Journal of Cybersecurity Education, Research and Practice

Volume 2022 | Number 2 Article 5

January 2023

Risk perceptions about personal Internet-of-Things: Research directions from a multi-panel Delphi study

Paul M. Di Gangi
University of Alabama at Birmingham, pdigangi@uab.edu

Barbara A. Wech
University of Alabama-Birmingham, bawech@uab.edu

Jennifer D. Hamrick
University of Alabama at Birmingham, jdhamrick@uab.edu

James L. Worrell
University of Alabama - Birmingham, worrellj@uab.edu

Samuel H. Goh
University of Alabama at Birmingham, sgoh@uab.edu

Recommended Citation

Di Gangi, Paul M.; Wech, Barbara A.; Hamrick, Jennifer D.; Worrell, James L.; and Goh, Samuel H. (2023) "Risk perceptions about personal Internet-of-Things: Research directions from a multi-panel Delphi study," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2022: No. 2, Article 5.
DOI: 10.32727/8.2023.4
Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2022/iss2/5

Risk perceptions about personal Internet-of-Things: Research directions from a multi-panel Delphi study

Abstract

Internet-of-Things (IoT) research has primarily focused on identifying IoT devices' organizational risks with little attention to consumer perceptions about IoT device risks. The purpose of this study is to understand consumer risk perceptions for personal IoT devices and translate these perceptions into guidance for future research directions. We conduct a sequential, mixed-methods study using multi-panel Delphi and thematic analysis techniques to understand consumer risk perceptions. The results identify four themes focused on data exposure and user experiences within IoT devices. Our thematic analysis also identified several emerging risks associated with the evolution of IoT device functionality and its potential positioning as a resource for malicious actors to conduct security attacks.

Keywords

Internet-of-Things, Delphi, thematic analysis, risk perceptions, Internet-of-Behaviors

Cover Page Footnote

Not Applicable

INTRODUCTION

This study seeks to understand the security risks associated with personal Internet-of-Things (IoT) devices. Industry reports predict that personal IoT devices will reach 125 million devices in the next decade (Strous, von Solms, & Zúquete, 2021), representing the beginning of an 8 trillion U.S. dollar market (Oberländer, Röglinger, Rosemann, & Kees, 2017). While no unifying definition for IoT exists, research has generally conceptualized it as "*uniquely identifiable physical objects embedded with electronics, sensors/actuators, software, and wireless network connectivity that enable these objects to exchange data over the internet with low energy consumption*" (Adamopoulos, Todri, & Ghose, 2020, p. 1). The data capturing abilities of these devices enable organizations to generate consumer insights that promise to disrupt society and organizations over the coming decades (Baesens, Bapna, Marsden, Vanthienen, & Zhao, 2016; Nicolescu, Huth, Radanliev, & De Roure, 2018).

While IoT has drawn interest from a range of disciplines, scholars have advocated for a deliberate examination of the risks IoT pose to organizations and consumers (Choo, Gai, Chiaraviglio, & Yang, 2021; Goad, Collins, & Gal, 2021; Jacobsson, Boldt, & Carlsson, 2016; March, 2019). For instance, Chanson, Bogner, Bilgeri, Fleisch, and Wortmann (2019) note how IoT creates challenges for organizations concerning their privacy policies and adoption of security measures. More recently, President Biden raised awareness for understanding the security risks of IoT devices, with the National Institute of Standards and Technology (NIST) releasing guidance to organizations about assessing consumer IoT device security (National Institute of Standards and Technology, 2022).

Organizationally-oriented IoT research has responded with a sense of urgency (Chang, Chang, & Liao, 2020), while consumer-oriented research has focused on general risk perceptions affecting IoT adoption and usage (e.g., Klobas, McGill, & Wang, 2019). Given the link between corporate and consumer interest in embedding IoT devices within their personal lives, personal IoT risk research must advance as systematically as the research on the organization side. Thus, the purpose of this study is to understand personal IoT device risk perceptions.

There are several differences between personal and organizational IoT environments (Strous et al., 2021; Teubner & Stockhinger, 2020). IoT within an organization is typically centrally managed and secured by security professionals. In contrast, home networks are usually less sophisticated, with few Internet-connected devices (Goad et al., 2021). Adopting personal IoT devices increases home network complexity, making them targets for malicious actors (Blythe & Johnson, 2021; Menard & Bott, 2020). More troublesome is that many of these devices are susceptible to attack (Barcena & Wueest, 2015; Jacobsson et al., 2016;

Klobas et al., 2019). Understanding how consumers view personal IoT device risks could inform research directions that may contribute to IoT research and practice.

This study addresses the following research questions: *What risks do consumers identify concerning personal IoT devices?* and *How can these perceptions about personal IoT risk guide future research?* In doing so, this study makes several contributions. First, we demonstrate the variety of risks consumers consider when evaluating personal IoT devices. Second, we highlight ways scholars can contextualize risk when researching personal IoT devices.

This study unfolds as follows. First, we synthesize the IoT risk literature and identify underlying trends. We then discuss our research approach, which includes a multi-panel Delphi to understand what risks consumers perceive are the most dangerous to personal IoT devices. We validate these perceptions by replicating the approach with three distinct panels. A thematic analysis was conducted on the rationales behind panelists' risk decisions to identify additional risk factors and themes. We conclude by discussing how these risks may be positioned within the existing literature and propose research directions to guide scholars to maximize both academic and practitioner impact.

RESEARCH ON THE INTERNET-OF-THINGS

IoT devices are objects embedded with electronics, sensors/actuators, and software that wirelessly connect with other objects to exchange data (Adamopoulos et al., 2020). A critical characteristic defining these devices is that they reside on low energy-consuming hardware (Jacobsson et al., 2016). As a result, these devices are relatively simple to deploy and present numerous business and consumer opportunities but limit the ability of the IoT device to offer security protections.

Organization-focused IoT research has noted the importance of quality data extracted from these devices to enhance business value through new consumer insights (Baesens et al., 2016; Côrte-Real, Ruivo, & Oliveira, 2020). For instance, vehicle telematics data provides insurance organizations with driving behavior insights to obtain a more accurate risk assessment when profiling drivers and calculating insurance premiums tailored to their consumers (Baecke & Bocca, 2017). Personal IoT research, in contrast, has primarily focused on wearables, such as smartwatches and fitness trackers (Benbunan-Fich, 2019; Goad et al., 2021; Shin, 2017; Tarafdar & Bose, 2021; Wessel et al., 2019) and smart home devices (e.g., Jacobsson et al., 2016; Klobas et al., 2019; Lin & Bergmann, 2016; Menard & Bott, 2020). Research on wearables has shown they empower consumers to control their health status (De Moya & Pallud, 2020; Wessel et al., 2019) by reducing the active effort of the consumer (Tarafdar & Bose, 2021).

Unsurprisingly, there have been numerous calls for studying IoT consumer privacy concerns and potential legal or regulatory efforts (Jacobsson et al., 2016; Nicolescu et al., 2018; Sicari, Cappiello, De Pellegrini, Miorandi, & Coen-Porisini, 2016; Whitmore, Agarwal, & Xu, 2015). Sicari et al. (2016) argues privacy will be fundamental to IoT research, with Li, Xu, and Zhao (2015) noting its enhanced role given the focus on tracking personal activities and sharing data with organizations. However, little beyond this observation is developed within the IoT risk literature. Oberländer et al. (2017) found very few studies have explored IoT in a Business-to-Consumer context, with Strous et al. (2021) specifically concerned that research has not considered IoT-specific risks.

Several scholars present personal IoT device use cases to highlight these risks while calling for research on IoT devices (e.g., Jacobsson et al., 2016; Lin & Bergmann, 2016). Personal IoT risk has continued to focus on wearable devices in terms of the adverse side effects (e.g., disempowerment and privacy concerns from using wearables (De Moya & Pallud, 2020)). Other personal IoT devices, such as smart home devices have also received attention, highlighting privacy concerns influencing adoption and usage decisions made by consumers (Klobas et al., 2019; Menard & Bott, 2020; Wunderlich, Veit, & Sarker, 2019). Menard and Bott (2020) highlight IoT risks concerning remote management, connectivity between devices, and the lack of transparency concerning data sharing by businesses in discussing IoT's importance as a focal phenomenon of study while adopting a non-IoT-specific risk belief construct. It is difficult to ascertain whether contextualizing survey items with IoT-specific risks may reveal additional insights on privacy concerns or consumer behaviors such as adoption and disclosure behaviors.

Only a handful of studies appear to account for specific risks unique to the personal IoT setting (e.g., Blythe & Johnson, 2021). Goad et al. (2021), for instance, operationalizes their contextual variables concerning the type of information shared in their discrete choice model for IoT device purchase choice by referencing information sharing with third parties for commercial and non-commercial purposes. Wunderlich et al. (2019) focus on privacy risk relating to information disclosure (i.e., sharing information outside its intended purpose) and control over one's data. Personal IoT risk research's limited progress relative to organization-focused IoT risk suggests personal IoT risk is underdeveloped within the current literature. Furthermore, the impact specific risks associated with IoT devices may play, as advocated by prior scholars (Jacobsson et al., 2016; Strous et al., 2021), indicates identification and examination of relative criticality could provide opportunities for the advancing understanding within the security field.

METHODOLOGY

We adopted a multi-panel Delphi approach to understand, verify, and validate consumer risk perceptions by consumers concerning personal IoT devices. Additionally, we utilized thematic analysis to draw further insights into consumer risk perceptions based on panelists' risk decision explanations.

Delphi Methodology

The Delphi method is "*a structured, iterative group decision process where a fixed-sized panel of individuals are tasked with reaching consensus on a specific task or issue*" (Di Gangi, Johnston, Worrell, & Thompson, 2018, p. 1104). The technique is used in a variety of disciplines that seek to understand risk perceptions, including information systems (Skinner, Nelson, Chin, & Land, 2015) and information security (Chang et al., 2020). The technique synthesizes individual participant concerns into a refined, consensus-driven, prioritized list that provides a framework for further inquiry (Di Gangi et al., 2018; Skinner et al., 2015; Worrell, Di Gangi, & Bush, 2013). In the present study, we utilize a seeded, ranking-type Delphi study using three distinct panels of potential IoT consumers.

Panel Selection and Composition

The Delphi method relies on panelists' suitability to represent its intended target audience (Skinner et al., 2015; Worrell et al., 2013). Our intended target was consumers of personal IoT devices. We utilized a multi-panel design, with each panel drawing from their unique individual perspectives on the risk of IoT devices as consumers. Prior research indicates there is no a priori ideal panel size, nor are panels required to be evenly distributed when multi-panel designs are deployed (Worrell et al., 2013). For instance, Di Gangi et al. (2018) explored organizational social media risk perceptions with panel sizes ranging from 9 to 25 participants.

In the present study, an ideal panelist is a consumer of personal products. Consequently, a sample of undergraduate and graduate students enrolled in a medium-sized, urban university business program were solicited to participate as panelists. We conducted a multi-panel design to demonstrate reliability in our findings for personal IoT risk perceptions. In total, 149 individuals participated across three Delphi panels. For descriptive purposes, we adapted a 4-item measure of self-efficacy by Compeau and Higgins (1995) for personal IoT devices.

Each panel, identified as Group 1, Group 2, and Group 3, was conducted independently to avoid introducing external influences that may affect the consensus process that drives the Delphi method's success. Group 1 was composed of 23 undergraduate students, 20 males and 3 females, with an average age of 27 years old and a self-efficacy value of 4.1, indicating strong self-efficacy towards personal IoT devices. Group 2 was composed of 70 graduate students, 39 male and

31 female, with an average age of 34.9 years old and a self-efficacy value of 3.2, indicating reasonable self-efficacy towards personal IoT devices. Group 3 was composed of 56 undergraduate students, 40 male and 16 female, with an average age of 28.1 years old and a self-efficacy value of 4.0.

IoT Risk Identification

This study utilized a seeded Delphi method where an initial risk list is derived from existing literature (Worrell et al., 2013). Our inclusion criteria focused on risks associated with personal IoT devices, home networks, consumer threats, or the discussion of negative consequences associated with personal IoT device use. Three of the authors also utilized their industry experience as certified security and information assurance experts to generate additional risks to ensure a broad array of initial risks would be reviewed by each panel. Lastly, each panel was allowed to generate additional risks to be included in the risk list examined by the panels. Due to the study's sequential nature, we incorporated risks generated by earlier panels into later panels. The initial seed list is available in Appendix A.

Data Collection and Consensus Assessment

The Delphi technique utilizes several rounds of panel activity that begin with a risk generation and reduction process and end with ranking a reduced number of risks that are likely to generate consensus among the panelists. Each panel operated independently, with each receiving an emailed link to a survey containing a randomized list of the initial 22 personal IoT risks.

In the first round, panelists were asked to review the initial risk list, generate risks they believe were not captured by the initial list, and select what they would consider the ten most important risks associated with personal IoT devices. The risks were presented randomly to each panelist to avoid bias. This approach adheres to existing practices utilized in seeded Delphi studies (e.g., Di Gangi et al., 2018; Worrell et al., 2013). In the initial phase, three risks were generated by panel members, with one risk being retained in subsequent rounds of any panel, suggesting the initial risk list was exhaustive.

Following Worrell et al. (2013), the initial risk selections were reduced to a risk list based on majority rule. Each panel then received their unique reduced risk list in random order to prevent anchoring and adjustment bias and rank-ordered the risks from most to least important. The initial round outcome is a set of mean ranks for each risk and a preliminary risk ordering based on relative importance. Panelists were also asked to explain their most important risk via an open-ended question. These rationales were then presented to panelists in subsequent rounds to identify underlying factors that justify a risk's rank placement.

Kendall's Coefficient of Concordance (Kendall's W) was calculated to determine the degree to which consensus was achieved by each panel (Worrell et al., 2013). If strong consensus was not achieved (i.e., Kendall's W less than .7), the panelists were asked to re-rank the risks. This step repeats until either strong consensus is achieved, a plateau in the Kendall's W value indicates subsequent rounds will not improve consensus, or panelists indicate an unwillingness to participate further (Worrell et al., 2013).

One of the Delphi process's strengths is its test of panelist resolve in determining risk order. Over time, panelists are pressured slightly to increase the effort required through continued participation and evaluation of other panelists' rationales. While the panelists remain anonymous, the process tests their confidence in their rankings and forces them to ask whether their rankings are based on personal biases or whether they are amenable to deviations based on the group's mean ranking. As a result, consensus builds over time.

Thematic Analysis

This study also utilized a data-driven thematic analysis of the risk rationales provided by the panelists. No constraints are placed on data interpretation; instead, the focus of the data-driven approach is to understand underlying patterns and meaning, termed themes, within the contextual environment (Di Gangi, Goh, & Lewis, 2017; Guest, MacQueen, & Namey, 2012). Our focus is not on revalidating previously identified risks from the Delphi panels; instead, we seek to identify further insights that motivate panelist decisions about personal IoT device risk.

The first author reviewed the 145 panelist risk rationales to identify emergent themes relevant to our research purpose. Each theme was defined to form a working understanding of the theme for coding purposes. An additional author coded a subset of the dataset (approximately 30 responses) to assess coding reliability. A Cohen's Kappa coefficient of 70.9% suggests reliability was established (Straub, Boudreau, & Gefen, 2004). The results are presented in summary form to highlight relative importance among the emergent themes with qualitative exemplars.

RESULTS

Delphi Panel Results

In terms of panel consensus, Group 1 achieved strong consensus (W = .893) after three ranking rounds with 16 risks identified as important. Both Group 2 (W = .830) and Group 3 (W = .875) achieved strong consensus after two ranking rounds. Group 2 identified a total of 16 risks, with two risks dropped from Group 1's list and one new risk added. The final group, Group 3, identified 14 risks, removing three risks from Group 1's list and two risks from Group 2's list (one risk overlapping across Group 1 and 2). The results of the three Delphi panels are presented in Table 1. In addition to each group's final rankings, we highlight the deviations in Group 1 and 2 rankings against Group 3 rankings to identify similarities and differences across panels.

The most concerning theme was associated with vulnerability of personal IoT devices being subject to hacking attempts by malicious actors ($\bar{x}$ = 1.69, #1 rank across all panels). Following vulnerability to hacking, panelists identify several approaches to compromise IoT devices. The malware threat immediately follows hacking in Group 3 ($\bar{x}$ = 2.60, #2 rank) and remains within the top four risks across all panels. Interestingly, trojan horses were only identified by Group 1 (#5 rank). Groups 2 and 3 may have merged the trojan horse risk under malware or malicious code, given trojan horses are an example of malicious code.

Additionally, the panels identified concern with how devices interact with their ecosystem as a target of an attack (e.g., the communication from or to IoT devices ($\bar{x}$ = 4.28, #4 rank in Group 1 and 3) and securely accessing support sites ($\bar{x}$ = 7.96, #8 rank in Group 2 and 3)) as risks for personal IoT devices. Group 1 identified potential physical threats facing IoT devices where they can be sabotaged to introduce false data into the data stream (#12 rank). Similar to trojan horses, no other panel indicated physical sabotage as a key risk. Collectively, the results demonstrate that consumers are aware of the dangers of hacking and the means through which hack attempts can become successful.

The second theme also concerns data loss; however, the focus is on accidental data exposure. All panels indicated accidental exposure was a concern ($\bar{x}$ = 3.80, #3 in Group 3), with no group ranking it below third. One panelist noted, "*accidentally sending data and is not noticed by the manufacturer, then there is little to no accountability for this breach.*" Interestingly, panelists also identify data sharing with third parties that may align with accidental data exposure because a third party breach could compromise consumer data. Panelists indicated sharing data with third parties for non-commercial and commercial purposes with two panels (Group 1 and 2), placing commercial concerns higher than non-commercial concerns. Both risks were identified back-to-back by all panels, with Group 3 ranking non-commercial data sharing ($\bar{x}$ = 6.28, #6 in Group 3) and commercial data sharing ($\bar{x}$ = 7.68, #7 in Group 3).

Table 1. Group 3 Delphi Results (with Group 1 and Group 2 comparison)

Group 3 Mean Rank	Risk Item	Group 1 Final	Group 2 Final	Group 3 Final	Δ from Group 1	Δ from Group 2
1.68	IoT devices might be vulnerable to hacking	1	1	1	0	0
2.60	IoT devices susceptible to malware/ malicious code compromise	3	4	2	+1	+2
3.80	IoT devices might accidentally expose my data	2	2	3	-1	-1
4.28	IoT devices might not communicate securely (i.e., might not use encryption or authentication)	4	3	4	0	-1
4.84	IoT devices might collect too much data	6	5	5	+1	0
6.28	Data collected by my IoT devices might be shared with third parties for non-commercial purposes (e.g., sharing of data with IoT device partners)	8	7	6	+2	+1
7.68	Data collected by my IoT devices might be shared with third parties for commercial purposes (e.g., sale of aggregate data)	7	6	7	0	-1
7.96	Support websites and apps for IoT devices might not be securely connected to the device	11	8	8	+3	0
8.64	Unclear data collection policy statements by IoT device provider	9	9	9	0	0
9.40	Unclear privacy policy statements by IoT device provider	10	11	10	0	+1
11.12	Interoperability issues across IoT device providers	-	13	11	-	+2
11.52	Data collected by my IoT devices might be shared with law enforcement	13	16	12	+1	+4
12.28	IoT devices susceptible to service interruptions	16	14	13	+3	+1
12.92	Support for my IoT device might end if the device manufacturer goes out of business	15	15	14	+1	+1
N/A	Difficulty in updating IoT devices	-	10	-	-	-
N/A	IoT devices might be vulnerable to physical theft	14	12	-	-	-
N/A	IoT devices are not physically secure and might be vulnerable to sabotage	12	-	-	-	-
N/A	IoT devices may be used as trojan horses to infect the home network	5	-	-	-	-
Kendall's W Coefficient		**.893**	**.830**	**.875**		

While data sharing can increase accidental exposures by multiplying the potential sites where data resides, it can also be attributed to the volume and variety of data collected. Panelists were concerned with the collection of too much data (x̄ = 4.84, #5 in Group 2 and 3). Within the data sharing concern, panelists indicate interest in understanding policy documentation that the IoT device provider shares (i.e., data collection policy (x̄ = 8.64, #9 rank across all panels) and privacy policy (x̄ = 9.40, #10 in Group 1 and 3)). These risks indicate that control over one's data and the clarity of what is being collected are important factors to consumers. Combined with data sharing concerns, awareness of what is collected, how it is collected, and who accesses data suggests privacy concern shapes consumer perceptions. For instance, one panelist notes the linkage to data collection, other risks, and the role of data collection policy clarity when making decisions:

> *"While many providers disclose the way they use data collected by IoT devices, it is not always clear how they will use it… If those statements by manufacturers are clear and concise, you can make a well-informed decision about what and how much of your personal information you want to be out there, available for exploit."*

On a limited level, all three panels indicated sharing data with law enforcement was distinct from non-commercial sharing. However, this risk did not appear higher than 12th in any panel (x̄ = 11.52, #12 in Group 3). Collectively, privacy concerns from accidental exposure or policy clarity appear to extend into a more refined issue in secondary concerns raised by panelists. Panelists operationalize these risks in their concerns over policy and specific data sharing targets.

The final theme within the risks is associated with IoT devices operational aspects. For instance, interoperability across IoT devices (x̄ = 11.12, #11 in Group 3) was found in two panels. Along with challenges with updating these devices (#10 in Group 2), panelists raised concerns about failing to obtain support from IoT device manufacturers (x̄ = 12.92, #14 in Group 3). The interest in connectivity across device manufacturers and the maintenance aspects of IoT devices may point to concerns that failures would lead to service interruptions (x̄ = 12.28, #13 in Group 3). Taken collectively, IoT devices' user experience quality remains secondary to traditional privacy data loss concerns. One panelist expresses how concern over support and service availability are secondary factors by arguing:

> *"…with the manufacturer no longer in business, [consumers] may [not] have access to the device anymore and need to adapt to a new one… Alternatively, [consumers] can continue to use the current devices, but there will be no update or patches which over time could lead to vulnerabilities..."*

Thematic Analysis Results

The thematic analysis focuses on gaining further insights into consumer risk perceptions based on panelist explanations of their risk decision. Table 2 provides the descriptions of the six emergent risks from the Delphi panels.

Table 2. Thematic Analysis Results

Theme	Description	#
Behavioral Data	Concern over the collection of behavioral data that provides insights into consumer habits or personal activities considered private or are a byproduct of device usage.	22
Device Functionality	Concerns about the quality of service experienced by a consumer from a device due to a security event's impact (e.g., accessibility or data integrity).	12
Identity Theft	Concern over the use of sensitive or personal information leading to an individual's impersonation for malicious purposes.	29
Irrelevant Data Capture	Concern over the incidental capturing of data unintended for the IoT device's proper functioning (e.g., voice conversations unrelated to device commands).	21
Supply Chain Risk	Concern about the upstream or downstream use of an IoT device in the orchestration of a security attack (e.g., use in a Denial of Service attack or access to a corporate network).	20
Threat Severity By Device Type	Concern dependent upon the type of device compromised containing varying information levels that could affect risk perceptions (e.g., smart toaster versus smart car or home monitoring devices).	12

Panelists were primarily concerned with data collection by IoT devices and the consequences of retaining personal data. One theme that emerged as a secondary effect regardless of the means of data exposure was *Identity Theft* (n = 29). Panelists ordered risks based on how they may facilitate identity theft. Implied within this logic is that malicious actions from criminals or intentional disclosure were more likely to lead to identity theft than accidental disclosure. However, all disclosure risks led to identity theft concerns because some IoT devices require registration, financial, and other personal information to function correctly.

While identity theft is a concern to most individuals, the panelists also recognized the growing dangers of an increasingly complex digital home environment. As one panelist noted, *"connected appliances, surveillance cameras and smart toys all offer potential entry points to hackers…".* Panelists mentioned the dangers of personal IoT devices to personal information and saw a concern that these devices may facilitate compromising corporate networks (i.e., *Supply Chain*

Risk (n = 20)). In particular, the limited security functionality and the ability for devices to passively capture information flowing through one's home network can provide opportunities to compromise an organizational network in unconventional ways. One interesting concern was IoT devices' ability to facilitate dynamic denial-of-service attacks by flooding a target with connection requests.

Ultimately, the volume of information that could facilitate identity theft or other criminal activity weighed on panelists' minds as a growing risk. One emergent theme from the risk rationales noted the type of data captured as a factor for consumers. In particular, IoT devices utilize their sensors to passively capture *Behavioral Data* (n = 22) to provide deeper insights into consumer preferences and future behaviors. As one panelist noted:

> *"A hacker who collects data for smart-lock usage, for example, would be able to determine when the residents of that home are generally there and when they generally are not."*

Within the same concern about data type, the panelists recognized that not all devices are equal in the IoT device portfolio. Panelists noted that IoT devices are embedded within different aspects of an individual's life. The value of information in terms of potential to do harm may vary considerably (i.e., *Threat Severity By Device Type* (n = 12)). While panelists were willing to make a necessary tradeoff between the data needed to be collected for a satisfactory user experience and the potential of capturing more data than would be necessary to fulfill that objective, panelists raised concerns about *Irrelevant Data Capture* (n = 21). In particular, the primary concern over the passive recording of conversations was that it could provide information irrelevant to the functioning of the IoT device and unknowingly share sensitive information. For instance, personal assistant devices with passive recording capability may capture conversations about healthcare or financial information if discussed within the device's vicinity.

Ultimately, panelists highlight a concern that the current balance between functionality and data collection still needs improvement by IoT device manufacturers. Furthermore, the concern is not entirely about accidental data capture. On a less frequent basis, panelists noted the concern that security risks may inhibit the ability of an IoT device to deliver on its expected *Device Functionality* (n = 12). *"By taking over the functionality of the app they not only have the ability to steal data but also influence app functionality…"* which affects user experiences, and limits consumer satisfaction.

DISCUSSION & FUTURE RESEARCH

Our multi-panel Delphi shows that four unique themes emerge. The first three focus on fundamental aspects of data collection by IoT devices and the consequences of retaining such personal data. Data exposure due to malicious actors, accidental disclosure, and a general concern over the volume of information collected by IoT device providers were primary themes with IoT-specific underlying risks. The fourth highlights how a less than seamless integration of device manufacturers or service disruption limits the user experience.

Several observations can be drawn from the risks that were *not* selected by the panelists. IoT provider reputation was not seen as a concern even though reputations imply trust in the provider to mitigate privacy concerns when collecting and controlling consumer data. Two potential reasons would explain the lack of concern about reputation. Consumers may consider IoT devices to be manufactured by new organizations and have yet to form reputation opinions. Alternatively, a small group of manufacturers with established reputations may be driving consumer perceptions about personal IoT devices.

The combination of IoT maturity not being selected as a risk factor with panelists frequently identifying well-known brands (e.g., Google and Amazon) when discussing personal IoT devices suggests a "dominant design model" may be present. As a result, existing reputations may be transferring to the emerging personal IoT device market. Many providers also offer ecosystems that allow consumers to sidestep interoperability risks. Future research within the marketing discipline may be best suited to uncover whether brand reputation generalizes to the IoT product market and acts as a moderator of risk perceptions relating to device provider reputation and IoT maturity. Until this is examined, researchers should consider controlling for IoT device manufacturers when conducting their research.

It is also possible reputation was mistargeted by focusing on the device manufacturer rather than the ecosystem in which the IoT device is embedded. NIST (2022) guidance distinguishes between IoT product and IoT device, with IoT product focusing on how a set of system components work together to deliver functionality to a consumer. Recent research has noted vulnerabilities with vetting third party applications in IoT ecosystems (e.g., Amazon's Alexa "skills" (Lentzsch et al., 2021)). Within the risk rationale data, panelists cited specific IoT devices such as Amazon Echo devices. Panelists possibly associate their concerns more with the ecosystem provider rather than the device manufacturer. Future research should examine whether consumers consider such a view.

For future security research, we focus our efforts on several emerging points specific to the IoT risk literature and on connecting our findings to current security research trends. First, a trend within the information systems discipline has focused on specificity when contextualizing concepts (Hong, Chan, Thong, Chasalow, & Dhillon, 2014), particularly when adapting a theory to a new discipline (Crossler, Di Gangi, Johnston, Bélanger, & Warkentin, 2018). This study provides guidance when researchers want to focus on IoT-specific threats in their research.

Scholars have noted the critical role of targeting threats to an intended audience when designing fear appeals (Boss, Galletta, Lowry, Moody, & Polak, 2015; Johnston, Warkentin, & Siponen, 2015). The present findings identify a series of risks likely to elicit a robust consumer response concerning personal IoT threat severity and vulnerability. Furthermore, the results present linkages between IoT-specific risks and their more abstract theme that allows researchers to target the purpose of their fear appeal more directly. Suppose the intended target behavior of a fear appeal is to highlight the dangers associated with hacking. In that case, malware is an ideal threat choice with the lack of secure communication among devices or support sites to heighten perceptions about susceptibility to the threat. In contrast, focusing on data collection and privacy policy statements concerning non-commercial and commercial data sharing with third parties would heighten perceptions about susceptibility to accidental data exposure or privacy concerns from collecting too much data. Utilizing the present study results can ensure researchers are adopting the appropriate exigent threats facing IoT consumers.

Within the thematic analysis data, the identification of behavioral data as a concern suggests the emergence of Internet-of-Behaviors (IoB) may soon be upon consumers. Internet-of-Behaviors is a relatively new concept combining the sensor data from IoT devices with analytic capabilities to develop predictions about human behavior and preferences (Stary, 2020). The results presented here may help direct research in this emerging area based on IoT acting as the platform upon which IoB relies. In particular, the combination of irrelevant behavioral data capture taps into the heart of the concern about the volume of data captured. When combined with a malicious or accidental disclosure, this may heighten consumer stress or anxiety, leading to greater apprehension towards adopting IoT devices providing IoB features or, more broadly, consumer privacy concerns.

Future research should also consider the effects this has on shaping consumer perceptions about privacy concerns when presented in an abstract versus concrete form. Research using Construal Level Theory explores how abstract versus concrete messaging influences individual perceptions by manipulating their perceptions of time, physical space, social, and hypothetical distance (Schuetz, Lowry, Pienta, & Thatcher, 2020, 2021; Trope & Liberman, 2010). A fifth dimension based on informational distance focuses on the amount of information a consumer possesses about their decision options (Lee, Son, & Oh, 2021). Translating informational distance to security and consumer IoT devices could utilize the abstract versus concrete risks identified in our panel results. Specifically, the three highlighted themes associated with data exposure – malicious, accidental, and psychological (i.e., too much data collected). These could be operationalized in their general form as more abstract risks for consumers to consider when adopting or purchasing IoT devices. In contrast, the use of the underlying specific risks would make the informational distance more concrete.

Another area of development for privacy concern is its measurement relating to control and collection. The privacy concern measure developed by Malhotra, Kim, and Agarwal (2004) focused on three underlying dimensions relating to awareness, collection, and control of one's data. This study's findings distinguish between privacy and data collection policies, suggesting data collection policies may directly impact the collection dimension while privacy policies may speak to the control dimension. Furthermore, the type of data and device utilizing the data matters. Our thematic analysis noted the extent to which an IoT device could cause physical harm and irrelevant or behavioral data capture may impact a consumer's awareness and control concerns. Collectively, the influence on privacy concerns affects consumer decisions regarding IoT device adoption and use.

From a practitioner perspective, the present study's findings align well with NIST (2022) guidance on consumer IoT security protections in the areas of product configuration, data protection, interface access control, software updating, and documentation. Each area of guidance was present as a concern consumers are mindful of when assessing IoT device risk. One interesting finding from the panels was the operational aspects of IoT that potentially affect consumers' experiences with IoT products. Risks that are realized through a compromised device or the failure to maintain sufficient operating conditions to function within a consumer's home network due to either support or compatibility issues are seen as inhibiting factors that may affect consumer behaviors. Furthermore, consumers notice underlying risks associated with IoT devices for how malicious or accidental data exposures can occur. Manufacturers should directly address these issues by articulating the nature of device security to consumers as part of their technical specifications and features.

LIMITATIONS

All research contains limitations. In the present study, our panelists are young, educated consumers. Panelists were also students enrolled in a business school who may possess a strong understanding of information processes and the role of strategic partnerships to maximize organizational value and competitive advantage. The panels were also more male-centric than the wider population. Such panels may misrepresent the nature of risk within the personal IoT market.

The research team also made tradeoffs to balance the study's robustness against the cognitive effort required to complete the Delphi process. Abstract risks were retained and competed against more specific risks to determine how risks may be prioritized or related. Also, a relevant risk may have been missed due to the authors' access to relevant research. The limited number of risks suggested by the panelists in this study indicates a degree of robustness in the initial risk list. The thematic analysis was also used to determine whether any underlying risks were present such as identity theft that, while not suggested by the panel, emerged as a critical risk regardless of whether the disclosure was malicious or accidental.

Lastly, the personal IoT device market remains in its infancy. In the present study, the authors presented each panel without a specific IoT device in mind to increase generalizability. NIST (2022) notes that the existing heterogeneity of personal IoT devices limits its ability to offer explicit prescriptive guidance to consumers and IoT device manufacturers. Thus, research should consider emerging risks and provide empirical investigations on various IoT devices to demonstrate the current results' robustness or the unique circumstances that alter consumer risk perceptions. Future research may also want to consider the development of a typology of personal IoT devices to guide research in this area.

CONCLUSION

Research has primarily focused on organizational risks associated with IoT devices with limited exploration of the risks associated with personal IoT devices. By synthesizing the existing risk literature and prioritizing risks based on consumer perceptions, this study provides direction to researchers on contextualizing risk perceptions and identifying personal IoT-specific risks. We highlight several theories that may produce fruitful insights into risk perceptions that influence personal IoT device adoption and use. The results also highlight areas where organizations can focus on alleviating consumer risk concerns. At present, the personal IoT market will be a defining area of interest to society, businesses, and scholars for the foreseeable future.

REFERENCES

Adamopoulos, P., Todri, V., & Ghose, A. (2020). Demand effects of the Internet-of-Things sales channel: Evidence from automating the purchase process. *Information Systems Research, 32*(1).

Baecke, P., & Bocca, L. (2017). The value of vehicle telematics data in insurance risk selection processes. *Decision Support Systems, 98*, 69-79.

Baesens, B., Bapna, R., Marsden, J. R., Vanthienen, J., & Zhao, J. L. (2016). Transformational issues of big data and analytics in networked business. *MIS Quarterly, 40*(4), 807-818.

Barcena, M. B., & Wueest, C. (2015). *Security Response: Insecurity in the Internet of Things*. Retrieved from http://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/insecurity-in-the-internet-of-things-15-en.pdf

Benbunan-Fich, R. (2019). An affordance lens for wearable information systems. *European Journal of Information Systems, 28*(3), 256-271.

Blythe, J. M., & Johnson, S. D. (2021). A systematic review of crime facilitated by the consumer Internet of Things. *Security Journal, 34*, 97-125.

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.

Chang, S.-I., Chang, L.-M., & Liao, J.-C. (2020). Risk factors of enterprise internal control under the internet of things governance: A qualitative research approach. *Information & Management, 57*(6).

Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E., & Wortmann, F. (2019). Blockchain for the IoT: Privacy-preserving protection of sensor data. *Journal of the Association for Information Systems, 20*(9), 1274-1309.

Choo, K.-K. R., Gai, K., Chiaraviglio, L., & Yang, Q. (2021). A multidisciplinary approach to Internet of Things (IoT) cybersecurity and risk management. *Computers & Security, 102*.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly, 19*(2), 189-211.

Côrte-Real, N., Ruivo, P., & Oliveira, T. (2020). Leveraging internet of things and big data analytics initiatives in European and American firms: Is data quality a way to extract business value. *Information & Management, 57*.

Crossler, R. E., Di Gangi, P. M., Johnston, A. C., Bélanger, F., & Warkentin, M. (2018). Providing theoretical foundations: developing an integrated set of guidelines for theory adaptation. *Communications of the Association for Information Systems, 43*(1), 566-597.

De Moya, J.-F., & Pallud, J. (2020). From panopticon to heautopticon: A new form of surveillance introduced by quantified-self practices. *Information Systems Journal, 30*(6), 940-976.

Di Gangi, P. M., Goh, S., & Lewis, C. (2017). Using social media to support presentation skill development in traditional classroom environments. *Journal of Organizational and End User Computing, 29*(3).

Di Gangi, P. M., Johnston, A. C., Worrell, J. L., & Thompson, S. C. (2018). What could possibly go wrong? A multi-panel Delphi study of organizational social media risk. *Information Systems Frontiers, 20*(5), 1097-1116.

Goad, D., Collins, A. T., & Gal, U. (2021). Privacy and the Internet of Things - An experiment in discrete choice. *Information & Management, 58*(2), 103292.

Guest, G., MacQueen, K. M., & Namey, E. E. (2012). *Applied Thematic Analysis*. Thousand Oaks, CA: SAGE Publicaitons, Inc.

Hong, W., Chan, F. K. Y., Thong, J. Y. L., Chasalow, L. C., & Dhillon, G. (2014). A framework and guidelines for context-specific theorizing in information systems research. *Information Systems Research, 25*(1), 111-136.

Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems, 56*(Mar), 719-733.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly, 39*(1), 113-134.

Kim, D., & Solomon, M. G. (2018). *Fundamentals of Information Systems Security* (3rd ed.). Burlington, MA: Jones & Bartlett Learning.

Klobas, J. E., McGill, T., & Wang, X. (2019). How perceived security risk affects intention to use smart home devices: A reasoned action explanation. *Computers & Security, 87*.

Lee, S.-Y., Son, Y., & Oh, W. (2021). Effectiveness of integrated offline-and-online promotions in omnichannel targeting: A randomized field experiment. *Journal of Management Information Systems, 38*(2), 484-516.

Lentzsch, C., Shah, S. J., Andow, B., Degeling, M., Das, A., & Enck, W. (2021). *Hey Alexa, is this skill safe?: Taking a closer look at the Alexa skill ecosystem*. Paper presented at the Network and Distributed Systems Security (NDSS) Symposium, Virtual.

Li, S., Xu, L. D., & Zhao, S. (2015). The internet of things: A survey. *Information Systems Frontiers, 17*, 243-259.

Lin, H., & Bergmann, N. W. (2016). IoT privacy and security challenges for smart home environments. *Information & Management, 7*(3), 44-59.

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

March, S. T. (2019). Alexa, are you watching me? A response to Clarke, "Risks inherent in the digital surveillance economy: A research agenda". *Journal of Information Technology, 34*(1), 87-92.

Menard, P., & Bott, G. J. (2020). Analyzing IOT users' mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment. *Computers & Security, 95*.

National Institute of Standards and Technology. (2022). *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products*. https://doi.org/10.6028/NIST.CSWP.02042022-2

Nicolescu, R., Huth, M., Radanliev, P., & De Roure, D. (2018). Mapping the values of IoT. *Journal of Information Technology, 33*, 345-360.

Oberländer, A. M., Röglinger, M., Rosemann, M., & Kees, A. (2017). Conceptualizing business-to-things interactions: A sociomaterial perspective of the Internet of Things. *European Journal of Information Systems, 27*(4), 486-502.

Schuetz, S., Lowry, P. B., Pienta, D., & Thatcher, J. (2020). The effectiveness of abstract versus concrete fear appeals in information security. *Journal of Management Information Systems, 37*(3), 723-757.

Schuetz, S., Lowry, P. B., Pienta, D., & Thatcher, J. (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.

Shin, D.-H. (2017). Conceptualizing and measuring quality of experience of the internet of things: Exploring how quality is perceived by users. *Information & Management, 54*, 998-1011.

Sicari, S., Cappiello, C., De Pellegrini, F., Miorandi, D., & Coen-Porisini, A. (2016). A security- and quality-aware system architecture for Internet of Things. *Information Systems Frontiers, 18*, 665-677.

Skinner, R., Nelson, R. R., Chin, W. W., & Land, L. (2015). The Delphi method research strategy in studies of information systems. *Communications of the Association for Information Systems, 37*, 31-63.

Stary, C. (2020). *The Internet-of-Behavior as Organizational Transformation Space with Choreographic Intelligence*. Paper presented at the International Conference on Subject-Oriented Business Process Management.

Straub, D., Boudreau, M., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the AIS, 13*, 380-427.

Strous, L., von Solms, S., & Zúquete, A. (2021). Security and privacy of the Internet of Things. *Computers & Security, 102*.

Tarafdar, P., & Bose, I. (2021). Recognition of human activities for wellness management using a smartphone and a smartwatch: A boosting approach. *Decision Support Systems, 140*, 113426.

Teubner, R. A., & Stockhinger, J. (2020). Literature review: Understanding information systems strategy in the digital age. *Journal of Strategic Information Systems, 29*(4), 101642.

Trope, Y., & Liberman, N. (2010). Construal-level theory of psychological distance. *Psychological Review, 117*(2), 440-463.

Wessel, L., Davidson, E., Barquet, A. P., Rothe, H., Peters, O., & Megges, H. (2019). Configuration in smart service systems: A practice-based inquriy. *Information Systems Journal, 29*, 1256-1292.

Whitmore, A., Agarwal, A., & Xu, L. D. (2015). The Internet of Things - A survey of topics and trends. *Information Systems Frontiers, 17*, 261-274.

Worrell, J. L., Di Gangi, P. M., & Bush, A. (2013). Exploring the use of the Delphi method in accounting information systems research. *International Journal of Accounting Information Systems, 14*(3), 193-208.

Wunderlich, P., Veit, D. J., & Sarker, S. (2019). Adoption of sustainable technologies: A mixed-methods study of german households. *MIS Quarterly, 43*(2), 673-691.

APPENDIX A. DELPHI RISK SEED LIST

Risk Item	Source
IoT devices might be vulnerable to hacking	Klobas et al. (2019)
IoT devices susceptible to malware/ malicious code compromise	Chanson et al. (2019)
IoT devices might accidentally expose my data	Jacobsson et al. (2016)
IoT devices might not communicate securely (i.e., might not use encryption or authentication)	Menard and Bott (2020)
IoT devices might collect too much data	Jacobsson et al. (2016)
Data collected by my IoT devices might be shared with third parties for non-commercial purposes (e.g., sharing of data with IoT device partners)	Goad et al. (2021)
Data collected by my IoT devices might be shared with third parties for commercial purposes (e.g., sale of aggregate data)	Goad et al. (2021)
Support websites and apps for IoT devices might not be securely connected to the device	Menard and Bott (2020)
Unclear data collection policy statements by IoT device provider	Jacobsson et al. (2016)
Unclear privacy policy statements by IoT device provider	Whitmore et al. (2015)
Interoperability issues across IoT device providers	Lin and Bergmann (2016)
Data collected by my IoT devices might be shared with law enforcement	Goad et al. (2021)
IoT devices susceptible to service interruptions	Kim and Solomon (2018)
Support for my IoT device might end if the device manufacturer goes out of business	Kim and Solomon (2018)
Difficulty in updating IoT devices	Lin and Bergmann (2016)
IoT devices might be vulnerable to physical theft	Lin and Bergmann (2016)
IoT devices are not physically secure and might be vulnerable to sabotage	Lin and Bergmann (2016)
IoT devices may be used as trojan horses to infect the home network	Chanson et al. (2019)
IoT device manufacturer reputation not established	*Generated by study*
IoT devices are not physically secure and might be vulnerable to destruction	Lin and Bergmann (2016)
IoT devices are too costly	Kim and Solomon (2018)
IoT devices are too technologically immature	*Generated by study*
IoT devices may not be easy to implement	Lin and Bergmann (2016)