Management Information Systems*, 26(2), 97-121.

Ramachandran, M., & Chang, V. (2016). Towards performance evaluation of cloud service providers for cloud data security. *International Journal of Information Management*, 36(4), 618-625.

Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research*, 20(1), 121-139.

Samonas, S., Dhillon, G., & Almusharraf, A. (2020). Stakeholder perceptions of information security policy: Analyzing personal constructs. *International Journal of Information Management*, 50, 144-154.

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, 32(2), 314-341.

Shaw, N., & Sergueeva, K. (2019). The non-monetary benefits of mobile commerce: Extending UTAUT2 with perceived value. *International Journal of Information Management*, 45, 44-55.

Shin, B., Lee, S., & Lee, H. G. (2016). Examining an extended duality perspective regarding success conditions of IT service. *International Journal of Information Management*, 36(2), 226-239.

Shin, Y. Y., Lee, J. K., & Kim, M. (2018). Preventing state-led cyberattacks using the bright internet and internet peace principles. *Journal of the Association for Information Systems*, 19(3), 152-181.

Stacey, P., Taylor, R., Olowosule, O., & Spanaki, K. (2021). Emotional reactions and coping responses of employees to a cyber-attack: A case study. *International Journal of Information Management*, 58, 102298.

Susarla, A., Barua, A., & Whinston, A. B. (2003). Understanding the 'service' component of application service provision: An empirical analysis of satisfaction with ASP services. *MIS Quarterly*, 27(1), 91-123.

Syed, R. (2019). Enterprise reputation threats on social media: A case of data breach framing. The *Journal of Strategic Information Systems*, 28(3), 257-274.

Tan, L. M., & Newman, M. (1991). Computer misuse and the law. *International Journal of Information Management*, 11(4), 282-291.

Triche, J. H., & Walden, E. (2018). The use of impression management strategies to manage stock market reactions to IT failures. *Journal of the Association for Information Systems*, 19(4), 333-357.

Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, 7(6), 415-444.

Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems*, 15(10), 679-722.

Vedadi, A., & Warkentin, M. (2020). Can secure behaviors be contagious? A two-stage investigation of the influence of herd behavior on security decisions. *Journal of the Association for Information Systems*, 21(2), 428-459.

Venkatraman, S., MK Cheung, C., Lee, Z. W., D. Davis, F., & Venkatesh, V. (2018). The "darth" side of technology use: An inductively derived typology of cyberdeviance. *Journal of Management Information Systems*, 35(4), 1060-1091.

Wang, J., Xiao, N., & Rao, H. R. (2015). Research note—An exploration of risk characteristics of information security threats and related public information search behavior. *Information Systems Research*, 26(3), 619-633.

Xiao, B., & Benbasat, I. (2011). Product-related deception in e-commerce: A theoretical perspective. *MIS Quarterly*, 169-195.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, 12(12), 798-824.

Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of management information systems*, 26(3), 135-174.

Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2012). Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. *Information Systems Research*, 23(4), 1342-1363.

Yang, Q., Gong, X., Zhang, K. Z., Liu, H., & Lee, M. K. (2020b). Self-disclosure in mobile payment applications: Common and differential effects of personal and proxy control enhancing mechanisms. *International Journal of Information Management*, 52, 102065.

Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology*, 26(1), 60-77.

Yu, L., Li, H., He, W., Wang, F. K., & Jiao, S. (2020). A meta-analysis to explore privacy cognition and information disclosure of internet users. *International Journal of Information Management*, 51, 102015.

Online Supplementary Material II: Self Loading and Cross Loading

	Component											
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
CORPORATEREPUTATION_1	**0.867**	-0.009	-0.015	0.149	-0.042	-0.014	-0.070	0.000	0.037	-0.016	-0.022	-0.099
CORPORATEREPUTATION_2	**0.819**	-0.034	0.081	0.050	-0.079	-0.103	-0.127	0.022	0.096	0.079	0.073	-0.087
CORPORATEREPUTATION_3	**0.873**	0.029	0.039	0.101	-0.020	-0.084	-0.008	0.025	-0.012	-0.001	0.008	-0.025
CORPORATEREPUTATION_4	**0.862**	-0.097	0.131	0.003	-0.070	-0.087	-0.019	-0.006	0.060	-0.020	-0.061	0.016
FINANCIAKRISK_1	-0.074	0.201	-0.164	-0.017	0.296	0.159	0.230	0.032	0.164	0.227	0.136	**0.717**
FINANCIAKRISK_2	-0.052	0.154	-0.177	0.018	0.238	0.137	0.187	0.060	0.240	0.274	0.161	**0.733**
FINANCIAKRISK_3	-0.088	0.157	-0.228	0.008	0.415	0.003	0.348	0.114	0.168	0.137	0.271	**0.539**
PRIVACYRISK_1R	-0.108	0.002	-0.300	-0.254	0.040	**0.800**	0.021	-0.227	0.047	0.082	-0.025	0.096
PRIVACYRISK_2R	-0.106	-0.052	-0.332	-0.244	0.082	**0.786**	0.087	-0.224	0.115	0.084	-0.045	0.138
PRIVACYRISK_3R	-0.073	-0.069	-0.302	-0.335	0.071	**0.757**	0.089	-0.204	0.052	0.110	-0.139	0.076
PERFORMANCERISK_1	-0.123	0.155	-0.047	0.060	0.364	-0.013	**0.701**	0.155	0.107	0.115	0.294	0.080
PERFORMANCERISK_2	-0.059	0.181	-0.101	-0.024	0.200	0.082	**0.777**	0.081	0.085	0.173	0.239	0.290
PERFORMANCERISK_3	-0.049	0.186	-0.153	-0.049	0.197	0.143	**0.750**	0.065	0.113	0.199	0.213	0.316
PSYCHOLOGICALRISK_1	0.037	0.103	-0.153	0.019	0.127	0.237	0.340	0.006	0.120	**0.625**	0.149	0.312
PSYCHOLOGICALRISK_2	0.015	0.031	-0.108	-0.044	0.132	0.005	0.046	-0.112	0.179	**0.873**	0.058	0.071
PSYCHOLOGICALRISK_3	0.018	0.025	-0.011	0.005	0.081	0.079	0.122	-0.027	0.227	**0.846**	0.025	0.186
SOCIALRISK_1	0.047	0.184	0.034	0.175	0.224	-0.097	0.244	0.219	0.065	0.077	**0.796**	0.157
SOCIALRISK_2	0.012	0.203	0.010	0.175	0.233	-0.055	0.232	0.192	0.065	0.092	**0.806**	0.149
TIMERISK_1	-0.067	0.231	-0.058	0.016	**0.781**	0.093	0.248	0.113	0.076	0.183	0.198	0.291
TIMERISK_2	-0.041	0.221	-0.085	0.022	**0.779**	0.092	0.221	0.107	0.090	0.165	0.253	0.265
TIMERISK_3	-0.093	0.222	-0.101	0.028	**0.735**	0.047	0.280	0.122	0.063	0.118	0.287	0.272
PERCEIVEDSEVERITY_1	0.068	0.139	-0.002	0.036	0.037	0.216	0.081	0.076	**0.778**	0.189	0.053	0.128
PERCEIVEDSEVERITY_2	0.042	0.155	-0.120	-0.031	0.047	0.007	0.105	-0.033	**0.811**	0.105	0.144	0.239
PERCEIVEDSEVERITY_3	0.065	0.044	-0.155	-0.019	0.092	-0.028	0.044	-0.069	**0.820**	0.233	-0.012	0.036
RESPONSEEFFICACY_1	0.094	0.043	0.157	**0.886**	0.059	-0.145	0.018	0.178	-0.027	-0.047	0.101	0.009
RESPONSEEFFICACY_2	0.085	-0.018	0.166	**0.862**	0.001	-0.255	-0.002	0.172	-0.003	0.014	0.117	-0.004
RESPONSEEFFICACY_3	0.081	0.000	0.167	**0.854**	-0.001	-0.271	-0.009	0.148	0.021	0.002	0.139	-0.002

	Component											
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
RESPONSECOSTS_1	-0.021	**0.836**	0.024	0.080	0.180	-0.012	0.210	0.160	0.090	0.051	0.160	0.105
RESPONSECOSTS_2	-0.001	**0.827**	-0.045	-0.094	0.211	0.015	0.127	0.098	0.126	0.088	0.120	0.185
RESPONSECOSTS_3	-0.031	**0.679**	-0.088	-0.008	0.182	-0.071	0.169	0.090	0.290	0.059	0.330	0.220
RESPONSECOSTS_4	-0.090	**0.700**	-0.054	0.101	0.242	-0.070	0.181	0.187	0.126	0.047	0.327	0.211
SELFEFFICACY_1	0.031	0.027	0.147	0.228	0.086	-0.189	-0.004	**0.814**	-0.033	0.034	-0.046	-0.041
SELFEFFICACY_2	-0.012	0.170	0.088	0.128	0.090	-0.169	0.126	**0.774**	-0.003	-0.112	0.325	0.144
SELFEFFICACY_3	0.002	0.167	0.057	0.121	0.093	-0.164	0.138	**0.794**	0.010	-0.110	0.299	0.071
RETRANSACTIONINTEN_1	0.071	-0.033	**0.859**	0.201	-0.067	-0.259	-0.095	0.120	-0.114	-0.103	-0.015	-0.156
RETRANSACTIONINTEN_2	0.075	-0.018	**0.849**	0.183	-0.084	-0.286	-0.088	0.100	-0.131	-0.097	-0.023	-0.127
RETRANSACTIONINTEN_3	0.049	-0.049	**0.833**	0.167	-0.081	-0.315	-0.103	0.116	-0.099	-0.088	0.030	-0.164

Extraction Method: Principal Component Analysis.
Rotation Method: Equamax with Kaiser Normalization.

a. Rotation converged in 14 iterations.