Cybersecurity in Consumer Adoption of Smart Home Technology

by
Raed Iskandar
Supervised by Professor Mika Westerlund

A thesis submitted to the Faculty of Graduate and Postdoctoral Affairs in fulfillment of the requirements for the degree in

Masters of Applied Science
in
Technology Innovation Management

Summer 2017

Carleton University
Ottawa, Ontario

Abstract

The highly anticipated smart home technology for everyday life has been growing over the past quarter century. Using standard technology adoption models, previous research produced conflicting results that did not reflect the market accurately. Amongst the indicated challenges for the future of smart home technology is the commonly overlooked barrier cybersecurity. To better understand the market's expectation we conducted consumer interviews that produced a modified model for smart home adoption in the Canadian market. The resulting adapted model proposes a link between cybersecurity and the behavioral intent of potential consumers. Components of the cybersecurity determinant are identified as trust, safety, and privacy which are moderated by the consumer's level of technical knowledge. Implications of our findings could improve the performance of smart home technology in the market and inspire the creation of innovative solutions that increase the security of the IoT industry.

Glossary

- *Cybersecurity:* the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights.
- *Internet of Things (IoT):* a dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities, use intelligent interfaces, and are seamlessly integrated into the information network.
- *Smart Homes:* a residence equipped with computing and information technology which anticipates and responds to the needs of the occupants, working to promote their comfort, convenience, security, and entertainment through the management of technology within the home and connections to the world beyond.

Contents

List of Figures

List of Tables

ACKNOWLEDGEMENT

The completion of this thesis would not have been made possible without the continuous support of my family and friends. I am indebted to their patience and encouragement through the past year of my research. I am grateful for the efforts of my supervisor Dr. Mika Westerlund and his unwavering dedication in providing advice and support for the duration of my studies.

1 INTRODUCTION

This research examines the role cybersecurity plays in the adoption of smart home technology. Adoption factors have come into scrutiny over the last decade for this product market after years of failure to reach expected growth in sales. In 1970 information technology consultant James Martin and Adrian R.D. Norman published a book titled The Computerized Society, where they discussed the potential to use a computer in homes to aid in day-to-day tasks. Their vision of the future modern homes included automated control of home appliances through networks and over the internet, with incredible resemblance to what technology can do today and is widely considered the first introduction of smart homes concept (Martin & Norman, 1973, P.161).

By 1989 the concept of smart homes was no longer seen as significantly revolutionary (Forester, 1989, P. 224). Soon after, magazines such as Boys' Life, Vanity Fair, and House Beautiful began to publish articles about smart homes which at this point had become an appealing idea for the average home lifestyle (Aldrich, 2003). Although the past century has been marked by incredible advances in technology, the barriers to the smart home market have yet to be overcome. Research produced by organizations such as Cisco, Gartner, and General Electric have widely contradicting predictions of the future market for smart homes (Cisco; Savitz, 2012; Columbus, 2016).

The smart home concept is constructed from multiple layers of connected technological devices that operate together producing the immersive experience that is smart homes. Those devices and appliances are commonly referred to as smart or connected technologies; together those devices form the network of Internet of Things (IoT). The term IoT continues to evolve, with some debate as to what "Things" can be. A conceptual framework from Vermesan et al. (2011) explains IoT as "... a dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities, use intelligent interfaces, and are seamlessly integrated into the information network."

The literature on the current and future state of smart homes suggests that there are some critical challenges that must be addressed (Rose, Eldridge, & Chapin, 2015; Alam et al., 2012). Key fundamental factors of smart homes have been brought under examination that poses a question of whether the current adoption models need to be rethought. Research suggests that the security of the IoT could be a central part of the adoption challenge (Singh & Singh, 2015).

A recent study ran a group of IoT products from different manufacturers through extensive security testing and found some commonly known issues still existed in the technology (Stanislav & Beardsley, 2015). The academic literature presents a theoretical indication to the

risk of cybersecurity, but case evidence is more present through the media. The CNBC, as well as other news reporting agencies, reported on an incident involving IoT devices that affected thousands of home owners. Schlesinger and Day (2016) state, "In October, hackers took over 100,000 IoT devices and used them to block traffic to well-known websites, including Twitter and Netflix."

The risks mentioned above use the term cybersecurity to refer to threats affecting devices connected on a cyber-network. Craigen, Diakun-Thibault, & Purse (2014) provided a unification for the term cybersecurity that bridges amongst technical and non-technical academic streams resulting in the following definition "Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights."

Understanding the growing problems facing Smart homes, we believe now is the time to address the challenge of cybersecurity. Our research examines this critical factor through the use of potential consumer data to advance the technology adoption models.

In this research, we use the definition of smart homes given by Aldrich (2003). The definition focuses on technology within a home that provides the resident with automated management of technology in their home in response to their current needs or in anticipation of future

needs.

1.1 OBJECTIVE

This research aims to advance our understanding of consumer adoption of cybersecurity features by producing a modified adoption model supported by current potential consumers of smart homes. The model will provide a better understanding of the role that cybersecurity takes in the customer's purchasing decision of smart home technology. We state the research question as: *What role does Cybersecurity play in Smart Home technology adoption by consumers in the household market.*

1.2 DELIVERABLES

Readers examining this research should expect to find the following deliverables. (1) List of key components perceived to determine the level cybersecurity in the smart home market. (2) A conceptual technology adoption model specific to smart homes. (3) Propositions of the relationships between the model's adoption factors.

1.3 DELIMITATIONS

Delivering an improved understanding of the user acceptance of smart home technology requires a methodical structure of research. Defining our delimitations is equally important to this research as the declaration of deliverables.

The study will not focus on smart home technology products that are mandatory i.e., those that do not offer the consumer a choices for selection, such as government regulated installations. This focus ensures that the data collection and findings will reflect consumer choice adoption of the technology.

Exploration of adoption will focus on the individual household consumers, avoiding business to business relationships. This allows us to narrow down the factors involved in the adoption process to a smaller set of unknown variables.

The extensive literature on technology adoption has resulted in a widely accepted set of adoption factors which this research will not set to disprove. A higher value is delivered through focusing on the exploration of additional factors relevant to the adoption of smart home technology.

1.4 RELEVANCE AND VALUE OF DELIVERABLES

This research is valuable on two fronts. First, it provides relevant findings for the organizations invested in the smart home technology, or ones that are currently considering entering the market. Providing them with data that can guide the product development and design decisions to improve their chances of adoption in the Canadian mar-

ket. Secondly, from the literature perspective, this research provides information valuable to the research community where it poses new theoretical models and propositions that can help future research.

After examination of the research material and the expected deliverables, we anticipate providing value to the stakeholders in a number of ways. The list of key adoption factors identified will allow organizations and managers to develop their smart home technology using specifications that lead to quicker consumers product adoption which should enhance market share and profits. The components all form relations with one another and play a role in the adoption model developed through this research, and we expect to find the developed model to share a similar impact on other technologies affecting the market for IoT technology.

1.5 METHODOLOGY

This research is conducted in multiple stages, utilizing the existing literature and bringing in value from data collected from a sample of potential and current consumers of smart home technology through an interview process. This process is conducted utilizing these five stages: (1) Conducting a literature review followed by identification of the theoretical security factors that potentially influence adoption. (2) Selecting a study sample and conducting semi-structured interviews. (3) Structuring the collected research data and tabulating interview results. (4)

Analyzing of the data and identifying patterns. (5) Construction of adoption model and proposition of factor relationships.

1.6 ORGANIZATION OF THE THESIS

This thesis is organized into six chapters, each structured into sections and subsections. The first chapter introduces the research topic and lays out the plan for the full article. Chapter 2, "Literature Review," examines the literature available on the subject and categorizes the findings into streams then provides some key lessons. Chapter 3, "Research Design and Methodology," describes the methods used to conduct the research, develop the examination process, and the collection of data. Chapter 4 documents the resulting data from the conducted study and presents a summary of the results. Chapters 5 and 6 present a discussion of the results and conclusions.

2 LITERATURE REVIEW

The literature available about the research topic can be categorized into three self-contained and well-studied streams: (1) technology adoption models, (2) boundaries of smart homes, and (3) cybersecurity and challenges in connected technology. Next, we briefly examine what the main findings of the literature from each of the three streams and how it can aid our research. (see Table 1)

Table 1: Literature Review Streams

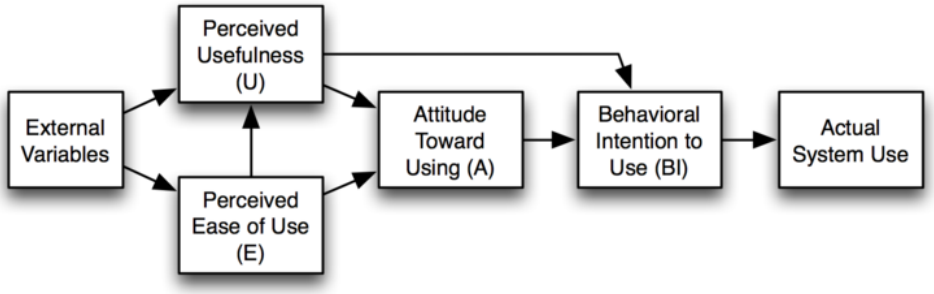
Stream	Key Highlights	Key References
Technology adoption models	Models of technology acceptance have been modified to better explain adoption. Contradictions are noticed in the literature when the models are applied to smart homes.	Davis Jr(1986) Venkatesh et al. (2003) Venkatesh et al. (2012) Kranz & Picot (2012) Mayer et al. (2011)
Boundaries of smart homes	Examines the history and identifies what makes a smart home. Shows a shift from the technology based identification of smart homes to interaction based.	Aldrich, (2003) Jiang et al. (2004) Alam et al. (2012) Camarinha-Matos & Afsarmanesh, (2014)
Cybersecurity and challenges in connected technology	Identification of challenges facing the future of smart home technology, the literature ranges from social barriers and speed of adaptability to cybersecurity and technological warfare.	Hong et al. (2009) Balta-Ozkan et al. (2013) Schrammel et al. (2011) Weber (2010) Komninos et al. (2014) Yang et al. (2015)

2.1 TECHNOLOGY ADOPTION MODELS

When we look to the past, organizations have always wanted to know more about what factors and specifications provide their products with

a market leading position, and we find that reflected well in the literature. Technology adoption models emerged in the literature in the mid 1980s, thanks to the efforts of Davis Jr. (1986). Initially, researchers provided a simple model, known as the technology acceptance model (TAM), which provided a better understanding of user acceptance of technology (see figure 1). Davis Jr.'s (1986) TAM model provided organizations with a theory for designing technology with higher potential of success.

Figure 1: Technology Acceptance Model (Davis Jr., 1986)



Davis (1989) intended to develop a measuring scale to predict users acceptance of the emerging and rapidly growing new technology of computers. He initially hypothesized the existence of two fundamental determinants of user acceptance as perceived usefulness and perceived ease of use. The study found that both perceived usefulness and ease of use were significantly correlated with self-reported indicants of system use (Davis, 1989).

The model developed by Davis (1989) presents a strong relationship between perceived usefulness and user acceptance. The effects of perceived ease of use to acceptance were also observed but proved to be less significant than that of usefulness. However for a product where all else is equal, higher perceived ease of use will increase the user's attitude towards acceptance.

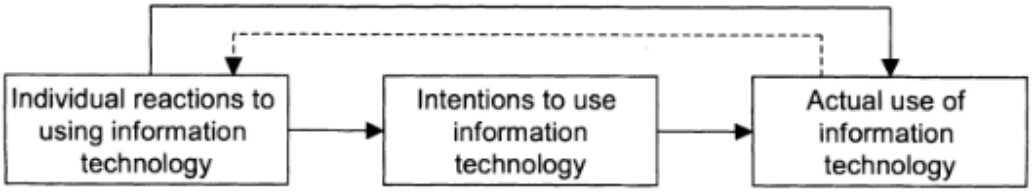
Perceived usefulness and ease of use formed the two key components of adoption models and have remained in the literature stream as it developed into larger models. Additionally, Davis's (1989) research provided some evidence that other external variables are favorable and play a role in the user acceptance process. The external variables factor was further studied in future research as suggested by the researcher

The study concluded that users acceptance of computing technology was determined by their perceived performance value. Davis (1989) provides a future goal to better understand user acceptance by stating "Given that this study indicates that people act according to their beliefs about performance, future research is needed to understand why performance beliefs are often in disagreement with objective reality."

Following Davis's research, another very distinguished researcher in the area of technology adoption is Viswanath Venkatesh who has published multiple highly reputable research papers that have been referenced by organizations and scholars. In earlier research, Venkatesh and

his colleagues produce a User Acceptance Model (see figure 2) that, to them, outlines the basic underlying concept of all user acceptance models (Venkatesh et al., 2003). This Model does share some resemblance to the technology acceptance model developed by Davis, as it shares the users' attitude towards technology, behavioral intent to use, and actual system use under different phrasing. However, the model does not take into account the effects of perceived usefulness, perceived ease of use, or external variables at its current stage.

Figure 2: User Acceptance Model (Venkatesh et al., 2003)

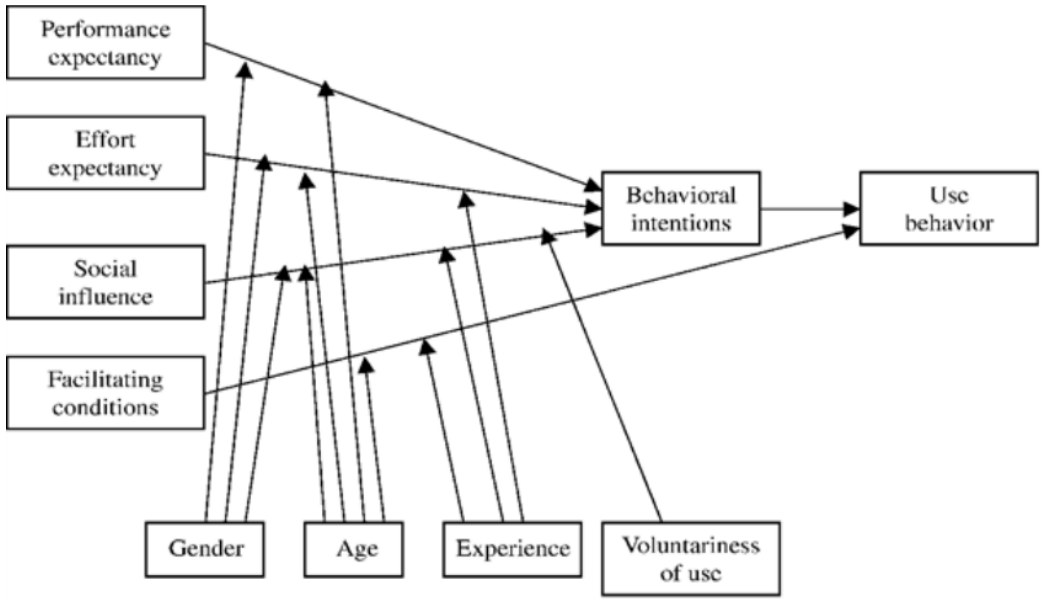


Venkatesh and his colleagues kept developing their model through the examination of the literature present at the time. A unified model was developed through the review of eight models: (1) the theory of reasoned action, (2) the technology acceptance model, (3) the motivational model, (4) the theory of planned behavior, (5) a model combining the technology acceptance model and the theory of planned behavior, (6) the model of PC utilization, (7) the innovation diffusion theory, (8) and the social cognitive theory.

The resulting model from the unification in 2003 was called the Uni-

fied Theory of Acceptance and Use of Technology (UTAUT)(See figure 3), which refined the works of other researchers providing a model with more variables and a higher interpretation of variance in user intention (Venkatesh et al., 2003).

Figure 3: Unified Theory of Acceptance and Use of Technology (Venkatesh et al., 2003)



The UTAUT model has four determinants of user behavior, and four key moderators to those determinants. The determinants are labeled as: performance expectancy, effort expectancy, social influence, and facilitating conditions. Their key moderators are labeled as: gender, age, experience, and voluntariness.

Performance expectancy is the perceived benefits in task performance gained by using the technology. This determinant is similar to the perceived usefulness component of the TAM model and is derived from that

model along with four other constructs of performance in other models.

Effort expectancy can be related to the perceived ease of use component from TAM, where it pertains to the degree of ease associated with the utilization of the technology.

The social influence determinant is determined by the effect other people have on the user through their perception on the importance of having and using the new system. This determinant is rooted in the sociological study of social normativity.

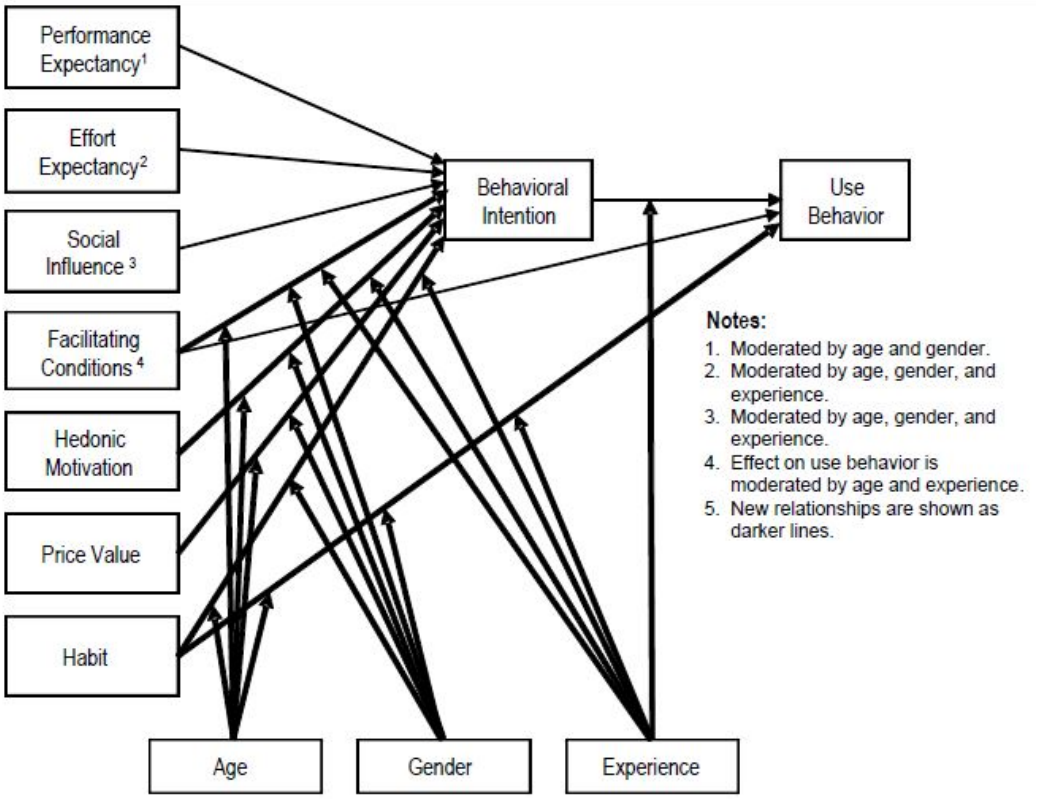
The last determinant of the UTAUT model, facilitating conditions, is defined by the existence of capability in terms of systems, organizations, and infrastructure to support the use of the new technology.

Four key moderators are identified in the UTAUT model, and each of the determinants is related to one or more of these moderators. Age and gender moderate performance expectancy. Effort expectancy has its moderating factors as age, gender, and experience. Social influence is the highest moderated with all four factors affecting the relationship between social influence and behavioral intent. Facilitating conditions are moderated by the age and experience of the users.

These adoption models have been studied and revised by many of the leading experts. In 2012, Venkatesh et al. revised the UTAUT model

to include new variables. The resulting model is the Unified Theory of Acceptance and Use of Technology 2 (UTAUT2), (see figure 4). This revised and expanded model, through regular testing, could explain behavioral intention up to 74 percent (Venkatesh et al., 2012).

Figure 4: Unified Theory of Acceptance and Use of Technology 2 (Venkatesh et al., 2012)



In the second iteration of their model, UTAUT2, Venkatesh and his colleagues added three new variables that relate to the behavioral intent of consumers: hedonic motivation, price value, and habit.

Hedonic motivation refers to the pleasure and fun that consumers experience from using the new technology. Price value is the cost struc-

ture of acquiring the technology and maintaining operation and considers the different effects from consumers incurring the direct cost versus being provided the technology through an organization that covers the cost, such as receiving a company computer. The final determinant, habit, is the tenancy of the user to perform behavior required for the technology automatically.

The models mentioned through this section have been deployed in real-life business applications to improve the performance of products and increase the levels of their adoption to a particular demographic. Literature on the application of the adoption models mentioned above in real life citations is abundant, offering valuable insight into the affects each of the determinants have on consumer behavior (Anderson & Schwager, 2004; Kijsanayotin, Pannarunothai, & Speedie, 2009; Raman & Don, 2013; Oechslein, Fleischmann, & Hess, 2014; Arenas-Gaitán, Peral-Peral, & Ramon-Jeronimo, 2015).

Similarly to Venkatesh et al. (2012), other researchers have continued to advance the model to provide a better explanation of the adoption curves in different technology sectors. Studies have introduced to the adoption model factors such as management effectiveness, program effectiveness, pervasiveness, health concerns, and socio-economic status (Abdulwahab, & Dahalin, 2010; Segura, & Thiesse, 2015; Xiong, & Mei, 2016). Upon examination of how these models behave in predicting smart home technology adoption, we find that the literature

provides contradicting results. The range of research into the future of smart homes varies from suggesting that the industry needs to re-think their product solution (Aldrich, 2003; Barlow & Venables, 2003) to suggesting rapid growth in the next few years (Rose et al., 2015), and others in between (Chan et al., 2008).

2.2 BOUNDARIES OF SMART HOMES

The second stream of literature about smart homes examines the core concepts and identifies what makes up a smart home. Researchers that worked in this stream focused on finding a definition for smart homes as well as setting the boundaries of what technologies should classify as smart home technology.

One of the earliest recorded mentions of the smart homes concept can be found in the 1970 book publication of The Computerized Society (Martin & Norman, 1973). The authors worked to disillusion the public of the capabilities of computer technology of the day. As part of their publication, they provided a vision of possible development in the ten years to follow their book given what capabilities were available at their time.

Among the list of automations envisioned by Martin & Norman (1973) were online banking and e-transfers, computerized dispatch and GPS navigation systems, computer-assisted education, electronic health-

care, and the smart home concept. They predicted that the smart home of the future could control entertainment systems, allow for work at home, and extend the educational system to connect to the homes. The capabilities did not end there. Mention of automated appliances and control through a mobile telephone give a shocking resemblance to the modern smart homes technology.

Innovation in computing technology aided the evolution of the smart home definition. Skrzypczak (1987) used a definition of smart homes that again relied on the automation of technology through processor units and envisioned the technology to be heavily present by 2010. Skrzypczak also identified the smart homes through having a control processor appliance incorporated into the home which would be capable of monitoring and controlling many functions of the household as well as provide a connection to the outside world.

The creator of Xanadu (a vision of future smart homes), Roy Mason, described the automated home of tomorrow with layers of capabilities (Bruce, 1987). At the core of it, the "home brain" would be capable of controlling the energy, lighting, and security systems in the house. Above that core layer came an endless pool of possibilities in the form of appliances that ranged from robots that could do house-cleaning jobs, and kitchens that are nutritional diagnosticians, to three-dimensional holographic art.

Moving forward with the technology, the industry focused on the growth of cellular technology. As the new market picked up speed during 1990, researchers began to investigate its possible future uses. One article found smart home technology could grant the cellular technology a promising area for collaborative growth, mentioning how the increased use of sensors in smart homes would extend the use of cellular phones as remote control systems (Jarratt & Coates, 1990).

The literature available on smart homes grew more rapidly after the 1980's as more articles gave definitions relating to smart homes. Key features of the smart homes emerged commonly in definitions, such as the purpose of smart homes in providing assistive technology, their potential to monitor for needs, their automated responses to these needs, and their connectivity to appliances around the homes (Allen, 1996; Warren, Craft, & Bosma, 1999; Covington, Moyer,& Ahamad, 2000; Aldrich, 2003). Emerging markets for smart home technology has become more evident in the literature. Amongst these markets were security, electronic health care, entertainment, and environmental control (Warren et al., 1999; Aldrich, 2003; Chan et al., 2009). Within these markets for the technology, a greater portion of articles focused primarily on the electronic health segment (Bellazzi et al., 2001; Demiris & Hensel, 2008; Chan et al., 2008).

We observe that although there are strong definitions for smart homes provided in the literature, studies continue to provide their own under-

standing of what smart homes are. This has led to some conflicting views and has kept the industry from setting an agreed standard for the definition. In our study we firmly support the definition of smart homes provided by Aldrich (2003) that states:

> "A 'smart home' can be defined as a residence equipped with computing and information technology which anticipates and responds to the needs of the occupants, working to promote their comfort, convenience, security, and entertainment through the management of technology within the home and connections to the world beyond".

The literature on smart home technology has been grouped into sectors based on the functions they serve. These sectors are defined with better clarity in more recently published articles. The distinct groups identified by the literature are (1) home automation, (2) entertainment, (3) security, (4) healthcare, (5) remote access control, and (6) energy efficiency (Chan et al., 2008; Alam, Reaz, & Ali, 2012; O'Malley & Munoz, 2014). As the boundaries of smart home technology becomes clarified by researchers, the methods of identification used to separate smart home technology has shifted from technology based to interaction based.

More on the development of smart home definitions and what the fu-

ture of smart home technologies might hold are present in the literature (Intille, 2002; Robles & Kim, 2010; Hamernik, Tanuska, & Mudroncik, 2012; Kadam, Mahamuni, & Parikh, 2015; Solaimani, Keijzer-Broers, & Bouwman, 2015).

2.3 CYBERSECURITY AND CHALLENGES IN CONNECTED TECHNOLOGY

The third stream in the literature revolved around the topic of challenges that have blocked smart home technology's reach. Studies indicated that, like many other early technologies, smart homes have unresolved issues on a number of fronts. Research on this topic is often multi-disciplinary and heavily focused on one issue. To present the issues clearly we present the literature separated by their selective primary challenge of smart homes technology.

2.3.1 Human interaction Challenges

In the move towards an integrated automated system for technologies within the homes, some researchers have investigated the human-system interaction challenges arising from the design. Given that one of the market sectors for this technology would involve elderly users for their heath care needs, it comes as no surprise that researchers have gathered information to challenges that they might face. In a set of interviews with a group of older adults - over the age of 65 - one study

found that a pressing challenge for this demographic is the lack of user-friendliness and the need for extensive training to operate the modern technology (Demiris et al., 2004).

Addressing the interaction challenges present in this technology could prove to have a larger impact on the market as it affects more that the elderly demographic. Edwards & Grinter (2001) explain in a study of the challenges of ubiquitous computing how the technology that has been weaved into the fabric of the home will require its occupants to become the systems' administrator. The technology faces an operational barrier as it moves from testing in a lab with state-of-the-art experts to the home of an average consumer. Researchers have focused on the technical limitations which have not been met, such as the collaboration between different smart home systems and the human-system interactions (Camarinha-Matos, & Afsarmanesh, 2014).

2.3.2 Social Barriers

It is part of human nature to accept and reject behavior based on its fit with social norms; actions made by technology and machines are not exempt from this judgment. Social barriers could impact the future of smart home technology, suggesting that technology that is incapable of fitting in with the pre-existing norms would be found unappealing (Balta-Ozkan et al., 2013). Social barriers could include the level of know-how required to operate the systems and the tolerance to errors

homeowners are willing to accept as Balta-Ozkan et al. (2013) indicate in their research. The level of control required in smart homes to technology that affects our daily lives challenges the boundaries of our social settings. On this topic, Davidoff et al., (2006) share their observation that "Interestingly, expanding system capabilities can easily overstep some invisible boundary, making families feel at the mercy of, instead of in control of that technology."

On the other hand, studies on the social development and impact of smart home devices suggest possible advantages from this human nature. As the technology is introduced into homes, the expected levels of behavior and activities to be undertaken at home grows, effectively broadening the scope of acceptability (Friedewald et al., 2005). Meaning that as time goes by, people naturally grow to expect certain behavior, making the availability of the technology part of the new social norm. Observations made by a study of the impact of the presence of the automated robotic vacuums, Roombas, on the behavior of householders provide evidence to support this social adaptation (Sung et al., 2007). The research indicated the development of intimacy to the robots, the attachment to the technology suggested social changes.

2.3.3 Cybersecurity issues

A major component of this stream of literature revolves around challenges caused by cybersecurity issues. The challenges of a smart home's

cybersecurity are abundant and the literature is aware of the complexity and inherent risk (Schrammel, Hochleitner, & Tscheligi, 2011; Yang et al., 2015; Weber, 2010; Komninos, Philippou,& Pitsillides, 2014; Hong, Suh, & Kim, 2009). Amongst many of the articles in this field, it is noted that although they intend to present a clear picture of challenges in the future of this technology, the set of issues presented is not exhaustive. With the increasing amount of ingenious ways people are connecting technologies together, the front for cyber attacks grows larger and with it so do the challenges relative to system security.

The challenge of cybersecurity has been separated into smaller more observable sections in order to better study and explain its effects. First, we must clarify how cyber attacks affect the technology and information within smart homes, then we move to the measures of a consumer's perceived cybersecurity of the technology. In studies, the system can be compromised when one or more of the following six security objectives have failed: confidentiality, integrity, availability, authenticity, authorization, and non-repudiation (Komninos et al., 2014).

The confidentiality of a system is generally related to the disclosure of the data, and assurance that it is only accessed by authorized personnel. Similarly, the integrity of a system reflects the degree to which it protects the data from unauthorized alterations and ensures its accuracy. Access to the resources of the system at all times when the allowed individuals requires it is described by the term availability. Authenticity

refers to the capability of the system and its representatives in insuring the identity of the people behind each interaction are known and who they claim to be. The authorization process ensures the legitimacy and roles assigned of access control to the system. Finally, the presence of undeniable proof and evidence verifying every claim within the system ensures its non-repudiation. In situations where any of these six objectives are compromised on purpose or accidentally, the cybersecurity protection of the technology and its users has failed. Such failures could lead to the users being put at a financial loss and possibly affect them in other ways that may increase their level of risk for fraudulent behavior and identity theft.

The implications of harm by the security risks of smart home technology extends beyond the cyber realm. The technology of smart home systems is part of Cyber-Physical Systems (CPS), which presents an additional set of challenges. Lee (2008) presents a definition of CPS and examines the challenges that it faces in connected technology such as smart homes. The provided definition for his research "CPS are integrations of computation and physical processes. Embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect computations and vice versa" (lee, 2008). In a CPS risks impact the physical space and can challenge the safety and reliability of such systems. Potential for harm and risks by CPS are examined in articles such as (Banerjee et al., 2012; Dutt, Jantsch, & Sarma, 2016; Lee 2008; Sha et al., 2008).

It is important to distinguish between actual and perceived levels of cybersecurity. Perceived security, similar to the perceived risk, is a direct factor that influences the consumers' acceptance of a product; whereas the actual level of security against cyber attacks does influence the perception of a consumer about the product, nor their acceptance of it. Examining consumer acceptance of electronic banking, Lee (2009) documented evidence based on the TAM and the theory of planned behavior (TPB) model, which highlights the strong relation consumers' perception of security and their attitude towards the product. Literature on the ways by which consumers perceive security in technology products often refer to three major factors: privacy, safety, and trust (Bellman, Lohse, & Johnson, 1999; Tan, & Teo, 2000; Miyazaki, & Fernandez, 2001; Gefen, Karahanna,& Straub, 2003; Nissenbaum, 2004; Lichtenstein, & Williamson, 2006). Each of the three major factors have been covered by a number of researchers who have provided insight into the definitions and the impact they have on smart home technology.

The literature provides a definition for privacy that focuses on the protection of the personal information for the occupants of the household. The protection of this information from disclosure to other unauthorized parties ensures the protection of privacy (Lichtenstein, & Williamson, 2006). Smart home technology relies in its operations on a continuous connection to devices and services often provided over the Internet.

The personal information of users operating within their homes becomes open to the world and the privacy wall disappears (Chan et al., 2008; Weber, 2010). Due to prolonged operation of occupants in close quarters with the smart home technology, often consumers become unaware of the amounts of information collected by the technology, leaving them vulnerable to exploitation.

Safety is defined as the protection of data as it is transfered across the internet where it is kept at a low risk of unauthorized access or manipulation (Lichtenstein, & Williamson, 2006). The terms selected by some researchers for this factor could differ and is often given as security; however, due to the generality of what that could encompass especially as a component of cybersecurity, we favor using the term safety. Government agencies have released publications researching the safety factors of smart home technology as the impact of attacks lead to the loss of control of IoT devices could affect the public's well being. Threats of IoT attacks have increased the risk of future warfare being conducted through this platform (Yang et al., 2015).

The third major factor of cybersecurity is trust, which is defined by how we expect the technology and/or service providers to act with our best interest in mind (Lichtenstein, & Williamson, 2006). In the settings such as those with smart home technology where there is a lack of the typical human interaction, building trust can be very difficult (Gefen et al., 2003) . From the introduction of online shopping till this

day, the topic of building trust over the internet has been the focus of many researchers (Babar et al., 2010; Ziefle, Rocker, & Holzinger, 2011; Mennicken, Vermeulen, & Huang, 2014).

To give a better visualization of how these three factors affect the security objectives if the technology we provided a table below (see table 2). The table indicates which of the six objectives would be subject to attack for each factor. Note that depending on the nature of the attack, it could affect any number of the major factors at once.

Table 2: Compromise of Cybersecurity Objectives by Component

	Privacy	Safety	Trust
Confidentiality	X	X	X
Integrity		X	
Availability		X	
Authenticity	X		X
Authorization	X	X	
Non-Repudiation			X

Provided this encompassing understanding the question now is not whether cybersecurity could be a barrier to the dissemination of smart home technology, but of how big of a role does it truly play and how can we better understand it and control it.

Other authors who examined the challenges in the future of smart home technologies further have examined context awareness and automation security, efficiency and optimization challenges, and other

cybersecurity constructs (Robles et al., 2010; Jose & Malekian, 2015; Chitnis, Deshpande, & Shaligram, 2016; Lobaccaro, Carlucci, & Löfström, 2016).

2.4 SUMMARY AND KEY FINDINGS

To conclude this chapter, we provide a brief summary of the information presented and highlights of the key findings. We began by looking at the evolution of the theories and models of technology adoption observing the difference from the simple TAM to the UTAUT2 model. The addition of more factors helped improve the models' accuracy and usability. We presented some of the earliest definitions of smart home technology and how such definitions evolved over time–making its way from being technology based to a behavioral focused definition. The literature kept pointing further into the future for when the technology will be available in every home. In the third stream of the literature the focus of future challenges gave us a look at how issues could stem from human and machine interaction, through social barriers, and from cybersecurity risks. We took a closer look into what makes cybersecurity describing six objectives that should be maintained to keep the technology secure as well as three main factors that affect how consumers perceive cybersecurity, namely, privacy, safety, and trust. Key findings that presented high value information to our study are shown below.

Independent empirical investigations conducted with existing mod-

els on smart home adoption showed contradicting results on the relationships between factors and the adoption. Leaving us with widely differing prospectives of of the future acceptance of the smart home technology (Kranz & Picot, 2012; Mayer et al., 2011).

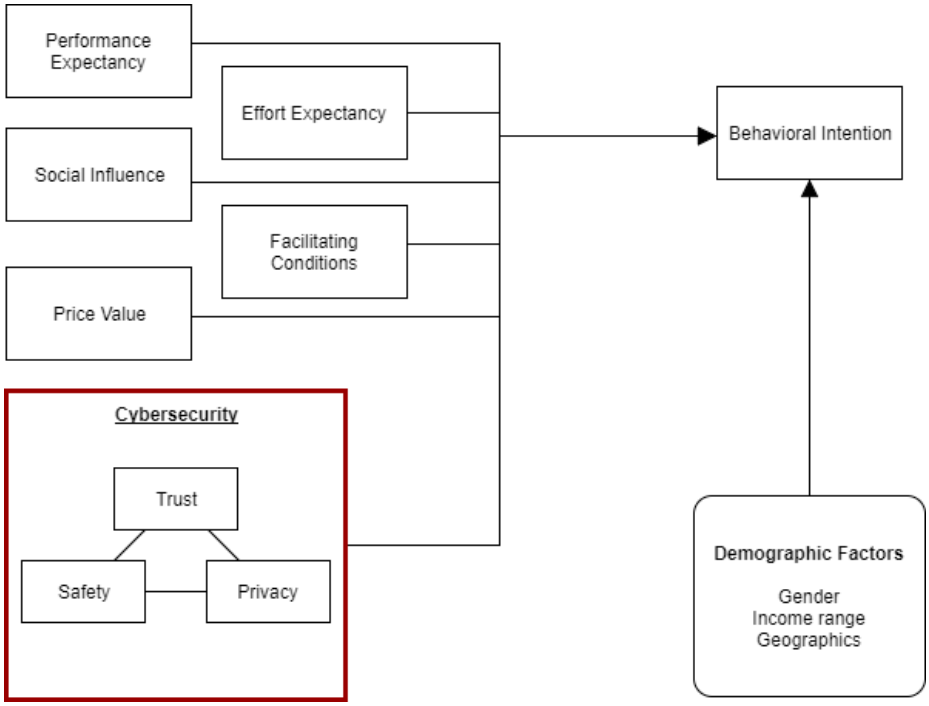
When it comes to homes and personal space, IoT devices have brought along some new challenges. Given the close level of interaction and integration between the technology and the user of smart homes, new considerations of privacy sensitivity are needed. Modifying the regulation on informing the user or introducing restrictions from selling the data (Schrammel et al., 2011).

The literature suggests three main components that make up cybersecurity and they are: trust, safety, and privacy. Trust is defined by the ability of the user to trust in service providers to take the right action towards their customers. Safety is about the transfer of data across the internet without having any unauthorized access or manipulation to that data during transfer. And finally, privacy is defined as the protection of the user's personal information making sure it is not used by or disclosed to others. The perception of these three parts combined determines the level of cybersecurity provided in a product.

From the points made above we can expect for observation of consumer behavior to indicate a relationship between cybersecurity and behavioral intention, as represented by the figure shown below (See fig-

ure 5). The figure shows modifications to the technology acceptance and adoption model, where the cybersecurity is a factor that is made-up of three core components: trust, safety, and privacy.

Figure 5: Preliminary Theoretical Model: Smart Home Technology Acceptance



The importance of cybersecurity in smart home technology goes beyond the acceptance and adoption of the technology by consumers largely because it affects the security of the general public. Studies suggest that without robust cybersecurity measures, the next generation of war tactics will utilize the vulnerability of IoT devices to launch attacks on a network-centric battlefield (Yang, 2015).

3 RESEARCH DESIGN AND METHODOLOGY

This chapter presents the research design and details of the method used to answer the research questions posed in Chapter 1. Specifically, the research question sets out to find the role cybersecurity plays in Smart Home technology adoption. This chapter is structured into five sections: (i) overview (ii) methods and instruments, (iii) description and details of the data collection, (iv) participants, and (v) importance and limitations. The methods and instructions section describes the overall research method and decisions taken in preparation of research conduction. In the third section which focuses on the details of the data collection, we emphasize important procedures that ensured the validity and ethical compliance regarding data collection. The participants section describes all the actions taken in selecting and acquiring volunteers to participate in the conduct of this research. Finally, the last section examines the research's overall value as well as when it should not apply due to certain restrictions in the data collection and analysis process.

3.1 OVERVIEW

We anticipate that findings would indicate when an organization sets out to provide improved cybersecurity of their smart home technol-

ogy their product's adoption rate should reflect an improved level of acceptance. We investigate by collecting data through an interview process with current and potential customers of smart home technology. We provided a series of questions that aim to better understand what factors the users consider before making a decision to purchase the technology for themselves.

A summary of the steps of the research method is presented in the table shown below (See Table 3). The table describes each activity and its outcome. First, the research examines potential research methods. Then, we describe the development and design of the interview script and how it was conducted. Next, we highlight the ethical precautions that were followed by the collection of interview data. Finally, the data was transcribed in the fifth step.

This research leans towards an exploratory approach based on the various challenges identified in the literature. To conduct the exploratory research, we adopt the qualitative analysis method which avoids the limitations of participants answers conforming to fit within required parameters. By conducting semi-structured interviews, the researcher could guide the conversation with the willing participants to the general discuss of interest then leave room for an open interpretation by the participant. The answers provided through this method can expand our model of technology adoption with new factors that affect the consumers behavior provided directly by the target market. Interviewees

Table 3: Steps of The Research Method

Step	Activity description	Outcome of the activity
1	Research method selection	Through the understanding of supportive literature and theories, we conclude the most suitable approach to conduct the research collection. Results indicate a qualitative approach with semi-structured interviews (pages 34-37).
2	Preparation of interview script	Construction of a semi-structured interview essentially relies on preparation of a script to lead the conversation towards obtaining responses that relate to the research topic. Taking into account the thought process of the respondents during script development improves the validity of collected information (page 37-39).
3	Ethical review	Prior to the collection of data through participant involvement, a review of the potential ethical impact and risks posed on participants is required. The process greatly reduces the presence of bias and ensures consensual agreement of data collection (page 37-39).
4	Conduct of semi-structured interviews	Identify the willing participants and arrange meeting to conduct individual interviews. Record the consumers perception of smart home technology and the influential factors involved in the acceptance and adoption process (pages 39-40).
5	Transcription of interview recordings	Following the conduct of the semi-structured interview process, the audio recorded data from each completed interview is transcribed. The written transcription is used in the analysis stage of the research.

are asked to provide what they believe the problems with the technology are. We purposefully avoid indicating cybersecurity as a potential factor to eliminate some of the biases in the study. more evidence supporting the benefits of the qualitative research approach are presented in the section below.

3.2 METHODS AND INSTRUMENTS

Research in the field of technology adoption has previously conducted analysis in a similar fashion. Mallat's (2007) qualitative study incorporated more situational factors in the adoption model. Additionally, they identified additional barriers to acceptance. Other studies have benefited from this analysis strategy for its capability to explain and describe situations that are not familiar to the research field, such as the prediction of smart home technology acceptance by the elderly (Renaud & Van Biljon, 2008). The versatility of qualitative research in providing a better understanding of emerging and growing markets makes it the optimal choice for our research requirements.

To analyze the data from the qualitative research, we chose to use a modified approach to Grounded Theory. This approach focuses on themes emerging from the discussions and conversations. The advantage to using this method is its capability to be primarily exploratory in nature, enabling the research to discover additional constructs to the adoption models (Glasser & Strauss, 1967; McCracken, 1988; Glaser, 2014).

There are five stages in our approach to analyze data from interview data. Those five stages are described in the table below (see table 4) and will be used in the discussion chapter to develop our theory.

Table 4: Steps of Conducting Modified Grounded Theory Analysis

Steps	Activity description	Outcomes
Step 1	Two stage identification of key observations from the transcribed data	A series of quotes from each of the interviews, and tabulated grouping of participant answers (pages 42-84).
Step 2	Observations are developed into descriptive and interpretive categories based on evidence presented	The categorization of the data is process that affects the overall organization and structure of the data. Selecting a balance between labels that are close to the original language of participants and knowledge of previous theories and findings (Each of the subheadings under section 4.4).
Step 3	Identification of connections between observations and development of patterns	We highlight and interpret relationships in the interpretation of findings section (pages 91-97).
Step 4	Testing the fit of observations against the developed patters and eliminating false patterns	Comparison to the literature examining unexpected observations and reflecting on propositions in the implications of findings section (pages 91-97).
Step 5	Examining and grouping of predominant themes contained in the data to develop theory	Presentation of implication results and development of the revised theoretical model (pages 95-97).

In this study, we selected target participants who are potential customers of the smart home technology market. Providers and manufacturers of the smart home technology products and services were not selected for the interview process to retain the focus on the acceptance and adoption factors. The presence of cybersecurity in smart homes technology relies on influence from both providers and consumers. However, in a new technology market for organizations to get ahead of competitors and grasp the available opportunities, they must utilize an exploratory based strategy of market-pull (Li et al., 2012). Research indicates the acceptance levels of smart homes technology are higher in

user-centric approach and market pull strategy (Penaud, Mokhtari,& Abdulrazak, 2004). In other words, in the study of consumer acceptance of emerging smart home technology the perception of the users has a higher impact on the adoption of the product/service than the perceptive of the providers.

To collect data for this research, we have selected a semi-structured interview format which allows the researcher to adapt the interview questions according to the progress of the discussion. The knowledge of the participants towards the discussion and their prioritization of some aspects provide insight into their behavioral motives. We draw reference from Venkatesh & Brown (2001) for the development of our questions used in the interview script, following a similar approach to their research methods that have been supported by their peers. The interview script was assessed for its presentation of required information and minimization of the introduction of bias. Once the information was found to be satisfactory, the script served as a guide to interviews. To ensure that the goals of the interviews are retained through the adaptation of the questions, we indicated the reason for selecting the questions in the script. Hence, when the researcher has to adapt an interview question to fit the situation, they can aim to find out information that can guide the data collection towards answering the research question.

The interview script (see Appendix A) has been broken into two sec-

tions. The first is used to understand the factors in product selection and adoption. And the second is used to identify the components of cybersecurity. Each of the sections has a set of questions along with goals for information identification. The goals are listed in the two paragraphs below.

Based on information from the literature review, we have determined that the first part of the interview should focus on the following five issues. (1) Identifying the depth of the participant's knowledge about smart homes. (2) Setting a shared understanding of the definition of smart home technology and what it means to the participant. (3) Determining the interviewee's willingness to own a smart home. (4) Identifying the key factors the participant uses to make the purchasing decision. (5) Finding the technology sector within smart homes that the contributor associated with the most. This marks the end of the first section of the interview script.

In the second section of the interview script, our aims are as follows. (1) Identify the level of cybersecurity the participants are familiar with. (2) Determine the relevance of the cybersecurity components to the participant's view of cybersecurity. (3) Find the level of importance each component plays. This builds the relationships between the model's adoption factors.

3.3 DETAILS OF DATA COLLECTION

To ensure the utmost ethical conduct in the interview process, we referred to the Canadian Institute of Health Research et al. (2014 December) publication on proper conduct of research involving humans. The publication provided guidelines for preparation and conduct of the interviews. The procedures also ensured that selection, elimination, and incentives to participants are within ethical standards. The tri-council policy statement of ethical research conduction (Canadian Institutes of Health Research et al., 2014) has been followed throughout the conduct of this research to the fullest capability of all those involved. An application was prepared by the researcher and supervisor of this research which highlights the important information regarding the methods for research conduct. Details of the information provided in the application are given below.

The research protocol form included information on: the project team, study overview, funding and approval, the participants themselves, recruitment methods of participants, informed consent, data collection methods, data storage and analysis, declarations, and additional comments. Additional information submitted along with the protocol form included: consent form, interview script, recruitment poster, and on-line recruitment material. The material was revised multiple times by the researcher and supervising professor to meet the requirements of the Canadian tri-council's guide on the ethical conduct of research

involving humans.

The accepted ethical procedure for this research can be briefly described as follows. There is no external source of funding to this research by individuals or entities other than the researcher. Participants interacted directly with the researcher through semi-structured interview. The sample of participants did not include individuals with any prior relationship to the researcher to eliminate any sense of obligation to participate or provide a specific type of answer. No financial or commercial conflict of interest was present to affect participants, and withdrawal from the research did not affect the compensation received by the volunteers. Contacting interviewees was accomplished through both posters on the campus grounds and posts on social media. The research conducted involved 25 participants who had met the qualification criteria and were willing to sign consent forms to carry out the interviews properly. Participants in the study would not be subject to any additional level of risk than experienced in daily life. Written consent forms were signed by both the participant and researcher prior to any data collection, with clarification on the nature of the research, withdrawal procedure, and insuring that any questions by the participants were answered clearly. An audio recording of the interview process was acquired with consent of the participants for future transcription of the data. Collected data is coded and anonymized, removing any identifying information. Throughout the research period all data is kept on a secure device stored in an encrypted format and

password protected. All recordings of participant information will be destroyed after one year of research completion to ensure their privacy protection.

3.4 PARTICIPANTS

Following the completion of the ethical review process, collection of willing volunteers begun. This stage involved posting fliers and information on social media sites that informed any interested individuals of the ongoing study. Information on the title, purpose, and requirements for the study was provided through the postings with instructions on the method of contacting the researcher if an individual was interested in participation. Participating in the study was voluntary for those who fit the criteria. As an incentive to participate in the study, the researcher provided a gift card to Starbucks®.

For the purposes of this study, we chose our the sample of volunteer participants based on four qualification criteria.Volunteers had to be over the age of 18 to be of legal age to make a purchasing decision for a home and be considered as potential customers. The interview script was prepared in English, therefore, fluency in the English language was selected as a required qualifying criterion. The qualifications also required candidates to have spent at least two years living in Canada to ensure that the participants had experienced the same standard of daily living and amenities reducing any errors caused by cultural differences.

Finally, to qualify for the study, participants must indicate an intent to purchase a house in the near future or within the past one year. This last criterion is essential to ensuring that the participants are potential customers of the smart home technology.

3.5 IMPORTANCE AND LIMITATION

The study was conducted in a manner to ensure the results could be widely applicable to the smart home technologies. However, the study sample sets a limitation to the global representation. In the interest of feasibility, we chose to conduct 25 interviews with participants who have spent at least two years in Canada, the small sample size in the geographic restriction is not representative of consumers external to Canada.

4 RESULTS

Chapter 4 presents the results of the study, and it is organized into four sections. The first section gives an overview of how the research data was acquired and who the participants were. The following two sections correspond to the structure of the interview script, beginning with the overview of consumers' awareness of smart homes followed by their predisposition to cybersecurity. The fourth section of this chapter goes into greater detail of the participants' responses from each of the eight aims identified on the interview script.

4.1 OVERVIEW

To reiterate, the research question covered by this study is: *what role does Cybersecurity play in Smart Home technology adoption by consumers in the household market.* Findings from the literature review chapter (earlier) provided evidence of a literature gap. A portion of the literature focused on identifying adoption factors for the smart home technology (Kranz & Picot, 2012; Mayer et al., 2011). A variety of factors which play a part in the consumer acceptance of smart homes are proposed by these studies. However, the studies do not include cybersecurity as a factor in the technology adoption process. On the other hand, we observe a separate portion of literature that examined the challenges in the future of smart homes (Komninos et al., 2014; Yang et al., 2015). Identified in this second group of research are a set

of cybersecurity challenges that can affect the experience of living in a smart home. Given the indications in the literature to the importance of both portions, we aim to study a crossover of both streams.

The literature provided theories which guided the creation of a preliminary theoretical model of smart home technology adoption. The model does not eliminate from the existing theories in the literature but builds on the UTAUT2 model discussed in chapter two. Based on arguments presented earlier, we propose that a link exists between cybersecurity and a consumer's behavioral intention. The theories also indicate components that form and affect the intensity of cybersecurity as a factor. A diagram representation of this theoretical model is provided earlier in chapter 2 (see figure 4).

We received a total of 34 volunteers interested in participating in the study. From these, seven volunteers were not involved in the interview process because they either failed to qualify or were unable to schedule a meeting time to go through the 45-minute interview. From the remaining 27 participants, two chose to withdraw their data from the study leaving 25 remaining. The findings from the study sample are summarized in the following sections. A demographic breakdown of the 25 remaining participants is shown in the table below (see table 5).

Table 5: Participant Demographics

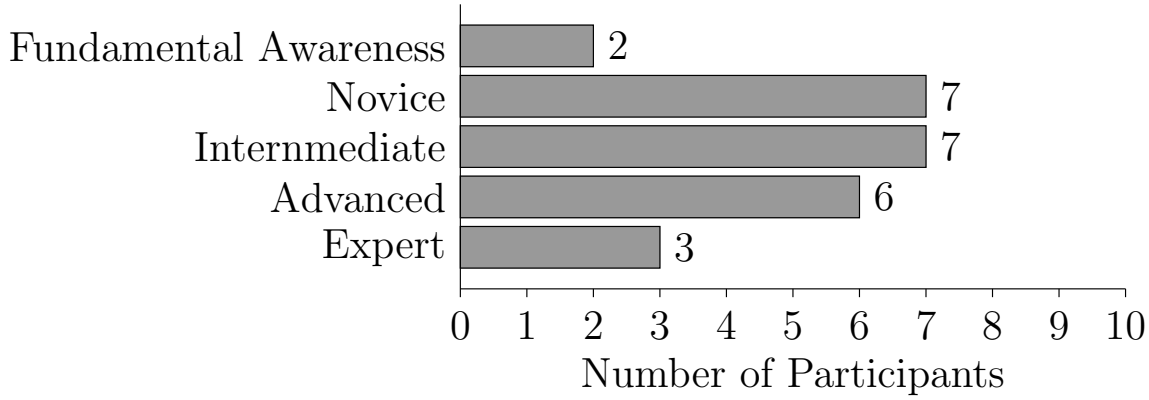
Interview Number	Gender	Age Group	House Ownership	Education	Employment
1	Male	18 - 24	Currently Searching	High school graduate	Part time job
2	Male	25 - 29	Currently Searching	Some College / University	Student / Part time Job
3	Male	18 - 24	Currently Searching	University Graduate	Full time Job
4	Male	25 - 29	Owns	University Graduate	Full time Job
5	Female	18 - 24	Currently Searching	Some College / University	Student / Part time Job
6	Male	18 - 24	Currently Searching	University Graduate	Full time Job
7	Female	25 - 29	Owns	College Graduate	Full time Job
8	Female	35 - 39	Owns	Some Postgraduate Work	Two Full time jobs
9	Male	18 - 24	Owns	Some College / University	Full time Job
10	Male	25 - 29	Currently Searching	Post Graduate Degree	Full time Job
11	Female	30 - 34	Owns	Post Graduate Degree	Two Full time Job
12	Female	30 - 34	Currently Searching	Some College / University	Student / Part time Job
13	Male	18 - 24	Currently Searching	Some College / University	Student / Full time Job
14	Male	25 - 29	Currently Searching	Some College / University	Student

Interview Number	Gender	Age Group	House Ownership	Education	Employment
15	Female	18 - 24	Currently Searching	High school graduate	Full time Job
16	Male	25 - 29	Currently Searching	University Graduate	Full time Job
17	Female	18 - 24	Currently Searching	High school graduate	Full time Job
18	Male	40 - 44	Owns	University Graduate	Full time Job
19	Male	25 - 29	Currently Searching	Some College / University	Student / Part time Job
20	Male	18 - 24	Currently Searching	Some College / University	Student / Full time Job
21	Male	18 - 24	Currently Searching	College Graduate	Full time Job
22	Male	25 - 29	Owns	Some College / University	Full time Job
23	Female	18 - 24	Currently Searching	College Graduate	Two Full time Jobs
24	Male	25 - 29	Currently Searching	Post Graduate Degree	Full time Job
25	Male	30 - 34	Currently Searching	Post Graduate Degree	Full time Job

4.2 CONSUMER AWARENESS OF SMART HOMES

During the interview, volunteers were asked to describe their level of technical knowledge. Information collected through the interview process indicates a normal distribution of the participants' technical knowledge (see Figure 6). When participants provided non-descriptive or subjective answers, they were asked to provide an indication of their regular activities with technology. This information was then mapped onto a five step competency scale; from "Fundamental Awareness" to "Expert" (National Institutes of Health, 2014).

Figure 6: Distribution of technical knowledge



Participants answered if they have any prior knowledge about smart homes if they gave a positive answer the researcher would follow-up with a question asking them to provide a definition of smart homes. From the sample, 20 participants had prior knowledge of smart homes, and they provided their definition of smart homes. Of these 20 participants, three provided definitions that were inadequate to properly identify the technology, seven provided definitions that shared similar-

ities with the literature, and then gave full definitions that included multiple key components of smart homes.

From the sample drawn two participants currently owned smart home technology, the 23 other volunteers indicated if they were inclined to install smart home technology in the future or if they were against it. Seven participants were opposed to installing smart home until their concerns regarding cybersecurity were met, and 16 participants indicated their interest in owning a smart home provided the right circumstances.

4.3 CYBERSECURITY PREDISPOSITION

In the second part of the interviews, we study the intensity of cybersecurity as a factor and what components contribute to cybersecurity as an influence on consumer acceptance.

An examination of the interview scripts indicated that 16 of the 25 participants mentioned some component of cybersecurity being a factor of concern to them when considering a smart home technology.

Out of the interviewed sample, the study found that six volunteers had some prior knowledge or training in cybersecurity. Each of the six participants had precaution measures in place to increase security. From the remaining 19 interviewees, 13 members had taken some pre-

cautions without any training or extensive knowledge of cybersecurity.

Participants were asked about their perception of risk to their information or belongings being affected by cybercrime. The result was an almost even split with 12 participants indicating a high level of perceived risk and 13 participants showed low perception of risk.

4.4 INDEPTH EXAMINATION OF RESULTS

The interviews with the participants collected information to aid in the understanding of smart home technology adoption. Questions presented by the researcher were grouped into sets according to their aim. The following subsections provide an in depth presentation of the results for each of the eight sets.

4.4.1 DEPTH OF TECHNICAL KNOWLEDGE

As mentioned earlier the five point mapping of the participant's level of technical knowledge was based on the National Institutes of Health's (2014) competencies proficiency scale (see table 6).

Table 6: Competencies Proficiency Scale

Score	Proficiency Level	Description
N/A	Not Applicable	You are not required to apply or demonstrate this competency. This competency is not applicable to your position.

Score	Proficiency Level	Description
1	Fundamental Awareness (basic knowledge)	You have a common knowledge or an understanding of basic techniques and concepts.
2	Novice (limited experience)	You have the level of experience gained in a classroom and/or experimental scenarios or as a trainee on-the-job. You are expected to need help when performing this skill. You understand and can discuss terminology, concepts, principles, and issues related to this competency. You utilize the full range of reference and resource materials in this competency.
3	Intermediate (practical application)	You are able to successfully complete tasks in this competency as requested. Help from an expert may be required from time to time, but you can usually perform the skill independently. You have applied this competency to situations occasionally while needing minimal guidance to perform successfully. You understand and can discuss the application and implications of changes to processes, policies, and procedures in this area.

Score	Proficiency Level	Description
4	Advanced (applied theory)	You can perform the actions associated with this skill without assistance. You are certainly recognized within your immediate organization as "a person to ask" when difficult questions arise regarding this skill. You have consistently provided practical/relevant ideas and perspectives on process or practice improvements which may easily be implemented. You are capable of coaching others in the application of this competency by translating complex nuances relating to this competency into easy to understand terms. You participate in senior level discussions regarding this competency. You assist in the development of reference and resource materials in this competency.

Score	Proficiency Level	Description
5	Expert (recognized authority)	You are known as an expert in this area. You can provide guidance, troubleshoot and answer questions related to this area of expertise and the field where the skill is used. You have demonstrated consistent excellence in applying this competency across multiple projects and/or organizations. You are considered the "go to" person in this area inside or outside your immediate organization. You create new applications for and/or lead the development of reference and resource materials for this competency. You are able to diagram or explain the relevant process elements and issues in relation to organizational issues and trends in sufficient detail during discussions and presentations, to foster a greater understanding among internal and external colleagues and constituents.

Adapted from the Competencies Proficiency Scale provided by the National Institutes of Health (2014).

The majority of participants indicated their technical knowledge proficiency level was equivalent to novice or intermediate scale, with a smaller portion represented by the advanced skill rating, and even fewer qualifying as experts and fundamental awareness respectively.

A participant with only a fundamental awareness proficiency level described their technical knowledge as follows;

"As far as electronics and stuff I have ideas on how these things work, but I wouldn't be able to operate [smart homes technology] by myself. I have never really used that technology before" (participant number 10).

Other participants provided responses that indicated their belonging to the novice or intermediate levels of proficiency, such as the ones shown below.

"I see my level of technical knowledge to be very similar to people in my age group [early twenties], I grew up with technology being everywhere around me. An even though I didn't study computer science, I still picked up a lot of things that my parents didn't" (participant number 7).

"I am not terribly advanced when it comes to technology, although I do manage a [cellular service] store so when it comes to cellphones, I am fairly savvy" (participant number 8).

Advanced technical skill levels were also demonstrated be a portion of the participants. Some responses are provided next.

"I am very comfortable using technology, I program sometimes and have a good understanding of how computers and electronics work [...] I have used some smart home technology before, I see its benefits in making things easier" (participant number 9).

One of the interviewees who categorized as an expert in technology gave the following answer.

"Well, I am a computer programmer, with a lot of technical knowledge. I have my own smart home devices, and I have done my own research on [the cybersecurity of IoT] topic as well" (participant number 11).

4.4.2 DEFINITION OF SMART HOME TECHNOLOGY

The given definition by the literature on the meaning of smart homes does not always reflect the common understanding shared by the general public. The interviews provided insight into how consumers define the technology.

The extent of understanding exhibited by the participants generally followed one of two types. On one hand, people gave examples that included different types of IoT devices connected together providing value for the home owners, and the other group gave a vague discretion of one product that could be associated with smart homes.

"I imagine it would be a house the interacts with your phone, and technology so security cameras, [thermostats], lighting, maybe locking

doors, starting the dishwashers, and operating Roombas or something. All that could be controlled together and work better together" (participant number 20).

"It would be like home monitoring, things like that. That's pretty much all I know. Every time it gets advertised it's about keeping your home safe and monitoring it" (participant number 8).

The two examples provided above belong to two participants who have both indicated having very little prior knowledge of smart home technology. Both participants demonstrated similar technical proficiency levels ranking them both at intermediate. The lack of a common definition of smart home technology is also reflected in the literature, and with service and product providers aiming to capture a larger share of the market, the dilution of the border that defines smart home technology keeps increasing. Theory suggests that a common understanding can be reached if we move away from the technical based definitions and into a behavioral focus. We explored the reactions of participants to a behaviorally based definition in the interview process and observed a bridging in the divide.

The researcher presented Aldrich's (2003) definition of smart homes to the participants and asked for their feedback after they had provided their own definition. The two participants provided above responded as follows respectively.

"That sounds reasonable and good. It sounds exactly like how I

would have hoped to answer" (participant number 20).

"For me, it reminds me of a few other things that I have heard about smart homes, and it's just the whole idea of it being intuitive and learning things making it easier for you. Makes life simple and would also make life more efficient" (participant number 8).

Participants of the study unanimously agreed with the definition provided by Aldrich (2003), and highlighted any concepts that their definition missed as being valuable to the technology.

4.4.3 WILLINGNESS TO OWN SMART HOME TECHNOLOGY

We examine the current willingness of the users to purchase the technology in order to understand what factors are at play that have helped them make their decision. From the sample of participants, two already owned some smart home technology. The technology components of smart homes that those participants had included home automation devices, entertainment systems, home security systems, and energy efficiency. From the complete sample eighteen participants were at the time being in favor of purchasing smart home technology and seven participants were against. To compare the relationship between the level of technical knowledge and the consumers willingness to purchase, we show below answers from four participants, two that have demonstrated high technical skill (rating at four or five) one in favor and the other opposed to installing, and similarly from two participants with

low technical knowledge (ratings of one or two).

From the strong technical proficiency group, a participant indicated their willingness to own the technology (as shown below) when asked by the researcher of how they would feel about owning smart home technology.

"I am intrigued by the technology and interested in eventually having something like it installed in my home. I would say I have had a positive experience so far" (participant number 14).

But when the conversation changed to the topic of convenience and risk the participant had more concerns about some of the risks associated with the technology.

"I see lots of small superficial benefits to a lot of these devices, but there are also a few major things like security where I think smart homes can come into their own, if proper security precautions are in place there are only so many ways you can get around it. I think coming in and out of the house easily is something a lot of people would be interested in installing, and maybe garage doors that open when you drive up to them, but those come with a lot of security risks which make me hesitant" (participant number 14).

On the other hand, another participant who ranked as an expert in technical knowledge was opposed to the idea of installing smart home technology. Even though they were of highly advanced technical knowl-

edge, their inclination to learn more about the technology was an important factor to consider before trusting it.

"I don't think it would be a good idea. I wouldn't be comfortable installing something I don't know too much about. But if I could trust and be convinced the my privacy is a high concern to the provider then I would consider it" (participant number 19).

Looking at the low end of the technical skill spectrum we observe a clear shift in the concerns that make participants opposed to the technology. A Novice in technology focused on their lack of need for the technology as the reason they wouldn't spend the money on owning the devices over their cybersecurity risks.

"No I wouldn't, but it's definitely something I would invest in if I really had the need for it. I mean the products I see are like thermostats, the cameras, and the doorbells, things like that so those are all things that right now to me I don't have a use for I guess but not that I don't see the use for them ... I wouldn't say I'm scared of the privacy risks or anything like that, it's no different that surfing the web realistically" (participant number 4).

Similarly we see different behavior in participants who have ranked at a two or one on the technical proficiency scale with a positive attitude to installing the technology where there is no display for concern for any risks associated with the technology.

"Coming from someone who is [unhappy with their thermostat] and

has never had the luxury of a security system in their places of residence, I would love a Smart Home. The idea of having technology at my fingertips to adjust whatever I desire in my home is really appealing to me ... So much stuff that would save a person time and energy that they could put towards things like a career, hobbies, enrichment, exercise, etc. and so much less to worry about" (participant number 7).

4.4.4 WHAT ARE THE KEY FACTORS AND CONCERNS

As we observed in the consumer's willingness to own section there as factors that inevitably play a role in the purchasing decision. We asked participants to indicate which of these factors they could identify following the question of their current intent to purchase. Participants indicated what motivated them as well as what concerned them about this technology. A summary of the key factors identified be participants is given in the table below (see table 7).

Table 7: Key factors

Num	Factors Identified	Number of Participants	Consumer Provided Explanation
#1	Performance and convenience Benefits	15	"I would look into what kind of things I would like to have made easier and see if I could save on a few things or make them more convenient" (participant number 9). "I would have a house that would know some things, so it could start making coffee as you get up, or preferably before you get up so that it is ready to drink as soon as you are awake. Everything would be pre-laid out you might have to manually adjust a few things but the house will start working on chores for you from morning till night" (participant number 13).
#2	Security Risks	9	"Having your home run by technology it's just one of those things with fear from hackers. So it's one thing to have your laptop or phone hacked, and with more Internet banking now on smart devices, just to think that your entire house is on a connected network like that. I guess there would be a high trade off from risk for the convenience" (participant number 8). "I have limited my use of smart home devices to things that don't harm me if they get hacked. When it comes to the [wireless door locks] I will need to consider the level of security and authentication on the device" (participant number 11).

Num	Factors Identified	Number of Participants	Consumer Provided Explanation
#3	Installation and Operation Costs	9	"My biggest factor for not installing is cost. My living situation right now as a student, I don't see it worthwhile to go through all that renovation expense. Maybe sometime down the road" (participant number 2). "The thing is, I would have to spend more time on researching it to decide if I am able to afford it and if the level of smart home technology I could get would make me feel safe. With the cheaper options, you just can't be sure if they will work properly" (participant number 9).
#4	Restricted Living Space	5	Some participants could not install smart home technology because of restrictions in their living area, either due to the small size or caused by shared ownership which could be problematic if the technology was not agreed on by all members. "My apartment is very small right now, maybe if I move to a bigger house down the road I would be more interested in automating my house" (participant number 5). "I would change some of the things and maybe get my house to be more energy efficient, as long as it isn't against my condo agreement" (participant number 12).

Num	Factors Identified	Number of Participants	Consumer Provided Explanation
#5	Time and Energy Savings	4	"Having some of these services like self-regulating temperature or fridges that keep track of the foods expiration dates there are many things that could save a person energy and time. You could optimize your monthly electricity usage and get a lower bill with all the information available at the tap of a screen" (participant number 7). "It could make me more productive, it can take care of simple tasks for me here and there. What I am thinking right now is mostly heating and lighting control. If a system is specifically monitoring that all the time, it can become more efficient in operation than any person could do manually" (participant number 9).
#6	Lack of Trust	3	"Based on what I see from TV I wouldn't trust any form of automated intelligence to control what I do in my home, I would need to have some form on a kill switch" (participant number 7). "I think I would be concerned with how the provider values my information, and I wouldn't be convinced that they deserve my trust until I try it" (participant number 19).

Num	Factors Identified	Number of Participants	Consumer Provided Explanation
#7	Lack of Social Norm	3	"I would have to see it being used in practice before I know if I am willing to make the trade off" (participant number 3). "A factor that would help me decide is if other people say that the product is good and they have used it" (participant number 14).
#8	Learning curve and ease of use	3	"It's important for me to have a good understanding of how it all works and be comfortable controlling the technology when I install it in my home. So I would need to do more research about it first" (participant number 9). "How well the interface is designed. I know there is a whole bunch of different smart home technology with different designs, and I think some of them are really annoying. So I want something that is easy to understand, and being able to have all of the different technologies share the interface and have a more consistent look and feel to them instead of it being all over the place" (participant number 12).

Num	Factors Identified	Number of Participants	Consumer Provided Explanation
#9	Value of the Technology	2	Two participants indicated the value gained from the technology is a factor to them, however one saw it as positive influence and the other saw the lack of current value as a negative. Their opinions are shared below respectively. "For the simple fact that everybody has such a busy lifestyle now, people don't have the luxury of a stay at home parent, everyone is working, I would be more inclined to using the technology. So anything the would make my life easier and would allow me to spend more time with my family and take a load of my shoulders sounds fantastic" (participant number 8). "With the type of place I live in there isn't much I can use the technology for. and living in a rural area I don't see much of a point just because if something goes wrong it's a lot more of a headache to try to get it fixed" (participant number 5).
#10	Reliance and Reliability	2	"I feel that if I do get smart home technology that within a few months I would become very lazy. It might become a problem if I just expect to have it at all time. What would happen if it breaks down at some point. If the system gets faulty and it messes up the comfort of your home there needs to be a manual override" (participant number 20).

Num	Factors Identified	Number of Participants	Consumer Provided Explanation
#11	Accessibility	1	"A valuable feature that my smart home has is the ability to make changes while I am away. I can change the temperature of the house, monitor activity in the house, and turn some things on or off. And I can access that from all of my devices" (participant number 11).
#12	Lack of Privacy	1	"I wouldn't be comfortable installing something I don't know too much about. But if I could trust and be convinced the my privacy is a high concern to the provider then I would consider it" (participant number 19).
#13	Closed Software	1	"I am a supporter of free and open software. In a closed software product manufacturers could place back-doors to their products and other insecurities. I don't think that there are any open software smart home products out there" (participant number 3).
#14	Retrofit	1	"A concern for me would be that it is hard to retrofit smart home technology into an already built house. It's not impossible, of course, but it would be expensive. I would much rather have a house that has been designed to include the technology in the first place" (participant number 13).

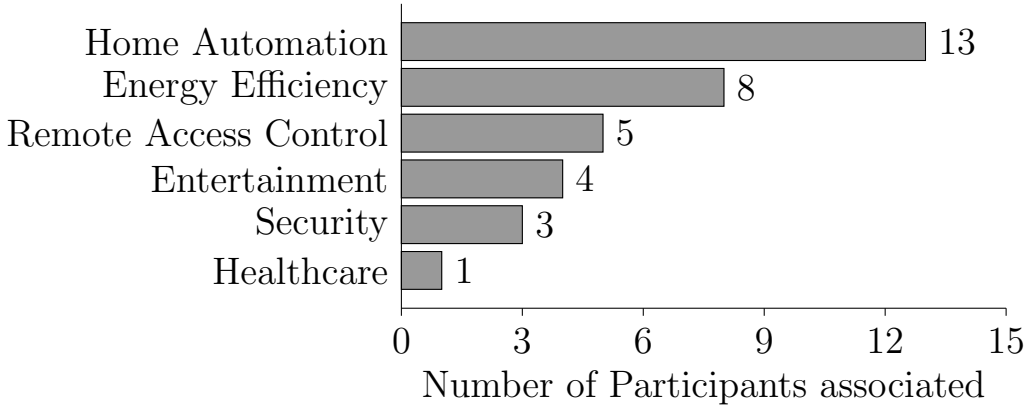
Aggregated results from the interview data collected

4.4.5 TECHNOLOGY SECTOR

Earlier in the study we identified six market sectors for the smart home technology: (1) home automation, (2) entertainment, (3) security, (4) healthcare, (5) remote access control, and (6) energy efficiency. We

asked participants in the study how they would use smart home technology in their daily life to identify which of these sectors they associated with. The data is represented in the figure below (see figure 7).

Figure 7: Technology Sector Distribution



The home automation technology sector was an area of interest for the largest portion of participants, as 13 participants in total mentioned that sector of technology from the sample. An example from the interviews is given below.

"I see the technology helping with my daily routine, for tasks that are easy to [perform] with smart home technology. Maybe some lighting control, at certain times, preparing coffee. I'm more into those technologies than major home security devices" (participant number 14).

The second largest sector identified by the contributers was the energy and efficiency sector. One of the eight responses that contained that sector is listed next.

"I think it would make my life easier in several small ways but I think

things like having easier control over my living situation are going to be much more important. Being able to instantly monitor how much electricity my house is using, and what is using the most energy" (participant number 2).

Five of the participants indicated an association with the remote access and control functionality of smart home technology. A portion from the interview is provided below.

"It would make some things easier. To some level it would increase laziness by letting me adjust electronics around my house without moving, like my lighting and heating, but that is also important when I am away from the house" (participant number 9).

In some situations interviewees indicated how they could use the systems as a source of entertainment, those were present in four of the interviews. An example is given below.

"I would probably become a lot more lazy to be honest with you if my day could be regulated like that. I would just probably feel happier and more content with my way of living. I would probably connect it to my home entertainment center and get to play my music anywhere in the house. It could also take care of a certain level of my daily tasks" (participant number 10).

Three participants provided answers that indicated their interest in utilizing the security measured of the technology. An example is listed

next.

"I would have more security, all my devices would be connected, and it all works together. The doors would be able to know when someone is there and who should be allowed in. I could monitor my kids when I am at work. I think it would make my mind at ease" (participant number 13).

The least represented market sector for the smart home technology amongst this data sample was the healthcare sector. Only one participant associated the technology with being used to monitor the health of occupants and improve their way of life.

"I see value from having this technology that would outweigh the risks we discussed. Especially in a situation where there are special needs at the home. For [some people] with limited mobility the devices that can be installed would allow [them] to live freely" (participant number 7).

4.4.6 FAMILIARITY TO CYBERSECURITY

Identification of the participant's awareness and standard precautions for their cybersecurity provides a bench mark to how they behave when operation technology and is important to consider when they indicate if such a factor could be a barrier to their adoption.

From the interviews, six participants indicated that they had received some form of training or had been self taught in skills that relate to cybersecurity. The remaining 19 participants where not familiar with

any form of training.

A participant indicated their knowledge in cybersicurity by indicating why they were required to undergo some training on the subject.

"I am from a military family so we have all received some training on how to keep our technology and information safe" (participant number 8).

Another participant who had not gone through certified training programs indicated that their knowledge on the subject gained be conducting research on their own.

"I make sure that all my critical and personal information is either stored on non-digital form, or kept in an encrypted format on an isolated device. Like on a flash drive or external hard drive that are not connected to any device unless something needs to be accessed" (participant number 9).

Other participants with a low level of knowledge on the matter indicated that their was no motivational factor for them to learn more in the skill.

"I don't know a lot about it. I have password on my devices, but I wouldn't do anything too complicated" (participant number 5).

Besides the level of training in cybersecurity we examined the participants' practices and precautions that they would regular use operation

of technological devices. 18 of the participants had anti-virus or anti-malware software set up on some of their devices to provide some form of low level protection to their technology and information.

One of the participants with no cybersecurity training or knowledge had this to say about their precaution measure when operating technology.

"I use things such as anti-virus and anti-malware, I stick to the sites I know and trust on the Internet. Basic things that everyone says you need to have" (participant number 10).

Every participant that had indicated having training or knowledge in cybersecurity also ran some form of anti-virus protection. Participants were more inclined to not have anti-virus software if they had no knowledge in cybersecurity. From the 19 participants with the low level of awareness in cybersecurity, seven had not operated their technology with the protection of anti-virus software.

A sample of the participants' responses to the inquiry on their standard measures of precaution are given below. The first is of a participant who was skeptical about the value of installing anti-virus software instead relying on avoiding suspicious links on the Internet.

"I don't click on ads, I have my firewall on, and I use long passwords. That is the extent of my precautions" (participant number 7).

From another participant we get a responses that indicates they feel completely protected without needing anti-virus technology guided by some information that they had heard about the security of Apple's products online.

"I wouldn't open emails that I am not sure where they are from. But that is about it. I have a Macbook which is secure and doesn't need any anti-virus. Also, I don't really download [movies or videos] I usually stream it to be safe" (participant number 16).

Making sure that the participants' level of cybersecurity is represented accurately we continued to probe by asking if they felt that their information or technology would be vulnerable or targeted by cyber criminals as it is at the time. This set of questions then resulted in a larger divide in the sample where 13 out of the 25 participants felt their electronics and information was secure in its current state while the remaining 12 were opposed to them.

From the seven participants who had not chosen to use anti-virus protection on their devices and had a low awareness in cybersecurity only one indicated they could be vulnerable in their current state (shown below).

"My answer hinges entirely upon my insignificance in the great aspect of things [...] That said if I did have a cause for concern that I was to be targeted I don't believe that it would be very difficult for someone with the know-how to get into my stuff, unfortunately" (par-

ticipant number 7).

Moving to the portion of the interviewees that have low cybersecurity knowledge but did indicate the use of protection software on their devices. Six of the 12 answered that they where vulnerable while the other half answered that they were not.

Some of the participants in this group had an attitude that their information was not of high value to anyone making their risk levels low enough to not require any additional precautions to the measures they had in place. An example is shown below.

"I feel pretty secure. I am not very important, and even if I was targeted I don't feel that it would reveal anything particularly compromising" (participant number 3).

The other part of this participant group resorted to keeping information which they felt was valuable off of their electronic devices or in a more secure format which they felt comfortable with. "My attitude towards the information that i put online and my own personal information. I treat it all as though it is not mine. I have an understanding that I cannot have total privacy over anything I upload. I do feel like it is targeted, not particularly because of me of course but I feel like it isn't private" (participant number 2).

The remaining participants (six people) were participants which had

a higher level of knowledge in cybersecurity through training or being self educated on the matter. though all six indicate that the use anti-virus protection on their devices, some of them responded to the vulnerability questions with some lack of risk expectancy.

Two participants had indicated that they haven't observed any increase in cyber attacks over the past few years. They generally attributed the heightened scene of concern for cybersecurity to the growth in media and its interest in the topic. A participant had the following to say.

"I really can't say that there are more [cyber] attacks going on now that before. So in a scene I don't feel that I am facing any higher risks now" (participant number 8).

Although the two participants had some disagreement with the statement presented by the interviewer around their perspective on personal vulnerability through reflecting on the increased number of reported cyber attacks in the media, they still felt that some risk was present.

The last four participants have given cybersecurity the highest level of familiarity out of all the others. they are knowledgeable and cybersecurity standards, their devices are protected by anti-virus and other precautionary measures of securing information, and they are concerned for the vulnerability of information and electronic devices they use regularly.

One interviewee gave us the detailed view of their perspective on vulnerability of information in the digital age.

"I guess it is possible that I would be vulnerable. I have information on places outside my own system. All the information that I can give to banks, university, work, and other organizations. Information that I have outside my control, if these places are compromised my information could get stolen. So I remain very careful on the Internet, so far I have never lost information or been hack to the extent of my knowledge. It could be partly luck because from what I know you can't be perfectly safe. Anyone could be targeted and anyone could be hacked" (participant number 9).

To provide a representation that can aid in visualizing the distribution of participants and their level of familiarity of cybersecurity we plotted a chart of the percentage of users indicating security awareness in relation to their technical proficiency level (See figures 8 and 9). From the data we observed a shift caused by an outlier from the group of participant with level one in technical knowledge (see figure 8). The outlier was removed and from the following chart (see figure 9).

Figure 8: Familiarity to Cybersecurity

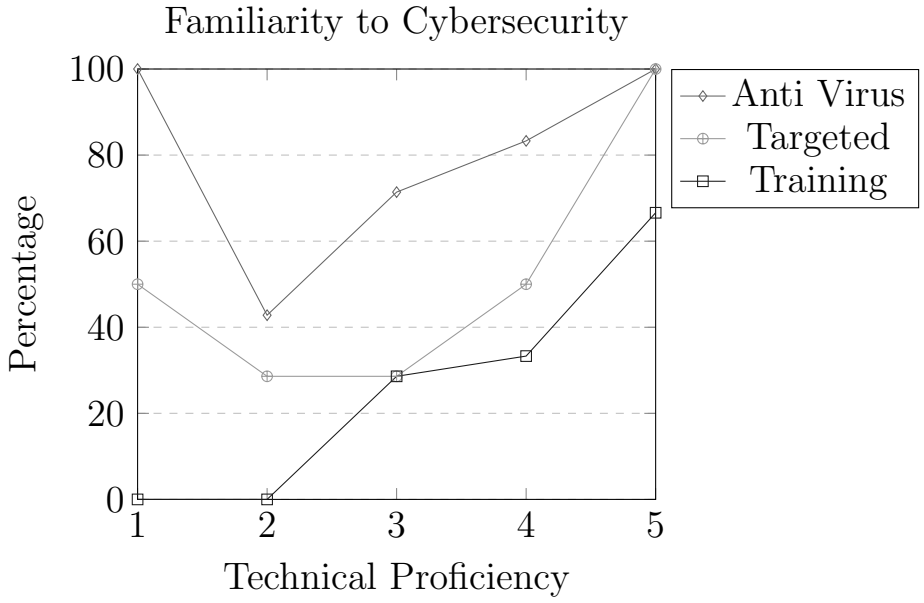
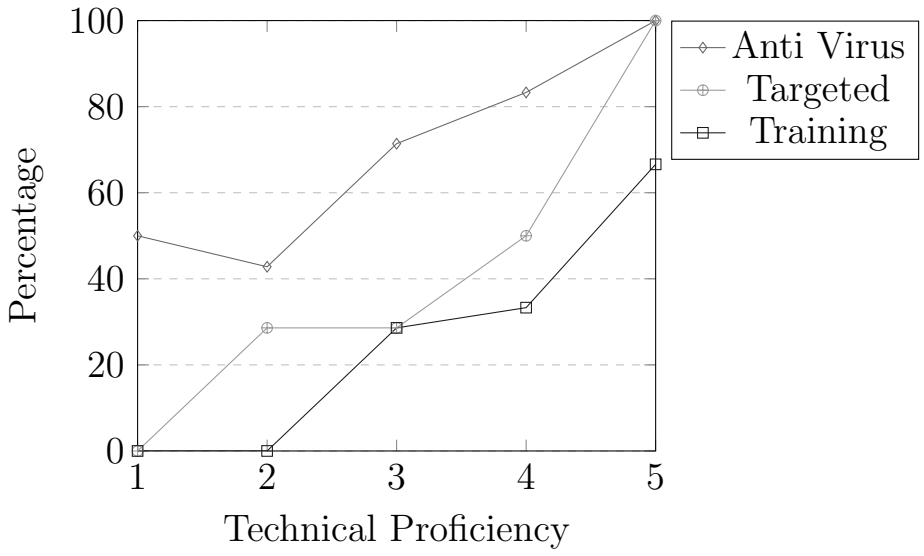


Figure 9: Adjusted Familiarity to Cybersecurity

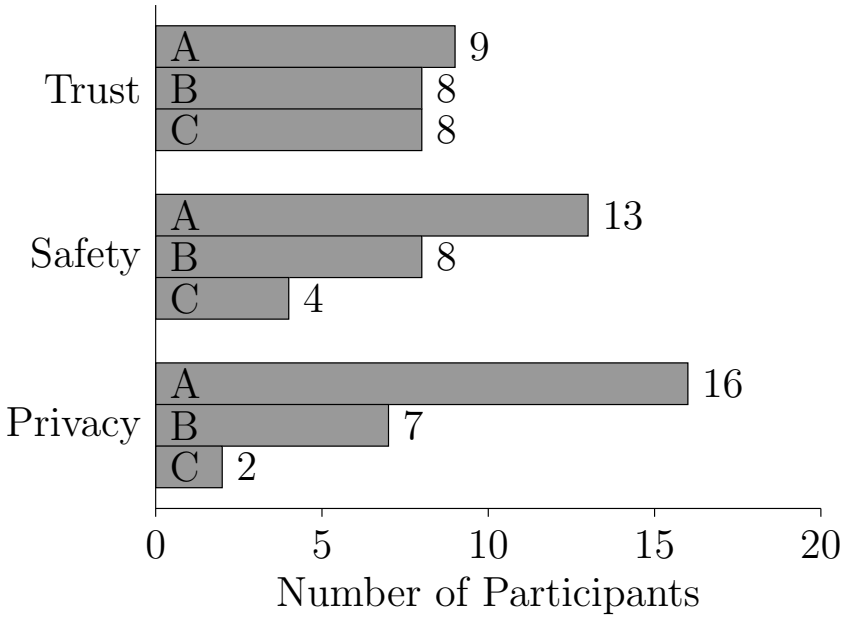


4.4.7 COMPONENTS OF CYBERSECURITY

From the literature we identified three components that make up the general public perspective on the cybersecurity of electronic devices:

trust, security, and privacy. For this component of the research we asked participants to listen to a brief description of what each of the three components entailed then provide their opinion, and whether they feel that component is one they relate to or not. A summary of the results is represented in the figure below (see figure 10).

Figure 10: Cybersecurity component intensity



A: High Impact Factor
B: Low Impact Factor
C: Circumstance Dependent Factor

In the diagram, each of the three cybersecurity components has three bars representing the number of participants with similar answers. Each bar on the chart is labeled "A", "B", or "C". Bars labeled "A" represent participants who answered that the component was an important factor that is currently increasing their perceived level of risk. Ones labeled with "B" illustrate the group of participants who feel that the

factor does not currently increase their perceived level of risk. The last portion of the participants indicated the factor was important to them, but its impact on the level of perceived risk was dependent on the circumstances or the organization providing the smart home technology. Those were represented in the diagram with the bars labeled "C".

For the first component of cybersecurity, trust, participants were given the following definition. "We define trust as the ability to trust service providers, and their personal, to do the right thing by you." 9 of the participants gave answers which indicate that they associate a high level of risk with the technology and service providers. Remaining were 8 participants that did not associate a higher level of risk with the amount of trust they have to service providers, as well as 8 other participants that where situationally dependent in their responses.

A participant with a view of a positive association between trust of service providers and cybersecurity had the following to answer.

"I think there is too much monetary benefit for Internet providers to share information about their clients, for it not to be a concern for everybody who browses the web. It makes sense as a component of cybersecurity, and one of the main things we should address. Internet and service providers should be heavily regulated" (participant number 14).

On the other hand a participant had indicated their view of trust for service providers didn't relate to them feeling any more or less secure

when using the services.

"Well if we were to not trust providers then they should all be out of business by now" (participant number 1).

From the remaining participants one who had indicated the value of trust as a cybersecurity factor and as an influencing component in their acceptance of the technology, but had no feelings of insecurity based on trust in the current circumstances.

"I would say [trust] is definitely a factor. Knowing that someone has your interest at heart, or thinking that they don't, goes a long way whether I would make a purchase or not. Right now I wouldn't say I'm distrusting but I'm definitely weary when it comes to Internet providers" (participant number 2).

The second of the cybersecurity components is safety and can be defined as follows. "If we define safety as relating to the transfer of data across the Internet, do you perceive unauthorised access to your data (fraudulent issues and inadvertent) to be likely." From the sample of participants, 13 perceived high risk levels from safety, 8 associate low to no increase in levels of risk, and 4 were situationally dependent.

An interview with one participant provided us with a dose of realism when they stated the inevitable vulnerability of most technology would be exploited if the incentive is valuable.

"There are some really smart people in the world looking for oppor-

tunities like this. With Smart Homes offering so much information, even if unauthorized access is not possible at first when the technology is released they would eventually figure it out. So I would err on the side of caution" (participant number 7).

One participant from the low risk impact portion of the sample indicated their opinion on the associated threat of data safety by stating that data on the Internet is never safe. See the quote below.

"I guess it is possible that access to the devices is possible, but it is the Internet and everything can be hacked. So I would sum it up as it is possible but no more likely that the risks you take when using public Wi-Fi" (participant number 10).

In the third portion of the sample where participants indicated situational dependencies one interviewee stated that the risk was present but its severity was dependent on the precaution of the users, their answer is given next.

"There is an inherent risk, but it depends. But it depends on how prepared you are, like you could use a secure connection when you are browsing the Internet" (participant number 15).

Finally in the third component of cybersecurity, privacy, we gave participants the following definition. "If we define privacy as the protection of personal information so it is not disclosed to or used by others, do you feel that your privacy is at risk." Responses were once again coded

into the three categories, 16 participants had a high level of increase in predictive risk, 7 indicate low to no increase in risk, and 2 were situationally dependent.

From the sample a volunteer related privacy with a significant impact on the level of risk through the highlighting the need to improve security features in devices to protect the users personal information. A portion of the interview is given below.

"I do feel that my privacy is at risk. I would prefer if there was a push to increase the privacy protection on Internet devices rather than retreating to hiding information, especially when it comes to Smart Home. That technology will know everything about me, not just the things I tell it" (participant number 3).

Another one of the participants indicated no impact on risk caused be privacy concerns as they felt their personal information would not be sold by the service providers, but rather a generic demographic representation of them. The example is given here.

"I feel like a lot of companies distribute or sell your demographic information, usually for advertising purposes. But I don't think they would give away your personal information." (participant number 18).

One of the remaining two participants who indicated a situational dependency referred to the different functionality of IoT devices which could enable access to personal information. Avoiding those particu-

lar devices would reduce the risk levels accordingly. The participants response is given next.

"Well the technology used in Smart Homes is very broad and not everything stores or transfers personal data, so it would depend on which technology and devices you are interested in installing I guess" (participant number 17).

4.4.8 RANKING THE COMPONENTS BY IMPACT LEVELS

The final part of the interview script aimed to identify which components played a more important role in the participants perspective and identify the relationships between the different factors and the technology acceptance. From the study sample, one participant indicated that none of the cybersecurity factors affected their purchasing decision. That participant had a novice proficiency in technical knowledge, had a positive predisposition towards installing smart home technology and did not associate any security risks from the technology. The remaining portion of the study sample ranked the three components in order of personal importance or indicated that all three are equally important.

Eleven participants would not rank any of the components above the others. One of the participants explained their reasoning with the following statement.

"They are all of the same level of importance, they are like the three pillars of cybersecurity. You can't really lose one without losing the others" (participant number 6).

To give a representation of the resulting responses a table of giving the cumulative rankings was constructed. Amalgamation of the rankings on each component where calculated through a logarithmic weighting system. When a component was ranked of highest importance (number one) it gains one hundred points, second place gets ten points, and third place gains one point (Altenbach, 1995). When two components are given equal ranking, they both receive the same amount of points given to that rank. The results of the 13 participants' answers are represented in the table below (See Table 8).

Table 8: Cybersecurity Component Ranking Amalgamation

Components	First place (X100)	Second Place (X10)	Third Place (X1)	Total
Trust	4	6	3	463
Safety	6	3	4	634
Privacy	3	5	5	355

Note: To calculate the total number of points we awarded: 3 points for each first place ranking, 2 points for second place and 1 point for thirst place.
e.g., Total point calculation for Trust; (100 points X 4) + (10 points X 6) + (1 point X 3) = 463 points

It is important to recognize here that the numbers given in the table above are a a visualization of the answers through interpretation of the results. Altenbach (1995) mentions that the conversion of these

qualitative answers into a numerical data is an aid to allow the analysis to take shape and does note represent a quantifiable measure of the importance each component has over the other.

For each of the components we have pulled out an example of a participant that ranked the component at the top rank, to give an idea of their reasoning and thoughts.

For the trust component a participant argues that a lack of trust in providers will inherently reduce the user's ability to believe in strong safety and privacy practices regardless of actual precautions. See details below

"Safety and privacy don't mean anything if you don't trust the people in charge of them to be doing their utmost best. Trust would be the most important, to me. The next would be privacy, so that information I don't want shared with others wouldn't be shared with others. Any information that I share with anyone involved in the security of said information, is information that I'm already willing to share, and so don't entirely mind having it be made known to someone I might not have intended for it to be shared with. The last would be safety, because in my opinion, it's the most vulnerable if the other two are taken care of, and so it's the one I could defend myself against with the most confidence. Don't offer any information that I don't want intercepted. If I can trust the service providers, and ensure that my privacy is protected, then the safety of any other information isn't my

highest priority. Besides, if I trust my service provider to do their best, then they'll work hard to make sure the security is protected, so there's that" (participant number 7).

The argument from another participant was that Safety played a more important role, where they could ensure their private and personal information could be kept secure by taking actions themselves to do so. However, the role of the company to do their job as well as protecting its clients creates the safer environment in which this participant would be willing to partake. A portion of the interview is given next.

"Safety is at the top, followed by trust, and then privacy. With my knowledge I can protect myself and the information that is important to me. I want to know the company has done their job and gone above and beyond to ensure the safety and security of my information on their end" (participant number 11).

A response from one of the interviewees to the priority of each of the cybersecurity components highlighted the importance of privacy above the other two components for one simple reason. That reason is that you can not change your identity. While cyber attacks on technology can cause monetary loses, identify theft and extortion are very serious risks that could be caused by the high level of invasion to privacy in this scenario. The response is shown below.

"Privacy and personal information is the most important thing in my eyes. I want to be able to know that my personal information is

safe, especially with the risk of identity theft and everything. If you put your trust into the providers and they break it, its gonna be very bad for you. So privacy is first, trust and safety are equally important but come in second" (participant number 15).

5 DISCUSSION

This chapter will talk about the findings of the study and what they might mean. We will examine how the findings can address the research question and the theories the explain them. The chapter is organized into six sections: (1) summary of results, (2) interpretation of results, (3) comparison to the literature, (4) implication of findings, (5) limitations, and (6) recommendations for future research.

5.1 SUMMARY OF RESULTS

In the summary section we will be revisiting the research question and propositions from the literature review, then going through the key patterns of findings from the results section highlighting the significance they hold.

As mentioned throughout this thesis, the research question focuses on examining the role cybersecurity plays in smart home technology adoption. This research question is formed from a literature gap which lacks the presence of a combination between research of cybersecurity challenges in the future of smart home technology and the technology acceptance and adoption theories.

From our research, we have identified three main propositions to explore. (1) Cybersecurity is a factor in the technology adoption model

which affects the acceptance of smart home technology. (2) Cybersecurity would be observed by the average consumer as components made out of the perceived areas of risk. (3) The components of cybersecurity are: trust, safety, and privacy.

From the results of our interviews, we observed in the identification of what smart home technologies mean to the participants, that there are significant variations and inconsistencies amongst definitions. The participants gave indication of the technology which would classify as part of the smart home technology umbrella but generally could not define what makes this technology suitable to be called smart home technology.

We could deduct from the interviews that some had formulated an opinion about smart and connected technologies from advertisements of one or two companies over media. That has caused the definition in consumers' minds to fall behind the literature where the definition still relates to a specific technology rather than the more accepted relation to the behavioral focus of the technology with the users' needs. Using a technology focus over a behavioral focus leads to a reduced ability in categorizing whether a particular device fits into the definition suggesting that the behavior of consumer would follow suit of the literature. This could be expected to show in observation of largely inconsistent arrays of definitions which get consolidated over time with standard practices emerging as use of the term and the technology become more

common and main stream.

Moving onto the intent to purchase questions, a key observation is made in the different levels of risk concerns by participants based on their technical proficiency. As we examine the answers of our volunteers, we notice the distinction of answers from highly proficient to novice technology users. Users with a higher rating of technical proficiency displayed concerns for security risks associated with the devices, often this group of participants identified one or more of the cybersecurity components directly while discussing their intent to purchase. Those concerns didn't always cause the user to lose interest in purchasing, but they were consciously aware of their existence. But on the other hand when consumers had a lower level of technical skill, their intent to purchase had no mention of security risk, but appeared to be related to other factors, such as costs or convenience.

The next key observation made builds on the evolution of the adoption model. The discussion of key factors and concerns with the participants revealed this information. Early in chapter 2 we introduced the UTAUT2 Model and stated the definitions of the determinants for user behavior. Later in that chapter, we used the literature to add cybersecurity as a determinant in our preliminary theoretical model with three components that make up cybersecurity. Those factors were safety, trust, and privacy. From the results of our interviews, we collected 14 different factors as identified by the users. Some of those

factor can be mapped directly to the UTAUT2 model and the preliminary theoretical model.

We demonstrate here how the user identified factor for adoption can be grouped under the determinants for the theoretical model. For each of the determinants Venkatesh et al. (2012) gave definitions and grouped smaller factors from other literature which fit the definition to increase the significance for each determinant. We will group our factors into the given definitions as well. The first given determinant, performance expectancy has a definition where three of the user defined factor fall under (numbers 1, 5, and 11) those are: performance and convenience benefits, time and energy saving, and accessibility. Effort expectancy can capture both the learning curve and the retrofit factors from our list (numbers 8 and 14). Social benefit is given by the identified lack of social norm (number 7), and price value by value of the technology (number 9). The last UTAUT2 determinant, facilitating conditions, is broadly defined and can be related to four of the user identified factors (numbers 3, 4, 10, and 13): installation and operation costs, living space restrictions, closed software, and reliance and reliability.

The additional determinant which we identify in this research, cybersecurity and its three components are captured by security risks, lack of trust, and lack of privacy (numbers 2, 6, and 12). Therefore we can construct the full preliminary theoretical model directly from the

answers provided by the interviewee sample. It is important to note that the grouping of the user identified factors into the determinants is based on the definitions of the determinants as given by research.

Smart home technology operates under many sectors and industries, the literature mentions home automation, entertainment, security, healthcare, remote access control, and energy efficiency to name a few. Out of those sectors, healthcare is the most dominant in research with a larger portion of journals dedicated to the subject and predictions of its future potential market value growing faster than all the other sectors. With that, it is important to make the observation of the data showing healthcare as the least pressing use of smart home technology in the consumers persxpective. When asked about the benefits and use of smart home technology, the users prioritized home automation the most and only gave one mention of healthcare placing it as the least important sector.

The cybersecurity section of our interview began with a series of questions to identify the user's perception of risk levels. There were three risk levels used, here they are given in order from highest risk perception to lowest: training in cybersecurity, potential information theft target, and basic precautionary protection software.

A trend is observed when the participant answers where represented in a graph based on their level of technical proficiency (see figures 8 and

9). The trend indicated a positive relationship between technical proficiency and risk perception. As we look at the data, we notice that with participants who had a lower level of technical knowledge the percentage of responses indicating perceived risk at each of the indicators we slow. Compared to the highly technical participants of whom a larger portion responded in a manner that indicates strong perception of risk.

Following familiarity to cybersecurity, the section moves into examining the components which define cybersecurity in the minds of the consumers. The literature supported three key components: trust, safety, and privacy. The data from our participants indicates the presence of a relationship between the component, and cybersecurity as a factor in adoption. All three of the components from the literature had answers indicating more participants make the connection to cybersecurity. We observe that privacy had the highest amount of agreement and largest impact on feeling secure, with 16 of the participants listing it as an important factor. Safety was second in order of importance followed by trust in third. It is important to note that this is the order of risk impact and not the order of personal value to each of the components.

The graph of cybersecurity component intensity (see figure 10) visualizes the ratio of participants who feel the component is high risk, no risk, or is dependent on the circumstances. Those three groupings were labeled “A”, “B”, and “C” respectively. An observation made clearer through the visualization of the data, as we move down the graph from

the trust component through safety and to privacy. While bar A grows, bar B keeps its size only being reduced by one participant when we get to privacy. The growth of bar A is causing a reduction in participants in bar C. Hence we interpret this observation by considering that following scenario; the strength of a cybersecurity component's risk sways over consumers from being undetermined to feeling that the component is high-risk value.

Ranking the components of cybersecurity in order by impact level is the last final part of the interview and in it observe the how the consumers chose their priority for cybersecurity focus. The table at the end of chapter four gives us an overall numerical total to identify the ranking of each component. (see Table 8). The order of importance as indicated by the ranking system is as follows: safety, trust, and privacy. The observation here is that this ranking does not line up with the data from the component risk intensity ranking, however it does match the ranking from the earlier key factors and concerns section.

5.2 INTERPRETATION OF FINDINGS

In this section, we will go through the key findings from the section above and discuss their meaning, provide what knowledge claims can be made from them, indicate how they relate to our propositions and research questions, and indicate any unexpected findings that have come

up.

We begin with the users' lack of a consistent definition of smart homes. To the extent of current research on the topic of smart homes, a standard definition is still being worked on, and the majority of consumers can only derive their definitions from its portrayal in the media . In two major ad campaigns, by Samsung and Nest Labs, we observe the companies instructing the consumers on how and why they should use smart home devices (Charara, 2015; Torres, 2016). The ads create an impression in the consumers' minds of what smart homes are based on the instructions of those campaigns. Those definitions could cause consumers to be confused as to which products are "smart" products and which are not.

Another area of difference between consumers and research is the priority of industry sectors under smart home technology. The literature suggests the largest sector to be healthcare with the Baby Boomers generation approaching and beginning their 70s and beginning to rely more on healthcare to keep to a normal level of daily functionality. These are some of the journals which indicate a focus on healthcare as main use of smart homes (Warren et al., 1999; Penaud et al., 2004; Demiris & Hensel, 2008; Chan et al., 2009; Ziefle et al., 2011; Alam et al., 2012; Ni, García Hernando, & de la Cruz, 2015). From our findings, the participants did not prioritise the use of smart home technology in the healthcare system, but focused more on home automation and en-

ergy efficiency.

Participants indicated which facilitating conditions they felt influenced their intent to purchase smart home technology. The observations made in that section supported the findings from the literature where factors were given to fit under each of the existing determinants from the UTAUT2 model. Additionally, the observations gave evidence that supports our first and third propositions. Amongst the factors identified by the participants in the section were trust, safety, and privacy. Those give supporting evidence to the existence of cybersecurity as a determinant of behavioral intent, as well as the main components of cybersecurity being the three factors mentioned.

The second proposition identified in our research is supported in the observations made through the cybersecurity component intensity section. The section examined the consumers' perception of risk for the three main components of cybersecurity. The literature identifies a relationship between risk perception and the consumer decision making process (Stampfl, 1978; Kim, Ferrin, & Rao, 2008). Respondents indicated that all three of the components exhibited some level of associated risk, which answers are question of whether cybersecurity is observed by consumers as components of perceived risk.

From the key observations, we note a few that do not relate to our propositions but provide some additional valuable insight into our re-

search question. These observations come from the intent to purchase and familiarity to cybersecurity sections, where a trend is observed that indicates a relationship between technical proficiency and level of perceived risk from cybersecurity. The relation indicates an increase in consumers' tendency to be more cautious and aware of the risks associated with the smart home systems when their level of skill and knowledge of technology was higher.

Reflecting on this observation we find theoretical support in research for a relationship between technical knowledge and cybersecurity. In examining the political dynamic core of cybersecurity and development of theoretical framework of the future development of cybersecurity Hansen & Nissenbaum (2009) gave reasoning for such a relationship. Their study reviled that at the rate of technological development and evolution of cyber-attack methods emphasized mastery of the field and expert knowledge to hold the privilege of being the speaking authority on such a topic. Reports for public safety strategies also emphasized the need for highly technical and capable individuals to be present in leading roles at every level of government operation to ensure the correct skills are available to defend against the threats of cyber-attacks (Evans & Reeder, 2010).

This observation changes the dynamic of the relationship proposed between cybersecurity and behavioral intent. With this additional observation, we could propose the relationship to be as follows; cyber-

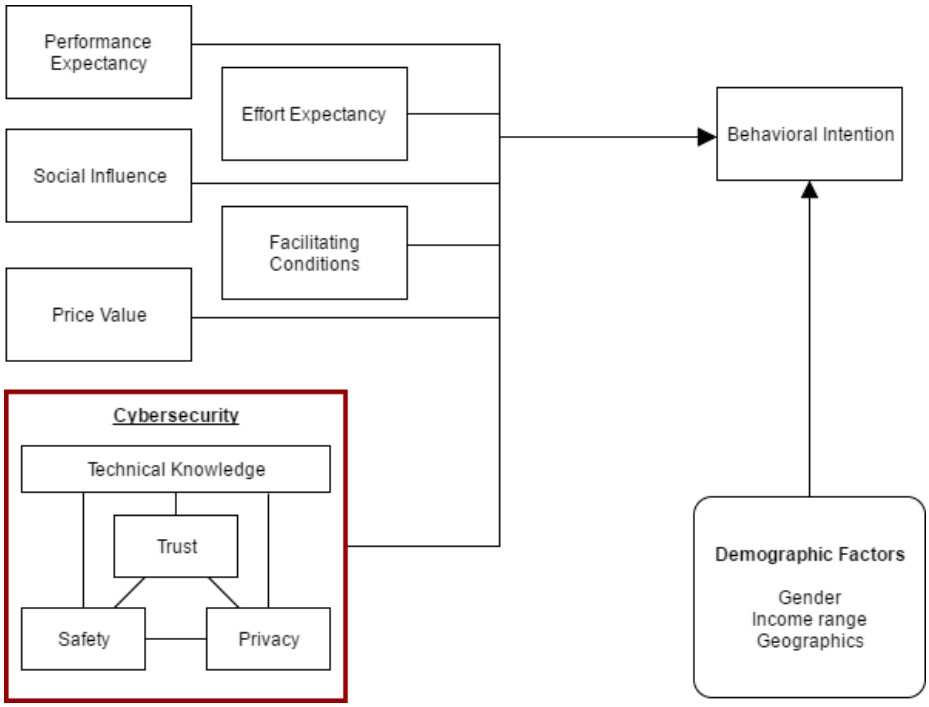
security is determined by three main components - trust, safety, and privacy - that are moderated by the consumers' technical knowledge.

Additionally, the observations reflect another knowledge claim that can be made of the three components of cybersecurity. From both the cybersecurity component intensity and the ranking of components section we can identify the strengths of each component. The two rankings measure different values, component intensity ranks the components based on the severity of risk, while the priority ranking orders them based on consumers' need for security assurance.

Finally, we arrive at our research question. What role does cybersecurity play in smart home technology adoption. Based on the observations made above, and the data in this research, we find that cybersecurity is a determinant of behavioral intent which has three main components - trust, safety, and privacy - that are moderated by the consumers' technical knowledge. We represent this new understanding in a revised model which includes the effects of technical knowledge (see figure 11).

The model represented in the figure above (see figure 11) visualizes the expected relationship between all the factors of adoption. As we have mentioned earlier, we do not set out to disprove the UTAUT2 model and although some of the labels and relationships are not shown that is for the purpose of simplification not elimination.

Figure 11: Revised Theoretical Model: Smart Home Technology Acceptance



Our contribution to the model is represented within the cybersecurity label and its relationship to the rest of the model. Cybersecurity is a determinant of behavioral intent an has a similar relationship to behavioral intent as those of determinants in earlier models (e.g., performance expectancy or social influence). We provide to following definition for the cybersecurity determinant; Cybersecurity is the organization and preparation of protective resources which provide the users with security in end-to-end operation of the technology which reflect on the consumers' perception of their trust, safety, and privacy. This definition is developed from the collection of examined literature along with the results of this study.

Within the cybersecurity label we find its three main components, trust, safety, and privacy as well as their moderator, technical knowledge. The three components of cybersecurity are all interlinked as we suggest their relationship to be codependent. From our observation the participants who stated that one of the components were of high importance to them also indicated a higher overall risk affecting their behavioral intent. That suggests a relationship where any of the components being present increases the overall perceived risk of cybersecurity. The technical knowledge connects to the three cybersecurity components as it relates their intensity and likelihood of their presence.

5.3 IMPLICATIONS TO THEORY

Our findings reflect consumers' perception of smart home technology providing valuable insight into the minds of users. This insight allows for the expansion of our understanding of consumer behavior, furthering the development of theoretical frameworks and models for the study of technology adoption patterns.

The developed models such as UTAUT2 can utilize our findings through the development quantitative and empirical studies that test the propositions brought forth through our exploratory research by adding statistically significant determinants of behavioral intent and increasing the accuracy of the adoption models. The value of such

exploratory research to the current technology adoption models are present and can be observed in the likes of research by Zeithaml (1988) and Meyers-Levy & Maheswaran (1991) which were later cited by Venkatesh et al. (2012) for the development of the UTAUT2.

Along with the determinants we suggest to use in expanding the adoption models we observed findings that have implications on the models as a whole. The perceptions and definitions of smart home technology products given by the consumers was influenced by advertising campaigns in the media. Consumers' understanding of what the products are affect all the determinants included in the adoption models. If a consumer perception of smart homes is inaccurate and limited, then their performance expectancy and price value would be inaccurate. The effects of consumer knowledge are not currently accounted for by the UTAUT2 model.

Adaptation of these findings into future research on technology adoption would provide additional value and improve the contribution to theoretical models. Consumer perception of emerging technology can have critical implications onto the future development of the field.

5.4 IMPLICATIONS TO PRACTITONERS

One of the key observations of our study indicates that cybersecurity does have an impact when it comes to smart home technology acceptance. These findings could prove to be valuable for organizations and practitioners in the smart home industries as well as others marketing IoT devices towards individual consumers in settings that are similar to those of smart home markets.

Entrepreneurs and managers using the model to anticipate the adoption of smart home technology would allow them to gear their products towards the right market and audience when designing and marketing its key features. Hence, a company might choose to market to a low technical demographic and emphasize the low effort expectancy of their technology without worrying about its cybersecurity. Alternatively, if they decide to target a more technologically skilled demographic they could indicate their cybersecurity by emphasizing one or more of the three main components of cybersecurity.

The three components of cybersecurity could be utilized as differentiators between competitors or as value propositions which could result in a competitive advantage. Each component would provide potential for research and development allowing companies to develop products centered around cybersecurity.

For academics and the educational system, the implications of our findings give reason to improve the mandate of studying cybersecurity as we expect to have a higher demand for cybersecurity experts with the growth of the IoT industry.

Developers of connected devices would be able to use information from our theoretical model to identify the critical areas of focus in their software. It is important for developers to understand their users and how they intend to interact with the technology to be able to reduce the barrier of human computer interaction. Improving the consumer experience through enhancing features valued by the user increases technologies changes of success and reduces the costs of support.

The development of adoption models that utilize user perspective to define determinants across the model helps move companies towards a user-centric design. When organizations utilize user-centric development strategies, both the organization and the consumers benefit (Hoyer et al., 2010). The implications of focusing on improving the cybersecurity of smart home technologies would benefit the companies bottom line, but also increase the security of the technology users.

5.5 LIMITATIONS

Through our research, we have aimed to maintain an unbiased collection and interpretation of our data. However, limitations in research are unavoidable. This section will list the limitations of our research to the best of our capabilities.

At the beginning of our research we introduce some definitions that are used to identify key terms used throughout the article. We took to the literature in our process of identifying the most appropriate definitions for cybersecurity, smart homes, and other critical terms. The selection of those definitions restricts and limits the scope of research. If different definitions were used, this research might have arrived at different results.

The research examines cybersecurity of smart home devices with potential consumer, most of whom have never owned this type of connected technology before. The implication of security risks in a cyber-physical system are higher than those from devices that do not control physical objects. A possible limitation comes from the participants inability to perceive the severity of these risk implications without prior experience.

During the literature review process challenges were identified for the future of smart home technology other than cybersecurity. How-

ever those challenges, such as human interaction and social barriers, were not included in the interview structure. This could have limited the exploration of available data on acceptance and adoption of the technology.

Qualitative research in its nature faces a large challenge in its conduct to maintain objectivity and reliability. Although the qualitative research method was selected to avoid limiting participant responses, the mixed method approach would have allowed for benefits from both qualitative and quantitative methods (Creswell, 2013).

The sample of participants was drawn from the location of our research (the city of Ottawa), and the majority of our participants are residents of this city. For the sample to be representative of the country as a whole, the data must be drawn from a larger pool and with a larger sample size. Our sample also contained a fairly large concentration of younger participants, there are a number of factors that could have caused this. This is likely due to the nature of the topic of study relating to technology. This may have resulted in a portion of potential participants, generally older population, avoiding taking part in the questionnaire if they have lower technical knowledge. Additionally the qualifying criteria for participants required respondents to be looking to purchase a home or have done so within the past year. With those factors, access to older age groups was difficult. The lack of participants over the age of 39 implies that our results are not generalizable

to older generations.

5.6 FUTURE RESEARCH

We suggest that future work could be done to further this area of research through addressing the limitations in our research. As the literature moves towards an accepted standard for definitions, the scope of research should adapt with it to develop an inclusive adoption model.

The lack of adopted standard definitions by the general public for many of the terms used throughout this study has a large impact on the outcome of the study. We believe the results are dependent on our choices of definitions, a different outcome might be reached with other definitions. As a more standardized definition emerges new research using the standard definitions would provide valuable information for this field.

We identified factors that could influence consumer behavioral intent from the literature review that do not relate to cybersecurity (i.e., human-computer interaction and social barriers to adoption). Those factors did not meet the scope of our research. Future research could examen those factors for their relation to consumer behavioral intent to purchase and expand on the adoption model.

Our qualitative exploration of the data provided valuable informa-

tion on the relationships proposed by consumers; however, validation of those relationships with numerical data was not presented by our research. As the market for this technology becomes more well understood, and with larger study samples, other research methods can be used to improve on the findings. We suggest the in future research conduct of the mixed method approach could by used to provide more statistical support of the relationships identified in our research.

The demographies of our study sample are limiting and do not include older age groups. Studies can be conducted in different geographic locations and would be valuable in introducing new findings that would affect the theoretical model. Studies that investigate the perception of the elderly on the subject would significantly improve the model's capability to explain the behavior of consumers of that age group.

We explore the role cybersecurity plays in the acceptance and adoption of technology, yet we have not provided any solutions to mitigate the risks associated with it. More research in needed in the field of cybersecurity to help in the protection of our future.

6 CONCLUSION

Lack of predictability in the behavior of new smart home technology products in the markets lead to the need for research identifying and improving the factors determining consumer acceptance and adoption. The literature examines the extent of research available on adoption model, the boundaries and definitions of smart homes, and the future cybersecurity challenges.

This research conducts exploratory examination of the consumer behavior and uses semi-structured interviews to collect its data. The research methodology guides the development and conduct of the research to minimize bias and assure adherence to the ethical guidelines.

The results were transcribed from a final count of 25 participants from 34 initially interested in participating. Following a five stage modified grounded theory approach, the results were organized to give a clear representation of the collective responses. Observations were highlighted for further interpretation. Development of connections between observations revealed the key patterns which were used to identify the relationships and determinants in the adoption models.

Our findings introduce the determinant of cybersecurity to the UTAUT2 model with three components and a moderating factor. Trust, safety, and privacy are the components of cybersecurity moderated by the

consumers' technical knowledge. We discuss the implication of those findings as well as their limitations. From there we identify suggestions for future research that could improve the adoption models of smart home technology.

Cybersecurity is often overlooked, but observations suggest it is rapidly becoming a critical factor in our technology. Developers and manufacturers of smart home technology should work together towards making cybersecurity a clear priority which we value in our homes and our technology.

7 APPENDICES

7.1 APPENDIX A - INTERVIEW SCRIPT

Knowledge questions

Q1: Have you heard about smart homes before or have you been made aware of the Internet of things technology?

Q2: How would you describe your level of technical knowledge?

Q3: Could you provide some examples of the way you regularly interact with technology?

Q4: What are some of the challenges you encounter when working with technology?

Q5: In your own words, how do you define smart homes?

Aim: understand the depth of knowledge participants have towards smart homes.

Q6: This study adopts a definition of smart homes by Frances K. Aldrich (2003), After I read this definition to you, could you indicate how this definition reflects on your understanding on what you believe are smart homes?

Quote: "A 'smart home' can be defined as a residence equipped with computing and information technology which anticipates and responds to the needs of the occupants, working to promote their comfort, convenience, security, and entertainment through the management of technology within the home and connections to the world beyond" (Aldrich, 2003).

Q7: What stood out for you from the definition we gave of smart homes?

Aim: provides a common understanding of the key meaning of smart homes and what it means to the participants.

Q8: Have you used smart technology before? How was your experience with the technology?

Q9: Do you currently own a house, or are in the process of purchasing a house? (if you don't own a house, what are the key features that would appeal to you in your future home?)

Q10: Do you currently have smart home technology at your living area? How do you use the smart home technology you have?

Q11: Would you currently be inclined to install smart home technology in your residence? Could you tell me why you would buy?

Aim: provides indicators of the participants predisposition and willingness to own smart home technology.

Q12: What factors influence your decision about smart homes?

Q13: If a house was equipped with Smart Home technology, how would the value of that house change in your opinion?

Aim: Identifying the key factors the participant uses to make the purchasing decision and adoption of smart homes.

Q14: How would you expect living in a smart home could affect you day to day life?

Q15: In terms of personal changes to your day-to-day activities, what benefits can using smart homes provide for you?

Aim: find the technology services that participants value when con-

sidering an investment in smart homes.

Cybersecurity Questions

Q16: What level of training are you subject to in maintain the security of your software and hardware?

Q17: What level of security precaution (run and updating anti-virus software, firewall, suspicious of emails from unknown sources, using secure password, updating passwords) do you take no regular basis?

Q18: With the large number of reported cyber attacks reported lately in the media, do you feel your information is targeted?

Aim: identify the level of cybersecurity the participants are familiar with when using regular daily technology

Q19: What does cybersecurity mean to you?

Q20: We have identified three components of cybersecurity (trust, safety, and privacy). We read to you a brief description for each component then ask you to provide your opinion, and whether you feel that component is related to cybersecurity and affecting your intent to purchase.

Trust - We define trust as the ability to trust the service providers and their personal to "do the right thing by you".

Safety - We define safety as relating to the transfer of data across the internet, do you think unauthorised access to your data (fraudulent issues and inadvertent) is likely?

Privacy - We define privacy as the protection of personal information so it is not disclosed to or used by others, do you feel that your privacy

is at risk?

Aim: Determine the relevance of the cybersecurity components to the participant's view of cybersecurity.

Q21: how would you rank the three components we identified earlier (trust, safety, and privacy) in terms of importance?

Aim: Find the level of importance each component plays.

Q22: Do you have any further questions?

8 REFERENCES

Abdulwahab, L., & Dahalin, Z. M. (2010). A conceptual model of Unified Theory of Acceptance and Use of Technology (UTAUT) modification with management effectiveness and program effectiveness in context of telecentre. African Scientist, 11(4), 267-275.

Adams, P. (2016) Cyber security in the IoT smart home and city. Retreived on Aug 30th 2016 from URL: http://insight.nokia.com/users/paul-adams

Alam, M. R., Reaz, M. B. I., & Ali, M. A. M. (2012). A review of smart homes—past, present, and future. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 42(6), 1190-1203

Aldrich, F. K. (2003). Smart homes: past, present and future. In Inside the smart home (pp. 17-39). Springer London

Allen, B. (1996). An integrated approach to smart house technology for people with disabilities. Medical engineering & physics, 18(3), 203-206.

Altenbach, T. J. (1995). A comparison of risk assessment techniques from qualitative to quantitative (No. UCRL-JC–118794; CONF-950740–36). Lawrence Livermore National Lab., CA (United States).

Anderson, J. E., & Schwager, P. H. (2004, February). SME adoption of wireless LAN technology: applying the UTAUT model. In Pro-

ceedings of the 7th annual conference of the southern association for information systems (Vol. 7, pp. 39-43).

Arenas-Gaitán, J., Peral-Peral, B., & Ramon-Jeronimo, M. A. (2015). Elderly and internet banking: an application of UTAUT2. The Journal of Internet Banking and Commerce, 20(1), 1-23.

Babar, S., Mahalle, P., Stango, A., Prasad, N., & Prasad, R. (2010, July). Proposed security model and threat taxonomy for the Internet of Things (IoT). In International Conference on Network Security and Applications (pp. 420-429). Springer Berlin Heidelberg.

Balta-Ozkan, N., Davidson, R., Bicket, M., & Whitmarsh, L. (2013). Social barriers to the adoption of smart homes. Energy Policy, 63, 363-374.

Banerjee, A., Venkatasubramanian, K. K., Mukherjee, T., & Gupta, S. K. S. (2012). Ensuring safety, security, and sustainability of mission-critical cyber–physical systems. Proceedings of the IEEE, 100(1), 283-299.

Barlow, J., & Venables, T. (2003). Smart home, dumb suppliers? The future of smart homes markets. In Inside the Smart Home (pp. 247-262). Springer London.

Bellazzi, R., Montani, S., Riva, A., & Stefanelli, M. (2001). Web-based telemedicine systems for home-care: technical issues and experiences. Computer Methods and Programs in Biomedicine, 64(3), 175-187.

Bellman, S., Lohse, G. L., & Johnson, E. J. (1999). Predictors of online buying behavior. Communications of the ACM, 42(12), 32-38.

Bruce, M. (1987). Science fiction utopias and social realism. Futures, 19(6), 713-715.

Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, & Social Sciences and Humanities Research Council of Canada (2014, December) Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans.

Camarinha-Matos, L. M., & Afsarmanesh, H. (2014, October). Collaborative systems for smart environments: trends and challenges. In Working Conference on Virtual Enterprises (pp. 3-15). Springer Berlin Heidelberg.

Chan, M., Campo, E., Estève, D., & Fourniols, J. Y. (2009). Smart homes—current features and future perspectives. Maturitas, 64(2), 90-97.

Chan, M., Estève, D., Escriba, C., & Campo, E. (2008). A review of smart homes—Present state and future challenges. Computer methods and programs in biomedicine, 91(1), 55-81.

Charara, S. (2015, September). What smart home adverts tell us about the potential power of connected home tech: You know you want it, you're just not sure what you'll do with it. Retreived on July 20th 2017 from URL: https://www.wareable.com/smart-home/adverts-whats-it-for-556

Chitnis, S., Deshpande, N. & Shaligram, A. (2016). An Investigative Study for Smart Home Security: Issues, Challenges and Countermeasures. Wireless Sensor Network, 8: 61-68.

Cisco. (n.d.). Securely Integrating the Cyber and Physical Worlds. Online at http://www.cisco.com/web/solutions/trends/tech-radar/securing-the-iot.html

Columbus, L., (2016). Roundup Of Internet Of Things Forecasts And Market Estimates, 2016. Forbs. Retrived on January 23rd 2017 from http://www.forbes.com/sites/louiscolumbus/2016/11 /27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#59cf40f24ba5

Covington, M. J., Moyer, M. J., & Ahamad, M. (2000). Generalized role-based access control for securing future applications. Georgia Institute of Technology.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(10).

Creswell, J. W. (2013). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.

Davidoff, S., Lee, M. K., Yiu, C., Zimmerman, J., & Dey, A. K. (2006, September). Principles of smart home control. In International Conference on Ubiquitous Computing (pp. 19-34). Springer Berlin Heidelberg.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and

user acceptance of information technology. MIS quarterly, 319-340.

Davis Jr, F. D. (1986). A technology acceptance model for empirically testing new end-user information systems: Theory and results (Doctoral dissertation, Massachusetts Institute of Technology).

Demiris, G., & Hensel, B. K. (2008). Technologies for an aging society: a systematic review of "smart home" applications. Yearb Med Inform, 3, 33-40.

Demiris, G., Rantz, M. J., Aud, M. A., Marek, K. D., Tyrer, H. W., Skubic, M., & Hussam, A. A. (2004). Older adults' attitudes towards and perceptions of 'smart home'technologies: a pilot study. Medical informatics and the Internet in medicine, 29(2), 87-94.

Dutt, N., Jantsch, A., & Sarma, S. (2016). Toward smart embedded systems: A self-aware system-on-chip (soc) perspective. ACM Transactions on Embedded Computing Systems (TECS), 15(2), 22.

Edwards, W. K., & Grinter, R. E. (2001, September). At home with ubiquitous computing: Seven challenges. In Ubicomp 2001: Ubiquitous Computing (pp. 256-272). Springer Berlin Heidelberg

Evans, K., & Reeder, F. (2010). A human capital crisis in cybersecurity: Technical proficiency matters. CSIS.

Forester, T. (1989). The myth of the electronic cottage. ACM SIGCAS Computers and Society, 19(2), 4-19.

Friedewald, M., Da Costa, O., Punie, Y., Alahuhta, P., & Heinonen,

S. (2005). Perspectives of ambient intelligence in the home environment. Telematics and informatics, 22(3), 221-238.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: an integrated model. MIS quarterly, 27(1), 51-90.

Glaser, B. G., & Strauss, A. L. (1967). The Discovery of Grounded Theory: Strategies for Qualitative Research Adline De Gruyter. New York

Glaser, B. G. (2014). Applying Grounded Theory: A Neglected Option. Sociology Press.

Hamernik, P., Tanuska, P. & Mudroncik, D. (2012). Classification of Functions in Smart Home. International Journal of Information and Education Technology, 2(2): 149-155.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. International studies quarterly, 53(4), 1155-1175.

Harper, R. (2003). Inside the smart home: Ideas, possibilities and methods. In Inside the smart home (pp. 1-13). Springer London.

Hong, J. Y., Suh, E. H., & Kim, S. J. (2009). Context-aware systems: A literature review and classification. Expert Systems with Applications, 36(4), 8509-8522.

Hoyer, W. D., Chandy, R., Dorotic, M., Krafft, M., & Singh, S. S. (2010). Consumer cocreation in new product development. Journal of

service research, 13(3), 283-296.

Intille, S. S. (2002). Designing a home of the future. IEEE pervasive computing, 1(2), 76-82.

Jarratt, J., & Coates, J. F. (1990). Future use of cellular technology: Some social implications. Telecommunications Policy, 14(1), 78-84.

Jose, A.C. & Malekian, R. (2015). Smart Home Automation Security: A Literature Review. Smart Computing Review, 5(4): 269-285.

Kadam, R., Mahamuni, P. & Parikh, Y. (2015). Smart Home System. International Journal of Innovative Research in Advanced Engineering, 2(1): 81-86.

Kijsanayotin, B., Pannarunothai, S., & Speedie, S. M. (2009). Factors influencing health information technology adoption in Thailand's community health centers: Applying the UTAUT model. International journal of medical informatics, 78(6), 404-416.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decision support systems, 44(2), 544-564.

Komninos, N., Philippou, E., & Pitsillides, A. (2014). Survey in smart grid and smart home security: Issues, challenges and countermeasures. IEEE Communications Surveys & Tutorials, 16(4), 1933-1954.

Kranz, J., & Picot, A. (2012). Is it money or the environment? An empirical analysis of factors influencing consumers' intention to adopt the smart metering technology.

Lee, E. A. (2008, May). Cyber physical systems: Design challenges. In Object oriented real-time distributed computing (isorc), 2008 11th ieee international symposium on (pp. 363-369). IEEE.

Lee, M. C. (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. Electronic commerce research and applications, 8(3), 130-141.

Li, Y., Hou, M., Liu, H., & Liu, Y. (2012). Towards a theoretical framework of strategic decision, supporting capability and information sharing under the context of Internet of Things. Information Technology and Management, 13(4), 205-216.

Lichtenstein, S., & Williamson, K. (2006). Understanding consumer adoption of internet banking: an interpretive study in the Australian banking context. Journal of Electronic Commerce Research, 7(2), 50.

Lobaccaro, G., Carlucci, S., & Löfström, E. (2016). A review of systems and technologies for smart homes and smart grids. Energies, 9(5), 348.

Mallat, N. (2007). Exploring consumer adoption of mobile payments–A qualitative study. The Journal of Strategic Information Systems, 16(4), 413-432.

Martin, J., & Norman, A. R. (1973). The Computerized Society. ISBN 10: 0140215581 ISBN 13: 9780140215588

Mayer, P., Volland, D., Thiesse, F., & Fleisch, E. (2011). User Acceptance of 'Smart Products': An Empirical Investigation. Wirtschaftsinformatik, 9.

McCracken, G. (1988). The long interview. Newbury Park, CA: Sage Publication.

Mennicken, S., Vermeulen, J., & Huang, E. M. (2014, September). From today's augmented houses to tomorrow's smart homes: new directions for home automation research. In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (pp. 105-115). ACM.

Meyers-Levy, J., & Maheswaran, D. (1991). Exploring differences in males' and females' processing strategies. Journal of Consumer Research, 18(1), 63-70.

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

National Institutes of Health. (2014). The NIH proficiency scale. National Institutes of Health website. https://hr.od.nih.gov/workingatnih/compete Accessed March, 2017.

Ni, Q., García Hernando, A. B., & de la Cruz, I. P. (2015). The el-

derly's independent living in smart homes: A characterization of activities and sensing infrastructure survey to facilitate services development. Sensors, 15(5), 11312-11362.

Nissenbaum, H. (2004). Will Security Enhance Trust Online or Support It?. in P.Kramer and K.Cook (eds) Trust and Distrust Within Organizations: Emerging Perspectives, Enduring Questions, Russell Sage Publications, 155-188.

Oechslein, O., Fleischmann, M., & Hess, T. (2014, January). An application of UTAUT2 on social recommender systems: Incorporating social information for performance expectancy. In System Sciences (HICSS), 2014 47th Hawaii International Conference on (pp. 3297-3306). IEEE.

O'Malley, L., & Munoz, C., (2014, October). The Connected Home: Smart automation enables home energy management. MaRS Discovery District. Retrived from https://www.marsdd.com/news-and-insights/connected-home-smart-automation/

Penaud, C., Mokhtari, M., & Abdulrazak, B. (2004). Technology Usage for dependant people: Towards the right balance between user needs and technology. Computers Helping People with Special Needs, 624-624.

Poon, E. G., Jha, A. K., Christino, M., Honour, M. M., Fernandopulle, R., Middleton, B., ... & Kaushal, R. (2006). Assessing the level of healthcare information technology adoption in the United States: a

snapshot. BMC Medical Informatics and Decision Making, 6(1), 1.

Raman, A., & Don, Y. (2013). Preservice teachers' acceptance of learning management software: An application of the UTAUT2 model. International Education Studies, 6(7).

Renaud, K., & Van Biljon, J. (2008, October). Predicting technology acceptance and adoption by the elderly: a qualitative study. In Proceedings of the 2008 annual research conference of the South African Institute of Computer Scientists and Information Technologists on IT research in developing countries: riding the wave of technology (pp. 210-219). ACM.

Robles, R. J., & Kim, T. H. (2010). Applications, Systems and Methods in Smart Home Technology: A. Int. Journal of Advanced Science And Technology, 15.

Robles, R. J., Kim, T. H., Cook, D., & Das, S. (2010). A review on security in smart home development. International Journal of Advanced Science and Technology, 15.

Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. The Internet Society (ISOC).

Savitz, E. (2012). Gartner: 10 Critical Tech Trends For The Next Five Years. Online at http://www.forbes.com/sites/ericsavitz/2012/10/22/gartner-10-critical-tech-trends-for-the-next-five-years/

Schlesinger, J., & Day, A. (2016, December). Suddenly hot smart

home devices are ripe for hacking, experts warn. CNBC website. http://www.cnbc.c
hot-smart-home-devices-are-ripe-for-hacking-experts-warn.html Accesses
on March, 2017.

Schrammel, J., Hochleitner, C., & Tscheligi, M. (2011, November). Privacy, trust and interaction in the internet of things. In International Joint Conference on Ambient Intelligence (pp. 378-379). Springer Berlin Heidelberg.

Segura, A. S., & Thiesse, F. (2015, May). Extending UTAUT2 to Explore Pervasive Information Systems. In ECIS.

Sha, L., Gopalakrishnan, S., Liu, X., & Wang, Q. (2008, June). Cyber-physical systems: A new frontier. In Sensor Networks, Ubiquitous and Trustworthy Computing, 2008. SUTC'08. IEEE International Conference on (pp. 1-9). IEEE.

Singh, S., & Singh, N. (2015, October). Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce. In Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on (pp. 1577-1581). IEEE.

Skrzypczak, C. (1987). The intelligent home of 2010. IEEE Communications Magazine, 25(12), 81-84.

Solaimani, S., Keijzer-Broers, W., & Bouwman, H. (2015). What we do–and don't–know about the Smart Home: an analysis of the Smart Home literature. Indoor and Built Environment, 24(3), 370-383.

Stampfl, R. W. (1978). Perceived Risk and Consumer Decision Making. International Journal of Consumer Studies, 2(3), 231-245.

Stanislav, M., & Beardsley, T. (2015). HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities. Rapid 7.

Sung, J. Y., Guo, L., Grinter, R. E., & Christensen, H. I. (2007, September). "My Roomba is Rambo": intimate home appliances. In International Conference on Ubiquitous Computing (pp. 145-162). Springer Berlin Heidelberg.

Tan, M., & Teo, T. S. (2000). Factors influencing the adoption of Internet banking. Journal of the AIS, 1(1es), 5.

Torres, I., 2016 January, Samsung SmartThings ads show benefits of having a smart home. Retreived on July 20th 2017 from URL: https://androidcommunity.com/samsung-smartthings-ads-show-benefits-of-having-a-smart-home-20160128/

Venkatesh, V., & Brown, S. A. (2001). A longitudinal investigation of personal computers in homes: adoption determinants and emerging challenges. MIS quarterly, 71-102.

Venkatesh, V., Morris, M. G., Davis, G. B.,& Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS quarterly, 425-478.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of

acceptance and use of technology. MIS quarterly, 36(1), 157-178.

Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., ... & Doody, P. (2011). Internet of things strategic research roadmap. Internet of Things-Global Technological and Societal Trends, 1, 9-52.

Warren, S., Craft, R. L., & Bosma, B. (1999, April). Designing smart health care technology into the home of the future. In Workshops on Future Medical Devices: Home Care Technologies for the 21st Century (Vol. 2, p. 667).

Weber, R. H. (2010). Internet of Things – New security and privacy challenges. Computer law & security review, 26(1), 23-30.

Xiong, X., & Mei, Q. (2016). Study on the Factors Influencing User's Acceptance Intention for Smart Medical and Health Care Equipment Based on UTAUT2. DEStech Transactions on Economics, Business and Management, (apme).

Yang, J. S., Lee, H. J., Park, M. W., & Eom, J. H. (2015). Security threats on national defense ICT based on IoT. Advanced Science and Technology Letters (UCMA), 97, 94-98.

Zeithaml, V. A. (1988). Consumer perceptions of price, quality, and value: a means-end model and synthesis of evidence. The Journal of marketing, 2-22.

Ziefle, M., Rocker, C., & Holzinger, A. (2011, July). Medical tech-

nology in smart homes: exploring the user's perspective on privacy, intimacy and trust. In Computer Software and Applications Conference Workshops (COMPSACW), 2011 IEEE 35th Annual (pp. 410-415). IEEE.