NAVIGATING THE LANDSCAPE OF IT THREATS: A LITERATURE REVIEW AND THE ROAD AHEAD

Completed Research Paper

Marco Meier, University of Bamberg, Bamberg, Germany, marco.meier@uni-bamberg.de

Abstract

说白了就是2024年又研究了一遍老话题?

Users face various information technology (IT) threats in their daily lives. They affect users by evoking emotions such as fear and require them to engage in behaviors such as changing their passwords. While research offers rich insights into how IT threats generally influence users, it does not contrast different types of IT threats that likely influence how they affect users. Drawing on the stimulus-organism-response model, we conducted a literature review on information systems (IS) research on IT threats to identify the different types of IT threats and their influence on users. Findings reveal different types of IT threats, how they influence users' perceptions, emotions, and behaviors, and the contextual factors that guide these relationships. We contribute to IS research by painting a holistic picture of extant knowledge on IT threats and crafting an agenda for future research.

Keywords: IT threat, User Behavior, Stimulus-Organism-Response Model, Literature Review.

1 Introduction

本文可以说是罔顾技术带来的便利, 只看缺点

Information technology (IT) threats such as data breaches, phishing attacks, and viruses are prevalent in users' daily lives (Brooks, 2023). IT threats describe any potential damages stemming from external IT related entities (Liang et al., 2019). They affect users, letting them develop emotions such as exhaustion and fear (Cheikh-Ammar, 2020; Schuetz et al., 2021) and requiring them to engage in behaviors such as using security IT (Liang et al., 2019). To help users navigate IT threats, it is essential to gain an overview of how users perceive IT threats and how they influence their behavior.

引出了关键点

Literature offers insights into users' perceptions of IT threats (Schuetz et al., 2021) and how users respond to them (Vedadi et al., 2021). When users encounter an IT threat, they develop perceptions about it, such as how threatening and avoidable it is to them (Liang et al., 2019). Their perceptions of the IT threat cause emotions such as fear (Mattson et al., 2023), which let them engage in behaviors such as spreading negative word of mouth against the IT they deem responsible (Son and Kim, 2008).

While there is rich research into IT threats in general (Liang and Xue, 2010; Lowry et al., 2023), IT threats related to users' privacy (Cheikh-Ammar, 2020), and IT threats related to users' security (Schuetz et al., 2021), conceptual boundaries of the different types of IT threats are fuzzy. For instance, research into privacy IT threats may include threats to users' security, such as spyware (Malhotra et al., 2004), and research into security IT threats may include threats to users' privacy, such as data breaches (Wang et al., 2015). However, indications suggest that different types of IT threats can vary in their influence on users. For instance, privacy IT threats such as data breaches let users switch away from the breached IT (Nikkhah and Grover, 2022), while security IT threats such as getting infected with malware let users adopt security IT (Liang et al., 2019). Such indications point to differences in how users perceive and respond to privacy and security IT threats, suggesting a need to differentiate types of IT threats and their influence on users.

We draw on the stimulus-organism-response (S-O-R) model to consider such differences. The S-O-R model suggests that individuals who perceive external stimuli develop organismic reactions, such as

引入一个模型, 居然还是跨领域的

The stimulus-response model was first procedure to understand the buyer behavior of consumers. The consciousness of the Buyer depends upon the marketing and environmental stimuli while purchase decisions are succefully done with the help of the Buyer's characteristics and decision process.

perceptions and emotions, which in turn shape their response in the form of behavior (Mehrabian and Russell, 1974). These insights align well with the IT threat context, in which different IT threats as external stimuli let users develop perceptions and emotions that influence their behavior.

We advance the understanding of IT threats by considering different types with previously studied perceptions, emotions, and behaviors to craft a holistic perspective that informs future research in that field. We ask the following research question:

这个问题太大了

What is the status quo of IS research on IT threats?

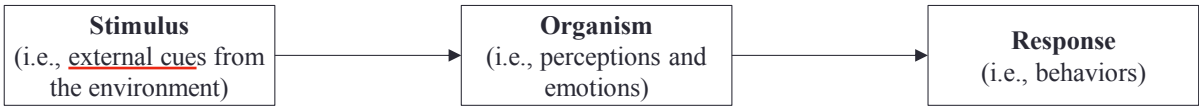
Following a concept centric literature review method (Wolfswinkel et al., 2013), we reviewed 29 IT threat studies to outline the status quo of IS research on IT threats. Our literature review identifies different types of IT threats and their influence on users' perceptions, emotions, and behaviors. In addition to that, we identify contextual factors that guide these relationships. We draw from these insights to sketch out an overview of extant knowledge of IT threats and develop an agenda for future research.

The remainder of this paper is structured as follows. After describing the S-O-R model as this study's theoretical lens, we present our methodological approach for reviewing the literature. We then describe our results and provide an overview of extant IT threat literature. We close by discussing our findings and their limitations and outlining an agenda for future IT threat research.

2 Stimulus-Organism-Response Model

The S-O-R model describes a conceptual framework to explain individuals' reactions to external cues (Mehrabian and Russell, 1974). It posits that when individuals experience an external cue from their environment, i.e., *stimulus*, it activates their internal cognitive and affective processes that let them develop perceptions and emotions, i.e., *organism*, which in turn determines their resulting behavior, i.e., *response* (see Figure 1) (Mehrabian and Russell, 1974). IS research draws on the S-O-R model to explain user behaviors across various contexts, for instance, why users discontinue using an IT (Luqman et al., 2017), contribute to crowdfunding campaigns (Hou et al., 2023), or spend money at certain websites (Benlian, 2015).

突出一下SOR模型是有用的



ie 换种说法

Figure 1. Stimulus-organism-response model.

In the context of IT threats, the S-O-R model helps understand how IT threats affect users, as it offers a theoretical framework for capturing the entire process from when users experience an IT threat to how they form their perceptions and emotions and how these shape their resulting behaviors. IT threats are defined as any potential damages stemming from external IT related entities (Liang et al., 2019), which aligns well with the S-O-R model's understanding of stimuli as external cues from individuals' environment (Belk, 1975). As such, the S-O-R model affords the opportunity to consider different types of IT threats as stimuli, such as IT threats related to users' privacy or security. Its organism component allows us to reflect on users' perceptions and emotions when experiencing IT threats and their vital role in users' behavioral response to IT threats. By considering IT threats as external stimuli and users' organisms in terms of their perceptions and behaviors, it provides a comprehensive framework to understand behavior as a response to IT threats. Next, we describe our methodological approach for reviewing IS literature on IT threats informed by the S-O-R model.

3 Methodology

We used a systematic and concept centric literature review method to review IS research on IT threats, allowing us to extend the theory by drawing on insights from extant literature (Wolfswinkel et al., 2013).

从文献找例子

This literature review method is established in IS research, offering insights into various contexts, such as disruptive events that influence user behavior (Meier et al., 2022), fake news (George et al., 2021), and digital transformation (Vial, 2019). We reviewed the literature focusing on IT threats and how they influence users to craft a holistic understanding of them. We outline the literature review procedure in Table 1.

可以借鉴, 把文献研究的过程列个表

广义到狭义

Step	Task	Application in this study
1. Definition	Defining criteria for inclusion and exclusion	IT threat studies from 1980-2023
	Identification of research disciplines	IS research
	Determination of appropriate sources	Top IS journals (AIS senior scholars' list of premier journals[1])
	Initial search terms	"IT threat", "information technology threat", "IS threat", "information system threat"
	哈哈这个我熟Iteratively added search terms	"Privacy threat", "Security threat"
2. Search	Search execution	Search in selected top IS journals using the Web of Science database, forward and backward citation searches 这里很重要, 看看老师怎么选
3. Selection	Sample refinement	Final sample of 29 articles 我们要找几篇做读后感???
4. Analysis	Open coding	Identification of IT threats and related concepts
	Axial coding	Refinement of IT threats and related concepts
	Selective coding	Categorization of identified concepts to stimuli (i.e., types), organism (i.e., perceptions, emotions), response (i.e., behaviors), and contextual factors related to IT threats and identification of the relationships between them
5. Present	Structure content	Crafting an overview of IT threat research

Table 1. Literature review method.

We began by determining the scope of the literature review. We included IS literature published since 1980 in eleven top IS journals to cover relevant articles on IT threats. We initially searched for relevant articles using the terms "IT threat", "information technology threat", "IS threat", and "information system threat" in the title, abstract, or keywords and iteratively added "privacy threat" and "security threat" as search terms, as they are commonly used terms for IT threats in relevant articles. We used wildcards with the identified search terms to include plurals (e.g., "IT threat$"). 额...

The initial search yielded 51 articles among the searched IS journals. We scanned those articles based on title, abstract, and subsequently full text to identify relevant articles on IT threats that align with our definition. While IT threats may target users or organizations (Liang & Xue, 2009; Yeh & Chang, 2007), we focus on users' perspectives to provide a holistic understanding of how IT threats affect them, so we filtered out articles on IT threats' influence on organizations (Yeh and Chang, 2007) or IT infrastructure (Ryan and Bordoloi, 1997). We also did not include articles that focus on users as originators of IT threats (Chatterjee et al., 2015), resulting in a sample of 21 articles on IT threats. We then conducted forward and backward citation searches to detect further relevant articles missed by the keyword search, identifying eight additional relevant articles. In total, we identified 29 articles on IT threats and their influence on users. In line with previous research (Meier et al., 2022), we present a flow chart of the literature search and selection procedure (see Figure 2).

[1] https://aisnet.org/page/SeniorScholarListofPremierJournals

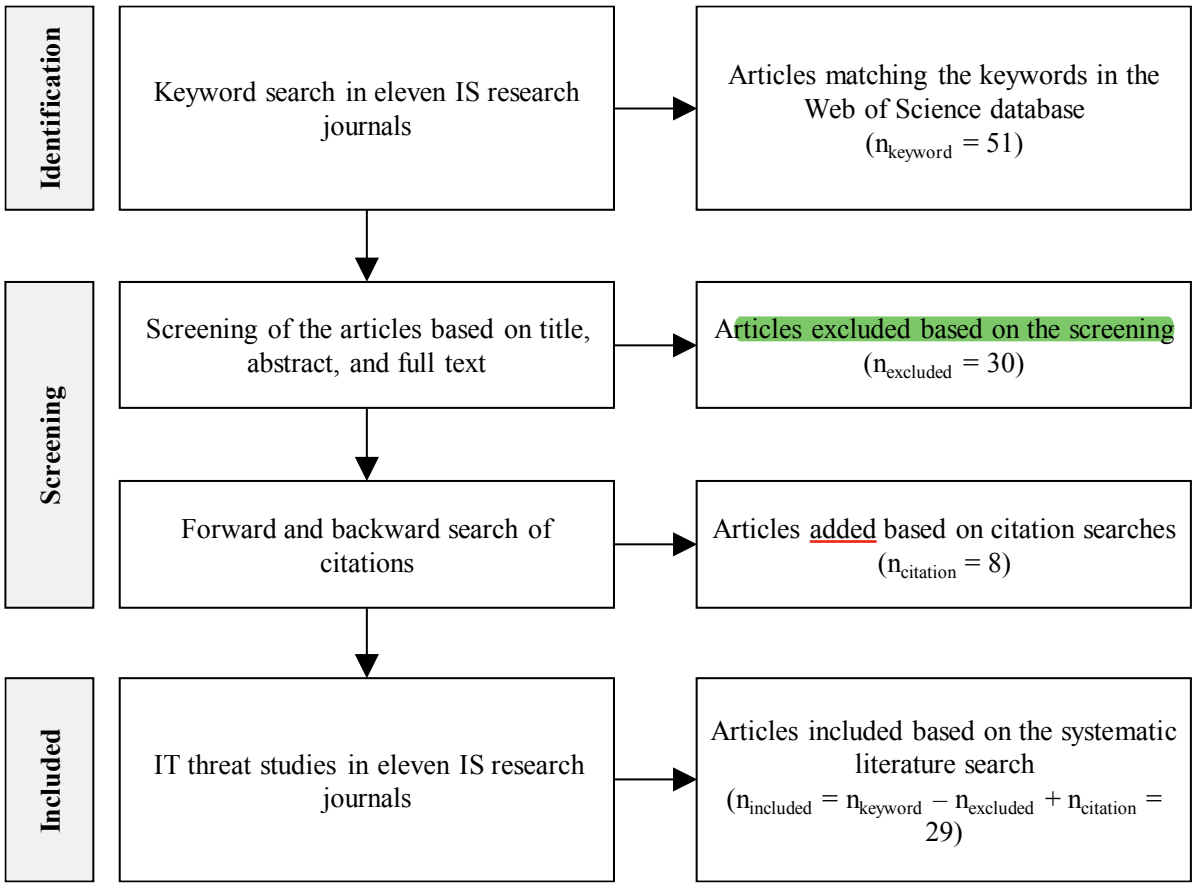


Figure 2. Flowchart of the literature search.

又能水页数了!

We reviewed the articles based on methodological recommendations for concept centric literature review approaches (Wolfswinkel et al., 2013). We first highlighted statements related to IT threats, i.e., any statements that describe potential damages stemming from external IT related entities (Liang et al., 2019). Using open coding, we then identified the studied IT threats and related concepts, i.e., concepts that influence IT threats or are influenced by them. For instance, we coded the following statement as an *IT threat*: "*[…] Internet users may face many other threats, such as man-in-the-middle attacks, typosquatting, cybercrimes, and fake websites […]*" (Chen et al., 2022). Similarly, we coded this statement as a *related concept* to an IT threat: "*Seeking help focuses on users' efforts to seek information and advice in dealing with security threats*" (Chen and Zahedi, 2016).

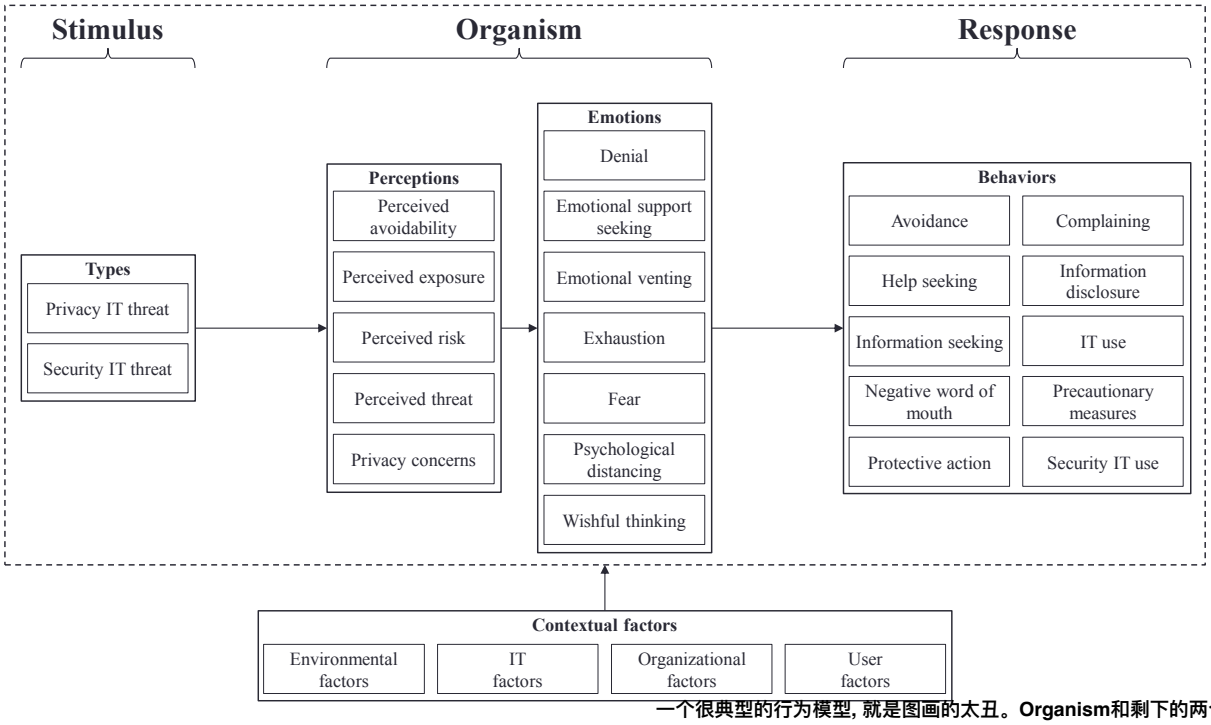
下定义

We used axial coding to refine the resulting codes for IT threats and related concepts. For instance, we refined the code *IT threat* to *security IT threat* and *related concept* to *help seeking*. Informed by the S-O-R model (Mehrabian and Russell, 1974), we then used selective coding to identify the concepts' relationships and categorize them into *types* (i.e., stimulus), *perceptions* and *emotions* (i.e., organism), *behaviors* (i.e., response), and *contextual factors*. For instance, we identified *security IT threat* as a *type* of IT threat and *help seeking* as a *behavior* in response to IT threats. This enables us to craft a comprehensive overview of how IT threats evoke, how users perceive them, and how they are influenced by them.

4 Results

We summarize the findings of our literature review in this section. Drawing on various theoretical lenses, including conservation of resources theory (Cheikh-Ammar, 2020), protection motivation theory (Schuetz et al., 2020), technology threat avoidance theory (Liang and Xue, 2009), and health belief model (Ng et al., 2009), extant literature studies stimuli in the form of different types of IT threats,

organism in the form of perceptions and emotions, responses in the form of behaviors, and contextual factors that influence the relationships between them (see Figure 3 and Table 2 in the Appendix).



一个很典型的行为模型, 就是图画的太丑。Organism和剩下的两个都不是一类
但是图中没有区分

Figure 3. Overview of research on IT threats.

4.1 Types as stimulus

无论人家有没有缺陷, 都得自夸一下

IT threats are facilitated by IT, either stemming directly from IT (Liang and Xue, 2010) or from human actors using IT (Chen et al., 2021). Our literature review reveals that extant work either studies IT threats in general (Lowry et al., 2023) or specifically focuses on privacy IT threats (Ozdemir et al., 2017) or security IT threats (Chen et al., 2022) (see Table 2 in the Appendix). Privacy IT threats encompass threats directed at unauthorized disclosure or misuse of personal information (Chen et al., 2021). They include, for instance, data breaches (Chen et al., 2021; Wang et al., 2015), data misuse (Ozdemir et al., 2017), and potential loss associated with disclosing personal information in general (Cheikh-Ammar, 2020; Malhotra et al., 2004; Son and Kim, 2008).

Security IT threats encompass threats directed at harming users' IT resources (Wang et al., 2015). They include, among others, cyberattacks such as hacking attacks (Schuetz et al., 2021), password theft (Vedadi et al., 2021), and phishing (Dincelli and Chengalur-Smith, 2020; Mady et al., 2023) and encounters with malicious IT such as adware (Wang et al., 2015), spyware (Mattson et al., 2023), and ransomware (Mady et al., 2023; Marett and Nabors, 2021) (see Table 2 in the Appendix).

4.2 Perceptions and emotions as organism

When users experience a stimulus such as an IT threat, it initiates a cognitive process that lets them form their perceptions about it (Johnston and Warkentin, 2010). Based on the specific IT threat users experience, they evaluate how threatening it is to them and how they can respond to it (Liang et al., 2019). They assess how threatening it is to them based on the degree to which they believe its consequences will severely harm them and the degree to which they are susceptible to it. Following this argumentation, literature shows that users assess how exposed they are to an IT threat, which guides whether they feel at risk when using a specific IT (Chen et al., 2021). When users perceive it as

threatening, they assess if it is avoidable, i.e., if a behavior can protect them from the IT threat's potential negative consequences and if they are able to perform this behavior (Liang and Xue, 2009). When the IT threat potentially involves users' personal information, as is the case for most privacy IT threats (Cheikh-Ammar, 2020), users develop privacy concerns, which describes their subjective view of fairness related to the collection of their personal information by third parties, their control over their personal information, and their awareness of what the third party does with their personal information (Malhotra et al., 2004).

Based on their perceptions of an IT threat, users develop different emotions. IT threats can make them feel tired and mentally drained, such that they feel exhausted about an IT related to an IT threat (Cheikh-Ammar, 2020). When users perceive an IT threat as highly threatening, it evokes negatively valenced emotions, such as anxiety, worry, and fear (Liang and Xue, 2009; Mattson et al., 2023; Schuetz et al., 2021). To defend themselves against such negative emotions, users engage in emotion focused coping, such as trying to distance themselves psychologically from the IT threat, denying that it happened, and engaging in wishful thinking (Liang et al., 2019). It can also cause them to vent emotionally and seek emotional support (Liang et al., 2019).

这用词...

这重复...

4.3 Behavior as response

好主意! 就盯着几个大牛的文章引用

Based on the evoked emotions, users engage in different behaviors to respond to the IT threat. Users may seek help or additional information about an IT threat (Chen and Zahedi, 2016; Wang et al., 2015) and engage in protective actions such as using security IT (Chen et al., 2022; Mattson et al., 2023) or choosing complex passwords (Chen and Zahedi, 2016). To avoid future IT threats, users may take precautionary actions, such as regularly backing up their data and being more cautious when engaging with IT (Liang and Xue, 2010; Marett and Nabors, 2021). They may also reduce their information disclosure (Dincelli and Chengalur-Smith, 2020) or stop using IT related to an IT threat (Cheikh-Ammar, 2020). IT threats can also let users engage in negative behaviors directed at the third party they deem responsible, such as blaming an organization related to the IT threat by complaining and spreading negative word of mouth (Son and Kim, 2008).

4.4 Contextual factors

好一个环境因素!

In addition to type as stimulus, perception and emotion as organism, and behavior as a response, literature on IT threats identifies various contextual factors related to the environment, IT, organization, or user that guide the relationships between identified types, perceptions, emotions, and behaviors, i.e., if and how users perceive and respond to IT threats.

Regarding environmental factors, studies identify users' social environment as an important contextual factor influencing their perceptions and responses to IT threats (Liang and Xue, 2009). Users who feel highly uncertain about how to proceed regarding an IT threat may discount their own information and imitate others in their behavior to use security IT or not, irrespective of their own perceptions (Vedadi et al., 2021). Related to that, the literature suggests that the different contexts users are embedded in, e.g., cultural, geographic, philosophical, political, and task context, guide whether users perceive to be susceptible to IT threats (Frank et al., 2022) and how their IT threat perceptions influence behaviors (Marett and Nabors, 2021). For instance, users who witnessed severe adverse effects of an IT threat nearby without themselves being directly affected seem to be more likely to engage in precautionary measures such as using security IT (Marett and Nabors, 2021).

Regarding IT factors, studies suggest that the type of information users share with an IT influences how they feel at risk of IT threats, such that users who disclose more sensitive information to an IT feel more at risk (Malhotra et al., 2004). Similarly, concrete warnings make them more likely to perceive a potential IT threat as actually threatening (Schuetz et al., 2020). Related to that, users who trust in a used IT are less likely to expect an IT threat related to it (Chen et al., 2021), and users who rely on security IT have better chances of avoiding and mitigating IT threats (Zahedi et al., 2015). Maladaptive rewards, i.e., the rewards gained from not mitigating an IT threat, make users less likely to engage in protective behaviors (Schuetz et al., 2020). While perceived usefulness makes them more likely to continue using

an IT despite it being related to an IT threat (Chen et al., 2021), psychological ownership toward an IT lets them engage in protective actions directed to it (Anderson and Agarwal, 2010). Similarly, perceived usefulness and ease of use make users more likely to use security IT (Herath et al., 2014).

新瓶装旧酒

Regarding organizational factors, users' perceived justice of how an organization related to an IT threat treats them makes them more likely to keep disclosing their personal information to the organization's IT. Societal benefits associated with complaining about the organization make them more likely to complain directly to the organization or other third parties (Son and Kim, 2008). At work, sanction severity, i.e., the degree to which violations of security policies are perceived as problematic, and sanction certainty, i.e., how promptly sanctions follow violations, guide whether users comply with security policies such as changing passwords (Johnston et al., 2015). Related to that, users' commitment to their organization guides how their perceptions and emotions influence their protective actions (Posey et al., 2015).

就是把别人不同的多种观点组织一下, 再划分段落写成自己的文章

In terms of user factors, users' disposition to value privacy guides how concerned they are about potential IT threats (Chen et al., 2021), and their risk tolerance influences if they perceive an IT event as a threat and how they respond to it (Liang and Xue, 2009). While users who previously experienced IT threats are more concerned about experiencing IT threats (Ozdemir et al., 2017), those who conducted security education, training, and awareness (SETA) measures (Dincelli and Chengalur-Smith, 2020) and gained knowledge on IT threats are more likely to avoid IT threats (Mady et al., 2023; Marett and Nabors, 2021). In addition, their psychological capital in terms of hope, self-efficacy, optimism, and resilience makes them more likely to use security IT to protect themselves from IT threats (Mattson et al., 2023). Citizen effectiveness, i.e., users' belief that they can make a difference for the better in a specific situation, lets them engage in protective action toward an IT resource (Anderson and Agarwal, 2010).

5 Discussion

嗯, 确实是全盘的, 挺全面就是言之无物 😐

Our study draws on the S-O-R model to provide a holistic overview of research on types, perceptions, emotions, behaviors, and contextual factors related to IT threats. We next discuss how our findings contribute to IS literature to foster an understanding of IT threats and their influence on users.

贡献可以夸大

5.1 Implications for research

IS literature studies IT threats in general (Liang and Xue, 2009), privacy IT threats (Ozdemir et al., 2017), and security IT threats (Schuetz et al., 2021). In doing so, the literature largely focuses on distinct IT threats without distinguishing and contrasting them, resulting in some conceptual overlap between privacy and security IT threats. By comprehensively reviewing the literature on IT threats, we distinguish between different types of IT threats. Privacy IT threats describe threats directed at unauthorized disclosure or misuse of users' personal information, such as data breaches that expose their data to unauthorized third parties (Chen et al., 2021). Contrary to that, security IT threats describe IT threats directed at harming a user's IT resources, such as malware that infects their personal computers (Liang et al., 2019). This suggests that privacy and security IT threats are conceptually different, the former targeting users' personal information and the latter targeting their IT resources. We contribute to IS research on IT threats by suggesting that privacy and security IT threats should be differentiated from each other and require distinct theoretical attention.

这种总结还是不错的

While cumulative research essentially covers the whole nomological network around IT threats, studies largely focus on a narrow set of perceptions such as perceived threat (Chen and Zahedi, 2016), emotions such as fear (Boss et al., 2015), and behaviors such as protective action (Posey et al., 2015) (see Table 2 in the Appendix). By drawing on the S-O-R model, we emphasize that two different types of IT threats as stimuli work as antecedents to established perceptions, suggesting a need to consider them in explanations of IT threats' influence on users. In addition to that, our literature review sheds light on the diverse perceptions, emotions, and behaviors studied in the context of IT threats (see Figure 3), affording opportunities for crafting more comprehensive explanations for how IT threats influence users. We add

to IS literature on IT threats by offering a comprehensive overview of relevant factors for a holistic understanding of IT threats and drawing on these insights to develop an agenda for future research.

Studies identify contextual factors that guide the relationship between types, perceptions, emotions, and behaviors related to IT threats (see Figure 3). For instance, social influence and risk tolerance influence whether users perceive a specific IT event as a threat and how they respond to it (Liang and Xue, 2009). Our literature review reveals that contextual factors along the dimensions of environmental factors, such as users' social environment (Frank et al., 2022), IT factors such as the perceived usefulness of an IT related to an IT threat (Chen et al., 2021), organizational factors such as perceived justice of an organization related to an IT threat (Son and Kim, 2008), and user factors such as psychological capital guide how users perceive and respond to IT threats (Mattson et al., 2023). With this, we contribute to IS literature on IT threats by pinpointing the relevant dimensions of contextual factors requiring attention when studying IT threats.

5.2 Implications for practice

这里分成不同的条目来说明论文对实践的贡献, 还是不错的

Our study offers a starting point for organizations to navigate potential IT threats associated with the IT they offer to their users.

Managing stimuli. Users may eventually experience IT threats related to your organization, causing them to develop perceptions and emotions about it that guide their response. Their perceptions and emotions depend on the available information about an IT threat, making it essential that your organization proactively manages how the IT threat is communicated to users. To avoid unfavorable user responses to IT threats, organizations should craft efficient communication strategies beforehand that they can rely on in case of IT threats.

Guiding organisms. Foster users' perceptions of IT threats when they occur to support them in taking protective actions. Whether users engage in behaviors that protect them from potentially negative consequences of IT threats is subject to their perceptions of it (Liang and Xue, 2009). This makes it essential that users recognize potentially harmful IT events as IT threats. Organizations can foster users' perceptions of IT threats by issuing concrete warning messages (Schuetz et al., 2020), e.g., by communicating information on an IT threat and its specific negative consequences via email to potentially affected users.

Controlling responses. Beware of users' behaviors that are harmful to your organization. Users may take actions to protect themselves from an IT threat's negative consequences while at the same time engaging in behavior harmful to the organization related to the IT threat, such as spreading negative word of mouth (Son and Kim, 2008). One reason users may engage in such behaviors is privacy concerns related to an IT threat, so organizations should strive to alleviate users' privacy concerns by, for instance, certifying their processes involving collecting or processing users' personal information with established privacy seals.

5.3 Limitations

Our study has some limitations. While this study reviews eleven top IS journals to provide a broad overview of previous work on IT threats, future research should complement these insights by extending the scope to include IS studies published in conference proceedings and IS journals for emerging topics. This study provides a comprehensive overview of the status quo on IT threats from the users' perspective but does not consider IT threats from an organizational or technological perspective. As such, it excludes the negative consequences of IT threats on organizations (Yeh and Chang, 2007) and their IT infrastructure (Ryan and Bordoloi, 1997). While we used iteratively refined keywords for the literature search in combination with forward and backward citation searches to ensure we identified all relevant studies on IT threats in the IS discipline, we did not include keywords for specific IT threats such as typosquatting and logic bomb (see Table 2 in the Appendix). We encourage future research to build on our study and identify the full bandwidth of diverse IT threats and their influence on users, organizations, and technical infrastructure.

如此检索

5.4 Avenues for future research

Our findings point to several promising avenues for future research.

Research opportunity 1: Process. Extant literature largely builds on users' perceptions to explain their emotions and behaviors (Liang et al., 2019). Future work should explain users' thought processes that let them develop their perceptions, e.g., whether a specific IT event is threatening or avoidable. A promising starting point may be to draw on information processing theory (Simon, 1978) to offer a richer understanding of how users translate initial information about a potential IT threat, e.g., reading about it on the news for the first time, into a set of perceptions that guides their emotions and behaviors. To offer insights into users' processing of IT threats and how their perceptions, emotions, and behaviors evolve over time, future research may profit from leveraging longitudinal study designs. Since users' perceptions and emotions that guide their behaviors may change as they gain more information about an IT threat, revealing users' processing of IT threats can provide valuable insights for research and practical information security measures.

Research opportunity 2: Different IT threat types. Our findings reveal privacy and security IT threats as two distinct types of IT threats. Future research should compare privacy and security IT threats to contrast how they differ in their influence on users' perceptions. One opportunity is to employ configurational perspectives (Meier et al., 2023; Tan et al., 2016), thus identifying the paths from different types of IT threats to the same or different perceptions, emotions, and behaviors.

Research opportunity 3: IT threat experience. Another promising direction for future research is considering users' prior experiences with similar IT threats. While research shows that users who previously experienced IT threats are more concerned about IT threats (Ozdemir et al., 2017), it offers no empirical insights into how such experience may influence their emotions and behaviors in case they experience a similar IT threat again. For instance, users may know how to react to an IT threat due to their previous experiences (Lowry et al., 2023), making them more likely to engage in effective protective behaviors. We encourage research taking theoretical perspectives considering such repeated events, e.g., habituation (Vance et al., 2018), to study how users' prior experiences guide their protective behavior when encountering repeated IT threats.

Research opportunity 4: Interventions. Extant literature offers insights into why users are concerned about IT threats (Chen et al., 2021) and what makes them more or less likely to fall victim to IT threats (Dincelli and Chengalur-Smith, 2020). While such studies provide organizations with a lever to influence users' experience and perception of IT threats, they offer few insights into the factors that guide how their perceptions of IT threats relate to their emotions and behaviors when they experience IT threats. Future research should identify interventions that influence the relationship between perceptions, emotions, and behaviors. For instance, studies may investigate if behavioral interventions, such as digital nudges (Carmichael et al., 2022; Falconnet et al., 2023), provide opportunities to make users more likely to engage in protective behavior when they encounter IT threats, e.g., nudge them to change passwords after they fall victim to a data breach.

Research opportunity 5: Positive consequences. Extant literature largely focuses on the negative consequences of IT threats and behaviors to avoid them (see Figure 3). Future research should extend these insights by investigating potential positive consequences. For instance, users who encounter an IT threat may initially face its negative consequences but may profit from it by growing stronger after successfully dealing with it. While they may be able to use this experience to fend off similar IT threats in the future (see research opportunity 3), it may also help them build up knowledge that helps them successfully cope with other stressful IT events, such as IT interruptions (Addas and Pinsonneault, 2018).

Research opportunity 6: Additional contextual factors. Previous work offers insights into a variety of contextual factors, including environmental factors such as the cultural context (Chen and Zahedi, 2016), IT factors such as perceived usefulness (Chen et al., 2021), organizational factors such as organizational commitment (Posey et al., 2015), and user factors such as the disposition to value privacy (Chen et al., 2021). Future research should extend these insights by incorporating additional contextual factors, such as users' digital literacy level or emotional resilience. In doing so, a promising avenue is

to determine if there are boundary conditions for users' behaviors (Meier et al., 2024), e.g., if users need to have high digital literacy levels to protect themselves from an IT threat's potential negative consequences.

6 Conclusion

Users frequently encounter IT threats that affect them in various ways. Following indications that different types of IT threats vary in their influence on users, we draw on the S-O-R model to conduct a literature review that leverages the status quo of IS research on IT threats and integrates types, perceptions, emotions, behaviors, and contextual factors related to IT threats. We contribute by identifying privacy and security IT threats as conceptually different IT threats that require distinct theoretical attention, providing a holistic overview of research on IT threats, and pinpointing dimensions of contextual factors that guide users' perceptions, emotions, and behaviors related to IT threats. In doing so, we support future research on IT threats by pointing to promising research directions.

References

Addas, S. and Pinsonneault, A. (2018). "E-Mail Interruptions and Individual Performance: Is There a Silver Lining?," *MIS Quarterly* 42 (2), 381–405.

Anderson, C. L. and Agarwal, R. (2010). "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly* 34 (3), 613–643.

Belk, R. W. (1975). "Situational Variables and Consumer Behavior," *Journal of Consumer Research* 2 (3), 157–164.

Benlian, A. (2015). "Web Personalization Cues and Their Differential Effects on User Assessments of Website Value," *Journal of Management Information Systems* 32 (1), 225–260.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and 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.

Brooks, C. (2023). "Cybersecurity Trends & Statistics For 2023; What You Need To Know," *Forbes*.

Carmichael, L., Poirier, S.-M., Coursaris, C. K., Léger, P.-M., and Sénécal, S. (2022). "Users' Information Disclosure Behaviors during Interactions with Chatbots: The Effect of Information Disclosure Nudges," *Applied Sciences* 12 (24), 12660.

Chatterjee, S., Sarker, S., and Valacich, J. S. (2015). "The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical IT Use," *Journal of Management Information Systems* 31 (4), 49–87.

Cheikh-Ammar, M. (2020). "The bittersweet escape to information technology: An investigation of the stress paradox of social network sites," *Information & Management* 57 (8), 103368.

Chen, R., Kim, D. J., and Rao, H. R. (2021). "A study of social networking site use from a three-pronged security and privacy threat assessment perspective," *Information & Management* 58 (5), 103486.

Chen, Y., Luo, X., and Li, H. (2022). "Beyond adaptive security coping behaviors: Theory and empirical evidence," *Information & Management* 59 (2), 103575.

Chen, Y. and Zahedi, F. (2016). "Individual's Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China," *MIS Quarterly* 40 (1), 205–222.

Dincelli, E. and Chengalur-Smith, I. (2020). "Choose your own training adventure: designing a gamified SETA artefact for improving information security and privacy through interactive storytelling," *European Journal of Information Systems* 29 (6), 669–687.

Falconnet, A., Coursaris, C. K., Beringer, J., Van Osch, W., Sénécal, S., and Léger, P.-M. (2023). "Improving User Experience with Recommender Systems by Informing the Design of Recommendation Messages," *Applied Sciences* 13 (4), 2706.

Frank, M., Jaeger, L., and Ranft, L. M. (2022). "Contextual drivers of employees' phishing susceptibility: Insights from a field study," *Decision Support Systems* 160, 113818.

George, J., Gerhart, N., and Torres, R. (2021). "Uncovering the Truth about Fake News: A Research Model Grounded in Multi-Disciplinary Literature," *Journal of Management Information Systems* 38 (4), 1067–1094.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., and Rao, H. R. (2014). "Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service," *Information Systems Journal* 24 (1), 61–84.

Hou, J.-R., Zhang, J., and Zhang, K. (2023). "Pictures that are Worth a Thousand Donations: How Emotions in Project Images Drive the Success of Online Charity Fundraising Campaigns? An Image Design Perspective," *MIS Quarterly* 47 (2), 535–584.

Johnston, A. C. and Warkentin, M. (2010). "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* 34 (3), 549.

Johnston, A. C., Warkentin, M., and Siponen, M. (2015). "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric," *MIS Quarterly* 39 (1), 113–134.

Liang, H. and Xue, Y. (2009). "Avoidance of Information Technology Threats: A Theoretical Perspective," *MIS Quarterly* 33 (1), 71–90.

Liang, H. and Xue, Y. (2010). "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems* 11 (7), 394–413.

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

Lowry, P. B., Moody, G. D., Parameswaran, S., and Brown, N. J. (2023). "Examining the Differential Effectiveness of Fear Appeals in Information Security Management Using Two-Stage Meta-Analysis," *Journal of Management Information Systems* 40 (4), 1099–1138.

Luqman, A., Cao, X., Ali, A., Masood, A., and Yu, L. (2017). "Empirical investigation of Facebook discontinues usage intentions based on SOR paradigm," *Computers in Human Behavior* 70, 544–555.

Mady, A., Gupta, S., and Warkentin, M. (2023). "The effects of knowledge mechanisms on employees' information security threat construal," *Information Systems Journal* 33 (4), 790–841.

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

Marett, K. and Nabors, M. (2021). "Local learning from municipal ransomware attacks: A geographically weighted analysis," *Information & Management* 58 (7), 103482.

Mattson, T., Aurigemma, S., and Ren, J. (2023). "Positively Fearful: Activating the Individual's HERO Within to Explain Volitional Security Technology Adoption," *Journal of the Association for Information Systems* 24 (3), 664–699.

Mehrabian, A. and Russell, J. A. (1974). *An approach to environmental psychology*, Cambridge, MA, US: The MIT Press.

Meier, M., Maier, C., Thatcher, J. B., and Weitzel, T. (2022). "Shocks and IS user behavior: a taxonomy and future research directions," *Internet Research* 33 (3), 853–889.

Meier, M., Maier, C., Thatcher, J. B., and Weitzel, T. (2023). "Cooking a telework theory with causal recipes: Explaining telework success with ICT, work and family related stress," *Information Systems Journal*.

Meier, M., Maier, C., Thatcher, J. B., and Weitzel, T. (2024). "Chatbot interactions: How consumption values and disruptive situations influence customers' willingness to interact," *Information Systems Journal*.

Ng, B.-Y., Kankanhalli, A., and Xu, Y. (2009). "Studying users' computer security behavior: A health belief perspective," *Decision Support Systems* 46 (4), 815–825.

Nikkhah, H. and Grover, V. (2022). "An Empirical Investigation of Company Response to Data Breaches," *MIS Quarterly* 46 (4), 2163–2196.

Ozdemir, Z. D., Jeff Smith, H., and Benamati, J. H. (2017). "Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study," *European Journal of Information Systems* 26 (6), 642–660.

Posey, C., Roberts, T. L., and Lowry, P. B. (2015). "The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets," *Journal of Management Information Systems* 32 (4), 179–214.

Ryan, S. D. and Bordoloi, B. (1997). "Evaluating security threats in mainframe and client/server environments," *Information & Management* 32 (3), 137–146.

Schuetz, S. W., Lowry, P. B., Pienta, D. A., and Thatcher, J. B. (2020). "The Effectiveness of Abstract Versus Concrete Fear Appeals in Information Security," *Journal of Management Information Systems* 37 (3), 723–757.

Schuetz, S. W., Lowry, P. B., Pienta, D. A., and Thatcher, J. B. (2021). "Improving the Design of Information Security Messages by Leveraging the Effects of Temporal Distance and Argument Nature," *Journal of the Association for Information Systems* 22 (5), 1376–1428.

Simon, H. A. (1978). "Information-processing theory of human problem solving," In *Handbook of learning & cognitive processes*, 271–295. Oxford, England: Lawrence Erlbaum.

Siponen, M., Adam Mahmood, M., and Pahnila, S. (2014). "Employees' adherence to information security policies: An exploratory field study," *Information & Management* 51 (2), 217–224.

Son and Kim. (2008). "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly* 32 (3), 503–529.

Tan, C.-W., Benbasat, I., and Cenfetelli, R. T. (2016). "An exploratory study of the formation and impact of electronic service failures," *MIS Quarterly* 40 (1), 1–29.

Vance, A., Jenkins, J. L., Anderson, B. B., Bjornn, D. K., and Kirwan, C. B. (2018). "Tuning Out Security Warnings: A Longitudinal Examination of Habituation Through fMRI, Eye Tracking, and Field Experiments," *MIS Quarterly* 42 (2), 355–380.

Vedadi, A., Warkentin, M., and Dennis, A. (2021). "Herd behavior in information security decision-making," *Information & Management* 58 (8), 103526.

Vial, G. (2019). "Understanding digital transformation: A review and a research agenda," *Journal of Strategic Information Systems* 28 (2), 118–144.

Wang, J., Xiao, N., and Rao, H. R. (2015). "An Exploration of Risk Characteristics of Information Security Threats and Related Public Information Search Behavior," *Information Systems Research* 26 (3), 619–633.

Wolfswinkel, J. F., Furtmueller, E., and Wilderom, C. P. M. (2013). "Using grounded theory as a method for rigorously reviewing literature," *European Journal of Information Systems* 22 (1), 45–55.

Yeh, Q.-J. and Chang, A. J.-T. (2007). "Threats and countermeasures for information system security: A cross-industry study," *Information & Management* 44 (5), 480–491.

Zahedi, F., Abbasi, A., and Chen, Y. (2015). "Fake-Website Detection Tools: Identifying Elements that Promote Individuals' Use and Enhance Their Performance," *Journal of the Association for Information Systems* 16 (6), 448–484.

Appendix

Reference	Stimuli	Organism	Response	Contextual factors	Theoretical lens
(Anderson and Agarwal, 2010)	Types: Security IT threat (hacking attack)	Perceptions: Security threat concern, self efficacy	Behaviors: Protective action	Environmental factors: Subjective norm, descriptive norm User factors: psychological ownership, citizen effectiveness	Protection motivation theory

(Boss et al., 2015)	Types: Security IT threat (data loss, virus)	Perceptions: Perceived threat severity, perceived threat vulnerability, response efficacy, self efficacy, response costs Emotions: Fear	Behaviors: Protective action, Security IT use	IT factors: Maladaptive rewards	Protection motivation theory
(Cheikh-Ammar, 2020)	Types: Privacy IT threat (potential loss associated with disclosure of personal information)	Emotion: Exhaustion	Behaviors: IT use	/	Regulatory focus theory, conservation of resources theory
(Chen and Zahedi, 2016)	Types: Security IT threat (phishing)	Perceptions: Perceived threat (perceived susceptibility, perceived severity), perceived response efficacy, perceived self-efficacy	Behaviors: Protective action, help seeking, avoidance	Environmental factors: Cultural context, philosophical context, political context, technological context	Protection motivation theory
(Chen et al., 2021)	Types: Privacy IT threat (privacy breach), security IT threat (cyber attack)	Perceptions: Perceived cyber-attack exposure, perceived SNS risk, privacy breach concern, internet risk perception	Behaviors: IT use	IT factors: Perceived usefulness, trust in social networking site (SNS) members, trust in SNS User factors: Disposition to value privacy	/
(Chen et al., 2022)	Types: Security IT threat (man in the middle attack, typosquatting, cybercrimes, fake websites, malware)	Perceptions: Perceived security threat (perceived susceptibility, perceived severity), perceived coping efficacy (perceived self-efficacy, perceived response efficacy)	Behaviors: Protective action, help seeking, avoidance	IT factors: Internet trust	Extended parallel process theory, coping theory
(Dincelli and Chengalur-Smith, 2020)	Types: Security IT threat (phishing, spear phishing, burglary, password hacking, identity theft)	/	Behaviors: Online self disclosure	User factors: Security education, training, and awareness (SETA)	/
(Frank et al., 2022)	Types: Security IT threat (phishing)	Perceptions: Phishing susceptibility	/	Environmental factors: Social context (help desk reliance, team leadership, team size), task context (job level, job experience, job status), physical context (workspace, region)	/
(Herath et al., 2014)	Types: Security IT threat (phishing, spam, malware)	Perception: Risk perception, self efficacy, privacy concerns	Behavior: Security IT use	IT factors: perceived usefulness, perceived ease of use	Technology acceptance model, technology threat avoidance theory

(Johnston and Warkentin, 2010)	Types: Security IT threat (spyware)	Perceptions: Perceived threat severity, perceived threat susceptibility, response efficacy, self efficacy	Behaviors: Security IT use	Environmental factors: Social influence	Protection motivation theory
(Johnston et al., 2015)	Types: Security IT threat (password theft, USB theft, data theft)	Perceptions: Perceived threat severity, perceived threat susceptibility, perceived self efficacy, perceived response efficacy	Behaviors: Compliance (password change)	Organizational factors: Formal sanction certainty, informal sanction certainty, formal sanction severity, informal sanction severity	Protection motivation theory, deterrence theory
(Liang and Xue, 2009)	Types: IT threat (malicious IT)	Perceptions: Perceived threat (perceived susceptibility, perceived severity), perceived avoidability (perceived effectiveness, perceived costs, self efficacy) Emotions: Emotion focused coping	Behaviors: Avoidance	Environmental factors: Social influence User factors: Risk tolerance	Cybernetic loop, technology threat avoidance theory
(Liang and Xue, 2010)	Types: IT threat (malicious IT)	Perceptions: Perceived threat (perceived severity, perceived susceptibility), safeguard effectiveness, safeguard costs, self-efficacy	Behaviors: Avoidance	/	Technology threat avoidance theory
(Liang et al., 2019)	Types: IT threat (malware)	Perceptions: Perceived threat, perceived avoidability Emotions: Denial, psychological distancing, wishful thinking, emotional support seeking, venting	Behaviors: Security IT use	/	Coping theory
(Lowry et al., 2023)	Types: IT threat	Perceptions: Perceived threat severity, perceived threat vulnerability, self-efficacy, response efficacy, response cost Emotions: Fear	Behaviors: Protection motivation	/	Extended parallel process model, protection motivation theory
(Mady et al., 2023)	Types: Security IT threat (phishing, ransomware)	Perceptions: Threat undesirability, coping feasibility	Behaviors: Protection motivation	User factors: Knowledge breadth, knowledge depth, knowledge finesse	Construal level theory
(Malhotra et al., 2004)	Types: Privacy IT threat (disclosing personal information to a website)	Perceptions: Privacy concerns (collection, control, awareness), risk beliefs	Behaviors: Information disclosure	IT factors: Type of information, trusting beliefs	Social contract theory

(Marett and Nabors, 2021)	Types: Security IT threat (ransomware)	/	Behaviors: Precautionary measures	Environmental factors: Geographic context (distance to recent ransomware attack) User factors: Information security learning efforts, IT security threats experience	Social learning theory
(Mattson et al., 2023)	Types: Security IT threat (spyware)	Perceptions: Perceived threat severity, perceived response efficacy, perceived threat vulnerability, perceived response costs Emotions: Fear	Behaviors: Security IT use	User factors: Psychological capital (hope, self efficacy, resilience, optimism)	/
(Ng et al., 2009)	Types: Security IT threat (virus)	Perceptions: Perceived susceptibility, perceived severity, self efficacy	Behaviors: Protective action	IT factors: Perceived benefits	Health belief model
(Ozdemir et al., 2017)	Types: Privacy IT threat (data misuse)	Perceptions: Privacy concerns, risk	Behaviors: Information disclosure	IT factors: Benefits, trust User factors: Privacy experiences, privacy awareness	/
(Posey et al., 2015)	Types: Security IT threat	Perceptions: Threat vulnerability, threat severity, response efficacy, self efficacy, response costs Emotions: Fear	Behaviors: Protection motivation, protective action	IT factors: Maladaptive rewards Organizational factors: Organizational commitment User factors: Security education, training, and awareness (SETA)	Protection motivation theory
(Schuetz et al., 2020)	Types: Security IT threat (spear phishing)	Perceptions: Perceived severity, perceived vulnerability, response efficacy, self efficacy, response costs Emotions: Fear	Behaviors: Protection motivation, compliance	IT factors: Maladaptive rewards, message abstractness	Protection motivation theory, construal level theory
(Schuetz et al., 2021)	Types: Security IT threat (hacking attack)	Perceptions: Threat severity, threat vulnerability, response efficacy, self efficacy, response costs Emotions: Fear	Behaviors: Security IT use	/	Construal level theory
(Siponen et al., 2014)	Types: Security IT threat (hacking attack)	Perceptions: Severity, vulnerability, response efficacy, self efficacy	Behaviors: Compliance	Environmental factors: Normative beliefs	Protection motivation theory, theory of reasoned action, cognitive evaluation theory

(Son and Kim, 2008)	Types: Privacy IT threat (online companies requesting personal information)	Perceptions: Privacy concern	Behaviors: Refusal, misrepresentation, removal, negative word of mouth, complaining	Organizational factors: Perceived justice (interactional justice, procedural justice, distributive justice), societal benefits from complaining	/
(Vedadi et al., 2021)	Types: Security IT threat (password theft)	Perceptions: Perceived uncertainty, response efficacy, self efficacy	Behaviors: Security IT use	Environmental factors: Popularity information, discounting own information, imitation	Protection motivation
(Wang et al., 2015)	Types: Security IT threat (spyware, adware, hacking attack, data breach, phishing, virus, spam, malware, logic bomb	Perceptions: risk characteristics (unknown risk, dread risk)	Behaviors: Information seeking	/	Information foraging theory
(Zahedi et al., 2015)	Types: Security IT threat (fake website)	Perceptions: Security IT response efficacy, coping self efficacy, threat severity, threat susceptibility	Behaviors: Security IT reliance	IT factors: Security IT accuracy, security IT speed, cost of security IT error	Protection motivation theory, theory of detection tool impact

Table 2. IS literature on IT threats.