Antecedents and Consequences of Consumer Internet of Things Security Self-Efficacy

Dissertation

Raeesa Behardien

BHRRAE003

Presented to the University of Cape Town Department of Information Systems in fulfilment of the requirements for the Part-Time Information Systems Master's Degree (INF5005W)

Research Supervisor: Professor Irwin Brown

2022

Plagiarism Declaration

Compulsory Declaration

1. This dissertation has been submitted to Turnitin (or equivalent similarity and originality checking software) and I confirm that my supervisor has seen my report and any concerns revealed by such have been resolved with my supervisor.
2. I certify that I have received Ethics approval from the Commerce Ethics Committee.
3. This work has not been previously submitted in whole, or in part, for the award of any degree in this or any other university. It is my own work. Each significant contribution to, and quotation in, this dissertation from the work, or works of other people has been attributed, and has been cited and referenced.

Student Number	BHRRAE003
Student Full Name	Raeesa Behardien
Student Signature	Signed by candidate
Date	31 January 2023

Acknowledgements

I would like to express my thanks and appreciation to my supervisor Dr Irwin Brown for his advice, encouragement, and support over the course of this research. Sincere appreciation goes to my family and friends for their emotional support and overall help and understanding during this time, and for agreeing to be a part of my pilot study. Special thanks go to my parents, Shanaaz and Raeed, for affording me all the opportunities I have been blessed to experience, as well as to my husband, M. Yaaseen, who continues to be a provider of encouragement and part of my support structure.

I would also like to acknowledge the special effort of my friends and family who selflessly took the time to review my work, Salmah and Atheelah, you are greatly appreciated. Lastly, I would like to thank Qualtrics and the participants of this study for the contribution to this research, as it would not have been possible without their involvement and expertise.

Abstract

The Internet of Things (IoT) is defined as the next great era of communication and comes with the promise of massive transformations to society and the way the internet works. The growth and demand of IoT devices has led to the increased production of unsecure connected devices that have managed to enter the physical world with many distinct applications. Consumer IoT devices are increasingly available and adopted in all its various forms. Consumer IoT devices can connect to any environment using an internet connection, so it becomes important to secure them against vulnerabilities and security threats. Users of Consumer IoT may be aware of and understand the information security threats they face; however, their self-efficacy affects their ability to protect themselves. The consumers self-efficacy represents the ability to carry out responsive behaviours and the belief that the applied responsive behaviour will have the desired impact. It has been determined to affect their ability to secure Consumer IoT devices and their ability to appropriately respond to the various threats. This research study contributes to the information security area of knowledge by means of a quantitative study with 230 South African respondents. Here, the focus is on the antecedents and consequences of consumer IoT security self-efficacy while evaluating the constructs: IoT Security Behavioural Practices, Behavioural Intention, IoT Security Technology Practices, IoT Security Self-Efficacy, IoT Device Knowledge, IoT Device Experience, IoT Security Breach Incidents, and Consumer IoT General Controllability.

The findings from this study show that the consumer IoT device knowledge and consumer IoT general controllability of the user are the antecedents of consumer IoT security self-efficacy. The consequences of consumer IoT security self-efficacy are IoT security technology practices, behavioural intention and IoT security behavioural practices. Similarly, the findings show that there is a positive relationship between the consumers behavioural intention and the IoT security behavioural practices that they carry out.

Keywords: Consumer Devices, Device Experience, Device Knowledge, Information Security, Internet of Things, IoT, IoT Devices, Consumer IoT, IoT Security, IoT Security Self-efficacy, Security, Security Practices, Self-efficacy

Glossary of terms

Term/Acronym	Definition
BI	Behavioural Intention
CK	Consumer IoT Device Knowledge
DE	Consumer IoT Device Experience
GC	Consumer IoT General Controllability
IoT	Internet of Things
ISSE	Consumer IoT Security Self-Efficacy
PLS	Partial Least Squares
SBI	IoT Security Breach Incidents
SEM	Structural Equation Modelling
SP-B	IoT Security Behavioural Practices
SP-T	Consumer IoT Security Technology Practices
SEM	Structural Equation Modelling

Table i: Glossary of terms

Table of Contents

Tables

Figures

1. Introduction

1.1. Contextual Background

Internet of Things (IoT) devices are becoming increasingly available and adopted in various forms at a rapid pace (Alladi et al., 2020; Hatlevik et al., 2017; Philip et al., 2023). The term IoT refers to the network of interconnected physical devices as well as systems embedded with connectivity, electronic capability, software, and sensors (Abiodun et al., 2021; Alladi et al., 2020; Atlam & Wills, 2020; Du et al., 2018; Gartner Inc, n.d.). These capabilities allow the devices or objects to collect, share and store data (Alissa et al., 2018; Blythe et al., 2020; Lee et al., 2019; LV & Singh, 2021; Subahi & Theodorakopoulos, 2019). IoT has the ability to offer promising solutions to a variety of existing problems and systems (Zhang & Chen, 2020). It has the ability and the potential to revolutionise the way in which tasks are carried out in various industries as well as in day-to-day life by allowing for automation of tasks, increased efficiency, and the collection and analysis of the data gathered through these processes (Bott & Menard, 2020; Hassija et al., 2019; Isaacs et al., 2019).

IoT has a significant impact on the way users carry out various activities in their daily lives and is relevant in various areas such as smart cities (Al-Turjman et al., 2022; Kirimtat et al., 2020), manufacturing (Malik et al., 2021; Wang et al., 2020), healthcare (Mamdiwar et al., 2021; Uddin et al., 2019), and for general or personal use (Al-Turjman et al., 2022; Perez et al., 2018). The implementation of IoT in these areas can address societal and living issues by improving quality of life as well as sustainability in some cases. Examples of these include traffic management, public transport, lighting, agriculture, manufacturing research and development, and health and fitness tracking (Al-Turjman et al., 2022; Demestichas et al., 2020; Dian et al., 2020; Farooq et al., 2019; Farooq et al., 2020; Kirimtat et al., 2020; Khan et al., 2020; Malik et al., 2021; Mamdiwar et al., 2021; Perez et al., 2018; Poongodi et al., 2019; Stoyanova et al., 2020; Wang et al., 2020; Wu et al., 2020). However, due to the nature of IoT devices, it is important to secure them against ever present and evolving vulnerabilities and security threats (Alladi et al., 2020; Atlam & Wills, 2020; Bastos et al., 2018).

There are several security concerns in relation to consumer IoT devices and their usage, with some of them being related to connectivity protocols, inefficient software updates, and weak passwords (Abiodun et al., 2021; Alissa et al., 2018; Al-Turjman et al., 2022; Bastos et al., 2018; Hassija et al., 2019; Hina et al., 2019; Philip et al., 2023; Stoyanova et al., 2020). In order to alleviate the threats posed on consumer IoT devices, best practices can be employed to address these security concerns.

However, to address the concerns raised, the user of the consumer IoT device needs to implement the required safeguards (Abiodun et al, 2021; Atlam & Wills, 2020; Bott & Menard, 2020). The behaviour of the user has the ability to significantly impact the security of the consumer IoT device and its associated networks, therefore it is beneficial for the device users to be aware of IoT security and the best practices in relation to their chosen consumer IoT (Bott & Menard, 2020; Blythe et al., 2020; Philip et al., 2023). Previous studies have shown that although users may be aware of and understand the various information security threats they face (Jeske & van Schaik, 2017), their self-efficacy affects their ability to protect themselves against these threats (Hina et al., 2019). Self-efficacy has been determined to affect the ability of users to secure their consumer IoT devices and their ability to respond to the various threats (Chen et al., 2019: Reychav et al., 2019; Sharevski et al., 2019). Consumer self-efficacy is defined as the ability to carry out responsive behaviours and the belief that the applied responsive behaviour will have the desired impact (Belanger & Crossler, 2019; Rieder et al., 2020; Hall et al., 2018; Hina et al., 2019). Therefore, it is important to understand the self-efficacy of the consumer IoT user in relation to the IoT security behavioural practices carried out (Belanger & Crossler, 2019; Bott & Menard, 2020; Blythe et al., 2020; Rieder et al., 2020).

1.2. Research Purpose

The purpose of this research is to identify the antecedents of consumer IoT security self-efficacy as well as its influence on consumer security practices. It is therefore an explanatory study in that it explains both the influences on, and the influence of consumer IoT security self-efficacy with respect to users securing their consumer IoT devices in the context of South Africa.

1.3. Research Objectives

The main objective of this research is to determine the antecedents and consequences of consumer IoT security self-efficacy. In order to reach this objective, the following sub-objectives need to be addressed:

1. Identify the antecedents of consumer IoT security self-efficacy.
2. Identify the consequences of consumer IoT security self-efficacy.

1.4. Research Question

This research aims to answer the following question: What are the antecedents and consequences of consumer IoT security self-efficacy. To answer this question, the following sub-questions will be addressed:

1. What are the antecedents of consumer IoT security self-efficacy?
2. What are the consequences to consumer security practice?

1.5. Dissertation Layout and Structure

This dissertation is laid out as follows: Section 2 focuses on the literature review conducted for this study which details the findings in literature related to the theoretical understandings of the antecedents and consequences of consumer IoT security self-efficacy. Section 3 focuses on the development of the hypothesis as they relate to literature and the model built within this study. Section 4 contains the research design and methodology, where philosophical assumptions are discussed, as well as the research approach, strategy, timeframe, and instrument are highlighted. Section 5 consists of the research analysis and results which cover the demographic analysis completed as well as the various statistical analysis, such as descriptive statistics, outer model assessment, inner model assessment and the hypothesis testing and path coefficient analysis. Within this section, the research findings are discussed. And to finish, in Section 6, conclusions and recommendations for future research are made.

2. Literature Review

The growth of IoT and the demand for low-cost, easily deployable technology has led to the increased production of unsecure connected devices (Isaacs et al., 2019) which have managed to enter various aspects of the physical world to realise many distinct and unique applications (Du et al., 2018). The aim of IoT is to enable better information gathering to understand, control, and respond to the collected information to support the consumer (Abiodun et al., 2021). Users are encouraged to approach the usage and adoption of IoT networks into their daily lives with caution and to employ proper security and privacy protocols to secure their chosen devices (Belanger & Crossler, 2019). The advancement in information systems (IS) and information technology (IT) brings about the potential for external and internal malicious threats (Hina et al., 2019). Along with the vast availability and adoption of IoT devices and applications comes the challenge of privacy and security (Hassija et al., 2019). The influence of user behaviour on security practices is a challenge in the domain of information security; consumers show a disconnect between acknowledging threats faced and carrying out the appropriate preventive actions or behaviours required to alleviate them (Hina et al., 2019).

2.1. The Internet of Things (IoT)

According to the glossary of the research and advisory firm Gartner, Inc. (n.d.), IoT is made up of a network of products with technology embedded within to communicate, sense, and interact internally and externally with different environments. Abiodun et al. (2021), Atlam and Wills (2020) and Du et al. (2018) describe IoT as a next generation paradigm, which integrates billions of digital technologies such as sensors and smart nodes with people, services, and objects capable of connecting to the internet. These physical objects or devices can freely connect and exchange information “bi-directionally” (Abiodun et al., 2021, p. 2) over the internet. This connection and exchange make allowance for data collection, knowledge formation and automation (Alissa et al., 2018; Atlam & Wills, 2020; Blythe et al., 2020; Kim & Park, 2022; Lee et al., 2019; LV & Singh, 2021; Subahi & Theodorakopoulos, 2019).

IoT is one of the fastest growing technologies due to its rapid development and its capabilities to provide new service platforms and decision-making by way of collaboration with several technologies (Alissa et al., 2018; Bastos et al., 2018; Lee et al., 2019; LV & Singh, 2021; Subahi &

Theodorakopoulos, 2019). Due to the function of interconnectivity, IoT can send data without needing “human-to-human or human-to-computer interaction” (Abiodun et al., 2021, p. 7; Atlam & Wills, 2020). The aim of IoT is to connect devices to the internet that were previously unable to do so (Isaacs et al., 2019), thus enabling smart devices. Emergence of the IoT allows for the utilisation of modern technologies to manipulate and control items that were previously not network-capable (Bott & Menard, 2020).

2.1.1. IoT Devices

IoT devices can be either connected or interconnected and activated (Abiodun et al., 2021). These heterogeneous devices connect with millions of other devices to gather, sense, and analyse vast amounts of data (Alissa et al., 2018; Atlam & Wills, 2020; Kim & Park, 2022; Stoyanova et al., 2020). The ability of physical objects and things to connect and integrate with the internet enables remote access to sensors, devices, and their data (Bott & Menard, 2020). IoT allows for physical devices to create, exchange, and receive data seamlessly (Hassija et al., 2019).

IoT is widely diverse, it is visible in smart cities, automation of homes, buildings, and cities, monitoring devices or services, and other smart wearables. IoT is prevalent among users and can transcend various industries. It contributes to and lays the foundation for many digital and composable business initiatives. In addition, the use of IoT has the proven ability to increase business productivity, as it allows for improved customer service and the increase of sales revenue. (Abiodun et al., 2021; Atlam & Wills, 2020; Bott & Menard, 2020; Demestichas et al., 2020; Dian et al., 2020; Farooq et al., 2019; Farooq et al., 2020; Iqbal et al., 2016; Khan et al., 2020; Kim & Park, 2022; Lheureux et al., 2021; Malik et al., 2021; Mamdiwar et al., 2021; Perez et al., 2018; Poongodi et al., 2019; Sharevski et al., 2019; Stoyanova et al., 2020; Subahi & Theodorakopoulos, 2019; Wang et al., 2020). Common applications and useful functionality of IoT include sensors, sensor data, smartphones, smart or intelligent software and consumer connected devices, e.g., smart speakers, smart TVs, toys, appliances, and wearable devices (Abiodun et al., 2021; Atlam & Wills, 2020; Bott & Menard, 2020; Perez et al., 2018; Ren et al., 2019; Zeng & Roesner, 2019).

2.1.2. Applications of IoT

There are various applications of IoT, some of these include industrial IoT (IIoT), agricultural IoT, smart city IoT, wearable IoT (WioT), and consumer IoT (Al-Turjman et al., 2022; Demestichas et al., 2020; Dian et al., 2020; Farooq et al., 2019; Farooq et al., 2020; Kirimtat et al., 2020; Khan et al., 2020; Malik et al., 2021; Mamdiwar et al., 2021; Philip et al., 2023; Poongodi et al., 2019; Stoyanova et al., 2020; Wang et al., 2020; Wu et al., 2020). IioT refers to the automation of smart objects and things in order to collect, communicate, sense and process real-time events in the industrial sector and industrial systems (Khan et al., 2020; Malik et al., 2021; Wang et al., 2020). The integration of IoT connected devices have brought about vast amounts of business and industrial opportunities which have been made available due to the implementation of IoT technologies (Abiodun et al., 2021; Du et al., 2018). IioT has been referenced and studied in prior research conducted by Khan et al. (2020) who highlighted the recent advances and challenges in the IioT area, Malik et al. (2021) who focused on the applications of IioT and the manner in which it finds itself in most industries, and Wang et al. (2020) who investigated the possible privacy risks and security vulnerabilities related to IioT.

Agricultural IoT refers to the application of IoT in areas such as precision farming, greenhouses, and livestock monitoring (Demestichas et al., 2020; Farooq et al., 2019; Farooq et al., 2020). Studies conducted by Farooq et al. (2019) and Farooq et al. (2020) realise the importance and possible impacts that IoT can bring to the agricultural sector and summarise that agricultural IoT can be used and developed in order to monitor and maintain agriculture with minimal human involvement. Farooq et al. (2020) discusses the agricultural IoT framework as well as the opportunities available and the possible challenges in the sector. Agricultural IoT has also been the focus of previous research by Demestichas et al. (2020) who stresses the importance of the role agriculture has in human society and highlights the integration of information and communication technologies in the agricultural space brings about several existing as well as emerging security threats.

Smart city IoT or smart cities relate to the solutions of IoT, cloud computing and big data being brought together to establish a connection with the layers of a city. These “key technologies” (Kirimtat et al., 2020, p. 1) come together to create a working smart city with a wide variety of applications that are based off human requirements (Al-Turjman et al., 2022; Kirimtat et al., 2020; Wu et al., 2020). Smart cities provide intelligent solutions to citizens by means of smart buildings, public safety, and smart parking to name a few (Al-Turjman et al., 2022). In literature focused on smart city IoT, previous studies have highlighted the advances in smart cities, its vulnerabilities, and

future trends. Such as the research conducted by Kirimtat et al. (2020), which aims to raise awareness to the phenomenon of smart cities and the future trends which include the alternative of floating cities. Research by Al-Turjman et al. (2022) also considers the significant advancements brought to society by smart cities and evaluate the security and privacy issues that may arise in this environment.

WioT relates to increasingly popular IoT or smart devices that can be worn day-to-day by the user as accessories, these items may also be embedded on to the users clothing or body using adhesive, be inserted into the body via implant and even tattooed onto the users skin (Dian et al., 2020; Mamdiwar et al., 2021; Poongodi et al., 2019; Zeng & Roesner, 2019). Previous studies by Poongodi et al. (2019) highlight WioT as a means to automatically bring users to IoT as it allows users to interact with the physical objects around them. It is also stressed that WioT will need to keep evolving in order to cope with the future needs or anticipated needs of its users (Poongodi et al., 2019). There have also been references to WioT in the medical and healthcare sector, such as a study conducted by Mamdiwar et al. (2021) who investigated the advances in WioT for healthcare monitoring; a comparative analysis is also conducted around the available WioT for healthcare and analyses the current challenges faced as well as probable challenges in the future. WioT is classified into the clusters of health, sports, tracking and safety by Dian et al. (2020). Through their study, they reveal the many advantages and applications of WioT or Cellular IoT (CioT) as well as the associated disadvantages (Dian et al., 2020). While WioT has been individually focused on in previous research, its falls under the classification of consumer IoT in the study conducted by Perez et al. (2018).

2.1.3. Consumer IoT

IoT has a significant impact on the way users carry out various activities in their daily lives. The use of IoT contributes to these activities by making them much easier and more efficient to perform (Abiodun et al., 2021; Atlam & Wills, 2020; Johnson et al., 2020; Perez et al., 2018). Consumer IoT devices are devices or systems that the average consumer or general public has the ability to obtain quite easily. These devices generally fall into the categories of mobile IoT, smart homes and wearables (Al-Turjman et al., 2022; Johnson et al., 2020; Perez et al., 2018).

The category of mobile IoT is quite broadly defined in literature as it encompasses everything from smartphones to smart cars and everything in between, such as bicycles and drones (Perez et al., 2018). The smart homes category relates to IoT devices that are made use of in the homes of users

with the aim of simplifying daily life. This can be related to comfort, entertainment as well as home security. Wearables or WioT refer to computers with sensors and actuators that have been developed as an accessory, item of clothing or a device that is worn by the consumer (Aboidun et al., 2021; Dian et al., 2020; Mamdiwar et al., 2021; Perez et al., 2018; Poongodi et al., 2019).

Table 1 below is adapted from Perez et al. (2018) to highlight the multiple use cases for consumer IoT devices. It describes the type of consumer IoT, the related type of device and the possible embedded sensor and actuator technology that power these consumer IoT devices.

Type of IoT	**Type of Device**	**Embedded technology**	**Possible examples**
Mobile IoT	Drone	Cameras, GPS, Gyroscopes, Lights, Microphones	3D Robotics solo Quadcopter, Parrot Bebop
	Smart Bicycle	Compass, GPS, Hooter, Lights, Speedometer, Speakers	SmartHalo, VanMoof SmartBike, Volata Cycles
	Smart Car	Autonomous Driving, GPS, In-car Air Quality Monitoring, In-car Sensors, Microphones, Remote Engine Start, Voice-based Navigation	Audi Q8, Tesla, Volvo V90
Smart Home (Perez et al., 2018; Zeng & Roesner, 2019)	Alarm System	Cameras, Entry Sensors, Motion Sensors, External Communications, Smoke Sensors	LiveWatch Security System
	Appliances	Cameras, Dust Particle Sensors/Displays, Lights, Physical Controls i.e., buttons and touch screens, Speakers, Thermometer, Vacuum	iRobot Roomba, LG SmartThinQ washing machine, Smart TV, Samsung Family Hub Refrigerator
	Energy Monitor	Ammeter	Neurio Home Energy Monitor

Type of IoT	Type of Device	Embedded technology	Possible examples
	Gardening	Flow Sensors, Rain Sensors, Soil Sensors	Rachio Smart Sprinkler
	Intelligent Voice Assistant	Microphone, Speaker, Other IoT devices	Apple HomePod, Amazon Echo, Google Home
	Smart Light	Microphones, Motion Sensors	GE Link Connected, Phillips Hue
	Thermometer	Infrared Sensors, Thermometers	EcoBee, Nest Learning Thermostat
Wearables	Chest strap	Accelerometers, Body Temperature, Breath Depth, Breath Rate, ECG, Heart Rate, Skin Conductivity	Polar Heart Rate Sensor, Zephyr BioHarness
	Glasses	Accelerometers, Camera, Gyroscopes, Microphone, Speakers, Vibration	Google Glass, Oculus Rift, Microsoft HoloLens
	Smartwatches	Accelerometers, LCD Screen, Heart Rate Monitor, Lights, Microphone, Oxygen-levels Monitor, Skin Conductivity, Speaker, Vibration	Apple Watch, Samsung Gear
	Wristband	Accelerometers, LCD Screen, Heart Rate Monitor, Lights, Microphone	Fitbit

Table 1: Consumer IoT devices [Adapted from Perez et al., 2018]

One of the aims of consumer IoT devices is to improve the lives of those who make use of them (Atlam & Wills, 2020; Bastos et al., 2018). These users value characteristics such as low costs and ease of deployment (Isaacs et al., 2019). Many IoT devices are aimed at the everyday users who are not necessarily technical and are often required to make decisions in relation to their consumer IoT devices with little to no skills in IT (Bott & Menard, 2020).

In the home or personal environment, users of consumer IoT encounter significant challenges (Bott & Menard, 2020). Users are often more enamoured with the usefulness of the consumer IoT device and are not too concerned about the consequent security. There is a general lack of security awareness among users relating to software vulnerabilities, and many experience a false sense of privacy. Due to this, the consumer IoT devices are vulnerable to preventable threats (Bott & Menard, 2020). Bott and Menard (2020) identified that there is a high potential for user data exposure in the IoT environment and the characteristic lack of privacy concerns shown may lead to the unintended compromise of sensitive information, it is reasonable to assume that these concerns prove true in the specific case of consumer IoT. Consumer IoT contributes to the generation of big data (Abiodun et al., 2021), and with the large amounts of data gathered, consumer IoT can use advanced data processing, analysing, and mining techniques to extract the useful information from the data that is collected (Du et al., 2018). Due to the non-technical nature of many users, they are often not aware of the importance of information security and don't understand the extent to which the data and information about them and their environments are being collected, stored, and shared (Bott & Menard, 2020; Subahi & Theodorakopoulos, 2019).

Privacy and security are the main concerns for users in the adoption of consumer IoT devices (Blythe et al., 2020). Although these concerns exist, there are many who still prefer the affordances that the connectedness of consumer IoT brings (Blythe et al, 2020). Blythe et al. (2020) refers to this as the "privacy paradox" (Blythe et al., 2020, p. 4) in which users are concerned about privacy and security but do not undertake protective behaviours to secure their devices and things.

2.1.3.1. The Benefits of Consumer IoT

The consumer IoT area is growing exponentially and has not yet reached its limit, it is expanding beyond the realm of things or objects (Hassija et al., 2019). There are various benefits attached to the era of consumer IoT. Users benefit by receiving increased control, the ability of remote management, and huge volumes of information (Bott & Menard, 2020). Among these strengths of consumer IoT is the effect that the technology has on the various areas of day-to-day life and user behaviour. Tasks are made simpler and are able to be completed in a much more efficient way, and this can be done with minimal human interaction (Abiodun et al., 2021; Bastos et al., 2018; Lee et al., 2019; Uddin et al., 2019). In addition, Apthorpe et al. (2022) determined that consumer IoT devices have the ability to strengthen interpersonal relationships and connections, promotes the ease of managing households, and also contributes to the simplification of communication by allowing users

to do so remotely. Consumer IoT also inspires playfulness among its users and goes a long way to support the independence, empowerment, and quality of life of ordinary users as well as those who may have special needs. It improves overall peace of mind and provides feelings of safety by having the ability to enhance security (Apthorpe et al., 2022; Uddin et al., 2019). Another one of the major benefits of consumer IoT is the overall enjoyment experienced by the user of the device, this is achieved by using the various devices for entertainment and other lifestyle applications such as fitness tracking and home monitoring (Uddin et al., 2019).

2.1.3.2. The Challenges of Consumer IoT

Along with the benefits of consumer IoT, it also brings about unique challenges (Blythe et al., 2020; Johnson et al., 2020; Ren et al., 2019; Uddin et al., 2019), with many of these being attributed to the fact that the devices are low powered and have limited processing capabilities (Johnson et al., 2020). Consumer IoT has the ability to enhance but also threaten the privacy and security of the user (Alladi et al., 2020; Blythe et al., 2020; Uddin er al., 2019). There is a large diversity in protocols, technologies, and devices in a consumer IoT application and several challenges have been uncovered and addressed in literature in relation to these. Some of these challenges and trade-offs include connectivity, cost-effectiveness, reliability, scalability, big data, heterogeneity, security, and privacy (Abiodun et al., 2021; Alissa et al., 2018; Al-Turjman et al., 2022; Bastos et al., 2018; Hassija et al., 2019; Hina et al., 2019; Stoyanova et al., 2020; Uddin et al., 2019). Abiodun et al. (2021) identifies privacy and security concerns as issues which require timely solutions as the low levels of security in consumer IoT devices makes it a vulnerable target for hackers, criminals and those who have malicious intentions toward the user and their data (Abiodun et al., 2021; Alladi et al., 2020; Al-Turjman et al., 2022; Stoyanova et al., 2020; Zeng & Roesner, 2019).

Blythe et al. (2019) states that IoT is recognised as being generally insecure due to the lack of security features encased in the technology. The management in the field of telecommunications and IT is quite complex (Abiodun et al., 2021), specifically in relation to privacy and security. This is due to majority of the security issues relating to the complexity of creating safe, private, and secure communications (Abiodun et al., 2021; Al-Turjman et al., 2022; Stoyanova et al., 2020). Among the consumer IoT challenges, it is found that consumer IoT devices can assist in surveillance and tracking, this can cause mistrust because of undesired monitoring. The transparency of data collection is also lacking, and this can evoke differences in expected information and functionality preferences of the user (Apthorpe et al., 2022). For successful advancement to take place, these

issues need to be confronted (Abiodun et al, 2021) and it is important for users of consumer IoT to be confident about the security of their devices and applications (Atlam & Wills, 2020).

2.2. Self-Efficacy

Self-efficacy is an important concept which is a form of self-evaluation that acts as a determinant of the users eventual behaviour (Kim et al., 2009). Self-efficacy is the belief in the ability to carry out certain behaviours and deal with threats. This belief influences the users application of skills and whether they are being put to good use (Belanger & Crossler, 2019; Hall et al., 2018; Hina et al., 2019; Kim et al., 2009). Hall et al. (2018) describe self-efficacy as the users belief that a task or goal will be successfully achieved in a specific setting. Users tend to engage in behaviours or actions that they believe will get them the outcome that they want, and that they believe they can carry out (Gosselin & Maddux, 2012).

Self-efficacy is situation-specific and can be different according to the circumstances or issue being faced. This implies that users may be more confident in dealing with one situation as compared to a different one (Hall et al., 2018; Rieder et al., 2020). Belanger and Crossler (2019) note that self-efficacy impacts information security behaviours, and that self-efficacy is directly related to favourable information security behaviours and intentions. There have been various studies that have investigated self-efficacy in technology related research, mainly focused on different areas such as computer and mobile technology (Rieder et al., 2020).

2.3. Literature Review Summary

As previous studies have highlighted, the emergence and growth of consumer IoT increases the propensity for the existence of malicious information security threats (Abiodun et al., 2021; Hassija et al., 2019; Hina et al., 2019; Isaacs et al., 2019; Uddin et al., 2019). IoT enables items and devices that were previously unable to connect to the internet to now do so and allows them to share data and information between each other (Abiodun et al., 2021; Atlam and Wills, 2020). The aim of IoT is to improve the lives of those who make use of them, whether it be in the commercial or private capacity (Atlam & Wills, 2020; Bastos et al., 2018; Du et al., 2018; Iqbal et al., 2016; Lee et al., 2019; Perez et al., 2018). Due to significant improvements and usefulness provided by IoT and its devices,

users are not too concerned about the associated security challenges, and there appears to be a general lack of security awareness relating to potential vulnerabilities, as a result many users experience a false sense of privacy (Abiodun et al., 2021; Alissa et al., 2018; Bastos et al., 2018; Hassija et al., 2019; Hina et al., 2019). Due to the lack of security awareness, it is necessary to understand how behaviour contributes toward IoT information security, and how the users self-efficacy relates to those security practices. It is expected that the users self-efficacy is directly related to favourable information security behavioural practices and intentions (Belanger & Crossler, 2019; Hall et al., 2018; Rieder et al., 2020).

3. Hypothesis Development

The aim of this section is to discuss the hypotheses and its development for identification of the antecedents and consequences of consumer internet of things security self-efficacy. The research in this study follows a deductive approach which implies that an a priori theoretical model will be tested. The conceptual model for this study is adapted from the research model presented by Rhee et al. (2009) which illustrated antecedents of self-efficacy in information security, and the influence of self-efficacy on computer end-user's information security practices. This research study aims to similarly identify the antecedents as well as the consequences of consumer IoT security self-efficacy. The factors relevant to this study include: IoT Security Behavioural Practices (Lee et al., 2019; Ngoqo & Flowerday, 2015; Rhee et al., 2009; Snyman et al., 2018; Yoon et al., 2012; Zhou et al., 2020), Behavioural Intention (Das & Khan, 2016; Rhee et al., 2009), IoT Security Technology Practices (Goodreau, 2021; Lee et al., 2019; Microsoft, 2021; Rhee et al., 2009; Yoon et al., 2012), IoT Security Self-Efficacy (Rhee et al., 2009; Zhou et al., 2020), IoT Device Knowledge (Davis, 2013), IoT Device Experience (Rhee et al., 2009; Zhou et al., 2020), IoT Security Breach Incidents (Rhee et al., 2009; Williams et al., 2021), and IoT General Controllability (Aurigemma & Mattson, 2017; Rhee et al., 2005; Rhee et al., 2009).

3.1. IoT Security Behavioural Practices

Information systems end-user behavioural research focuses on the users behavioural intentions, behavioural practices, and the various influences impacting behavioural practices as it pertains to the information system (Behardien & Brown, 2022). User security behaviour is cited as a significant concern in the area of information systems. This is due to the fact that human behaviour can be considered as "irrational, difficult to understand, and challenging to manage" (Snyman & Kruger, 2020, p. 1). Security behavioural practices can be defined as the behaviour or action taken by the user to strengthen their information security and adhere to security practices (Rhee et al., 2009). It is possible for security behaviour to be deliberate or unintentional (Hall et al., 2018; Rhee et al., 2009; Snyman & Kruger, 2020; Taylor & van Schaik, 2022; Yoon et al., 2012; Zhou et al., 2020). Poor security behavioural practices are a major threat to end-users (Aigbefo et al., 2022). Most studies have focused their research on IT artefacts such as computers, mobile devices, smartphones, etc (Hall et al., 2018; Rhee et al., 2009; Taylor & van Schaik, 2022; Yoon et al., 2012; Zhou et al., 2020). Security concerns persist and are perhaps amplified with digital technologies such as consumer IoT.

It is therefore important to consider consumer IoT devices and associated security behavioural practices (Lee et al., 2019; Zeng & Roesner, 2019).

3.2. Behavioural Intention

Behavioural intention is a key concept in the widely accepted theory of planned behaviour (TPB) (Ajzen, 1991; Lu, 2021). The behavioural intention of the individual relates to their willingness to display effort to perform specified behavioural practices. The technology users' behavioural intention has a strong influence on the manner in which they behave (e.g., make use of their chosen technology and its related functions) (Ajzen, 1991; Gupta & Maurya, 2022).

The users behavioural intention is implicated as being influential in various technology related behaviours, such as usage, security, and privacy (Aigbefo et al., 2022; Belanger & Crossler, 2019; Gupta & Maurya, 2022; McGill et al., 2017). In information security, the user behavioural intention suggests that the individual's tendency or determination to protect their information system leads to security behavioural practices being put in place (Aigbefo et al., 2022; Belanger & Crossler, 2019; Deng & Gu, 2021; Gupta & Maurya, 2022; McGill et al., 2017). As a result, the users behavioural intention affects future security behavioural practices. This is shown in studies by Das and Khan (2016), Kim & Park (2022), McGill et al. (2017), and Rhee et al. (2009), who employed the behavioural intention construct in areas of research focused on computers, mobile devices, smartphones, and IoT. It is important to consider the implications of the growth in digital technologies such as consumer IoT and the associated behavioural intentions and security practices. In this study, behavioural intention (BI) refers to the consumer IoT device users intention for use and persistence with IoT security. The users behavioural intention can affect their future IoT security behavioural practices (Das & Khan, 2016; Kim & Park, 2022; Rhee et al., 2009). Therefore, it is hypothesised that:

H1: *Behavioural intention positively influences IoT security behavioural practices*

3.3. IoT Security Technology Practices

Security technology practices refer to the security related functionalities and software provided by the information system and the adoption of these functionalities by the user (Rhee et al., 2009). Security technology practices have been established in the areas of information systems security research focussing on technologies such as computers, mobile devices, smartphones, and IoT (Goodreau, 2021; Lee et al., 2019; Rhee et al., 2009; Yoon et al., 2012). Security technology practices adopted by the user reflects their effort in putting safeguards in place to protect against security challenges (Goodreau, 2021; Lee et al., 2019; Microsoft, 2021; Rhee et al., 2009). Based on the continuous growth of digital technologies such as IoT, it is important to consider security technology practices in the case of consumer IoT device security.

IoT security technology practices in this study refers to the security functionalities provided by the consumer IoT device and the adoption of those functionalities by the consumer IoT user. The security technology practices put in place by the user on their consumer IoT devices reflects the individual's eventual behaviour in putting eliciting safeguards to prevent security breaches and address security challenges. It is expected that users of consumer IoT devices who employ good IoT security technology practices will display more secure consumer IoT security behavioural practices (Goodreau, 2021; Lee et al., 2019; Microsoft, 2021; Rhee et al., 2009). It can be hypothesised that:

H2: *IoT security technology practices positively influence IoT security behavioural practices.*

3.4. Consumer IoT Security Self-Efficacy

Self-efficacy is a key concept of the social cognitive theory (Bandura, 1986), it is a form of self-evaluation that affects users eventual behaviour (Kim et al., 2009). Self-efficacy is the belief in the ability to carry out certain behaviours and influences the users application of skills (Belanger & Crossler, 2019; Hall et al., 2018; Hina et al., 2019; Kim et al., 2009).

Information security self-efficacy is defined as the belief in one's capability to protect information systems, their resultant data and information from threats (Rhee et al, 2009). Various research studies by Ahmad et al. (2018), Cuganesan et al. (2018), Rhee et al. (2009), Shahri et al. (2016), Wu et al. (2014), and Zhou et al. (2020) for example, refers to the users' perceived abilities to take

precautions in ensuring information systems security (Zhou et al., 2020). Self-efficacy is used to determine the amount of effort and persistence the user makes in the face of information security threats. Prior information security studies have been conducted in respect of technologies such as computers, mobile devices, and smartphones.

Due to digital growth, it is important to consider the area of consumer IoT as well. Therefore, consumer IoT security self-efficacy refers to the consumer IoT device users perceived ability to take precautions to ensure information security. It is expected that users of consumer IoT devices with a greater consumer IoT security self-efficacy belief would adopt more secure IoT security technology practices and display more secure consumer IoT security behavioural intentions and security behavioural practices (Goodreau, 2021; Lee et al., 2019; Microsoft, 2021; Rhee et al., 2009). It is hypothesised that:

H3: *Consumer IoT security self-efficacy positively influences behavioural intention.*

H4: *Consumer IoT security self-efficacy positively influences IoT security technology practices.*

H5: *Consumer IoT security self-efficacy positively influences IoT security behavioural practices.*

3.5. Consumer IoT Device Knowledge

Device knowledge encompasses the users' competencies, motives, and traits (Eschenbrenner & Nah, 2014). Knowledge relates to the abilities the individual possesses to perform specific tasks (Eschenbrenner & Nah, 2014) and contributes to the users' belief in their ability to make use of a particular information system capably and successfully (Davis, 2013; Eschenbrenner & Nah, 2014). As a result, it can be expected that the users knowledge of an information system contributes toward their ability to ensure their information security (Davis, 2013). It is important to consider the knowledge the user has of consumer IoT devices and their ability to ensure the security of the chosen consumer IoT. Therefore, in this study, consumer IoT device knowledge refers to the users knowledge of consumer IoT devices. It is expected that a user's knowledgeable experience with consumer IoT devices contributes toward their perceived ability to ensure their consumer IoT security. It can be hypothesised that:

H6: *Consumer IoT device knowledge positively influences consumer IoT security self-efficacy.*

3.6. Consumer IoT Device Experience

Device experience refers to the skill, level of literacy, or past experience a user has with the specified information system. Rhee et al. (2009) states that "enactive mastery experience is a primary influencing source of efficacy belief" (Rhee et al., 2009, p. 4). It is expected that individuals who have device experience will have an increased self-perceived ability to use the information system and its functions, including the security functions and protocols. It is expected that having prior experience with the information system e.g., computers, mobile phone, or smartphones, would contribute toward their ability ensure security of these devices (Rhee et a., 2009; Zhou et al., 2020). Therefore, consumer IoT device experience refers to the skill, level of literacy, or experience the consumer IoT user has with their device(s). It is expected that having prior experience with consumer IoT devices contributes toward the users perceived ability ensure security and improves their self-efficacy. It can be hypothesised that:

H7: *Consumer IoT device experience positively influences IoT security self-efficacy.*

3.7. IoT Security Breach Incidents

Security breach incidents refers to the user having previously had a negative experience in relation to information systems security (Rhee et al., 2009; Williams et al., 2021). Previous studies have shown that users who have experience with a particular information system would display the belief in their ability to secure their chosen device (Rhee et al., 2009). The same applies for users who have experience with security threats or breaches on their information systems devices. The security breach incident may affect the user's confidence in their ability to ensure the security of their information system device going forward (Rhee et al., 2009; Williams et al., 2021). Since this has been shown in the areas of computers and network security, it is reasonable to consider the applicability in the area of consumer IoT security. Therefore, IoT security breach incidents refer to the consumer IoT device users experience with IoT security breaches. It is expected that having previously had a negative experience with their consumer IoT device security may affect their

confidence in the perceived ability to ensure information security in future. It can be hypothesised that:

H8: *IoT security breach incidents negatively influence consumer IoT security self-efficacy.*

3.8. Consumer IoT General Controllability

General controllability relates to the users belief that there are means and solutions available to control information systems and their threats (Rhee et al., 2009). It is expected that the users perceived ability and competence to control information systems security threats with the resources available will affect their perceived ability or self-efficacy to do so (Aurigemma & Mattson, 2017; Rhee et al., 2005, Rhee et al., 2009). This concept has been used and tested in the area of computer security (Aurigemma & Mattson, 2017; Rhee et al., 2005; Rhee et al., 2009). Consequently, and due to the growth in digital technology, it is reasonable to consider the applicability of general controllability with respect to consumer IoT devices. Therefore, consumer IoT general controllability refers to the consumer IoT device users perception in being able to control general information security threats as well as consumer IoT security threats. It is expected that the users perceived ability and competence to control consumer IoT security threats with the resources available will affect their perceived ability or self-efficacy to do so. It can be hypothesised that:

H9: *Consumer IoT general controllability positively influences consumer IoT security self-efficacy.*

The hypotheses for this study are summarised in Table 2, and the research model for investigating the antecedents and consequences of consumer IoT security self-efficacy is illustrated in Figure 1.

	Hypothesis description
H1	Behavioural intention positively influences IoT security behavioural practices.
H2	IoT security technology practices positively influence IoT security behavioural practices.
H3	Consumer IoT security self-efficacy positively influences behavioural intention.
H4	Consumer IoT security self-efficacy positively influences IoT security technology practices.
H5	Consumer IoT security self-efficacy positively influences IoT security behavioural practices.
H6	Consumer IoT device knowledge positively influences consumer IoT security self-efficacy.
H7	Consumer IoT device experience positively influences IoT security self-efficacy.
H8	IoT security breach incidents negatively influence consumer IoT security self-efficacy.
H9	Consumer IoT general controllability positively influences consumer IoT security self-efficacy.

Table 2: Research Study Hypotheses

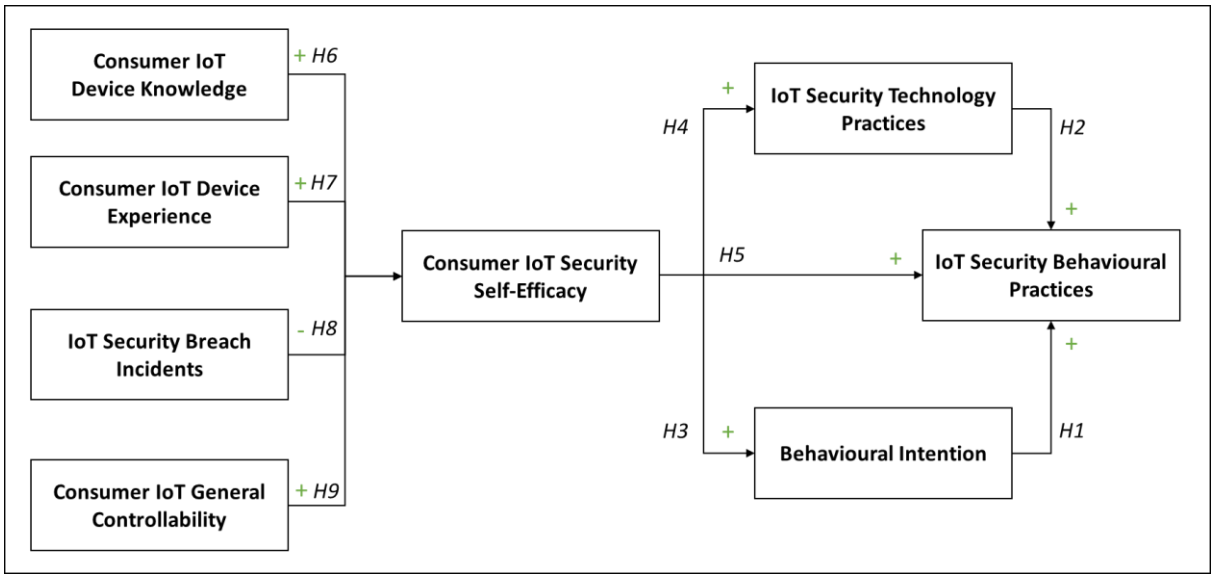

Figure 1: Conceptual model – Antecedents and Consequences of Consumer IoT Security Self-Efficacy

4. Research Methodology

This section presents the research methodology followed for this study. It outlines the purpose of the research as well as the research objectives and resultant questions. Key focuses in this section include the philosophical assumptions, research approach, strategy, and timeframe, it also looks at the research instrument as well as the procedures followed for data collection and analysis.

4.1. Philosophical Assumptions

There are various research perspectives that can be used in relation to behavioural information systems, namely: the interpretive philosophy, the critical philosophy and the positivist philosophy (Orlikowski & Baroudi, 1991). The philosophy used in this research is positivism. This implies that the research works with the observable reality to produce generalisations. Positivist research aims to discover ways in which to describe, explain and/or predict human activity or behaviours (Kivunja & Kuyini, 2017). The researcher remains independent of the study to make objective decisions, in doing so, the knowledge gathered from this study is clear and accurate (Saunders et al., 2019).

The focus of epistemological assumptions about knowledge in this study determines observable and measurable facts and regularities. This implies that meaningful data was originated from phenomena that is observable and measurable (Saunders et al., 2019).

4.2. Research Approach

This research adopts a deductive approach as opposed to the inductive approach, which implies that the reasoning works from the more general down to the more specific, adopting a top-down approach from theory selection to confirmation of that theory. Deductive reasoning occurs due to the conclusion of the study being based on theory-driven premises. This means that the research strategy is designed to test the identified hypotheses (Saunders et al., 2019).

4.3. Research Strategy

The methodology adopted to carry out this study is quantitative as is in line with the positivist approach (Saunders et al., 2019). This study uses the survey questionnaire research strategy to gather quantitative data, this is seen as the most efficient way to gather data for a larger sample (Saunders et al., 2019).

4.4. Research Timeframe

The research follows a cross sectional timeframe as it examines the antecedents and consequences of self-efficacy in information security and its effects on consumer IoT device security behaviour at the specific point in time at which the research was carried out. This approach is consistent with carrying out a research survey strategy (Saunders et al., 2019).

4.5. Research Instrument

To measure self-efficacy in consumer IoT and identify its antecedents and consequences, existing measures such as developed by Rhee et al., (2009) have been reviewed. He et al. (2014) carried out a study into the instruments measuring the self-efficacy variable in behavioural information security research. The measure for used IoT security self-efficacy is derived from He et al. (2014).

As highlighted in the conceptual framework, this study investigates eight (8) factors, namely: IoT Device Knowledge, IoT Device Experience, Security Breach Incidents, General Controllability, IoT Security Self-Efficacy, IoT Security Behavioural Practices, Behavioural Intention, and IoT Security Technology Practices. Table 3 provides an overview of these measures and their respective resources.

Appendix 4 details the final questionnaire statements used in the research study.

		No. of measures	Resource
CK	Consumer IoT Device Knowledge	4	(Davis, 2013; Eschenbrenner & Nah, 2014)
DE	Consumer IoT Device Experience	4	(Rhee et al., 2009; Zhou et al., 2020)
SBI	IoT Security Breach Incidents	2	(Rhee et al., 2009; Williams et al., 2021)
GC	General Controllability	7	(Aurigemma & Mattson, 2017; Rhee et al., 2005; Rhee et al., 2009)
ISSE	Consumer IoT Security Self-Efficacy	7	(Ahmad et al., 2018; Cuganesan et al., 2018; Rhee et al., 2009; Shahri et al., 2016; Taneja, 2006; Workman et al., 2008; Wu et al., 2014; Zhou et al., 2020)
SP-B	IoT Security Behavioural Practices	7	(Blythe et al., 2019; Lee et al., 2019; Ngoqo & Flowerday, 2015; Rhee et al., 2009; Snyman et al., 2018)
BI	Behavioural Intention	4	(Das & Khan, 2016; Rhee et al., 2009)
SP-T	IoT Security Technology Practices	3	(Blythe et al., 2019; Goodreau, 2021; Lee et al., 2019; Microsoft, 2021; Rhee et al., 2009)

Table 3: Research instrument: Antecedents and Consequences of Internet of Things Security Self-Efficacy

4.6. Data Collection

A survey questionnaire was used to gather quantitative data for this research study and was managed online using Qualtrics. The survey questionnaire made use of a mix between multiple choice questions for the demographic data and the Likert rating system to collect granular opinion data (Bhattacharjee, 2012; Saunders et al., 2019). Here, the research participant was asked rating questions so that the study may gather participant opinion data. To maintain comprehension of the survey questions, the order of response categories was used consistently. The five-point Likert rating scale was used in the questionnaire, the participants were able to state how strongly they agree or disagree with the statements presented to them.

The five-point Likert rating scale used in this study was as follows:

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree

4.6.1. Sampling

4.6.1.1. Target Population

The target population for this sample consisted of users of consumer IoT devices in South Africa. Consumer IoT device users are individuals who make use of consumer IoT devices as outlined in the literature review, this includes:

1. Users who own and make use of one or more consumer IoT devices.
2. Consumer IoT device users regardless of their level of advancement.

4.6.1.2. Sampling Strategy

This research study made use of an online panel survey. A panel survey is a commonly used method for data collection. The panel survey consists of the design, collection and analysing of responses from a range of people to a specified set of question (Wardropper et al., 2021). The online panel survey allows for the questionnaire to be distributed among the target audience (Qualtrics, Provo, UT). The panel survey is used to gain a larger sample and to ensure a lower margin of error in relation to the research and analysis done. Following Lowry & Gaskin (2014), since the conceptual model for this study contains 8 factors, the minimum required sample size was 80.

In order to carry out the panel survey, the researcher made use of the Qualtrics Online Panel (Qualtrics, Provo, UT) to uncover the required data. A pilot study was also conducted in order to test the reliability and validity of the research instrument, prior to finalising it.

4.6.1.3. Pilot Study Sample

Snowball sampling was chosen for the pilot study to collect a sample for the purpose of gathering data relevant to characteristics of individuals within the population (Abubakar et al., 2015; Bhattacherjee, 2012; Handcock & Gile, 2011). Snowball sampling in this pilot study aims to identify a few consumer IoT device users as respondents and then make use of those IoT device users to identify more individuals who fit in to the target population (Bhattacherjee, 2012).

4.6.1.4. Qualtrics Online Panel Surveys

The Qualtrics Online Panel (https://www.qualtrics.com/uk/core-xm/survey-software/) (Qualtrics, Provo, UT) was used to gather data for this study. Qualtrics Online Panel provides various insights from the specified audience, in this respect: consumer IoT device users. The use of the Qualtrics Online Panel is justified by Lowry et al. (2016) who state that the use of methods such as the panel can result in "breakthrough ideas" (Lowry et al., 2016, p. 16) and remains valid because it does not make any changes to the study, or the data gathered. In order to reach the specified audience and carry out the data collection, the criteria in Table 4 were derived in conjunction with the Qualtrics team which allowed the sourcing and filtering of research participants as required by the study.

Criteria	
Sample Size	~220.5
Target Country	South Africa
Target Demographic	Users of consumer IoT devices
Age	18-24: 19.3% 25-34: 29.4% 35-44: 19.5% 45-54: 13.4% 55+: 18.3%
Length of Survey	5-10 Minutes
Field Time	12 Days

Table 4: Qualtrics Online Panel Criteria

4.6.2. Research Cover Letter

Prospective research participants reviewed a cover letter as part of the survey to ensure that they are aware of the purpose of the study and what their survey questionnaire data will be used for. The letter can be found in Appendix 3.

4.6.3. Ethical Considerations

This research complied with the code of ethics prescribed for survey questionnaires. The research study had garnered approval from the UCT Ethics Committee prior to circulation.

Upon requesting participation, the research purpose is detailed to the potential research participant, and they are made aware that their participation is entirely voluntary. They were also able to exit the questionnaire at any time should they have felt the need to do so.

According to some of the ethical questions asked in terms of the research study, this study:

1. Does not require the collection or disclosure of personal information.
2. Does not aim to identify an individual or definable group within the published data.
3. Does not involve minors.
4. Does not contain any relationships of dependency
5. Does not offer remuneration for completing the study.
6. Does collect racial, minority and cultural variables.

In order to obtain approval from the UCT Ethics Committee, the submitted and approved ethics application is captured in Appendix 5.

4.6.4. Pilot Study Analysis and Results

A pilot study was conducted to determine whether there were any potential issues in the research instrument being used and to ensure that the measures being used were valid and reliable. The sample for the pilot study consisted of a subset of the identified target population and yielded 26 respondents. Of the 26 survey responses received, 4 surveys were left incomplete, and 3 surveys

contained missing values or unanswered questions. The questionnaire used for the pilot study can be found in Appendix 2.

Statistica software was used to carry out the pilot study analysis, and when completed the analysis was captured with 2 decimal points.

4.6.4.1. Pilot Study - Descriptive Analysis

Table 5 below illustrates the descriptive statistics derived from the pilot study respondents. The descriptive statistics highlight the pilot study sample mean, mode, frequency of mode as well as standard deviation among the aggregate factors initially identified for the study, i.e.: IoT Device Experience, IoT Security Breach Incidents, IoT General Controllability, IoT Security Self-Efficacy, IoT Security Practices, IoT Behavioural Intention, and IoT Security Behaviour.

Variable	Valid N	Mean	Mode	Freq. of Mode	Standard Deviation
IoT Device Experience	22.00	1.98	1.80	10.00	0.79
IoT Security Breach Incidents	21.00	3.31	3.33	9.67	1.09
IoT General Controllability	21.86	2.71	2.86	9.71	0.92
IoT Security Self-Efficacy	22.00	2.32	2.00	10.00	0.98
IoT Security Technology Practices	22.00	2.98	2.67	7.33	1.08
IoT Behavioural Intention	22.00	2.66	2.50	9.75	1.02
IoT Security Behavioural Practices	22.00	2.33	1.83	9.33	1.09

Table 5: Pilot Study – Descriptive Analysis

4.6.4.2. Pilot Study - Reliability and Validity Testing

Reliability and validity testing was carried out on the pilot study results to test to which extent the results are related to the aimed construct or underlying set of variables, and that the results relate

to the same thing and produce the same outcome each time the tests are carried out (Salkind, 2012). Cronbach's alpha correlation coefficient was used as a measure of consistency to test the reliability of the study (Bonett & Wright, 2015), Table 6 illustrates the pilot study results according to the Cronbach alpha value exceeding 0.60.

Variable	Cronbach alpha correlation coefficient
IoT Device Experience (DE)	0.66
IoT Security Breach Incidents (SBI)	0.80
IoT General Controllability (GC)	0.81
IoT Security Self-Efficacy (ISSE)	0.91
IoT Security Technology Practices (SP-T)	0.50
IoT Behavioural Intention (BI)	0.90
IoT Security Behavioural Practices (SP-B)	0.30

Table 6: Pilot Study–- Cronbach Alpha Correlation Coefficient

The pilot study results show IoT security technology practices and IoT security behavioural practices loading below the required 0.60. Therefore, a deeper analysis was conducted into these items and is illustrated in Table 7 and Table 8.

For the IoT security technology practices construct, the analysis showed that if the SP-T1 variable were to be removed, the Cronbach alpha value would improve to 0.83. And for IoT security behavioural practices, the variables needed to be revisited in order to ensure reliability.

IoT Security Technology Practices (SP-T)					
Cronbach alpha: 0.501434 Standardized alpha: 0.539773 | Average inter-item corr.: 0.326135					
Variable	**Mean if**	**Var. if**	**StDv. if**	**Item-Total**	**Alpha if deleted**
SP1	6.14	3.30	1.82	0.07	0.83
SP2	5.95	2.59	1.61	0.45	0.18
SP3	5.82	2.51	1.59	0.52	0.07

Table 7: Pilot Study–- IoT Security Practices Cronbach alpha

IoT Security Behavioural Practices (SP-B)					
Cronbach alpha: 0.303097 Standardized alpha: 0.371199 | Average inter-item corr.: 0.095111					
Variable	**Mean if**	**Var. if**	**StDv. if**	**Item-Total**	**Alpha if deleted**
SB1	11.68	6.67	2.58	0.27	0.16
SB2	10.86	8.48	2.91	-0.01	0.36
SB3	12.45	7.16	2.68	0.45	0.11
SB4	12.09	7.45	2.73	0.13	0.27
SB5	11.86	7.39	2.72	0.12	0.27
SB6	10.82	7.51	2.74	0.01	0.39

Table 8: Pilot Study— IoT Security Behaviour Cronbach alpha

Factor analysis was used to check the construct validity, this test was carried out using the Statistica software. The analysis carried out made use of a Varimax Raw rotation, where factors were set to be highlighted where loadings were greater than 0.40. Table 9 illustrates the factor analysis achieved through the iterative process, which makes use of a maximum value of 7 factors and an eigenvalue of 1.000.

The factor analysis shows that at the point of the pilot study, majority of the measures were not truly representative of the constructs. However, the behavioural intention (BI) construct is shown to be representative with its factors being highlighted above 0.80.

Variable	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	Factor 6	Factor 7
DE1	-0.20	0.38	-0.03	0.01	-0.11	0.10	0.79
DE2	0.01	0.26	0.02	0.04	-0.14	0.72	0.49
DE3	0.12	0.23	0.23	0.33	0.31	0.77	0.01
DE4	0.20	-0.03	0.06	0.92	-0.06	0.03	-0.12
DE5	0.13	0.34	0.06	0.65	0.23	0.13	0.32
SBI1	0.13	-0.03	0.82	-0.17	0.05	0.14	0.19
SBI2	0.13	-0.02	0.83	0.28	0.03	0.19	0.19
SBI3	0.05	0.34	0.61	-0.06	0.10	0.54	-0.17
GC1	0.60	0.09	0.24	-0.20	0.19	-0.02	0.40
GC2	0.27	-0.02	0.41	-0.33	0.15	0.24	0.59

Variable	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	Factor 6	Factor 7
GC3	0.09	0.20	0.19	0.01	0.10	-0.03	0.86
GC4	0.72	0.34	0.05	0.14	0.09	0.31	0.38
GC5	0.42	0.09	0.20	0.00	0.30	0.64	-0.04
GC6	-0.06	0.71	0.21	0.18	0.35	0.15	0.03
GC7	0.62	0.36	0.11	-0.20	0.11	0.54	0.16
SE1	0.29	0.80	0.07	0.08	0.04	0.26	0.20
SE2	0.58	0.66	0.03	0.22	0.10	0.03	0.22
SE3	0.09	0.68	0.10	0.00	-0.16	-0.09	0.31
SE4	0.11	0.76	-0.05	0.01	-0.03	0.46	0.05
SE5	0.09	0.73	0.11	0.01	-0.10	0.22	0.45
SE6	0.52	0.48	0.29	0.13	0.54	0.19	0.07
SE7	0.48	0.54	-0.04	-0.13	-0.05	0.34	0.47
SP-T1	0.14	-0.54	-0.64	0.14	0.24	0.15	0.04
SP-T2	0.48	0.54	-0.35	-0.15	0.37	0.18	0.17
SP-T3	0.48	0.38	0.10	0.05	0.63	0.01	0.22
BI1	0.87	0.25	0.07	0.18	0.06	0.05	-0.04
BI2	0.92	0.16	-0.03	0.14	-0.12	0.16	0.07
BI3	0.83	-0.15	0.25	-0.13	0.08	-0.01	-0.26
BI4	0.83	-0.07	0.11	0.11	0.16	0.21	-0.03
SP-B1	0.22	0.52	0.15	-0.42	-0.07	-0.08	0.36
SP-B2	-0.48	-0.20	-0.01	-0.03	0.62	-0.07	0.24
SP-B3	-0.09	0.10	0.00	0.02	-0.84	-0.10	0.19
SP-B4	-0.53	-0.19	-0.66	-0.22	-0.22	0.04	-0.05
SP-B5	0.54	0.05	0.02	-0.09	-0.19	0.70	-0.02
SP-B6	0.40	-0.22	0.35	-0.34	0.08	0.14	-0.44

Table 9: Pilot Study— Factor Analysis

4.6.4.3. Pilot Study - Discussion and Findings

Based on the results of the pilot study, of concern are the factors: IoT Security Technology Practices and IoT Security Behavioural Practices; these factors and their measures are captured in Table 10 and Table 11 below.

Upon evaluating, the SP-T1 variable proved to be an issue in the reliability testing. On face value it seems that the mention of "firewalls" may have been difficult for the pilot study respondents. And since the IoT Security Behavioural Practices construct failed reliability as well as validity testing, the variables were re-evaluated in preparation for the final study.

Variable	Statement
SP-T1	I make use of firewalls on my home IoT networks
SP-T2	I often check and apply security updates to the operating systems and critical applications on my IoT devices
SP-T3	I use forms of wireless encryption features on my IoT wireless connections

Table 10: Pilot Study–- IoT Security Technology Practices Questionnaire Statements

Variable	Statement
SP-B1	I store confidential information on my IoT devices
SP-B2	I reuse passwords for different IoT accounts
SP-B3	I share my IoT devices with others
SP-B4	I use a IoT password that is very difficult to guess such as a combination of upper and lower cases, symbols, and numbers
SP-B5	I lock my IoT device(s) with a PIN or password
SP-B6	I review security features of apps before installing them on my IoT device(s)

Table 11: Pilot Study–- IoT Security Behavioural Practices Questionnaire Statements

While the device experience construct met the required loadings for the reliability and validity testing carried out, the results were still relatively low in comparison to the other constructs with the Cronbach alpha coefficient at 0,66 and the factor loadings not proving representative of the construct. Based on these results, coupled with the feedback received in relation to IoT knowledge (as seen in Table 13), the device experience construct visible in Table 12 was re-evaluated in preparation for the final research study to account for the separate IoT device knowledge and IoT device experience constructs.

Variable	Statement
DE1	I have made use of IoT devices for more than 2 years.
DE2	I currently make use of 1 or more IoT devices.
DE3	I am an experienced IoT device user
DE4	I make use of all the features available on my IoT devices
DE5	I have strong IoT device literacy levels

Table 12: Pilot Study - Device Experience Questionnaire Statements

Pilot study respondents were also able to provide open text feedback to the survey. Of the feedback received, Table 13 contains the feedback provided by the survey respondents that were most useful in terms of the study that was conducted. Based on the feedback received, the final research survey was modified and improved (Al-Emran et al., 2018) to account for a greater age variance in the population, to provide a short definition of IoT and to ensure that the questionnaire/survey questions was clear and concise.

Due to the amount of pilot study survey respondents who expressed confusion and/or lack of knowledge in relation to IoT, the questionnaire was adjusted to be more specific around the types of IoT devices or engagement being investigated. The questionnaire was refined to emphasise specifically on Consumer IoT devices and engagement. Since the pilot study was carried out using snowball sampling of the researcher'' own networks and the final research study was to be conducted using Qualtrics panel with the defined sample being users of consumer IoT, it was expected that the respondents of the final research study would not experience the same issues as the pilot.

	Feedback
1	(1) "Why 45+ as upper age limit? Large population over 45. " (2) "Difference between practices and behaviour?"
2	"Didn't give definition of IoT and was confusing at first."
3	"Wish you gave a definition of IoT"
4	"The options for certain of the questions have too many options and therefore I'm uncertain which one to select at times"

Table 13: Pilot Study–- Respondent's feedback received

4.7. Data Collection Procedure

Qualtrics Panel was used to collect the desired sample of quantitative data to aid this research study (Qualtrics, 2022). According to the defined steps from the Qualtrics Panel Projects, the research questionnaire went through the following stages: Pre-launch, Soft Launch, Full Launch, Review and Approval (Qualtrics, 2022). Table 14 defines the Qualtrics panel project stages.

Panel Project Stages	
Pre-launch	Prior to fielding when confirmation and final survey logic is required.
Soft Launch	~10% of the sample size is collected and data is reviewed to identify any potential discrepancies.
Full Launch	Remaining sample is collected.
Review and Approval	Data collected and shared with researcher.

Table 14: Qualtrics Panel Projects Stages (Qualtrics, 2022)

4.8. Data Analysis Procedure

After successful data collection by means of the Qualtrics Panel Survey, the gathered data was exported into MS Excel for data clean up and initial analysis to be carried out. As part of the initial analysis the panel survey completion rate was analysed as well as the demographic split of the survey respondents and a summary provided.

Following the demographic analysis, descriptive statistics could be gathered relating to the data sample, and significant relationships realised through construct correlation testing. Once the initial analysis had been completed, Partial Least Squares (PLS) Structural Equation Modelling (SEM) (Bhattacherjee, 2012; Lowry & Gaskin, 2014) was used to analyse the data collected. Structural Equation Modelling (SEM) is a common statistical technique used in literature across disciplines and has also been used countless times in behavioural research fields, including information systems (Al-Emran et al., 2018; Hair et al., 2016; Lowry & Gaskin, 2014; Urbach & Ahlemann, 2010). The use of PLS-SEM to test the relationships between dependent and independent variables is supported and provides a great amount of value in the field of behavioural research by allowing complex model analysis with interpretations for both causal and consequent constructs (Hair et al., 2017). Based on

this, PLS-SEM analysis techniques were deemed appropriate for use to conduct the analysis of this study by making use of the SmartPLS 4 software (Ringle et al., 2022).

In order to carry out the PLS-SEM analysis, an outer model assessment, inner model assessment, as well as hypotheses testing, and path coefficient analysis needed to be conducted. As part of measuring the outer model findings: Internal consistency reliability assessment, construct reliability assessment, convergent validity test, and the discriminant validity test have been conducted. In order to measure the inner model findings, the coefficient of determination (R^2) and the goodness of fit tests are used. And lastly the hypotheses were verified using bootstrapping in SmartPLS 4 (Ringle et al., 2022) to test the model.

A summary of the tests carried out can be found in Table 15.

PLS-SEM Analysis Summary
Outer Model Assessment
Internal consistency reliability assessment
Construct reliability assessment
Convergent validity test
Discriminant validity test
Cross-loadings
Fornell-Larcker criterion
Hetrotrait-Monotrait ratio of correlation
Inner Model Assessment
Coefficient of determination
Goodness of fit
Hypothesis Testing and Path Coefficients

Table 15: PLS-SEM analysis testing summary

5. Research Analysis and Results

This section illustrates the data analysis techniques specified in section 4.10 Data Analysis. First, an overview is provided focusing on the participants of the research study and the scenario provided to them as well as the data controls and procedures put in place. The resultant completion rate of the research study is provided. Second, the demographic profiles of the research study respondents are provided, including their age, gender, and race distributions. Next, the statistical analysis of the study is conducted and validated.

5.1. Participants and Scenario

Approximately ~416 respondents were recruited across South Africa to take part in this research survey making use of the Qualtrics Online Panel. Table 16 illustrates the validating question that was presented at the beginning of the survey to ensure that the required demographic of consumer IoT device users were being recorded.

Following the Likert scale measurement, if the response to the question was “Disagree” or “Strongly Disagree,” the survey was automatically terminated in order to ensure the data collected would be representative of consumer IoT device users.

Appendix 8 demonstrates the summary of the results gathered by means of the Qualtrics survey.

State how strongly you agree or disagree with the following statement relating to consumer Internet of Things (IoT) usage	
1	I am aware of what a consumer Internet of Things (IoT) device is
2	I am a user/consumer of Consumer Internet of Things (IoT) devices

Table 16: Survey validating question

5.2. Data Controls and Procedures

In order to minimise bias or surveys being completed incorrectly, the respondents were assured of their anonymity (Menard et al., 2018). Whilst taking part in the survey, it was mandatory for the respondents to complete a question in order to move on to the next part of the survey, however, respondents were free to exit and stop the survey at any time. In accordance with quantitative Information Systems research carried out by Menard et al. (2018) and Behardien and Brown (2022), where incomplete surveys were encountered, responses were excluded deeming them to not be of high quality.

5.3. Completion Rate

Table 17 illustrates the completion rate of the online survey measuring the antecedents and consequences of consumer IoT security self-efficacy. A total of 416 respondents were reached via the Qualtrics panel. Of the total panel respondents reached, 55.288% of the surveys, which equate to 230 respondents, have been seen as valid and high-quality data that is used to conduct this research. 14.904% of the responses were culled during data collection due to low quality since the responses contained missing data or an incomplete survey. 22.837% of the survey respondents were terminated at the validating question as outlined in Section 5.1., and 6.971% of surveys were cut off and not used due to still being in progress at the survey end time.

	Number of survey respondents	
Total respondents reached	416	
Survey responses received – Total	**292**	
Valid survey responses – High quality data	230	55.288%
Invalid survey responses – Low quality/missing data	62	14.904%
Respondents terminated at validating question	95	22.837%
Surveys still in progress at cut off point (Incomplete)	29	6.971%
Survey respondents reached–- Total	**416**	**100%**

Table 17: Number of survey respondents

5.4. Demographic Profile

This section covers the demographic profile of the survey participants that contributed to the research data analysis.

5.4.1. Age Distribution

Figure 2 illustrates the age distribution of the survey responses used in this study. Majority of the respondents, who account for 35.65% of the responses, were made up of the 25- to 34-year-old category, a close second was the 18 -24-year-old category which made up 28.70% of respondents, 22.17% representing 35- to 44-year-olds, 11.30% representing 45- to 54-year-olds, 1.74% representing 55 – 64-year-olds and 0.43% representing 65-years and older.

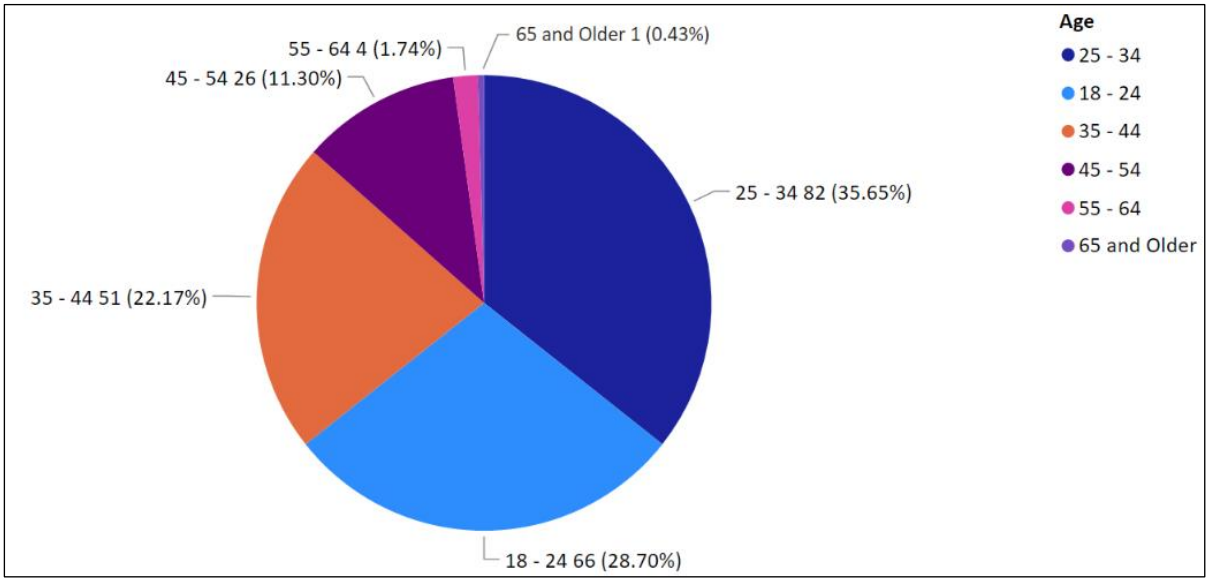

Figure 2: Survey responses–- Age distribution

5.4.2. Gender Distribution

Figure 3 illustrates the gender distribution of the survey responses used in this study. Majority of the respondents, who account for 57.39% of the responses, were made up of the Female category. 41.74% of respondents identified as Male, while 0.43% identified as non-binary/third gender and another 0.43% of respondents selected “Other” as their gender distribution.

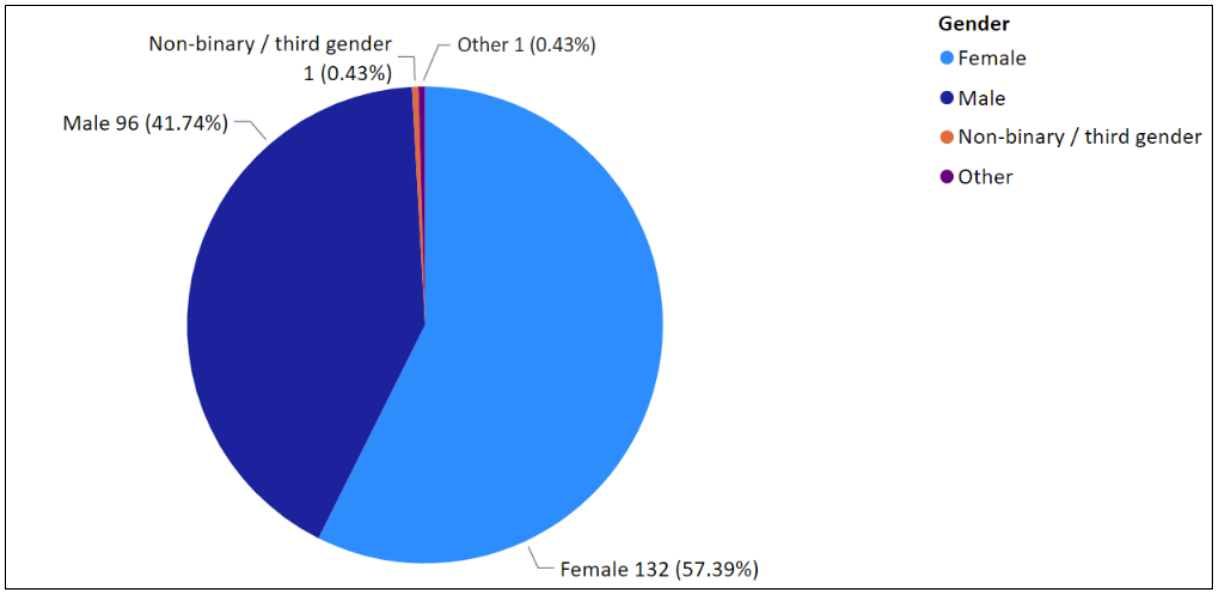

Figure 3: Survey responses–- Gender distribution

5.4.3. Race Distribution

Figure 4 illustrates the race distribution of the survey responses used in this study. The majority of the respondents, who account for 66.25% of the responses, were made up of the African race category. 15.65% identified as White, 12.17% as Coloured, 5.22% as Indian, and one survey respondent making up 0.43% selected "Other" and identified themselves as "Asian".

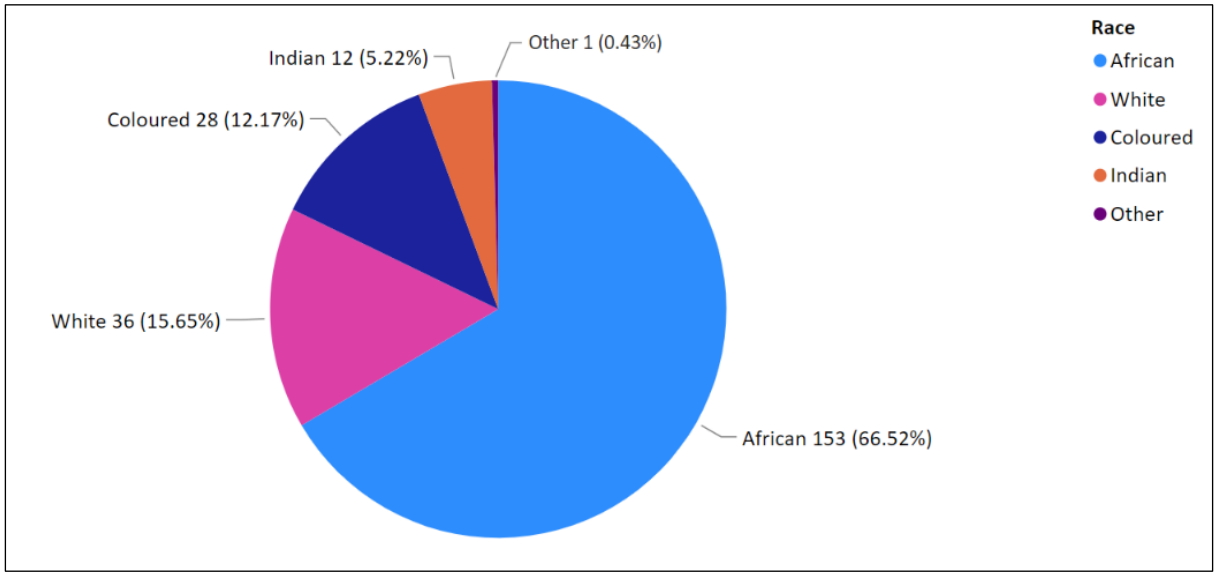

Figure 4: Survey responses - Race distribution

5.4.4. Demographic Profile Summary

A summary of the survey respondents' demographic profile is presented in Figure 5 and Table 18. The summary illustrates the respondents per age category, according to their gender and race split. This highlights majority of respondents falling into the categories of 25 -34 years old, being African and Female.

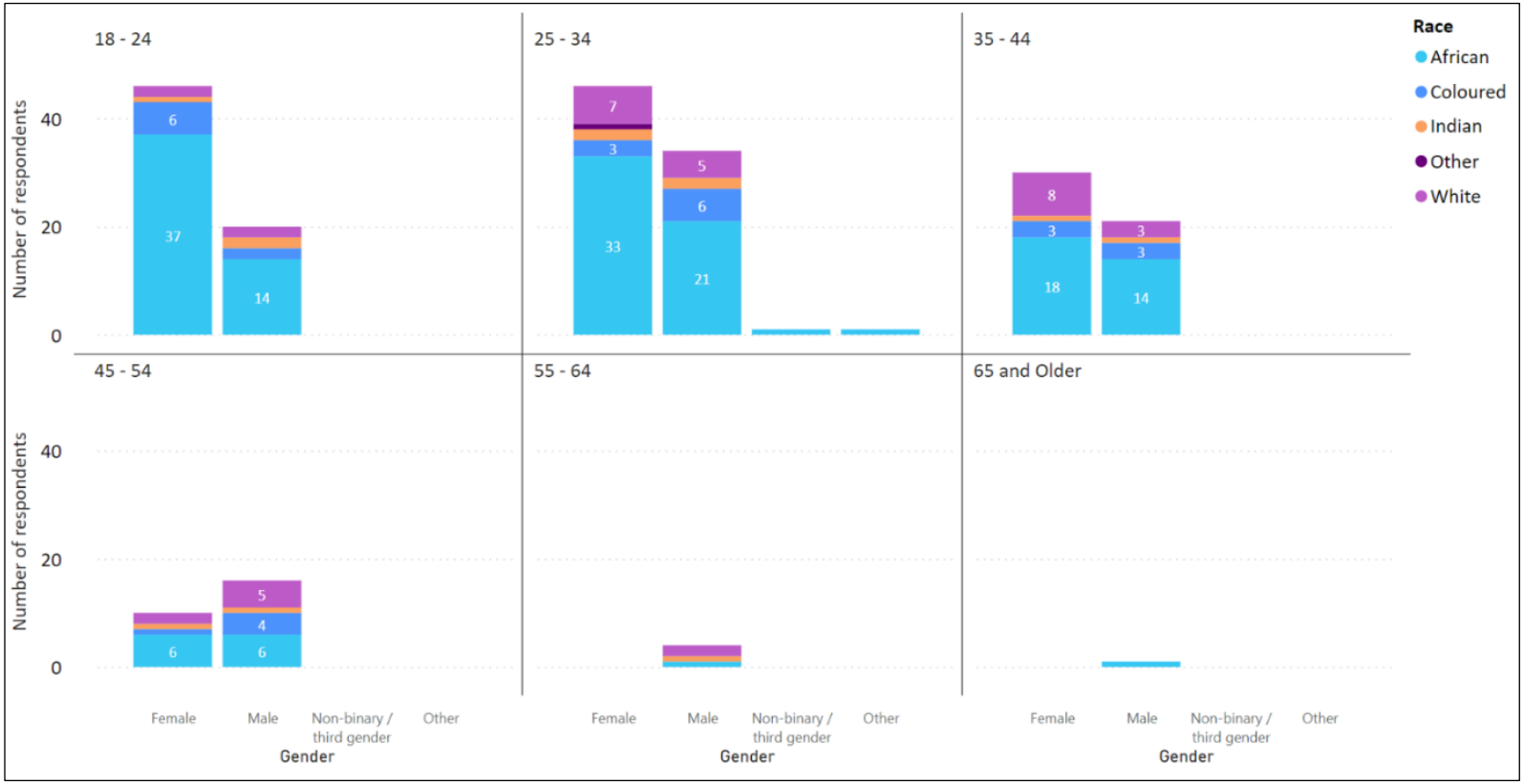

Figure 5: Survey responses - Demographic profile summary

Demographic	Variable	Number of respondents	Percentage
Age	**Under 18**	0	0.00%
	18 - 24	66	28.70%
	25 – 34	82	35.65%
	35 – 44	51	22.17%
	45 – 54	26	11.30%
	55 -64	4	1.74%
	65 and Older	1	0.43%
Gender	**Male**	96	41.74%
	Female	132	57.39%
	Non-binary/Third Gender	1	0.43%
	Prefer not to answer	0	0.00%
	Other	1	0.43%
Race	**African**	153	66.52%
	White	36	15.65%
	Coloured	28	12.117%
	Indian	12	5.22%
	Prefer not to answer	0	0.00%
	Other	1	0.43%

Table 18: Demographic profile summary

5.5. Statistical Analysis

As mentioned in Section 4.10, SEM analysis and SmartPLS 4 is used to conduct the statistical analysis in this study. To do so, the models' descriptive statistics will be evaluated. And, in order to be a valid quantitative study, the outer model and inner model assessment are completed. Once that is done, the hypothesis testing, and path coefficient analysis is conducted to determine the findings of this research. The graphical models generated using the SmartPLS 4 software (Ringle et al., 2022) are captured in Appendix 9.

5.5.1. Descriptive Statistics

Descriptive statistics are being used to allow for a further definition of the survey data distribution characteristics (Creswell 2009; Salkind, 2012). Included in the descriptive statistics are the Sample Mean, Sample Median, Sample Standard Deviation, Excess kurtosis, and Skewness (Al-Emran et al., 2018) among the factors identified for the study. The 8 factors include: IoT Security Behavioural Practices (SP-B), Behavioural Intention (BI), IoT Security Technology Practices (SP-T), IoT Security Self-Efficacy (ISSE), IoT Device Knowledge (CK), IoT Device Experience (DE), IoT Security Breach Incidents (SBI) and General Controllability (GC). Table 19 highlights the descriptive statistics derived from the research sample.

Based on the results gathered, within IoT device knowledge majority of the respondents attested to having and knowing where and how to get valuable knowledge relating to consumer IoT devices. Similarly, majority of the survey respondents indicated experience using consumer IoT devices and indicated strong consumer IoT device literacy. And majority of the respondents have indicated not having experience with security breaches while some indicate that they may have been targeted by incidents such as phishing.

Respondents of this study have also indicated that there exists means in which to control IoT threats and that they have the means to control consumer IoT threats in relation to their device(s). Majority of the survey respondents have a strong belief in their confidence to secure their IoT devices and deal with possible threats. Survey respondents have indicated that while they have a strong intention to enforce security practices and take steps to ensure information security, majority do employ the relevant security technology practices made available by the technology and they indicate employing security behavioural practices to ensure IoT device security.

	Mean	Median	Standard deviation	Excess kurtosis	Skewness	Count
CK1	2.026	2.000	0.796	0.082	0.577	230
CK2	2.117	2.000	0.854	-0.145	0.572	230
CK3	2.013	2.000	0.831	0.397	0.798	230
CK4	2.074	2.000	0.899	-0.295	0.613	230
DE1	2.087	2.000	0.974	-0.304	0.705	230
DE2	1.883	2.000	0.785	0.204	0.699	230
DE3	2.257	2.000	0.874	-0.294	0.378	230
DE4	2.148	2.000	0.906	-0.673	0.373	230
DE5	2.209	2.000	0.918	-0.493	0.387	230
SBI1	2.978	3.000	1.185	-1.080	-0.147	230
SBI2	3.383	4.000	1.184	-0.606	-0.620	230
SBI3	3.113	3.000	1.242	-1.097	-0.257	230
GC1	2.309	2.000	0.907	0.399	0.617	230
GC2	2.257	2.000	0.932	0.017	0.504	230
GC3	2.087	2.000	0.814	0.617	0.619	230
GC4	2.452	2.000	1.057	-0.563	0.327	230
GC5	2.326	2.000	1.001	-0.367	0.539	230
GC6	2.196	2.000	0.909	0.004	0.615	230
GC7	2.143	2.000	0.855	-0.108	0.475	230
ISSE1	1.965	2.000	0.812	1.100	0.848	230
ISSE2	2.104	2.000	0.869	0.500	0.758	230
ISSE3	1.991	2.000	0.813	0.984	0.798	230
ISSE4	1.917	2.000	0.790	0.805	0.788	230
ISSE5	1.943	2.000	0.824	0.992	0.856	230
ISSE6	2.204	2.000	0.936	-0.269	0.510	230
ISSE7	2.004	2.000	0.852	0.578	0.756	230
SP-T1	2.209	2.000	0.894	-0.081	0.494	230
SP-T2	2.039	2.000	0.861	0.515	0.746	230
SP-T3	2.204	2.000	0.922	-0.465	0.421	230
BI1	1.874	2.000	0.795	0.718	0.805	230
BI2	1.835	2.000	0.757	0.628	0.710	230
BI3	2.143	2.000	0.961	0.061	0.656	230

	Mean	Median	Standard deviation	Excess kurtosis	Skewness	Count
BI4	1.700	2.000	0.686	1.191	0.795	230
SP-B1	2.443	2.000	1.117	-0.591	0.454	230
SP-B2	1.683	2.000	0.785	1.691	1.224	230
SP-B3	1.700	2.000	0.819	1.260	1.179	230
SP-B4	1.848	2.000	0.913	1.022	1.101	230
SP-B5	1.743	2.000	0.813	1.582	1.140	230
SP-B6	1.883	2.000	0.899	0.509	0.921	230

Table 19: Descriptive statistics

5.5.1.1. Construct Correlation

The correlation between the constructs being tested in the research study can be found in Appendix 6. In the appendix, significant relationships are highlighted in green where the correlation co-efficient is greater than 0.50.

The results show significant relationships across the research constructs. These relationships are summarised in Table 20.

	BI	CK	DE	GC	ISSE	SBI	SP-B	SP-T
Behavioural Intention	X			X	X			X
Consumer IoT Knowledge		X						
Consumer IoT Device Experience		X	X					
General Controllability		X	X	X				
IoT Security Self-Efficacy		X	X	X	X			
Security Breach Incidents			X			X		
IoT Security Behavioural Practices	X						X	
IoT Security Technology Practices				X	X			X

Table 20: Summary - Instrument correlation

5.5.2. Outer Model Assessment

The outer model assessment looks at the relationship and internal consistency between the independent variables and their constructs, this assessment is also proved by Hair et al. (2017) to be a valid test for quantitative studies. The following tests have been conducted in order to determine the outer model findings: Internal consistency reliability assessment, construct reliability assessment, convergent validity test, and the discriminant validity test (Hair et al., 2014; Hair et al., 2017).

5.5.2.1. Internal Consistency Reliability Assessment

It is important to measure the consistency of the construct items, the internal consistency reliability assessment aims to evaluate how well each measure within the research instrument represents its construct (Hair et al., 2014; Hair et al., 2017). Measuring the reliability of the instrument is related to the quality of the measurement. The instrument can be determined as reliable if it yields the same result through multiple iterations (Salkind, 2012; Venkatesh et al., 2013). Instrument reliability is seen as a prerequisite for instrument validity because without reliable results the research study is deemed invalid (Al-Emran et al., 2018; Venkatesh et al., 2013). This internal consistency is assessed in this study by observing the Cronbach Alpha coefficient and the Dillon-Goldstein's values (rho_A).

In order to measure how unified, the instruments are in the test, this research makes use of internal consistency reliability (Salkind, 2012), which is evaluated by the Cronbach's alpha correlation coefficient. The Cronbach alpha correlation coefficient is a widely recognised and used reliability measure in the area of social sciences. The correlation coefficients are deemed reliable where they are greater than or equal to 0.70 (Al-Emran et al., 2018; Bonett & Wright, 2015; Hair et al., 2013; Hair et al., 2014), therefore, according to the assessment captured in Table 19, the constructs are seen as reliable with the lowest Cronbach Alpha Coefficient being IoT Security Technology Practices with a value of 0.787.

For the composite reliability measure using the Dillon-Goldstein (rho_A) values, acceptable values are greater than 0.70 (Hair et al., 2014; Hair et al., 2017). According to the assessment captured in Table 21, the lowest rho_A value is IoT Security Technology Practices at 0.789. Therefore, all measured constructs are seen as consistent with each other and have passed the internal consistency reliability test using the rho_A.

Based on Table 21 and the analysis above, the Cronbach alpha coefficient and the Dillon-Goldstein values (rho_A) indicates that the constructs have high internal consistency and are reliable measures. The results illustrate that the study carried out was of quality and yielded reliable results.

	Cronbach's Alpha Coefficient	Dillon-Goldstein (rho_A)
Behavioural Intention	0.839	0.844
Consumer IoT Knowledge	0.895	0.895
Consumer IoT Device Experience	0.877	0.881
General Controllability	0.889	0.892
IoT Security Self-Efficacy	0.907	0.908
Security Breach Incidents	0.805	0.975
IoT Security Behavioural Practices	0.829	0.838
IoT Security Technology Practices	0.787	0.789

Table 21: Internal consistency reliability assessment

5.5.2.2. Construct Reliability Assessment

In Information Systems research, it is necessary for the study design and analysis to be validated (Venkatesh et al., 2013). Instrument validity testing ensures that the instrument being used measure the constructs that need to be measured and ensures the legitimacy of the findings (Al-Emran et al., 2018; Salkind, 2012; Venkatesh et al., 2013). The construct reliability assessment aims to evaluate the relationship between the measures of each construct to each other and the manner in which they are related to the measures or items of the other constructs. The construct reliability assessment was carried out by observing the outer factor loadings. Construct items are seen as reliable where the factor loadings are greater than 0.70 (Hair et al., 2014).

Table 22 illustrates the final factor loadings analysis; iterations of the analysis can be found in Appendix 7. The results show the measures for each construct are truly representative. Following the factor analysis, the refined item constructs are displayed in Table 23.

	BI	CK	DE	GC	ISSE	SBI	SP-B	SP-T
BI1	0.86							
BI2	0.84							
BI3	0.75							
BI4	0.82							
CK1		0.88						
CK2		0.89						
CK3		0.85						
CK4		0.87						
DE1			0.76					
DE2			0.78					
DE3			0.86					
DE4			0.83					
DE5			0.87					
GC1				0.73				
GC2				0.71				
GC3				0.76				
GC4				0.82				
GC5				0.79				
GC6				0.81				
GC7				0.81				
ISSE1					0.79			
ISSE2					0.77			
ISSE3					0.77			
ISSE4					0.80			
ISSE5					0.86			
ISSE6					0.78			
ISSE7					0.84			
SBI1						0.90		
SBI2						0.81		
SBI3						0.79		
SP-B2							0.84	
SP-B3							0.79	
SP-B4							0.77	

	BI	CK	DE	GC	ISSE	SBI	SP-B	SP-T
SP-B5							0.72	
SP-B6							0.73	
SP-T1								0.84
SP-T2								0.86
SP-T3								0.81

Table 22: Construct reliability assessment - Factor analysis

Measure	Identifier	Statement
Consumer IoT Device Knowledge	CK1	I have valuable knowledge relating to various consumer IoT devices
	CK2	I have valuable knowledge relating to the software and applications available on consumer IoT devices
	CK3	I have valuable knowledge in how to make use of the various applications and uses of consumer IoT devices
	CK4	I know where to get additional valuable information regarding consumer IoT devices
Consumer IoT Device Experience	DE1	I have made use of IoT devices for more than 2 years.
	DE2	I currently make use of 1 or more IoT devices.
	DE3	I am an experienced IoT device user
	DE4	I make use of all the features available on my IoT devices
	DE5	I have strong IoT device literacy levels
IoT Security Breach Incidents	SBI1	I have experienced a security breach with IoT
	SBI2	I have fallen victim to cyber fraud with IoT
	SBI3	I have experienced phishing attacks with IoT
Consumer IoT General Controllability	GC1	Threats to IoT security are controllable
	GC2	IoT is advanced enough to prevent security threats
	GC3	There exist means to control IoT security threats
	GC4	I have the means to control IoT security threats
	GC5	I have the ability to execute IoT security practices to avoid security threats
	GC6	I have access to the necessary resources to protect my IoT devices

Measure	Identifier	Statement
	GC7	I can exercise a course of action to avoid an IoT security breach
Consumer IoT Security Self-Efficacy	ISSE1	I feel confident managing security on my IoT devices
	ISSE2	I have the necessary knowledge and skills to protect my IoT device
	ISSE3	I feel confident getting help for problems related to my IoT security
	ISSE4	I feel confident learning the method to protect my information and IoT device
	ISSE5	I feel confident updating security to the IoT operating system
	ISSE6	I am confident in my ability to protect my IoT device(s) from hackers
	ISSE7	I am confident and at ease in adopting IoT device protection
Consumer IoT Security Technology Practices	SP-T1	I employ security protocols on my IoT networks
	SP-T2	I often check and apply security updates to the operating systems and critical applications on my IoT devices
	SP-T3	I use forms of wireless encryption features on my IoT wireless connections
Behavioural Intention	BI1	I intend to enforce stronger IoT security procedures
	BI2	I intend to add additional security measures to protect my information and my IoT devices
	BI3	I intend to buy more software to mitigate impacts of IoT information security breaches
	BI4	I intend to learn more about how to strengthen my IoT information security
IoT Security Behavioural Practices	SP-B2	I lock my IoT device(s) with a PIN or password
	SP-B3	I use a IoT password that is very difficult to guess such as a combination of upper and lower cases, symbols, and numbers
	SP-B4	I make use of unique passwords for different IoT devices or applications

Measure	Identifier	Statement
	SP-B5	I do not share my IoT devices with others
	SP-B6	I review security features of apps before installing them on my IoT device(s)

Table 23: Refined item constructs

5.5.2.3. Convergent Validity Test

The convergent validity test aims to test the relationship between the measures and the manner in which they represent their construct (Hair et al., 2014). Average Variance Extracted (AVE) and Composite Reliability (CR) are measured and observed in order to establish convergent validity. Convergent validity is established when the measure of two constructs corresponds to each other (Hair et al., 2014).

AVE assesses the resultant variance of the construct's actual variance, based on the influence that the measurement error has on the value. A sufficient convergent validity is observed where the average variance extracted is greater than or equal to 0.50 (Hair et al., 2014). In this study, the lowest observed AVE is noted for IoT security behavioural practices, with an AVE value of 0.595. It is also recommended to assess composite reliability (CR) when making use of structural equation modelling, it determines how well the items of the construct correlate within the construct. Convergent reliability is seen to be established where composite reliability values are greater than or equal to 0.70 (Hair et al., 2014). In this study, the lowest CR value is observed for Security Breach Incidents, where the CR value is 0.875.

Based on Table 24 and the analysis above, the average variance extracted, and the composite reliability observed it is determined that convergent validity does exist within the model for this research study.

	Average variance extracted (AVE)	Composite reliability (CR)
Behavioural Intention	0.675	0.892
Consumer IoT Knowledge	0.760	0.927
Consumer IoT Device Experience	0.672	0.911
General Controllability	0.601	0.913
IoT Security Self-Efficacy	0.642	0.926
Security Breach Incidents	0.700	0.875
IoT Security Behavioural Practices	0.595	0.880
IoT Security Technology Practices	0.701	0.876

Table 24: Convergent validity assessment

5.5.2.4. Discriminant Validity Test

The discriminant validity test aims to determine the degree to which the different constructs of the model are not related. It is used to ensure that there is no relationship with the different constructs that are not meant to have a relationship (Hair et al., 2014). This is to ensure that each construct being measured represents a unique factor that would then impact the dependent constructs. The assessment of cross loadings, the Fornell-Larcker criterion, and the Hetrotrait-Monotrait (HTMT) were conducted in order to determine the result of discriminant validity for this study.

5.5.2.4.1. Cross-loadings

Discriminant validity is assessed using cross loadings by expecting items of a construct to load together with higher values on their own construct than they do on other constructs (Hair et al., 2014). Table 25 illustrates the cross-loadings for the constructs of this study, based on this, it is observed that the item constructs loaded at a higher value under their own measurement construct.

	BI	CK	DE	GC	ISSE	SBI	SP-B	SP-T
BI1	**0.863**	0.420	0.455	0.528	0.529	0.201	0.571	0.559
BI2	**0.843**	0.426	0.426	0.483	0.545	0.233	0.502	0.534

	BI	CK	DE	GC	ISSE	SBI	SP-B	SP-T
BI3	**0.753**	0.458	0.515	0.524	0.497	0.273	0.432	0.517
BI4	**0.823**	0.460	0.398	0.442	0.533	0.125	0.583	0.469
CK1	0.516	**0.880**	0.700	0.508	0.527	0.359	0.412	0.532
CK2	0.480	**0.892**	0.667	0.493	0.554	0.426	0.464	0.529
CK3	0.410	**0.846**	0.559	0.508	0.551	0.319	0.439	0.495
CK4	0.462	**0.869**	0.668	0.523	0.563	0.357	0.437	0.559
DE1	0.417	0.494	**0.757**	0.486	0.513	0.332	0.358	0.438
DE2	0.494	0.573	**0.781**	0.458	0.492	0.304	0.454	0.499
DE3	0.395	0.645	**0.857**	0.604	0.559	0.376	0.382	0.616
DE4	0.452	0.593	**0.833**	0.565	0.527	0.409	0.423	0.579
DE5	0.468	0.727	**0.867**	0.601	0.588	0.454	0.468	0.572
GC1	0.376	0.313	0.354	**0.728**	0.581	0.281	0.383	0.400
GC2	0.403	0.320	0.370	**0.708**	0.562	0.202	0.287	0.372
GC3	0.477	0.463	0.526	**0.757**	0.599	0.298	0.424	0.567
GC4	0.439	0.531	0.595	**0.815**	0.611	0.428	0.348	0.584
GC5	0.514	0.558	0.635	**0.794**	0.637	0.394	0.452	0.632
GC6	0.471	0.438	0.553	**0.806**	0.659	0.320	0.470	0.614
GC7	0.552	0.517	0.550	**0.810**	0.690	0.291	0.503	0.611
ISSE1	0.494	0.471	0.507	0.649	**0.788**	0.317	0.432	0.508
ISSE2	0.457	0.531	0.562	0.681	**0.769**	0.366	0.461	0.561
ISSE3	0.480	0.403	0.452	0.580	**0.767**	0.263	0.525	0.433
ISSE4	0.587	0.520	0.570	0.585	**0.800**	0.278	0.543	0.488
ISSE5	0.535	0.526	0.546	0.646	**0.857**	0.221	0.530	0.551
ISSE6	0.467	0.493	0.483	0.698	**0.780**	0.286	0.434	0.555
ISSE7	0.565	0.574	0.546	0.657	**0.844**	0.274	0.511	0.591
SBI1	0.262	0.455	0.472	0.435	0.406	**0.902**	0.216	0.394
SBI2	0.138	0.244	0.283	0.250	0.186	**0.812**	0.069	0.250
SBI3	0.182	0.271	0.337	0.270	0.213	**0.791**	0.125	0.325
SP-B2	0.577	0.442	0.489	0.436	0.525	0.177	**0.844**	0.491
SP-B3	0.476	0.422	0.380	0.420	0.478	0.147	**0.786**	0.454
SP-B4	0.484	0.356	0.383	0.343	0.405	0.179	**0.767**	0.375
SP-B5	0.410	0.262	0.316	0.360	0.423	0.075	**0.720**	0.308
SP-B6	0.499	0.430	0.370	0.481	0.515	0.125	**0.734**	0.428

	BI	CK	DE	GC	ISSE	SBI	SP-B	SP-T
SP-T1	0.533	0.518	0.557	0.561	0.511	0.354	0.445	**0.840**
SP-T2	0.585	0.527	0.537	0.594	0.584	0.269	0.483	**0.861**
SP-T3	0.465	0.479	0.570	0.609	0.558	0.395	0.427	**0.811**

Table 25: Cross loadings

5.5.2.4.2. Fornell-Larcker Criterion

The Fornell-Larcker criterion tests the discriminant validity by checking each construct and ensuring that their squared correlation is greater than those same constructs squared correlation value in relation to other constructs (Fornell & Larcker, 1981; Hair et al., 2017).

Results from the Fornell-Larcker criterion test are shown in Table 26. According to the results observed, all the constructs passed the test apart from those highlighted in red i.e., General Controllability (GC) whose squared correlation of 0.775 is less than their squared correlation in relation to IoT Security Self-efficacy (ISSE) of 0.802. Similarly, the ISSE squared correlation of 0.801 is less than the 0.802 correlation of GC and ISSE. Therefore, GC and ISSE do not pass the Fornell-Larcker criterion.

	BI	CK	DE	GC	ISSE	SBI	SP-B	SP-T
BI	**0.822**							
CK	0.535	**0.872**						
DE	0.542	0.744	**0.820**					
GC	0.599	0.583	0.665	**0.775**				
ISSE	0.640	0.630	0.655	0.802	**0.801**			
SBI	0.249	0.420	0.460	0.409	0.357	**0.837**		
SP-B	0.639	0.503	0.508	0.533	0.612	0.185	**0.771**	
SP-T	0.631	0.607	0.662	0.703	0.659	0.402	0.540	**0.837**

Table 26: Fornell-Larcker criterion

5.5.2.4.3. Hetrotrait-Monotrait (HTMT) Ratio of Correlations

Another method to ensure the discriminant validity testing is to use the Hetrotrait-Monotrait (HTMT) ratio of correlations (Henseler et al., 2014).

Table 27 and Table 28 illustrates the results of the HTMT test carried out in a matrix as well as a list form. Discriminant validity is established where the HTMT values are less than 0.90. Based on the results and the establishment criteria for HTMT, discriminant validity is established.

	BI	CK	DE	GC	ISSE	SBI	SP-B	SP-T
BI								
CK	0.621							
DE	0.639	0.836						
GC	0.694	0.649	0.746					
ISSE	0.734	0.696	0.732	0.892				
SBI	0.283	0.449	0.508	0.443	0.371			
SP-B	0.757	0.575	0.591	0.612	0.702	0.198		
SP-T	0.778	0.723	0.796	0.834	0.777	0.482	0.659	

Table 27: Hetrotrait-Monotrait (HTMT) ratio of correlations

	Heterotrait-monotrait ratio (HTMT)
CK -> BI	0.621
DE -> BI	0.639
DE -> CK	0.836
GC -> BI	0.694
GC -> CK	0.649
GC -> DE	0.746
ISSE -> BI	0.734
ISSE -> CK	0.696
ISSE -> DE	0.732
ISSE -> GC	0.892
SBI -> BI	0.283

	Heterotrait-monotrait ratio (HTMT)
SBI -> CK	0.449
SBI -> DE	0.508
SBI -> GC	0.443
SBI -> ISSE	0.371
SP-B -> BI	0.757
SP-B -> CK	0.575
SP-B -> DE	0.591
SP-B -> GC	0.612
SP-B -> ISSE	0.702
SP-B -> SBI	0.198
SP-T -> BI	0.778
SP-T -> CK	0.723
SP-T -> DE	0.796
SP-T -> GC	0.834
SP-T -> ISSE	0.777
SP-T -> SBI	0.482
SP-T -> SP-B	0.659

Table 28: Heterotrait-Monotrait ratio (HTMT) List

In order to complete the outer model assessment, the tests conducted included the internal consistency reliability assessment, the construct reliability assessment, the convergent validity test, and the discriminant validity tests. Upon completion of the various tests, all assessments were seen to be successful, apart from the Fornell-Larcker criterion test carried out for discriminant validity testing. Since Henseler et al. (2014) advised Fornell-Larcker criterion has not been able to accurately detect discriminant validity in other studies, the outer model of this research study is considered to be statistically significant.

5.5.3. Inner Model Assessment

The inner model assessment focuses on the relationship between the dependent and independent variables. This enabled the research to answer the related questions through hypothesis testing

(Hair et al., 2013). The inner model of the conceptual model identified to assess the antecedents and consequences of internet of things security self-efficacy is statistically tested using the coefficient of determination (R^2) and the goodness of fit tests.

5.5.3.1. Coefficient of Determination (R^2)

The coefficient of determination (R^2) assesses the hypothesized relationships of the inner model (Hair et al., 2017). R^2 predicts the variability of latent variables and how the variation in different latent variables can explain that variability (Hair et al., 2014). Table 29 contains the results of the coefficient of determination (R^2) test for the dependent variables behavioural intention, IoT security self-efficacy, IoT security behavioural practice, and IoT security technology practices.

The R^2 value is expected to be between 0 and 1, and a R^2 measure that is closer to 1 is expected to be a more accurate predictor of variability (Hair et al., 2017). Hair et al. (2014) categorises the coefficient of determination values as follows: where R^2 is less than 0.190, the measure is considered weak; where R^2 is between 0.333 and 0.670, the measure is considered moderately accurate; and where the R^2 value is greater than 0.670, the measure is seen to be a perfectly accurate predictor of variability.

Based on the results in Table 29, the dependant variable IoT Security Self-efficacy is a perfectly accurate predictor of variability with a R^2 value of 0.687. The dependant variables Behavioural Intention (R^2 = 0.410), IoT Security Behavioural Practices (R^2 = 0.483), and IoT Security Technology Practices (R^2 = 0.435) are seen to be moderately accurate predictors of variability with the R^2 values being between 0.333 and 0.670. Therefore, the results show that the dependant variables are proved to be predictable from the various independent variables.

	Coefficient of determination (R^2)
Behavioural Intention	0.410
IoT Security Self-efficacy	0.687
IoT Security Behavioural Practice	0.483
IoT Security Technology Practice	0.435

Table 29: Coefficient of determination

5.5.3.2. Goodness of Fit of the Model

The goodness of fit test is used in this research study to determine the best fit of the inner model. In order to execute the goodness of fit test, the Standardised Root Mean Square Residual (SRMR) is explained by the difference between the observed correlation matrix and the expected correlation matrix (Hair et al., 2017). SRMR is observed to assess the differences between the observed correlations and the expected correlation as an average (Hair et al., 2017). The recommended or expected value for the SRMR is less than 0.08 to define a good fit for the model (Hair et al., 2017; Henseler et al., 2014).

Table 30 shows the results of the SRMR test carried out using SmartPLS 4. The SRMR for this research study has a value of 0.064 which meets the criteria of being less than 0.08, therefore, the data used for this research study fits well with the conceptual model.

	Saturated model
Standardised Root Mean Square Residual (SRMR)	0.064

Table 30: Standardised Root Mean Square Residual (SRMR)

Following the inner model assessments conducted, including the coefficient of determination (R^2) and the model goodness of fit, all the tests were seen to be successful. Therefore, the inner model of this research study is considered to be statistically significant.

5.5.4. Hypotheses Testing and Path Coefficients

This study makes use of hypothesis testing and path coefficient analysis to test the research question (Roky & Al-Meriouh, 2015). The hypotheses developed as part of evaluating this research study are referenced and described in section 3. Hypothesis Development.

Based on the detailed hypotheses, Consumer IoT Security Self-Efficacy is the dependent variable to be tested against the independent variables Consumer IoT Device Knowledge, Consumer IoT Device Experience, IoT Security Breach Incidents and Consumer IoT General Controllability. In addition to this, Consumer IoT Security Self-Efficacy is seen as the independent variable contributing to the dependent variables IoT Security Technology Practices, Behavioural Intention, and IoT Security Behavioural Practices. IoT Security Technology Practices and Behavioural Intent are also tested as variables contributing to IoT Security Behavioural Practices.

Structural Equation Modelling (SEM) is used to test the relationships between the latent variables, and to determine the antecedents and consequences of IoT security self-efficacy, significance tests are performed to between each of the variables. In order to test the hypotheses, the bootstrapping method was used in SmartPLS 4 (Ringle et al., 2022) to assess the model.

Path coefficients were observed to determine the relationships between the latent variables. In order to perform the relevant statistical tests, the relationships between the latent variables are defined as paths and the path coefficient relates to the measure of significance on the latent variables' relationship (Cangur & Ercan, 2015). Where the value of the path coefficient is greater than 0.2, the coefficient is deemed significant for research following quantitative analysis (Cangur & Ercan, 2015). It is expected that a good significance value is based on the t-values and the corresponding p-values. This means that where p-values are less than 0.05, the corresponding t-value would need to be more significant than 1.95, 1.96 or greater. And if the p-value is less than 0.001, the corresponding t-value would need to be greater than or equal to 3.29 in order to be significant. If the p-values are less than or equal to 0.001, the relationship is deemed highly significant and when the p-values are less than or equal to 0.01, the relationship between latent variables are significant. Where the p-values are greater than 0.05, that means the relationship is insignificant (Hair et al., 2014; Hair et al., 2017; Roky & Al-Meriouh, 2015).

The results of the hypothesis testing can be found in Table 31. The results illustrate five of the nine hypotheses being accepted where their p-values are less than 0.001 and the corresponding t-values are greater than equal to 3.29. And one of the nine hypotheses being accepted where their p-value

is less than 0.01 and the corresponding t-value is greater than 1.95. The hypotheses and their findings are further described in section 5.6. Discussion and Findings.

Hypothesis	Relationship	Path Coefficient	Std Deviation	T-Values	P-Values	Supported
H1	BI -> SP-B	0.384	0.072	5.320	0.000	✓
H2	SP-T -> SP-B	0.098	0.061	1.615	0.106	✗
H3	ISSE -> BI	0.640	0.054	11.912	0.000	✓
H4	ISSE -> SP-T	0.660	0.043	15.238	0.000	✓
H5	ISSE -> SP-B	0.303	0.077	3.893	0.000	✓
H6	CK -> ISSE	0.198	0.065	3.073	0.002	✓
H7	DE -> ISSE	0.103	0.067	1.502	0.133	✗
H8	SBI -> ISSE	-0.032	0.037	0.886	0.376	✗
H9	GC -> ISSE	0.632	0.067	9.475	0.000	✓

Table 31: Hypothesis testing and path coefficient results

5.6. Discussion and Findings

This section focuses on the findings from the research analysis, which are discussed and interpreted against the defined hypothesis. According to the statistical analysis carried out testing the inner model by assessing the internal consistency reliability, the construct reliability, the convergent validity, and the discriminant validity, as well as the outer model by assessing the model's coefficient of determination (R^2) and goodness of fit; the model used for this research study is seen to be statistically significant. Following the analysis, the research study can be assumed to be accurate determinants of the antecedents and consequences of IoT security self-efficacy (Hair et al., 2014).

5.6.1. Behavioural Intention (BI)

In this study, behavioural intention (BI) refers to the consumer IoT device user's intention for use and persistence with IoT security. It can be expected that the user's behavioural intention can affect their future IoT security behavioural practices. The effects of behavioural intention on IoT security behavioural practices are tested with the following hypothesis and illustrated in Figure 6:

H1: *Behavioural intention positively influences IoT security behavioural practices*

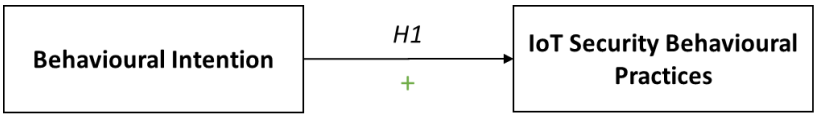

Figure 6: Hypothesis 1 - BI

From the results of the hypothesis testing, the positive relationship expected between the effects of behavioural intention and IoT security behavioural practices is supported, which is aligned to previous studies conducted by Das and Khan (2016) and Rhee et al. (2009). H1 is supported based on the path coefficient of 0.384 being greater than the required 0.2 or more, therefore, the BI -> SP-B relationship is deemed to be statistically significant (Cangur & Ercan, 2015). A favourable p-value of 0.000 and t-value of 5.320, demonstrates the significance of this relationship in accordance with Hair

et al. (2014; 2017) and Roky and Al-Meriouh (2015) who specify that where the p-value is less than 0.001 and the corresponding t-value is greater than 3.29, the relationship is deemed significant. Consequently, hypothesis 1 is supported.

5.6.2. IoT Security Technology Practices (SP-T)

In this study, IoT security technology practices refer to the practices put in place by the user on their consumer IoT devices. It is expected that users of consumer IoT devices with who employ IoT security technology practices eventually display more secure consumer IoT security behavioural practices. The effects of IoT security technology practices on IoT security behavioural practices is tested in this study through the following hypothesis and illustrated in Figure 7:

H2: *IoT security technology practices positively influence IoT security behavioural practices.*

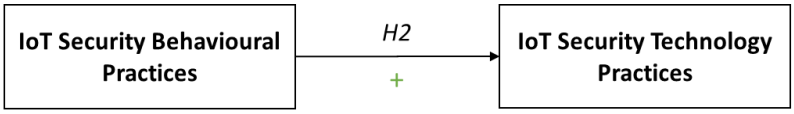

Figure 7: Hypothesis 2 – SP-T

According to studies carried out by Goodreau (2021), Lee et al. (2019) and Rhee et al. (2009), a positive relationship is expected between IoT security technology practices and IoT security behavioural practices, which expects users who display positive IoT security technology practices to display positive IoT security behavioural practices. Based on the results found in this study, hypothesis 2 is not supported according to the hypothesis testing carried out. The results of the hypothesis testing do not align with the previous studies carried out relating to the relationship between IoT security technology practices and IoT security behavioural practices.

H2 is not supported based on the path coefficient for this hypothesis being 0.098, which is below the required value of 0.2, thus the relationship, SP-T -> SP-B, is deemed to be insignificant statistically (Cangur & Ercan, 2015). In support of this finding, the p-value of this relationship is 0.106 and the t-value is 1.615, which shows that the insignificant p-value is accompanied by an insignificant t-value.

Since the p-value is greater than 0.001 and the corresponding t-value is less than 3.29, the relationship is seen to be insignificant. This also proves true according to the criteria where p-values are less than 0.05, the corresponding t-value would need to be more significant than 1.95, 1.96 or greater (Hair et al., 2014; Hair et al., 2017; Roky & Al-Meriouh, 2015). Therefore, hypothesis 2 is rejected.

Possible conjecture as to why H2 was rejected in this study and does not align to previous research relating to the relationship between IoT security technology practices and IoT security behavioural practices could be due to methodological issues, measurement issues, or missing conceptual elements, however these options do not appear feasible for the research conducted. In reviewing the research instrument, which can be referred to in Appendix 4, and comparing the constructs for IoT security technology practices and IoT security behavioural practices, possible reasons for the rejected H2 may be due to the fact that respondents align with the behavioural practices regardless of whether they employ the technology practices. The alternative would possibly be that respondents who consider having completed the technology related practices would deem those actions to be enough, therefore not employing the behavioural security practices.

5.6.3. Consumer IoT Security Self-efficacy (ISSE)

In this study, consumer IoT security self-efficacy refers to the belief in one's capability to protect information systems and their information from threats. IoT device users perceived ability to take precautions to ensure information security determines the amount of effort and persistence taken in the face of information security threats. It is expected that users of consumer IoT devices with a greater consumer IoT security self-efficacy belief would adopt more secure IoT security technology practices and display more secure consumer IoT security behavioural intentions and security behavioural practices. The consequences of consumer IoT security self-efficacy is tested through hypotheses 3, 4 and 5. These hypotheses are illustrated in Figure 8: Hypothesis 3 - ISSE, Figure 9: Hypothesis 4 – ISSE, and Figure 10: Hypothesis 5 - ISSE.

Hypothesis 3 is stated as:

H3: *Consumer IoT security self-efficacy positively influences behavioural intention.*

Figure 8: Hypothesis 3 - ISSE

Based on the results of the hypothesis testing, the positive relationship expected between the effects of consumer IoT security self-efficacy and behavioural intention is accepted. Therefore, the results of the hypothesis testing carried out for this study aligns to previous work by Rhee et al. (2009) and Zhou et al. (2020).

H3 is supported based on the path coefficient of 0.640 being greater than the required 0.2 or more, therefore, the relationship ISSE -> BI is deemed to be statistically significant (Cangur & Ercan, 2015). A favourable p-value of 0.000 and t-value of 11.912, proves the significance of this relationship where the p-value is less than 0.001 and the corresponding t-value is greater than 3.29, the relationship is deemed significant (Hair et al., 2014; Hair et al., 2017; Roky & Al-Meriouh, 2015). Therefore, hypothesis 3 is supported, proving that consumer IoT security self-efficacy positively effects behavioural intention.

Hypothesis 4 is stated as:

H4: *Consumer IoT security self-efficacy positively influences IoT security technology practices.*

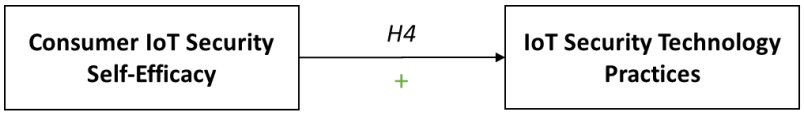

Figure 9: Hypothesis 4 – ISSE

From the results of the hypothesis testing, the positive relationship expected from the effects of consumer IoT security self-efficacy on IoT security technology practices is accepted. The accepted hypothesis aligns with previous studies by Rhee et al. (2009) as well as with Zhou et al. (2020).

H4 is supported since the path coefficient of 0.660 is greater than the required path coefficient of 0.2 or more, thus, the relationship ISSE -> SP-T is proven to be statistically significant (Cangur &

Ercan, 2015). The p-value of 0.000 and t-value of 15.238, shows that this relationship is significant since the p-value is less than 0.001 and the corresponding t-value is greater than 3.29 (Hair et al., 2014; Hair et al., 2017; Roky & Al-Meriouh, 2015). Therefore, hypothesis 4 is supported, proving that consumer IoT security self-efficacy positively effects IoT security technology practices.

Hypothesis 5 is stated as:

H5: *Consumer IoT security self-efficacy positively influences IoT security behavioural practices.*

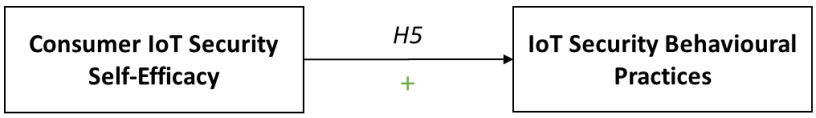

Figure 10: Hypothesis 5 - ISSE

Following the results of the hypothesis testing, the positive relationship expected between the effects of consumer IoT security self-efficacy and IoT security behavioural practices is accepted. The acceptance of H5 is aligned to results found in previous studies conducted by Rhee et al. (2009) and Zhou et al. (2020).

H5 is supported with a path coefficient of 0.303 being greater than the required value of 0.2 or more, based on this, the ISSE -> SP-B relationship is seen as statistically significant (Cangur & Ercan, 2015). The p-value of 0.000 and t-value of 3.893 are favourable, proves the significance of this relationship where the p-value is less than 0.001 and the corresponding t-value is greater than 3.29 (Hair et al., 2014; Hair et al., 2017; Roky & Al-Meriouh, 2015). Based on the above, hypothesis 5 is supported, proving that consumer IoT security self-efficacy positively effects IoT security behavioural practices.

5.6.4. Consumer IoT Device Knowledge (CK)

In this study, consumer IoT device knowledge refers to the user's knowledge of consumer IoT devices. It is expected that a user's knowledgeable experience with consumer IoT devices

contributes toward their perceived ability to ensure their consumer IoT security. The effect of the relationship between consumer IoT device knowledge and consumer IoT security self-efficacy is tested through the following hypothesis and illustrated in Figure 11:

H6: *Consumer IoT device knowledge positively influences consumer IoT security self-efficacy.*

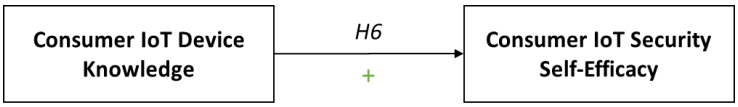

Figure 11: Hypothesis 6 – CK

The positive relationship expected between the effects of consumer IoT device knowledge and consumer IoT security self-efficacy is accepted based on the results of the hypothesis testing carried out and aligns with the results of the previous studies carried out (Davis, 2013; Eschenbrenner & Nah, 2014; Rhee et al., 2009; Zhou et al., 2020).

H6 is supported with a path coefficient of 0.198 which rounds up to 0.20 being greater than or equal to the required value of 0.2, based on this, the CK -> ISSE relationship is referred to as being statistically significant (Cangur & Ercan, 2015). The p-value of 0.002 and t-value of 3.073 are favourable according to the criteria of: where p-values are less than 0.05, the corresponding t-value would need to be more significant than 1.95, 1.96 or greater (Hair et al., 2014; Hair et al., 2017; Roky & Al-Meriouh, 2015). Based on this, hypothesis 6 is supported, proving that consumer IoT device knowledge positively effects consumer IoT security self-efficacy.

5.6.5. Consumer IoT Device Experience (DE)

Consumer IoT device experience refers to the skill or level of literacy the IoT user has with their devices. It is expected that having prior experience with consumer IoT devices contributes toward the user's perceived ability ensure security and improves their self-efficacy. The relationship between consumer IoT device experience a consumer IoT security self-efficacy is tested with the following hypothesis and illustrated in Figure 12:

H7: *Consumer IoT device experience positively influences IoT security self-efficacy.*

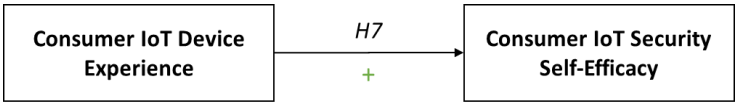

Figure 12: Hypothesis 7 - DE

Results of previous studies carried out by Rhee et al. (2009) and studies carried out by Zhou et al. (2020) demonstrated that IoT device experience leads to displaying positive IoT security self-efficacy, this result is not aligned with the findings of this study. According to the hypothesis testing carried out, the positive relationship expected between IoT device experience and consumer IoT security self-efficacy, which expects users who display IoT device experience to display positive IoT security self-efficacy is not supported.

H7 is not supported based on the path coefficient for this hypothesis being 0.103, which is below the required value of 0.2, therefore the relationship, DE -> ISSE, is deemed to be statistically insignificant (Cangur & Ercan, 2015). This result is supported by the p-value of this relationship being 0.133 and the accompanying t-value being 1.502, which shows that the insignificant p-value is accompanied by an insignificant t-value. Since the p-value is greater than 0.001 and the corresponding t-value is less than 3.29, the relationship is seen to be insignificant. This also proves true according to the criteria where p-values are less than 0.05, the corresponding t-value would need to be more significant than 1.95, 1.96 or greater (Hair et al., 2014; Hair et al., 2017; Roky & Al-Meriouh, 2015). Therefore, hypothesis 7 is rejected.

Conjecture for H7 being rejected in this study and not aligning to the literature relating to the relationship between consumer IoT device experience and consumer IoT security self-efficacy could be due to methodological issues, measurement issues, or missing conceptual elements. The expectation for H7 was that having prior experience with consumer IoT devices would contribute to their ability to ensure security. In reviewing the research instrument, it is possible that it could be re-evaluated to be more specific in identifying the consumers IoT device experience. It could also have been possible that the respondent perceived themselves as being experienced consumer IoT device users, but they were in fact not experienced.

5.6.6. Security Breach Incidents (SBI)

In this study, IoT security breach incidents refer to the consumer IoT device users experience with IoT security breaches. It is expected that having previously had a negative experience with their consumer IoT device security may affect their confidence in the perceived ability to ensure information security in future. In order to test the effects of IoT security breach incidents on the consumers IoT security self-efficacy, the following hypothesis is used and illustrated in Figure 13:

H8: *IoT security breach incidents negatively influence consumer IoT security self-efficacy.*

Figure 13: Hypothesis 8 – SBI

Rhee et al. (2009) and Williams et al. (2021) have provided studies stating that device users who have had experience with security breach incidents would then display negative IoT security self-efficacy, however, the results of this study do not align to those findings. Following the hypothesis testing, the negative relationship expected between IoT security breach incidents and consumer IoT security self-efficacy, which expects users who have experienced security breach incidents to display negative IoT security self-efficacy is not supported.

H8 is not supported since the path coefficient for this test is -0.032, which is below the required value of 0.2, therefore the SBI -> ISSE relationship is deemed to be statistically insignificant (Cangur & Ercan, 2015). This result is supported by the p-value of this relationship being 0.376 and the accompanying t-value being 0.886, which shows that the insignificant p-value is accompanied by an insignificant t-value. Since the p-value is greater than 0.001 and the corresponding t-value is less than 3.29, the relationship is seen to be insignificant. This also proves true according to the criteria where p-values are less than 0.05, the corresponding t-value would need to be more significant than 1.95, 1.96 or greater in order for the relationship to be significant (Hair et al., 2014; Hair et al., 2017; Roky & Al-Meriouh, 2015). Therefore, hypothesis 8 is rejected.

Possible reasons why H8 was rejected through the research analysis in this study and does not align to previous literature relating to the expected negative relationship between IoT security breach incidents and consumer IoT security self-efficacy could be related to the measurement instrument used or possible missing conceptual elements. In reviewing the instrument, and the research conceptual model, the expectant result for this study was that having previous experience or having experienced IoT security breach incidents would lower the users perceived ability to control security threats. Upon face value, it is possible that the instrument may have been more effective if it was phrased in the negative context which would change the expectant result to be that a lack of experience with IoT security breach incidents would improve the users perceived ability to control IoT security self-efficacy or it may have no further effect.

5.6.7. Consumer IoT General Controllability (GC)

In this study, consumer IoT general controllability refers to the consumer IoT device users' perception in being able to control general information security threats as well as consumer IoT security threats. It is expected that the users perceived ability and competence to control consumer IoT security threats with the resources available will affect their perceived ability or self-efficacy to do so. To test the relationship between the consumer's IoT general controllability and their consumer IoT security self-efficacy, the following hypothesis is used and illustrated in Figure 14:

H9: *Consumer IoT general controllability positively influences consumer IoT security self-efficacy.*

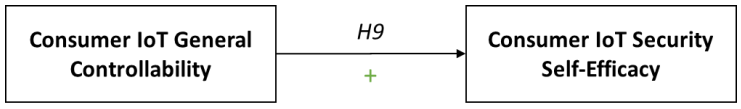

Figure 14: Hypothesis 9 – GC

Aurigemma and Mattson (2017) and Rhee et al. (2005; 2009) have provided studies stating that the users perceived ability and competence to control security threats faced with the resources that are available affects their ability or self-efficacy to do so, the findings of this study align to the findings of Aurigemma and Mattson (2017) and Rhee et al. (2005; 2009).

The positive relationship expected between the effects of consumer IoT general controllability on consumer IoT security self-efficacy is accepted based on the results of the hypothesis testing carried out. H9 is supported with a path coefficient of 0.632 which is greater than or equal to the required value of 0.2, based on this, the GC -> ISSE relationship is seen to be statistically significant (Cangur & Ercan, 2015). The p-value of 0.000 and t-value of 9.475 are favourable according to the criteria where the p-value is less than 0.001 and the corresponding t-value is greater than 3.29, the relationship is deemed significant (Hair et al., 2014; Hair et al., 2017; Roky & Al-Meriouh, 2015). Therefore, hypothesis 9 is supported, proving that consumer IoT general controllability positively effects consumer IoT security self-efficacy.

5.6.8. Summary of Findings

Following the hypotheses testing conducted, 6 of the 9 hypotheses have been found to be statistically significant and are therefore accepted. The findings of this research study are summarised in this section.

The expectation that the user's behavioural intention affects their future IoT security behavioural practices is supported, this finding aligns with prior studies concluded by Das and Khan (2016) and Rhee et al. (2009). Similarly, the expectation that the user's knowledgeable experience with consumer IoT devices contributes toward their perceived ability to ensure their consumer IoT security is supported by this research and reinforced by previous studies conducted by Davis (2013), Eschenbrenner and Nah (2014), Rhee et al. (2009) and Zhou et al. (2020). This study also expects the users perceived ability and competence to control consumer IoT security threats with the resources available to affect their perceived ability or self-efficacy to do so, the findings support this expectation and is further supported in literature by Aurigemma and Mattson (2017 and Rhee et al. (2005; 2009).

IoT security technology practices, IoT security behavioural practices and IoT security behavioural intentions are anticipated as the consequences of IoT security self-efficacy. Therefore, the expectation that users with a greater consumer IoT security self-efficacy belief would adopt more secure IoT security technology practices and display more secure consumer IoT security behavioural intentions and security behavioural practices is supported. Previous research conducted by Rhee et al. (2009) and Zhou et al. (2020) are in support of these findings.

The expectation that users of consumer IoT devices who employ IoT security technology practices eventually display more secure consumer IoT security behavioural practices is not supported by this research study, which contradicts the positive relationship expected according to studies carried out by Goodreau (2021), Lee et al. (2019) and Rhee et al. (2009). It is possible that this relationship is not supported due to survey respondents aligning with the behavioural practices regardless of whether they implement the technology practices or not. It could also be considered that respondents believe having completed the technology related practices would be enough, and therefore do not employ the behavioural security practices.

This study set out to indicate that having prior experience with consumer IoT devices contributes toward the user's perceived ability ensure security and improves their self-efficacy, however this expectation is not supported by the findings. The outcome of this finding does not align to the results of previous studies carried out by Rhee et al. (2009) and Zhou et al. (2020). There is a possibility that this measure could be re-evaluated to be more specific in identifying the consumers IoT device experience. However, it could also have been possible that the respondent perceived themselves as being experienced consumer IoT device users, but they were in fact not experienced.

It was also expected in this study that if a user had previously had a negative experience with their consumer IoT device security, their confidence may be affected in their perceived ability to ensure the future information security of their devices. However, this expectation is not supported by the findings of this study which differs from the result provided in previous studies by Rhee et al. (2009) and Williams et al. (2021). It is worth considering whether the instrument may have been more effective if it was phrased in the negative context which would change the expectant result to be that a lack of experience with IoT security breach incidents would improve the users perceived ability to control IoT security self-efficacy or it may have no further effect. It is also possible that the sample of respondents did not have sufficient experience with consumer IoT device security breaches in order for this measure to be accurately tested.

Table 32 highlights the result of the previously defined hypothesis based on the results of testing.

	Hypotheses	Result
H1	Behavioural intention positively influences IoT security behavioural practices	✓
H2	IoT security technology practices positively influence IoT security behavioural practices.	✗
H3	Consumer IoT security self-efficacy positively influences behavioural intention.	✓
H4	Consumer IoT security self-efficacy positively influences IoT security technology practices.	✓
H5	Consumer IoT security self-efficacy positively influences IoT security behavioural practices.	✓
H6	Consumer IoT device knowledge positively influences consumer IoT security self-efficacy.	✓
H7	Consumer IoT device experience positively influences IoT security self-efficacy.	✗
H8	IoT security breach incidents negatively influence consumer IoT security self-efficacy.	✗
H9	Consumer IoT general controllability positively influences consumer IoT security self-efficacy.	✓

Table 32: Hypothesis results

As an outcome of the hypotheses testing concluded, the following figures illustrate the resultant research models. Figure 15 illustrates the updated research model for this study after completing the hypothesis testing, and Figure 16 displays the resultant model of the Antecedents and Consequences of Consumer IoT Security Self-efficacy based on the findings of this study.

The resultant model in Figure 16 illustrates the positive relationship observed between Consumer IoT Device Knowledge and Consumer IoT General Controllability on Consumer IoT Security Self-Efficacy. There is also a positive relationship observed between Consumer IoT Security Self-Efficacy and IoT Security Technology Practices, IoT Security Behavioural Practices and Behavioural Intention; as well as the positive relationship between Behavioural Intention and IoT Security Behavioural Practices.

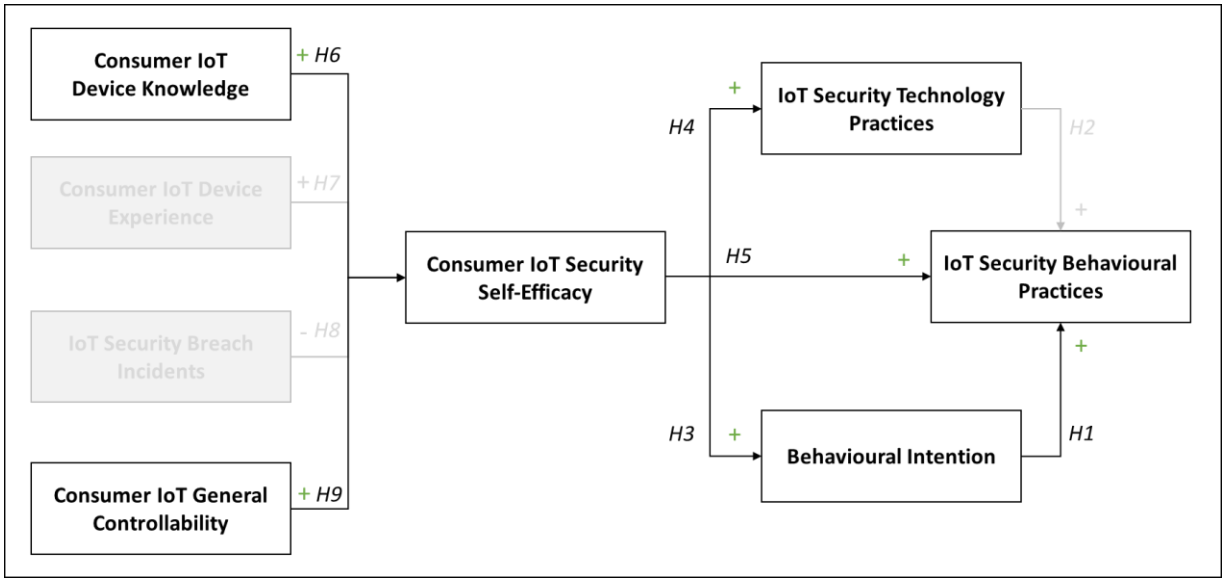

Figure 15: Research model post-hypothesis testing

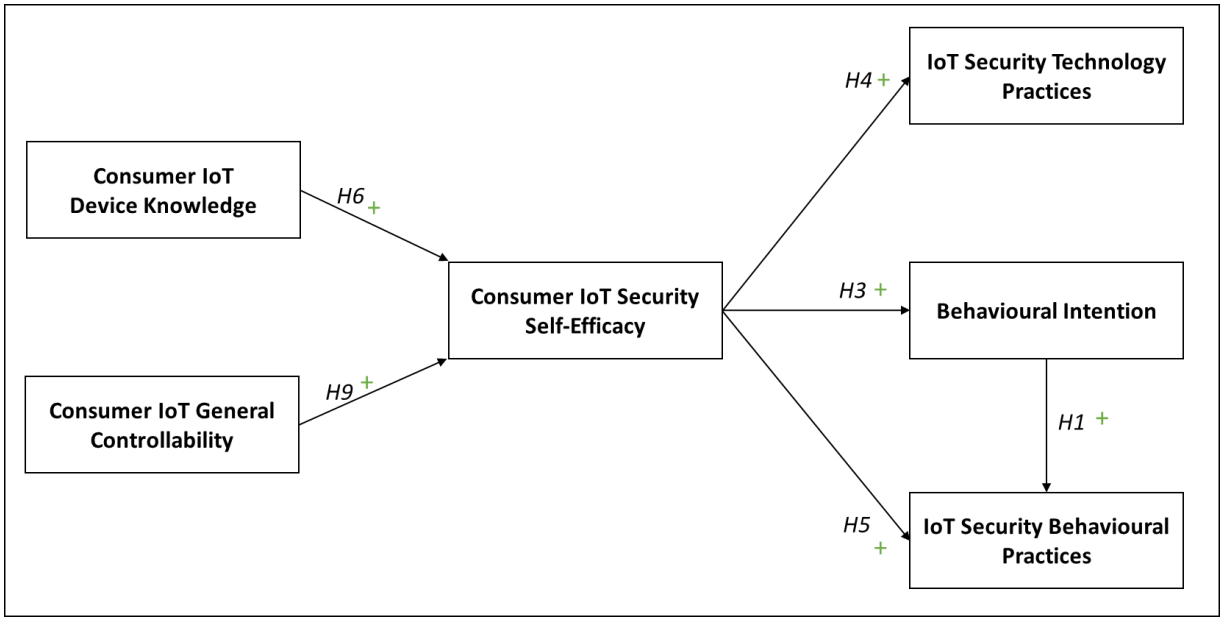

Figure 16: Resultant model - Antecedents and Consequences of Consumer IoT Security Self-efficacy

6. Conclusion

The purpose of this study was to determine and explain the influences on IoT security self-efficacy as well as the influence of IoT security self-efficacy on the consumers behaviour in securing their consumer IoT devices; this research was conducted in the context of consumer IoT device users in South Africa. The aim of this research was to determine which constructs acted as antecedents of consumer IoT security self-efficacy and which constructs were determined to be the consequences of it. Literature defined the following constructs as contributors to consumer IoT security self-efficacy: consumer IoT device knowledge, consumer IoT device experience, IoT security breach incidents and consumer IoT general controllability, while the resultant constructs of consumer IoT security self-efficacy were defined as being IoT security technology practices, behavioural intention and IoT security behavioural practices.

From the findings of this study, it can be concluded the relationships between consumer IoT device experience and IoT security breach incidents on consumer IoT security self-efficacy is not seen as significant. Similarly, the relationship between IoT security technology practices and IoT security behavioural practices is also seen to be insignificant. Significant relationships exist between the effects of consumer IoT device knowledge and consumer IoT general controllability on consumer IoT security self-efficacy. Following this, the effects of the relationship of consumer IoT security self-efficacy on IoT security technology practices, behavioural intention and IoT security behavioural practices are found to be significant. Therefore, consumer IoT device knowledge and consumer IoT general controllability can be defined as the antecedents of consumer IoT security self-efficacy. IoT security technology practices, behavioural intention and IoT security behavioural practices can be defined as the consequences of consumer IoT security self-efficacy. Similarly, the findings show that there is a significant relationship between the consumers behavioural intention and the IoT security behavioural practices that they adopt or carry out.

6.1. Practical Implications

Based on the results of this study, possible conjecture can indicate that the tangible measures, namely the exposure to consumer IoT security breaches incidents and consumer IoT device experience are not as influential as the cognitive influences on consumer IoT security self-efficacy; that being the consumer IoT device knowledge and the perceived consumer IoT general controllability. Due to this finding, it is possible that more emphasis should be placed on the

cognitive measures such as increasing the drive and circulation of knowledge relating to consumer IoT devices.

This study indicates that consumer IoT security self-efficacy can be seen as an area for societal awareness. Here, users, providers and manufacturers of consumer IoT should adopt the implication that perceived knowledge and controllability of users play an influential part in eventual behavioural practices.

6.2. Limitations and Recommendations for Future Research

The main objective of the study related to determining the antecedents and consequences of consumer IoT security self-efficacy, while identifying the antecedents of consumer IoT security self-efficacy, the consequences of consumer IoT security self-efficacy and the impact of consumer IoT security self-efficacy consequences on consumer IoT security practices and behaviour. In order to do this, 8 constructs were developed from literature to test the question proposed. From these 8 constructs, 2 of them were seen as not significant to the conclusion, namely consumer IoT device experience and IoT security breach incidents. Further research opportunities may lie in the interrogation of these constructs and the possible effects that they may have in the space of specific consumer IoT devices (e.g., see Table 1) and information security and behaviour. Another opportunity is based off of research by Belanger and Crossler (2017, 2019) which investigated self-efficacy in a way that splits the construct into a knowledge component, security/privacy component as well as technology component. Future research may be conducted around the antecedents and consequences of consumer Internet of Things security self-efficacy in a manner that specifies the security/privacy, and technology component of self-efficacy.

While the main objective of the research has been achieved, demographic data was collected and analysed for this study, although it did not form part of the final analysis and results. There lies an opportunity to test the concept by Johnson et al. (2020) who suggested that information security "concerns and behaviours vary with age" (Johnson et al., 2020, p. 3). Further research may be conducted to determine whether demographic factors display any influence on the 8 constructs being investigated and the result. Possible findings from this research are sure to bring about interesting results in the context of South Africa. In addition to this, within demographic data gathered, the research respondent is questioned relating to their awareness of consumer IoT devices, while the data did not form part of the analysis for this particular study, a future study may

derive useful insights. Following on this, future research could request respondents to mention the specific consumer IoT devices they make use of in order to provide a more practical view of the use and behaviours surrounding consumer IoT devices, and variations between different types.

Since this research study focuses on information security, a further area of elaboration may be explored with the incorporation of Rogers' (1983) Protection Motivation Theory (PMT) which aims to explain the consumers engagement in protective behaviours toward their information security and in relation to this study, their consumer IoT devices (Mou et al., 2022) . Possible outcomes from conducting this research may see the resultant model being adjusted or expanded upon. In addition, the significant relationships that have been identified as part of this research study could also be incorporated into future studies related to consumer IoT security, and the found antecedents and consequences can be used to better inform security regulation, policies and awareness in relation to information security.

7. References

1. Abiodun, M. K., Awotunde, J. B., Ogundokun, R. O., Adeniyi, E. A., & Arowolo, M. O. (2021). Security and Information Assurance for IoT-Based Big Data. Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities (pp. 189-211). Springer International Publishing. 10.1007/978-3-030-72236-4_8

2. Ahmad, Z., Ong, T. S., Liew, T. H., & Norhashim, M. (2019). Security monitoring and information security assurance behaviour among employees. Information and Computer Security, 27(2), 165-188. 10.1108/ICS-10-2017-0073

3. Aigbefo, Q. A., Blount, Y., & Marrone, M. (2022). The influence of hardiness and habit on security behaviour intention. Behaviour & Information Technology, 41(6), 1151-1170. 10.1080/0144929X.2020.1856928

4. Ajzen, I. (1991). The theory of planned behavior. Organizational behavior and human decision processes, 50(2), 179-211.

5. Al-Emran, M., Mezhuyev, V., & Kamaludin, A. (2018). PLS-SEM in Information Systems Research: A Comprehensive Methodological Reference. Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2018 (pp. 644-653). Springer International Publishing. 10.1007/978-3-319-99010-1_59

6. Alladi, T., Chamola, V., Sikdar, B., & Choo, K. R. (2020). Consumer IoT: Security Vulnerability Case Studies and Solutions. IEEE Consumer Electronics Magazine, 9, 17-25. 10.1109/MCE.2019.2953740 https://ieeexplore.ieee.org/document/8977812

7. Al-Turjman, F., Zahmatkesh, H., & Shahroze, R. (2022). An overview of security and privacy in smart cities' IoT communications. European Transactions on Telecommunications, 33(3), n/a. 10.1002/ett.3677

8. Apthorpe, N., Emami-Naeini, P., Mathur, A., Chetty, M., & Feamster, N. (2022). You, Me, and IoT: How Internet-connected Consumer Devices Affect Interpersonal Relationships. ACM Transactions on the Internet of Things, 3(4), 1-29. 10.1145/3539737

9. Atlam, H. F., & Wills, G. B. (2019). IoT Security, Privacy, Safety and Ethics. Digital Twin Technologies and Smart Cities (pp. 123-149). Springer International Publishing. 10.1007/978-3-030-18732-3_8

10. Aurigemma, S., & Mattson, T. (2017). Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. Computers & Security, 66, 218-234. 10.1016/j.cose.2017.02.006

11. Bandura, A. (1986). Social foundations of thought and action: a social cognitive theory. Englewood Cliffs, NJ, 1986 (23-28).

12. Bastos, D., Shackleton, M., & El-Moussa, F. Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments. Paper presented at the Living in the Internet of Things: Cybersecurity of the IoT - 2018, 30. 10.1049/cp.2018.0030 http://digital-library.theiet.org/content/conferences/10.1049/cp.2018.0030

13. Behardien, R., & Brown, I. (2022). Factors Influencing Smartphone End-User Security Behaviour - The Case of Young Adults in South Africa. Paper presented at the 2022 IST-Africa Conference (IST-Africa), 1-10. 10.23919/IST-Africa56635.2022.9845602 https://ieeexplore.ieee.org/document/9845602

14. Belanger, F., & Crossler, R. E. (2019). Dealing with digital traces: Understanding protective behaviors on mobile devices. The Journal of Strategic Information Systems, 28(1), 34-49. 10.1016/j.jsis.2018.11.002

15. Bhattacherjee, A. (2012). Social Science Research: Principles, Methods, and Practices. Global Text Project.

16. Blythe, J. M., Sombatruang, N., & Johnson, S. D. (2019). What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages? Journal of Cybersecurity (Oxford), 5(1)10.1093/cybsec/tyz005

17. Bonett, D. G., & Wright, T. A. (2015). Cronbach's alpha reliability: Interval estimation, hypothesis testing, and sample size planning. Journal of Organizational Behavior, 36(1), 3-15. 10.1002/job.1960

18. Cangur, S., & Ercan, I. (2015). Comparison of Model Fit Indices Used in Structural Equation Modeling Under Multivariate Normality. Journal of Modern Applied Statistical Methods, 14(1), 152-167. 10.22237/jmasm/1430453580

19. Chen, T., Hammer, J., & Dabbish, L. (2019). Self-Efficacy-Based Game Design to Encourage Security Behavior Online. Paper presented at the 2019 CHI Conference on Human Factors in

Computing Systems, Scotland. 1-6. 10.1145/3290607.3312935 http://dl.acm.org/citation.cfm?id=3312935

20. Crossler, R. E. and Bélanger, F. (2017), "The Mobile Privacy-Security Knowledge Gap Model: Understanding Behaviors," in Proceedings of the 50th Hawaii International Conference on System Sciences (2017), Kauai, Hawaii, USA, 2017, pp. 4071–4080, 10.24251/HICSS.2017.491 [Online].

21. Crossler, R. E. and Bélanger, F. (2019), "Why Would I Use Location-Protective Settings on My Smartphone? Motivating Protective Behaviors and the Existence of the Privacy Knowledge–Belief Gap," Information Systems Research, vol. 30, no. 3, pp. 995–1006, Sep. 2019, 10.1287/isre.2019.0846. [Online].

22. Creswell, J. W. (2009). Research Design Qualitative, Quantitative, and Mixed Methods Approaches. (3. ed. ed.). Sage.

23. Cuganesan, S., Steele, C., & Hart, A. (2018). How senior management and workplace norms influence information security attitudes and self-efficacy. Behaviour & Information Technology, 37(1), 50-65. 10.1080/0144929X.2017.1397193

24. Das, A., & Khan, H. U. (2016). Security behaviors of smartphone users. Information & Computer Security, 24(1), 116-134. 10.1108/ICS-04-2015-0018

25. Davis, J. M. (2013). Leveraging the IT competence of non-IS workers: social exchange and the good corporate citizen. European Journal of Information Systems, 22(4), 403-415. 10.1057/ejis.2012.36

26. Demestichas, K., Peppes, N., & Alexakis, T. (2020). Survey on Security Threats in Agricultural IoT and Smart Farming. Sensors (Basel, Switzerland), 20(22), 6458. 10.3390/s20226458

27. Deng, M., & Gu, X. (2021). Information acquisition, emotion experience and behaviour intention during online shopping: an eye-tracking study. Behaviour & Information Technology, 40(7), 635-645. 10.1080/0144929X.2020.1713890

28. Dian, F. J., Vahidnia, R., & Rahmati, A. (2020). Wearables and the Internet of Things (IoT), Applications, Opportunities, and Challenges: A Survey. IEEE Access, 8, 1. 10.1109/ACCESS.2020.2986329

29. Du, J., Jiang, C., Gelenbe, E., Xu, L., Li, J., & Ren, Y. (2018). Distributed Data Privacy Preservation in IoT Applications. IEEE Wireless Communications, 25(6), 68-76. 10.1109/MWC.2017.1800094

30. Eschenbrenner, B., & Nah, F. F. H. (2014). Information systems user competency: A conceptual foundation. Communications of the Association for Information systems, 34(1), 80.

31. Farooq, M. S., Riaz, S., Abid, A., Abid, K., & Naeem, M. A. (2019). A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming. IEEE Access, 7, 156237-156271. 10.1109/ACCESS.2019.2949703

32. Farooq, M. S., Riaz, S., Abid, A., Umer, T., & Zikria, Y. B. (2020). Role of IoT Technology in Agriculture: A Systematic Literature Review. Electronics, 9(2), 319. 10.3390/electronics9020319

33. Gartner Inc. Internet of Things (IoT). https://www.gartner.com/en/information-technology/glossary/internet-of-things

34. Giwah, A. D., Wang, L., Levy, Y., & Hur, I. (2020). Empirical assessment of mobile device users information security behavior towards data breach. Journal of Intellectual Capital, 21(2), 215-233. 10.1108/JIC-03-2019-0063

35. Goodreau, T. (2020). 7 Actionable Tips to Secure Your Smart Home and IoT Devices. https://search.proquest.com/docview/2386054378

36. Gupta, K. P., & Maurya, H. (2022). Adoption, completion and continuance of MOOCs: a longitudinal study of students' behavioural intentions. Behaviour & Information Technology, 41(3), 611-628. 10.1080/0144929X.2020.1829054

37. Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). A primer on partial least squares structural equation modeling (PLS-SEM) (Second edition ed.). SAGE.

38. Hair, J. F., Ringle, C. M., Smith, D., Reams, R., & Sarstedt, M. (2014). Partial least squares structural equation modeling (PLS-SEM): A useful tool for family business researchers. Journal of Family Business Strategy, 5(1), 105-115. 10.1016/j.jfbs.2014.01.002

39. Handcock, M. S., & Gile, K. J. (2011). Comment: On the concept of snowball sampling. Sociological Methodology, 41(1), 367-371. 10.1111/j.1467-9531.2011.01243.x

40. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. IEEE Access, 7, 1. 10.1109/ACCESS.2019.2924045

41. Hina, S., Panneer Selvam, Dhanapal Durai Dominic, & Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. Computers & Security, 87, 101594. 10.1016/j.cose.2019.101594

42. Iqbal, M. A., Olaleye, O. G., & Bayoumi, M. A. (2016). A Review on Internet of Things (Iot): Security and Privacy Requirements and the Solution Approaches A Review on Internet of Things (Iot): Security and Privacy Requirements and the Solution Approaches

43. Jeske, D., & van Schaik, P. (2017). Familiarity with Internet threats: Beyond awareness. Computers & Security, 66, 129-141. 10.1016/j.cose.2017.01.010

44. Johnson, S. D., Blythe, J. M., Manning, M., & Wong, G. T. W. (2020). The impact of IoT security labelling on consumer product choice and willingness to pay. PloS One, 15(1), e0227800. 10.1371/journal.pone.0227800

45. Khan, W. Z., Rehman, M. H., Zangoti, H. M., Afzal, M. K., Armi, N., & Salah, K. (2020). Industrial internet of things: Recent advances, enabling technologies and open challenges. Computers & Electrical Engineering, 81, 106522. 10.1016/j.compeleceng.2019.106522

46. Kim, J., & Park, E. (2022). Understanding social resistance to determine the future of Internet of Things (IoT) services. Behaviour & Information Technology, 41(3), 547-557. 10.1080/0144929X.2020.1827033

47. Kirimtat, A., Krejcar, O., Kertesz, A., & Tasgetiren, M. F. (2020). Future Trends and Current State of Smart City Concepts: A Survey. IEEE Access, 8, 86448-86467. 10.1109/ACCESS.2020.2992441

48. Kivunja, C., & Kuyini, A. B. (2017). Understanding and Applying Research Paradigms in Educational Contexts. International Journal of Higher Education, 6(5), 26. 10.5430/ijhe.v6n5p26

49. Lee, S., Park, N., & Suk, J. (2019). The Effects of Consumers' Information Security Behavior and Information Privacy Concerns on Usage of IoT Technology. Paper presented at the XX

International Conference on Human Computer Interaction, 1-2. 10.1145/3335595.3335600 http://dl.acm.org/citation.cfm?id=3335600

50. Lheureux, B., Kutnick, D., Williams, R., Velosa, A., & Reynolds, M. (2021). Hype Cycle for the Internet of Things 2021. G00747575 https://ssofed.gartner.com/sp/startSSO.ping?PartnerIdpId=http://adfs.uct.ac.za/adfs/services/trust&TargetResource=https%3A%2F%2Fwww.gartner.com%2Fdocument%2F4004463%3Fref%3Dd-linkShare

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

52. Lowry, P. B., & Gaskin, J. (2014). Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose It and How to Use It. IEEE Transactions on Professional Communication, 57(2), 123-146. 10.1109/TPC.2014.2312452

53. Lu, Y. (2021). Examining user acceptance and adoption of the internet of things. International Journal of Business Science and Applied Management, 16(3), 1-17. http://www.econis.eu/PPNSET?PPN=1761855840

54. Lv, Z., & Singh, A. K. (2021). Big Data Analysis of Internet of Things System. ACM Transactions on Internet Technology, 21(2), 1-15. 10.1145/3389250

55. Malik, P. K., Sharma, R., Singh, R., Gehlot, A., Satapathy, S. C., Alnumay, W. S., Pelusi, D., Ghosh, U., & Nayak, J. (2021). Industrial Internet of Things and its Applications in Industry 4.0: State of The Art. Computer Communications, 166, 125-139. 10.1016/j.comcom.2020.11.016

56. Mamdiwar, S. D., R, A., Shakruwala, Z., Chadha, U., Srinivasan, K., & Chang, C. (2021). Recent Advances on IoT-Assisted Wearable Sensor Systems for Healthcare Monitoring. Biosensors (Basel), 11(10), 372. 10.3390/bios11100372

57. McGill, T. J., Thompson, N., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. Computers & Security. doi:10.1016/j.cose.2017.07.003

58. Menard, P., & Bott, G. J. (2020). Analyzing IOT users mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment. Computers & Security, 95, 101856. 10.1016/j.cose.2020.101856

59. Microsoft. (2021). Keep your computer secure at home. https://support.microsoft.com/en-us/windows/keep-your-computer-secure-at-home-c348f24f-a4f0-de5d-9e4a-e0fc156ab221

60. Mou, J., Cohen, J. F., Bhattacherjee, A., & Kim, J. (2022). A test of protection motivation theory in the information security literature: A meta-analytic structural equation modeling approach. Journal of the Association for Information Systems, 23(1), 196-236.

61. Ngoqo, B., & Flowerday, S. V. (2015). Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users. Computers & Security, 53, 132-142. 10.1016/j.cose.2015.05.011

62. Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. Information systems research, 2(1), 1-28.

63. Park, E., Cho, Y., Han, J., & Kwon, S. J. (2017). Comprehensive Approaches to User Acceptance of Internet of Things in a Smart Home Environment. IEEE Internet of Things Journal, 4(6), 2342-2350. 10.1109/JIOT.2017.2750765

64. Perez, A. J., Zeadally, S., & Cochran, J. (2018). A review and an empirical analysis of privacy policy and notices for consumer Internet of things. Security and Privacy, 1(3), n/a. 10.1002/spy2.15

65. Philip, S. J., Luu, T. (., & Carte, T. (2023). There's No place like home: Understanding users intentions toward securing internet-of-things (IoT) smart home networks. Computers in Human Behavior, 139, 107551. 10.1016/j.chb.2022.107551

66. Poongodi, T., Krishnamurthi, R., Indrakumari, R., Suresh, P., & Balusamy, B. (2019). Wearable Devices and IoT. A Handbook of Internet of Things in Biomedical and Cyber Physical System (pp. 245-273). Springer International Publishing. 10.1007/978-3-030-23983-1_10

67. Qualtrics. (2022). Qualtrics, Provo, UT, USA. https://www.qualtrics.com

68. Ren, J., Dubois, D., Choffnes, D., Mandalari, A., Kolcun, R., & Haddadi, H. (2019). Information Exposure From Consumer IoT Devices. Paper presented at the Internet Measurement

Conference (ICM '19), 267-279. 10.1145/3355369.3355577 http://dl.acm.org/citation.cfm?id=3355577

69. Rhee, H., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users information security practice behavior. Computers & Security, 28(8), 816-826. 10.1016/j.cose.2009.05.008

70. Rhee, H., Ryu, Y., & Kim, C. (2005). I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security. Paper presented at the International Conference on Information Systems (ICIS), 26-32.

71. Rieder, A., Eseryel, U. Y., Lehrer, C., & Jung, R. (2021). Why Users Comply with Wearables: The Role of Contextual Self-Efficacy in Behavioral Change. International Journal of Human-Computer Interaction, 37(3), 281-294. 10.1080/10447318.2020.1819669

72. Ringle, C. M., Wende, S., & Becker, J. (2022). SmartPLS 4 [computer software]

73. Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. Social psychology: A source book, 153-176.

74. Salkind, N. J. (2012). Exploring research (8. ed.). Pearson Education.

75. Saunders, M., Lewis, P., & Thornhill, A. (2019). Chapter 4: Understanding research philosophy and approaches to theory development Participant selection View project. Research Methods for Business Students (8th ed.,). Pearson.

76. Shahri, A. B., Ismail, Z., & Mohanna, S. (2016). The Impact of the Security Competency on "Self-Efficacy in Information Security" for Effective Health Information Security in Iran. Journal of Medical Systems, 40(11), 1-9. 10.1007/s10916-016-0591-5

77. Sharevski, F., Treebridge, P., & Westbrook, J. (2019). Experiential User-Centered Security in a Classroom: Secure Design for IoT. IEEE Communications Magazine, 57, 48-53. 10.1109/MCOM.001.1900223 https://ieeexplore.ieee.org/document/8908550

78. Snyman, D. P., Kruger, H., & Kearney, W. D. (2018). I shall, we shall, and all others will: paradoxical information security behaviour. Information & Computer Security, 26(3), 290-305. 10.1108/ICS-03-2018-0034

79. Snyman, D., & Kruger, H. (2020). A Management Decision Support System for Evaluating Information Security Behaviour. Information and Cyber Security (pp. 15-27). Springer International Publishing. 10.1007/978-3-030-43276-8_2

80. Snyman, D., & Kruger, H. A. (2020). External contextual factors in information security behaviour. 10.5220/0009142201850194

81. Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. IEEE Communications Surveys and Tutorials, 22(2), 1191-1221. 10.1109/COMST.2019.2962586

82. Taneja, A. (2006). Determinants of adverse usage of information systems assets: A study of antecedents of IS exploit in organizations Available from ABI/INFORM Global (Corporate) https://search.proquest.com/docview/304904412

83. Taylor, J., & van Schaik, P. (2022). To what extent does time perspective predict online security behaviour? Behaviour & Information Technology, 1-9. 10.1080/0144929X.2022.2085172

84. Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. Computers & Security, 70, 376-391. 10.1016/j.cose.2017.07.003

85. Uddin, H., Gibson, M., Safdar, G. A., Kalsoom, T., Ramzan, N., Ur-Rehman, M., & Imran, M. A. (2019). IoT for 5G/B5G Applications in Smart Homes, Smart Cities, Wearables and Connected Cars. Paper presented at the 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 1-5. 10.1109/CAMAD.2019.8858455 https://ieeexplore.ieee.org/document/8858455

86. Urbach, N., & Ahlemann, F. (2010). Structural Equation Modeling in Information Systems Research Using Partial Least Squares. Jitta, 11(2), 5. https://search.proquest.com/docview/760866856

87. Wang, Q., Zhu, X., Ni, Y., Gu, L., & Zhu, H. (2020). Blockchain for the IoT and industrial IoT: A review. Internet of Things, 10, 100081. 10.1016/j.iot.2019.100081

88. Wardropper, C. B., Dayer, A. A., Goebel, M. S., & Martin, V. Y. (2021). Conducting conservation social science surveys online. Conservation Biology, 35(5), 1650-1658. 10.1111/cobi.13747

89. Williams, H., Leggett, O., Coleman, N., Shah, J. N., & Furnell, S. (2021). DCMS: Cyber Security Breaches Survey 2021. Network Security, 2021(4), 4. 10.1016/S1353-4858(21)00036-2

90. Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior, 24(6), 2799-2816. 10.1016/j.chb.2008.04.005

91. Wu H, Xiaohong Y, & Xin T (2018). The Self-Efficacy Variable in Behavioral Information Security Research. Paper presented at the 2014 Enterprise Systems Conference (ES), Shanghai, China. 28. https://search.proquest.com/docview/1684019117

92. Wu, H., Zhang, Z., Guan, C., Wolter, K., & Xu, M. (2020). Collaborate Edge and Cloud Computing With Distributed Deep Learning for Smart City Internet of Things. IEEE Internet of Things Journal, 7(9), 8099-8110. 10.1109/JIOT.2020.2996784

93. Yoon, C., Hwang, J., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. Journal of Information Systems Education, 23(4), 407. https://search.proquest.com/docview/1432293508

94. Zeng, E., & Roesner, F. (2019). Understanding and Improving Security and Privacy in {Multi-User} Smart Homes: A Design Exploration and {In-Home} User Study. In 28th USENIX Security Symposium (USENIX Security 19) (pp. 159-176).

95. Zhang, C., & Chen, Y. (2020). A Review of Research Relevant to the Emerging Industry Trends: Industry 4.0, IoT, Blockchain, and Business Analytics. Journal of Industrial Integration and Management: Innovation and Entrepreneurship, 5(1), 165-180. 10.1142/S2424862219500192

96. Zhou, G., Gou, M., Gan, Y., & Schwarzer, R. (2020). Risk Awareness, Self-Efficacy, and Social Support Predict Secure Smartphone Usage. Frontiers in Psychology, 11, 1066. 10.3389/fpsyg.2020.01066

Appendices

Appendix 1: Questionnaire Scale

This research study makes use of the Likert rating system to collect opinion data (Saunders et al., 2019). The five-point Likert rating scale will be made use of in the questionnaire, the participant will be able to state how strongly they agree or disagree with the statements presented to them.

The five-point Likert rating scale to be used in this study is as follows:

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree

Appendix 2: Pilot Study Questionnaire Statements

Pilot Study Measure	Identifier	Statement
IoT Device Experience	DE1	I have made use of IoT devices for more than 2 years.
	DE2	I currently make use of 1 or more IoT devices.
	DE3	I am an experienced IoT device user
	DE4	I make use of all the features available on my IoT devices
	DE5	I have strong IoT device literacy levels
Security Breach Incidents	SBI1	I have experienced a security breach with IoT.
	SB2	I have fallen victim to cyber fraud with IoT.
	SB3	I have experienced phishing attacks with IoT.
General Controllability	GE1	Threats to IoT security are controllable
	GE2	IoT is advanced enough to prevent security threats
	GE3	There exist means to control IoT security threats
	GE4	I have the means to control IoT security threats
	GE5	I have the ability to execute IoT security practices to avoid security threats
	GE6	I have access to the necessary resources to protect my IoT devices
	GE7	I can exercise a course of action to avoid an IoT security breach
Information Security Self-Efficacy	ISSE1	I feel confident managing security on my IoT devices
	ISSE2	I have the necessary knowledge and skills to protect my IoT device
	ISSE3	I feel confident getting help for problems related to my IoT security
	ISSE4	I feel confident learning the method to protect my information and IoT device
	ISSE5	I feel confident updating security to the IoT operating system
	ISSE6	I am confident in my ability to protect my IoT device(s) from hackers
	ISSE7	I am confident and at ease in adopting IoT device protection
IoT Security Practices	SP1	I make use of firewalls on my home IoT networks

Pilot Study Measure	Identifier	Statement
	SP2	I often check and apply security updates to the operating systems and critical applications on my IoT devices
	SP3	I use forms of wireless encryption features on my IoT wireless connections
Behavioural Intention	BI1	I intend to enforce stronger IoT security procedures
	BI2	I intend to add additional security measures to protect my information and my IoT devices
	BI3	I intend to buy more software to mitigate impacts of IoT information security breaches
	BI4	I intend to learn more about how to strengthen my IoT information security
IoT Security Behaviour	SB1	I store confidential information on my IoT devices
	SB2	I reuse passwords for different IoT accounts
	SB3	I share my IoT devices with others
	SB4	I use a IoT password that is very difficult to guess such as a combination of upper and lower cases, symbols, and numbers
	SB5	I lock my IoT device(s) with a PIN or password
	SB6	I review security features of apps before installing them on my IoT device(s)

Table 33: Pilot Study Questionnaire Statements

Appendix 3: Cover Letter

Department of Information Systems
Leslie Commerce Building
Engineering Mall, Upper Campus
OR
Private Bag X3 - Rondebosch - 7701
Tel: +27 (0) 21 650 2261 Fax: +27 (0) 21650 2280
Internet: http://www.commerce.uct.ac.za/informationsystems/

7 October 2021

Request to conduct research and questionnaire participation consent form

Dear Respondent,

In terms of the requirements for completing a Master of Commerce degree in Information Systems at the University of Cape Town a research study is required. The researcher, in this case Raeesa Behardien, has chosen to conduct a study entitled Antecedents and Consequences of Internet of Things Security Self-Efficacy. The purpose of this research is an explanatory study that identifies the influences on IoT security self-efficacy and the causal relationship on IoT device security behaviour. Therefore, the aim is to explain the influences on self-efficacy in Information Security and its effects on IoT device security behaviours. The findings from this research are meant to aid in the understanding of Information Security self-efficacy influences and how self-efficacy impacts IoT device security behaviours.

Your participation in this research is entirely voluntary. All information captured will be treated confidentially and used solely for the purpose of enabling this study. No personal information will be recorded or published. You will not be requested to supply any identifiable information to ensure the anonymity of your responses. In accordance with ethical research requirements, you can choose to withdraw participation from the research at any time.

The data collection method will be in the form of an online survey questionnaire. The questionnaire will take approximately 10 minutes to complete. If you are willing to participate in this study, kindly follow the link below.

https://ucpcommerce.eu.qualtrics.com/jfe/form/SV_ah0RpQlKsqxDeT4

Should you have any questions regarding this research, please feel free to contact me on 071 263 1012 or email: bhrrae003@myuct.ac.za

Your participation in this study would be greatly appreciated, however it is entirely voluntary, you are free to end your participation at any time.

Sincerely,

Raeesa Behardien

Researcher / MCom Student (UCT)

Department of Information Systems

University of Cape Town

Email: bhrrae003@myuct.ac.za

Professor Irwin Brown

Research Supervisor

Department of Information Systems

University of Cape Town

Email: irwin.brown@uct.ac.za

Appendix 4: Research Questionnaire

i. Final Research Questionnaire Statements

Measure	Identifier	Statement
Consumer IoT Device Knowledge	CK1	I have valuable knowledge relating to various consumer IoT devices
	CK2	I have valuable knowledge relating to the software and applications available on consumer IoT devices
	CK3	I have valuable knowledge in how to make use of the various applications and uses of consumer IoT devices
	CK4	I know where to get additional valuable information regarding consumer IoT devices
Consumer IoT Device Experience	DE1	I have made use of IoT devices for more than 2 years.
	DE2	I currently make use of 1 or more IoT devices.
	DE3	I am an experienced IoT device user
	DE4	I make use of all the features available on my IoT devices
	DE5	I have strong IoT device literacy levels
IoT Security Breach Incidents	SBI1	I have experienced a security breach with IoT
	SBI2	I have fallen victim to cyber fraud with IoT
	SBI3	I have experienced phishing attacks with IoT
Consumer IoT General Controllability	GC1	Threats to IoT security are controllable
	GC2	IoT is advanced enough to prevent security threats
	GC3	There exist means to control IoT security threats
	GC4	I have the means to control IoT security threats
	GC5	I have the ability to execute IoT security practices to avoid security threats
	GC6	I have access to the necessary resources to protect my IoT devices
	GC7	I can exercise a course of action to avoid an IoT security breach
Consumer IoT Security Self-Efficacy	ISSE1	I feel confident managing security on my IoT devices
	ISSE2	I have the necessary knowledge and skills to protect my IoT device

Measure	Identifier	Statement
	ISSE3	I feel confident getting help for problems related to my IoT security
	ISSE4	I feel confident learning the method to protect my information and IoT device
	ISSE5	I feel confident updating security to the IoT operating system
	ISSE6	I am confident in my ability to protect my IoT device(s) from hackers
	ISSE7	I am confident and at ease in adopting IoT device protection
Consumer IoT Security Technology Practices	SP-T1	I employ security protocols on my IoT networks
	SP-T2	I often check and apply security updates to the operating systems and critical applications on my IoT devices
	SP-T3	I use forms of wireless encryption features on my IoT wireless connections
Behavioural Intention	BI1	I intend to enforce stronger IoT security procedures
	BI2	I intend to add additional security measures to protect my information and my IoT devices
	BI3	I intend to buy more software to mitigate impacts of IoT information security breaches
	BI4	I intend to learn more about how to strengthen my IoT information security
Consumer IoT Security Behavioural Practices	SP-B1	I do not store sensitive or confidential information on my IoT devices
	SP-B2	I lock my IoT device(s) with a PIN or password
	SP-B3	I use a IoT password that is very difficult to guess such as a combination of upper and lower cases, symbols, and numbers
	SP-B4	I make use of unique passwords for different IoT devices or applications
	SP-B5	I do not share my IoT devices with others
	SP-B6	I review security features of apps before installing them on my IoT device(s)

Table 34: Final Research Questionnaire Statements

ii. Qualtrics Research Questionnaire

UNIVERSITY OF CAPE TOWN

FACULTY OF COMMERCE

Igniting Knowledge and Opportunity

Cover letter and participant consent

Dear Respondent,

In terms of the requirements for completing a Master of Commerce degree in Information Systems at the University of Cape Town a research study is required. The researcher, in this case Raeesa Behardien, has chosen to conduct a study entitled Antecedents and Consequences of Consumer Internet of Things Security Self-Efficacy.

The purpose of this research is an explanatory study that identifies the influences on IoT security self-efficacy and the causal relationship on consumer IoT device security behaviour. Therefore, the aim is to explain the influences on self-efficacy in Information Security and its effects on IoT device security behaviours. The findings from this research are meant to aid in the understanding of Information Security self-efficacy influences and how self-efficacy impacts consumer IoT device security behaviours.

Your participation in this research is entirely voluntary. All information captured will be treated confidentially and used solely for the purpose of enabling this study. No personal information will be recorded or published. You will not be requested to supply any identifiable information to ensure the anonymity of your responses. In accordance with ethical research requirements, you can choose to withdraw participation from the research at any time.

The data collection method will be in the form of an online survey questionnaire. The questionnaire will take approximately 10 minutes to complete. If you are willing to participate in this study, kindly continue

Should you have any questions regarding this research, please feel free to contact me by email: bhrrae003@myuct.ac.za.

Your participation in this study would be greatly appreciated, however it is entirely voluntary, you are free to end your participation at any time.

Sincerely,

Raeesa Behardien | MCom Student (UCT) Department of Information Systems, University of Cape Town | Email: bhrrae003@myuct.ac.za

Professor Irwin Brown Researcher | Research Supervisor Department of Information Systems University of Cape Town | Email: irwin.brown@uct.ac.za

Demographics

Age

- ○ Under 18
- ○ 18 - 24
- ○ 25 - 34
- ○ 35 - 44
- ○ 45 - 54
- ○ 55 - 64
- ○ 65 and Older

Gender

- ○ Male
- ○ Female
- ○ Non-binary / third gender
- ○ Prefer not to answer
- ○ Other

Race

- ○ African
- ○ White
- ○ Coloured
- ○ Indian
- ○ Prefer not to answer
- ○ Other

Are you aware of what an Internet of Things (IoT) device is?

- ○ Definitely not
- ○ Probably not
- ○ Might or might not
- ○ Probably yes
- ○ Definitely yes

Consumer IoT Device Knowledge

State how strongly you agree or disagree with the following statements relating to Consumer IoT Device Knowledge

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
I have valuable knowledge relating to various consumer IoT devices	○	○	○	○	○
I have valuable knowledge relating to the software and applications available on consumer IoT devices	○	○	○	○	○
I have valuable knowledge making use of the various applications and uses of consumer IoT devices	○	○	○	○	○
I know where to get additional valuable information regarding consumer IoT devices	○	○	○	○	○

Consumer IoT Device Experience

State how strongly you agree or disagree with the following statements relating to Consumer IoT Device Experience.

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
I have made use of IoT devices for more than 2 years	○	○	○	○	○
I currently make use of 1 or more IoT devices	○	○	○	○	○
I am an experienced IoT device user	○	○	○	○	○
I make use of all the features available on my IoT devices	○	○	○	○	○
I have strong IoT device literacy levels	○	○	○	○	○

IoT Security Breach Incidents

State how strongly you agree or disagree with the following statements relating to IoT Security Breach Incidents.

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
I have experienced a security breach with IoT	○	○	○	○	○
I have fallen victim to cyber fraud with IoT	○	○	○	○	○
I have experienced phishing attacks with IoT	○	○	○	○	○

Consumer IoT General Controllability

State how strongly you agree or disagree with the following statements relating to Consumer IoT General Controllability.

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
Threats to IoT security are controllable	○	○	○	○	○
IoT technology is advanced enough to prevent security threats	○	○	○	○	○
There exist means to control IoT security threats	○	○	○	○	○
I have the means to control IoT security threats	○	○	○	○	○
I have the ability to execute IoT security practices to avoid security threats	○	○	○	○	○
I have access to the necessary resources to protect my IoT devices	○	○	○	○	○
I can exercise a course of action to avoid an IoT security breach	○	○	○	○	○

Consumer IoT Security Self-Efficacy

State how strongly you agree or disagree with the following statements relating to Consumer IoT Security Self-Efficacy.

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
I feel confident managing information on my IoT device(s)	○	○	○	○	○
I have the necessary knowledge and skills to protect my IoT device(s)	○	○	○	○	○
I feel confident getting help for problems related to my IoT device(s) security	○	○	○	○	○
I feel confident learning new methods to protect my information and IoT device(s)	○	○	○	○	○
I feel confident updating my IoT device(s) security and operating software	○	○	○	○	○
I am confident in my ability to protect my IoT device(s) against hackers	○	○	○	○	○
I am confident and at ease in adopting IoT device protection	○	○	○	○	○

Consumer IoT Security Practices - Technology

State how strongly you agree or disagree with the following statements relating to Consumer IoT Security Practices (Technology).

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
I employ security protocols on my IoT networks	○	○	○	○	○
I often check and apply security updates to the operating systems and critical applications on my IoT devices	○	○	○	○	○
I use forms of wireless encryption features on my IoT connections	○	○	○	○	○

Behavioural Intention

State how strongly you agree or disagree with the following statements relating to Behavioural Intention.

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
I intend to enforce stronger IoT security procedures	○	○	○	○	○
I intend to add additional security measures to protect my information and my IoT device(s)	○	○	○	○	○
I intend to invest in software to mitigate impacts of IoT security breaches	○	○	○	○	○
I intend to learn more about how to strengthen my IoT security	○	○	○	○	○

IoT Security Practice Behaviour

State how strongly you agree or disagree with the following statements relating to IoT Security Practice Behaviour.

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
I do not store sensitive or confidential information on my IoT devices	○	○	○	○	○
I lock my IoT device(s) with a PIN or password	○	○	○	○	○
I use a IoT password that is very difficult to guess such as a combination of upper and lower cases, symbols, and numbers	○	○	○	○	○
I make use of unique passwords for different IoT devices or applications	○	○	○	○	○
I do not share my IoT devices with others	○	○	○	○	○
I review security features of apps before installing them on my IoT device(s)	○	○	○	○	○

Figure 17: Qualtrics Research Questionnaire

Appendix 5: Ethics in Research

i. Ethics Application

Commerce Ethics in Research — Powered by Submittable

Project title (this will be recorded on your clearance letter)	**Antecedents and consequences of Internet of Things Security Self-Efficacy** by **Raeesa Behardien** in **Commerce Faculty Ethics Applications** bhrrae003@myuct.ac.za	05/10/2022 id. 25132628

Original Submission — 05/10/2022

Applicant status	**Student**
Retrospective ethics approval is not granted by the Commerce Faculty. By ticking this box, I confirm that I have *not* begun data collection, and will not do so, before this proposal has been granted ethical clearance.	**checked**
Health research	**The Commerce Faculty Ethics Board is not registered and may therefore not grant approval to applications that are covered in the Health Act of South Africa and are defined as health research, which includes any research which contributes to knowledge of: - the biological, clinical, psychological or social processes in human beings; - improved methods for the provision of health services; - human pathology; - causes of disease(s); - the effects of the environment on the human body; - the development or new application of pharmaceuticals, medicines and; - the development of new applications of health technology. Any application fitting these criteria will be declined, and the applicant referred to the Faculty of Health Sciences.**
Department	**Department of Information Systems**
UCT student number	**BHRRAE003**
Degree being studied	**Master of Commerce specializing in Information Systems**
Telephone number	**27712631009.0**
Email address	**bhrrae003@myuct.ac.za**
1. PROJECT DETAILS	n/a
Project title (this will be recorded on your clearance letter)	**Antecedents and consequences of Internet of Things Security Self-Efficacy**
Supervisor name(s)	**Professor Irwin Brown**
Supervisor email address(es)	**irwin.brown@uct.ac.za**
Will any human subjects be interviewed or surveyed in this research?	**Yes**
Co-researcher(s) names	n/a
Co-researcher(s) email addresses	n/a
Review track	**Normal**
Brief description of the research project	**The purpose of this research is explanatory in that it explains both the influences on self-efficacy, and the influence of self-efficacy on consumer behaviour in securing their IoT devices.** **The main objective of this research is to determine the antecedents and consequences of IoT security self-efficacy. To reach this objective, the following sub-objectives need to be addressed:** **1. Identify the antecedents of IoT security self-efficacy.** **2. Identify the consequences of IoT security self-efficacy.** **3. Identify the impact of IoT security self-efficacy consequences on IoT security practices and behaviour.**
Data collection method	**Questionnaire**
Research proposal and other supporting documents	BHRRAE003_-_Research_Design_Revised_16_March_2022.pdf BHRRAE003_-_Cover_Letter_-_IndividualParticipants.pdf
2. PARTICIPANTS	n/a
2.1 Please indicate the affiliations of participants	**General public** **Students/learners** **Other**

* Other - please specify below	**Researchers networks**
2.2 Does the research differentiate between participants on the age, religion, income, handicap, illness or any similar classification? (Race/ethnicity and gender are addressed in later questions.)	**No**
2.3 Does the research require the participation of socially or physically vulnerable people (children, aged, disabled, etc.) or legally restricted groups?	**No**
2.4 Will you be able to secure the informed consent of all participants in the research (in the case of children, will you be able to obtain the consent of their guardians or parents)?	**Yes**
2.5 Will any confidential data or identifiable records of individuals be kept following the completion of the project?	**No**
2.6 In reporting on this research, is there any possibility that you will not be able to keep the identities of the individuals involved anonymous?	**No**
2.7 Does the research include making payments or giving gifts to any participants?	**No**
2.8 Race/ethnicity - Are you asking a question about race or ethnicity in your questionnaire?	**Yes**
Motivation	**For the possibility of drawing insights from demographic data. The respondent is not obliged to provide a response.**
Which race categories have been used?	**African** **Coloured** **Indian** **White/Caucasian** **Other**
Other: please specify	**Other**
Have you included the option: "Prefer not to answer" as part of your race/ethnicity question?	**Yes**
2.9 Gender - Are you asking a question about gender in your questionnaire?	**Yes**
Motivation	**For the possibility of drawing insights from demographic data. The respondent is not obliged to provide a response.**
Which gender categories have been used?	**Female** **Male** **Other**
Other: please specify	**Other**
Have you included the option: "Prefer not to answer" as part of your gender question?	**Yes**

3. PROVISION OF SERVICES	n/a
3.1 Does your research involve the provision of services to communities, and/or could it significantly influence decisions they make?	**No**
4. ORGANISATIONAL PERMISSION	n/a
4.1 Is your research going to be conducted inside an organisation (other than UCT)?	**No**
4.2 Are you making use of UCT students as respondents for your research?	**Yes**
Please acknowledge that approval from the Department of Student Affairs will be obtained before commencing research	**I confirm that approval from the Executive Director of Student Affairs will be obtained**
4.3 Are you making use of UCT staff as respondents for your research?	**No**
5. INFORMED CONSENT	n/a
5.1 What type of consent will be obtained from study participants?	**No consent required (e.g. anonymous survey questionnaire with covering letter)**
6. CONFLICT OF INTEREST	n/a
6.1 Is there any existing or potential conflict of interest between a research sponsor, academic supervisor, other researchers, or participants?	**No**
6.2 Will information that reveals the identity of participants be supplied to a research sponsor, other than with the permission of the individuals?	**No**
6.3 Are you aware of any other conflict of interest that you would like to declare?	**No**
7. RISK TO PARTICIPANTS	n/a
7.1 Does the proposed research pose any foreseeable physical, psychological, social, legal, economic, or other risks to participants, whether immediate or in the future?	**No**
8. DATA MANAGEMENT PLAN	n/a
8.1 After concluding the research, I intend to share my data on an open platform	**No**
Advisory: UCT Research Data Management Policy	**The UCT policy on research data states, inter alia, that: "All researchers are urged to include a data management plan, while grant holders and their research groups are obliged to do so. The data management plan relates to issues such as UCT's desire to encourage open-access data, to facilitate replication, transparency, and social engagement with research. The starting premise is that publically-funded research data are a public good, produced in the public interest and should be openly available free of charge to encourage extensive reuse." In light of this and other aspects of the Research Data Management Policy (linked below), please be aware that your research proposal should explain why you are not able to make your research data openly available. https://www.uct.ac.za/sites/default/files/image_tool/images/328/about/policies/TGO_Policy_Research_Data_Manage**

8.2 Data security during and after the study	**I intend to store the research data on my laptop/desktop** **I intend to store the research data on a password protected cloud platform (Google Docs, Dropbox etc.)**
9. CHECKLIST	n/a
9.1 I hereby undertake to carry out my research in such a way that:	**There is no anticipated legal objection to the nature or the method of research** **The research will not compromise staff or students or compromise the interests of the University** **Limitations and alternative interpretations of my findings will be considered** **The findings could be subject to peer review, and will be publicly available** **I will respect intellectual property rights, and avoid any practice that would constitute plagiarism**
9.2 I confirm that I have:	**Read the Commerce Faculty Ethics in Research Policy** **Attached a copy of my research proposal, including methodology, ethical considerations, and a data management plan** **Uploaded all interview schedules/questionnaires/forms and any other relevant documents** **Submitted organisational consent letters, where applicable and available** **Included a cover letter/consent form that includes the UCT logo, a clear explanation of the research, contact details of the researcher and supervisor (where applicable), as well as relevant guidance to participants drawn from the list below**
Examples of cover letter components	*** This research has been approved by the Commerce Faculty Ethics in Research Committee. * Your participation in this research is voluntary. You can choose to withdraw from the research at any time. * The questionnaire will take approximately X minutes to complete * You will not be requested to supply any identifiable information, ensuring anonymity of your responses. * If personal data are collected, published data will be anonymised. * Due to the nature of the study you will need to provide the researchers with some form of identifiable information however, all responses will be confidential and used for the purposes of this research only.**
Are you satisfied that your proposed research addresses possible ethical concerns, and can you confirm that your supervisor endorsed this application?	**Yes**
Signature form (must include supervisor's signature) **COM_Ethics_Signatories.pdf**	

ii. Ethical Approval Confirmation

From: Jacques Rousseau
To: Raeesa Behardien
Subject: Commerce Faculty Ethics approval: "Antecedents and consequences of Internet of Things Security Self-Efficacy"

Commerce_Ethics_Approval_Letter_Behardien_2022_05_006.pdf

Dear Raeesa Behardien,

Thank you for your submission to the Ethics in Research Committee.

Your application has been approved, and your signed ethics clearance and reference number is attached, and can also be downloaded via Submittable again in the future.

Regards,

Commerce Ethics in Research

Figure 18: Commerce Faculty Ethics Approval

Appendix 6: Instrument Correlation

The following represent the instrument correlation for this study. The data has been split across two tables and limited to 2 decimal places for ease of presentation.

	BI1	BI2	BI3	BI4	CK1	CK2	CK3	CK4	DE1	DE2	DE3	DE4	DE5	GC1	GC2	GC3	GC4	GC5	GC6	GC7
BI1	1.00	0.00	0.00	0.00	0.41	0.39	0.35	0.32	0.34	0.43	0.33	0.39	0.38	0.32	0.34	0.39	0.39	0.46	0.43	0.52
BI2	0.67	1.00	0.00	0.00	0.39	0.40	0.32	0.38	0.33	0.39	0.29	0.38	0.36	0.32	0.35	0.35	0.37	0.40	0.38	0.45
BI3	0.56	0.49	1.00	0.00	0.44	0.42	0.32	0.42	0.38	0.43	0.41	0.42	0.47	0.36	0.34	0.45	0.42	0.45	0.43	0.40
BI4	0.58	0.60	0.49	1.00	0.46	0.37	0.36	0.42	0.33	0.38	0.27	0.32	0.34	0.25	0.30	0.39	0.28	0.38	0.33	0.44
CK1	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CK2	0.00	0.00	0.00	0.00	0.74	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CK3	0.00	0.00	0.00	0.00	0.61	0.70	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CK4	0.00	0.00	0.00	0.00	0.73	0.66	0.63	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DE1	0.00	0.00	0.00	0.00	0.49	0.45	0.34	0.45	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DE2	0.00	0.00	0.00	0.00	0.53	0.54	0.42	0.52	0.57	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DE3	0.00	0.00	0.00	0.00	0.62	0.54	0.52	0.58	0.53	0.58	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DE4	0.00	0.00	0.00	0.00	0.57	0.53	0.44	0.53	0.50	0.54	0.66	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DE5	0.00	0.00	0.00	0.00	0.66	0.66	0.57	0.65	0.53	0.55	0.72	0.71	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
GC1	0.00	0.00	0.00	0.00	0.24	0.27	0.28	0.30	0.29	0.25	0.28	0.26	0.36	1.00	0.00	0.00	0.00	0.00	0.00	0.00
GC2	0.00	0.00	0.00	0.00	0.31	0.25	0.24	0.32	0.30	0.24	0.31	0.34	0.32	0.60	1.00	0.00	0.00	0.00	0.00	0.00
GC3	0.00	0.00	0.00	0.00	0.39	0.39	0.39	0.44	0.46	0.42	0.43	0.39	0.46	0.55	0.56	1.00	0.00	0.00	0.00	0.00

	BI1	BI2	BI3	BI4	CK1	CK2	CK3	CK4	DE1	DE2	DE3	DE4	DE5	GC1	GC2	GC3	GC4	GC5	GC6	GC7
GC4	0.00	0.00	0.00	0.00	0.47	0.46	0.47	0.46	0.38	0.40	0.59	0.52	0.54	0.50	0.50	0.48	1.00	0.00	0.00	0.00
GC5	0.00	0.00	0.00	0.00	0.50	0.48	0.49	0.48	0.42	0.45	0.59	0.55	0.58	0.39	0.44	0.50	0.71	1.00	0.00	0.00
GC6	0.00	0.00	0.00	0.00	0.35	0.36	0.42	0.39	0.37	0.39	0.54	0.48	0.48	0.50	0.40	0.51	0.61	0.63	1.00	0.00
GC7	0.00	0.00	0.00	0.00	0.47	0.45	0.45	0.43	0.40	0.34	0.50	0.50	0.50	0.46	0.42	0.54	0.62	0.61	0.67	1.00
ISSE1	0.00	0.00	0.00	0.00	0.39	0.40	0.47	0.38	0.39	0.37	0.45	0.43	0.44	0.49	0.44	0.52	0.51	0.51	0.50	0.55
ISSE2	0.00	0.00	0.00	0.00	0.41	0.49	0.52	0.43	0.46	0.37	0.49	0.49	0.49	0.48	0.39	0.49	0.56	0.59	0.60	0.57
ISSE3	0.00	0.00	0.00	0.00	0.34	0.37	0.30	0.40	0.34	0.33	0.38	0.38	0.42	0.41	0.47	0.34	0.48	0.49	0.47	0.48
ISSE4	0.00	0.00	0.00	0.00	0.45	0.47	0.41	0.48	0.47	0.48	0.43	0.47	0.49	0.39	0.43	0.45	0.41	0.45	0.44	0.59
ISSE5	0.00	0.00	0.00	0.00	0.42	0.46	0.46	0.49	0.46	0.48	0.42	0.41	0.48	0.50	0.48	0.52	0.45	0.50	0.55	0.51
ISSE6	0.00	0.00	0.00	0.00	0.46	0.39	0.44	0.42	0.35	0.30	0.48	0.37	0.47	0.54	0.49	0.50	0.53	0.53	0.59	0.60
ISSE7	0.00	0.00	0.00	0.00	0.47	0.51	0.47	0.54	0.41	0.43	0.48	0.40	0.50	0.45	0.46	0.53	0.49	0.51	0.54	0.57
SBI1	0.00	0.00	0.00	0.00	0.38	0.44	0.38	0.39	0.31	0.30	0.39	0.42	0.50	0.00	0.00	0.00	0.00	0.00	0.00	0.00
SBI2	0.00	0.00	0.00	0.00	0.22	0.28	0.17	0.19	0.22	0.18	0.24	0.26	0.27	0.00	0.00	0.00	0.00	0.00	0.00	0.00
SBI3	0.00	0.00	0.00	0.00	0.24	0.29	0.17	0.25	0.30	0.26	0.25	0.30	0.27	0.00	0.00	0.00	0.00	0.00	0.00	0.00
SP-B1	0.13	0.09	0.17	0.11	0.11	0.14	0.06	0.07	0.04	0.07	0.08	0.14	0.13	0.07	0.05	0.04	0.10	0.18	0.24	0.19
SP-B2	0.54	0.44	0.40	0.52	0.35	0.40	0.43	0.37	0.36	0.45	0.35	0.41	0.45	0.28	0.19	0.41	0.28	0.37	0.37	0.43
SP-B3	0.43	0.41	0.28	0.43	0.30	0.39	0.43	0.36	0.26	0.34	0.31	0.30	0.35	0.32	0.16	0.30	0.28	0.40	0.37	0.42
SP-B4	0.44	0.38	0.37	0.40	0.31	0.38	0.27	0.28	0.26	0.32	0.25	0.36	0.38	0.25	0.18	0.23	0.24	0.29	0.30	0.35
SP-B5	0.36	0.26	0.28	0.44	0.19	0.21	0.23	0.28	0.20	0.30	0.26	0.23	0.31	0.34	0.24	0.25	0.21	0.27	0.36	0.28
SP-B6	0.42	0.43	0.33	0.46	0.42	0.39	0.31	0.39	0.28	0.33	0.29	0.32	0.31	0.30	0.34	0.41	0.32	0.40	0.40	0.44
SP-T1	0.00	0.00	0.00	0.00	0.46	0.42	0.43	0.49	0.38	0.46	0.51	0.46	0.47	0.32	0.24	0.48	0.43	0.51	0.52	0.50

	BI1	BI2	BI3	BI4	CK1	CK2	CK3	CK4	DE1	DE2	DE3	DE4	DE5	GC1	GC2	GC3	GC4	GC5	GC6	GC7
SP-T2	0.00	0.00	0.00	0.00	0.45	0.46	0.44	0.49	0.34	0.43	0.53	0.48	0.42	0.34	0.33	0.52	0.47	0.51	0.49	0.54
SP-T3	0.00	0.00	0.00	0.00	0.43	0.44	0.38	0.42	0.39	0.37	0.51	0.51	0.55	0.35	0.35	0.42	0.57	0.57	0.53	0.50

Table 35: Instrument correlation - Table 1

	ISSE1	ISSE2	ISSE3	ISSE4	ISSE5	ISSE6	ISSE7	SBI1	SBI2	SBI3	SP-B1	SP-B2	SP-B3	SP-B4	SP-B5	SP-B6	SP-T1	SP-T2	SP-T3
BI1	0.45	0.38	0.42	0.50	0.43	0.39	0.41	0.21	0.12	0.15	0.00	0.00	0.00	0.00	0.00	0.00	0.47	0.52	0.42
BI2	0.39	0.39	0.44	0.52	0.48	0.36	0.49	0.22	0.16	0.20	0.00	0.00	0.00	0.00	0.00	0.00	0.42	0.50	0.42
BI3	0.38	0.42	0.35	0.37	0.37	0.45	0.46	0.29	0.17	0.17	0.00	0.00	0.00	0.00	0.00	0.00	0.46	0.47	0.37
BI4	0.40	0.32	0.38	0.53	0.48	0.36	0.51	0.16	0.02	0.09	0.00	0.00	0.00	0.00	0.00	0.00	0.41	0.44	0.32
CK1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CK2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CK3	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CK4	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DE1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DE2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DE3	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DE4	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DE5	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
GC1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.29	0.17	0.19	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

	ISSE1	ISSE2	ISSE3	ISSE4	ISSE5	ISSE6	ISSE7	SBI1	SBI2	SBI3	SP-B1	SP-B2	SP-B3	SP-B4	SP-B5	SP-B6	SP-T1	SP-T2	SP-T3
GC2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.25	0.09	0.10	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
GC3	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.30	0.19	0.22	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
GC4	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.44	0.31	0.27	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
GC5	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.42	0.23	0.27	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
GC6	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.35	0.20	0.19	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
GC7	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.30	0.17	0.21	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
ISSE1	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.36	0.20	0.16	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
ISSE2	0.68	1.00	0.00	0.00	0.00	0.00	0.00	0.41	0.23	0.20	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
ISSE3	0.48	0.49	1.00	0.00	0.00	0.00	0.00	0.28	0.13	0.19	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
ISSE4	0.59	0.46	0.65	1.00	0.00	0.00	0.00	0.29	0.15	0.22	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
ISSE5	0.60	0.59	0.60	0.69	1.00	0.00	0.00	0.25	0.08	0.16	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
ISSE6	0.52	0.56	0.54	0.46	0.60	1.00	0.00	0.34	0.16	0.13	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
ISSE7	0.56	0.53	0.58	0.63	0.71	0.69	1.00	0.35	0.10	0.14	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
SBI1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
SBI2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.56	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
SBI3	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.51	0.67	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
SP-B1	0.14	0.24	0.09	0.06	0.08	0.17	0.16	0.14	0.24	0.10	1.00	0.00	0.00	0.00	0.00	0.00	0.17	0.14	0.14
SP-B2	0.39	0.38	0.45	0.48	0.43	0.37	0.45	0.20	0.05	0.14	0.10	1.00	0.00	0.00	0.00	0.00	0.44	0.45	0.35
SP-B3	0.29	0.40	0.41	0.39	0.44	0.34	0.41	0.15	0.07	0.13	0.10	0.60	1.00	0.00	0.00	0.00	0.39	0.41	0.34
SP-B4	0.30	0.30	0.39	0.40	0.35	0.28	0.27	0.19	0.10	0.12	0.22	0.58	0.51	1.00	0.00	0.00	0.34	0.35	0.25
SP-B5	0.30	0.31	0.38	0.36	0.41	0.27	0.35	0.13	-0.02	0.02	0.13	0.53	0.48	0.43	1.00	0.00	0.24	0.27	0.26

	ISSE1	ISSE2	ISSE3	ISSE4	ISSE5	ISSE6	ISSE7	SBI1	SBI2	SBI3	SP-B1	SP-B2	SP-B3	SP-B4	SP-B5	SP-B6	SP-T1	SP-T2	SP-T3
SP-B6	0.38	0.38	0.39	0.45	0.41	0.40	0.47	0.16	0.05	0.06	0.09	0.48	0.43	0.47	0.42	1.00	0.28	0.37	0.43
SP-T1	0.36	0.45	0.33	0.38	0.39	0.47	0.47	0.31	0.25	0.33	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00
SP-T2	0.47	0.47	0.34	0.45	0.51	0.48	0.53	0.27	0.15	0.23	0.00	0.00	0.00	0.00	0.00	0.00	0.61	1.00	0.00
SP-T3	0.43	0.49	0.41	0.39	0.47	0.45	0.48	0.42	0.24	0.27	0.00	0.00	0.00	0.00	0.00	0.00	0.52	0.53	1.00

Table 36: Instrument correlation - Table 2

Appendix 7: Factor Analysis

i. Factor Analysis: Iteration 1

Iteration 1 of the factor analysis was conducted making use of Smart PLS 4 and the PLS-SEM Algorithm. The factors in red are highlighted where factor loadings are less than 0,70.

	BI	CK	DE	GC	ISSE	SBI	SP-B	SP-T
BI1	0.86							
BI2	0.84							
BI3	0.75							
BI4	0.82							
CK1		0.88						
CK2		0.89						
CK3		0.85						
CK4		0.87						
DE1			0.76					
DE2			0.78					
DE3			0.86					
DE4			0.83					
DE5			0.87					
GC1				0.73				
GC2				0.71				
GC3				0.76				
GC4				0.82				
GC5				0.79				
GC6				0.81				
GC7				0.81				
ISSE1					0.79			
ISSE2					0.77			
ISSE3					0.77			
ISSE4					0.80			
ISSE5					0.86			
ISSE6					0.78			

	BI	CK	DE	GC	ISSE	SBI	SP-B	SP-T
ISSE7					0.84			
SBI1						0.90		
SBI2						0.81		
SBI3						0.79		
SP-B1							0.25	
SP-B2							0.84	
SP-B3							0.78	
SP-B4							0.77	
SP-B5							0.72	
SP-B6							0.73	
SP-T1								0.84
SP-T2								0.86
SP-T3								0.81

Table 37: Factor Analysis - Iteration 1

ii. Factor Analysis: Iteration 2

Iteration 2 of the factor analysis was conducted making use of Smart PLS 4 and the PLS-SEM Algorithm. The variable SP-B1 was removed as it was below the required 0,70 loading in the previous iteration.

	BI	CK	DE	GC	ISSE	SBI	SP-B	SP-T
BI1	0.86							
BI2	0.84							
BI3	0.75							
BI4	0.82							
CK1		0.88						
CK2		0.89						
CK3		0.85						
CK4		0.87						
DE1			0.76					
DE2			0.78					
DE3			0.86					
DE4			0.83					
DE5			0.87					
GC1				0.73				
GC2				0.71				
GC3				0.76				
GC4				0.82				
GC5				0.79				
GC6				0.81				
GC7				0.81				
ISSE1					0.79			
ISSE2					0.77			
ISSE3					0.77			
ISSE4					0.80			
ISSE5					0.86			
ISSE6					0.78			

	BI	CK	DE	GC	ISSE	SBI	SP-B	SP-T
ISSE7					0.84			
SBI1						0.90		
SBI2						0.81		
SBI3						0.79		
SP-B2							0.84	
SP-B3							0.79	
SP-B4							0.77	
SP-B5							0.72	
SP-B6							0.73	
SP-T1								0.84
SP-T2								0.86
SP-T3								0.81

Table 38: Factor Analysis - Iteration 2

Appendix 8: Qualtrics Results Summary

The [output/code/data analysis] for this paper was generated using Qualtrics software, Version [insert version] of Qualtrics. Copyright © [insert year of copyright] Qualtrics. Qualtrics and all other Qualtrics product or service names are registered trademarks or trademarks of Qualtrics, Provo, UT, USA. https://www.qualtrics.com

i. Age

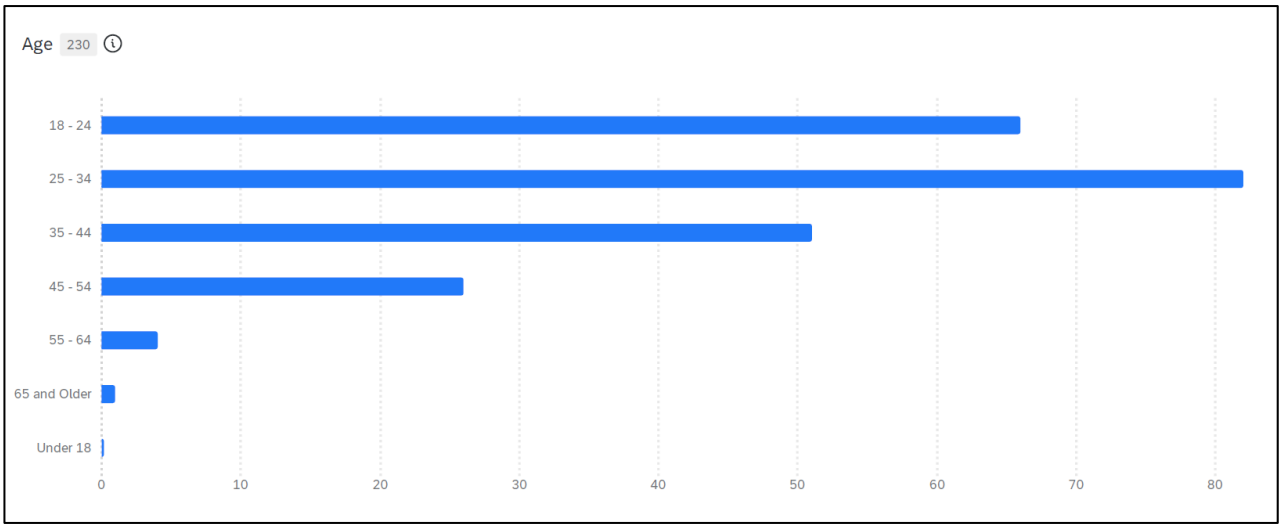

Figure 19: Qualtrics results summary – Age

ii. Gender

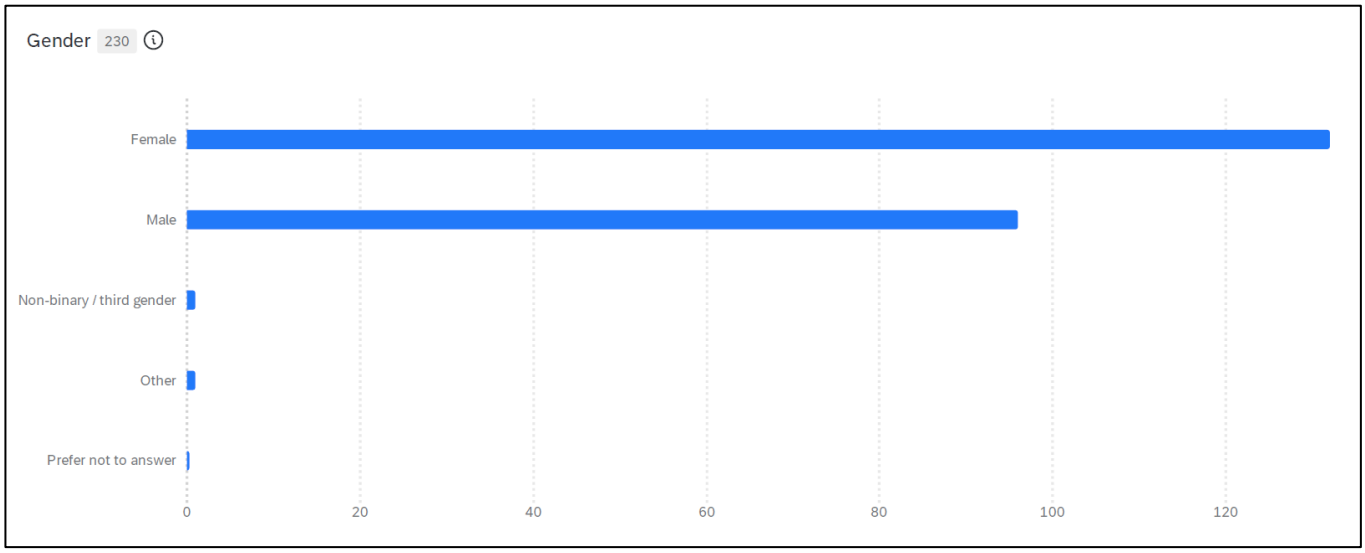

Figure 20: Qualtrics results summary – Gender

iii. Race

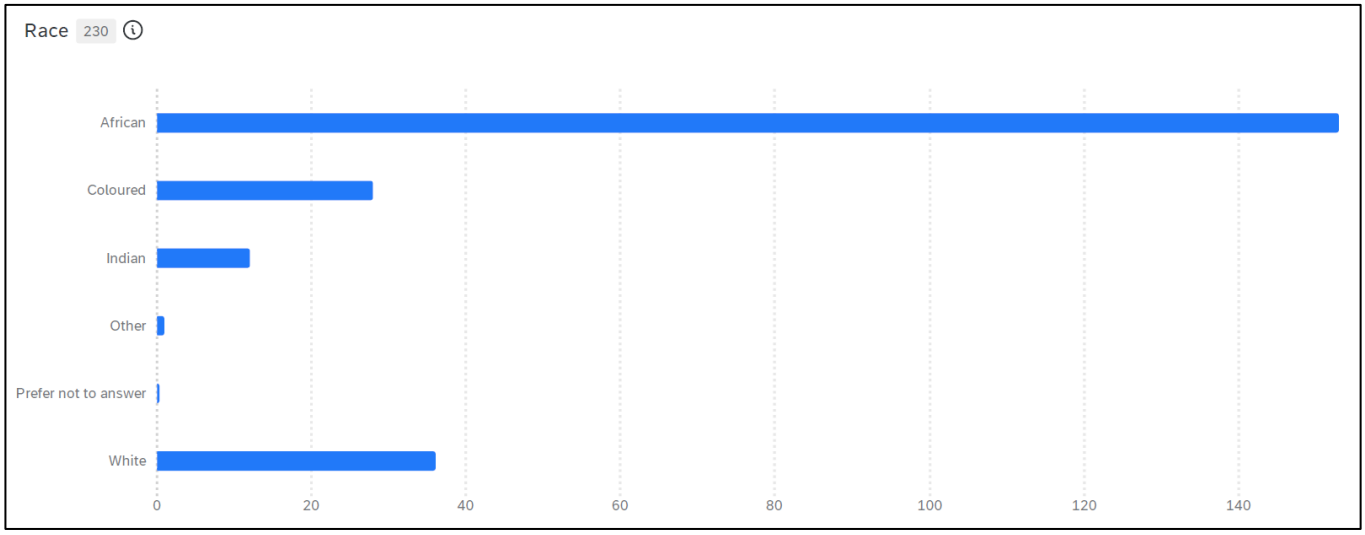

Figure 21: Qualtrics results summary - Race

iv. Consumer Internet of Things (IoT) usage

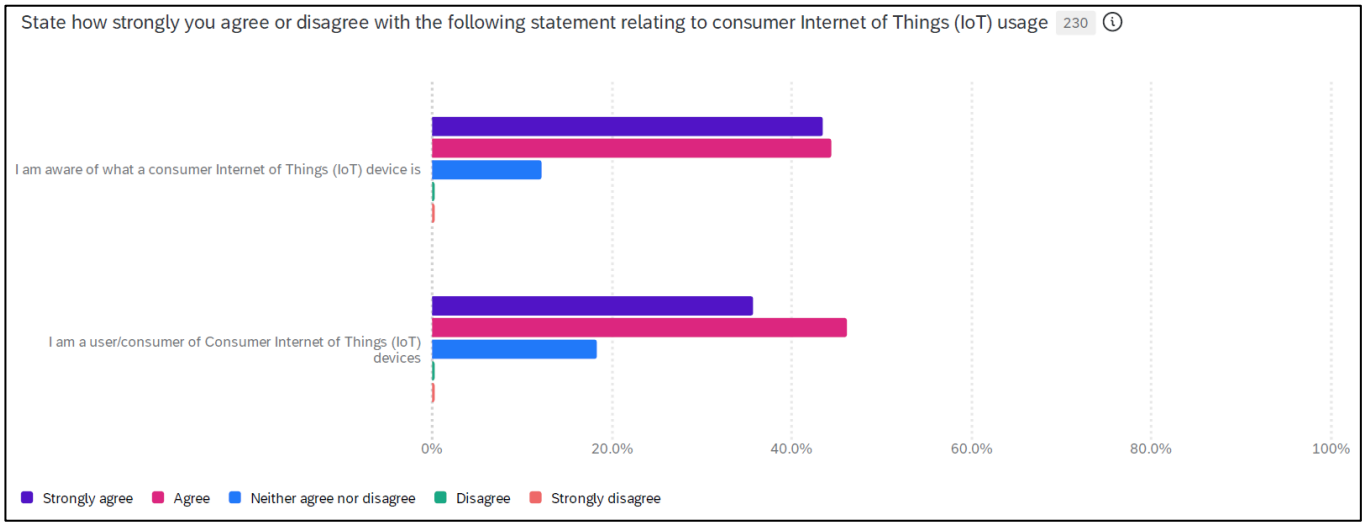

Figure 22: Qualtrics results summary - Consumer IoT usage

v. Consumer IoT Device Knowledge

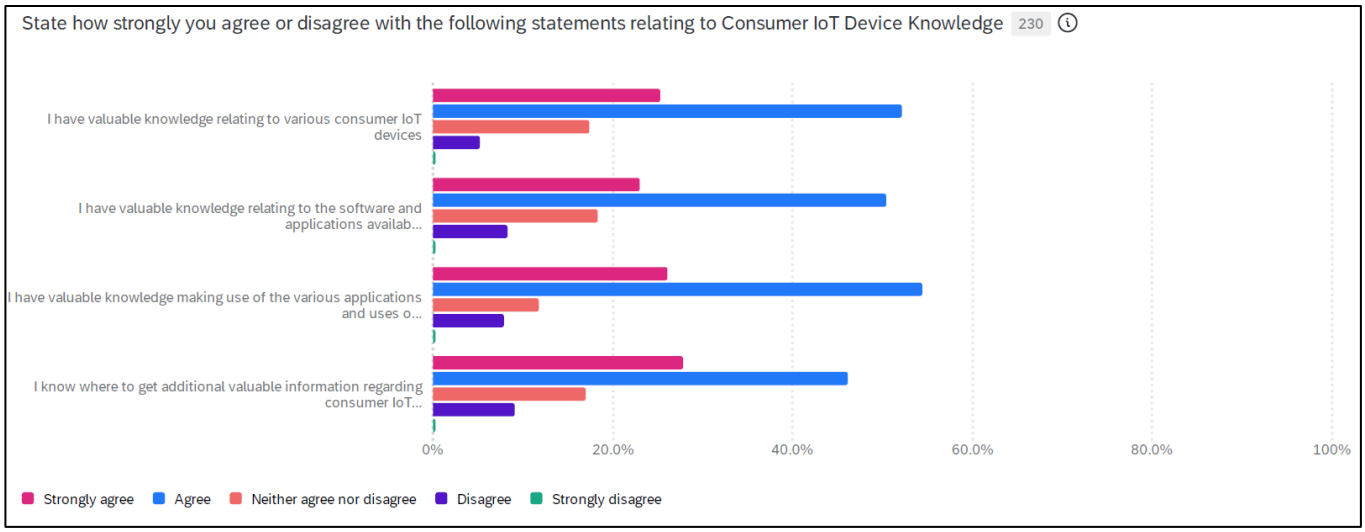

Figure 23: Qualtrics results summary - Consumer IoT device knowledge

vi. Consumer IoT Device Experience

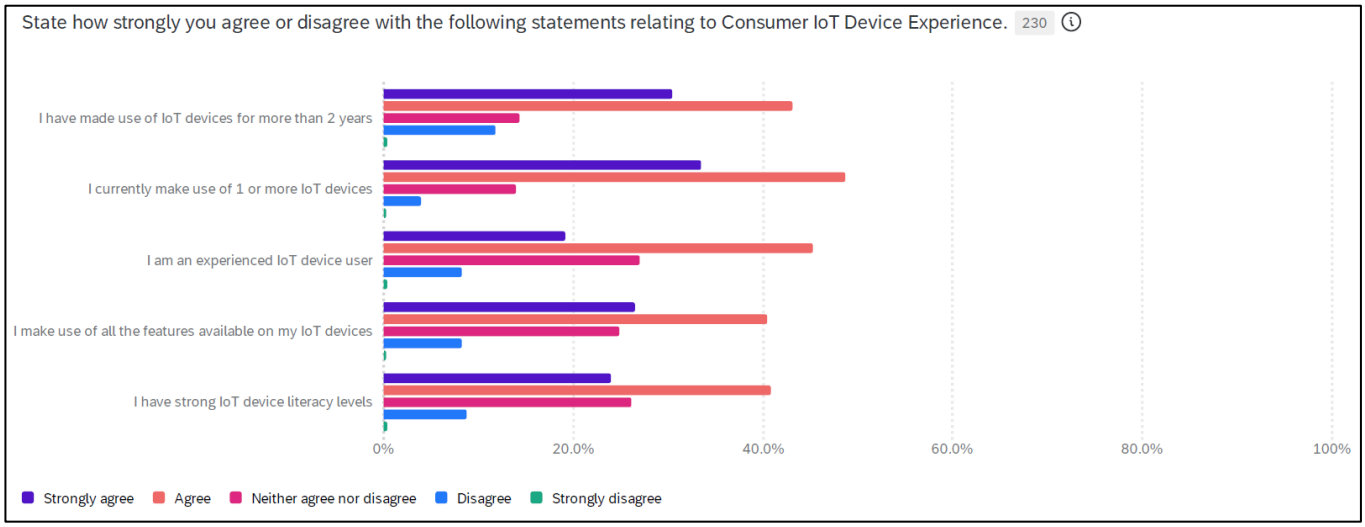

Figure 24: Qualtrics results summary - Consumer IoT device experience

vii. IoT Security Breach Incidents

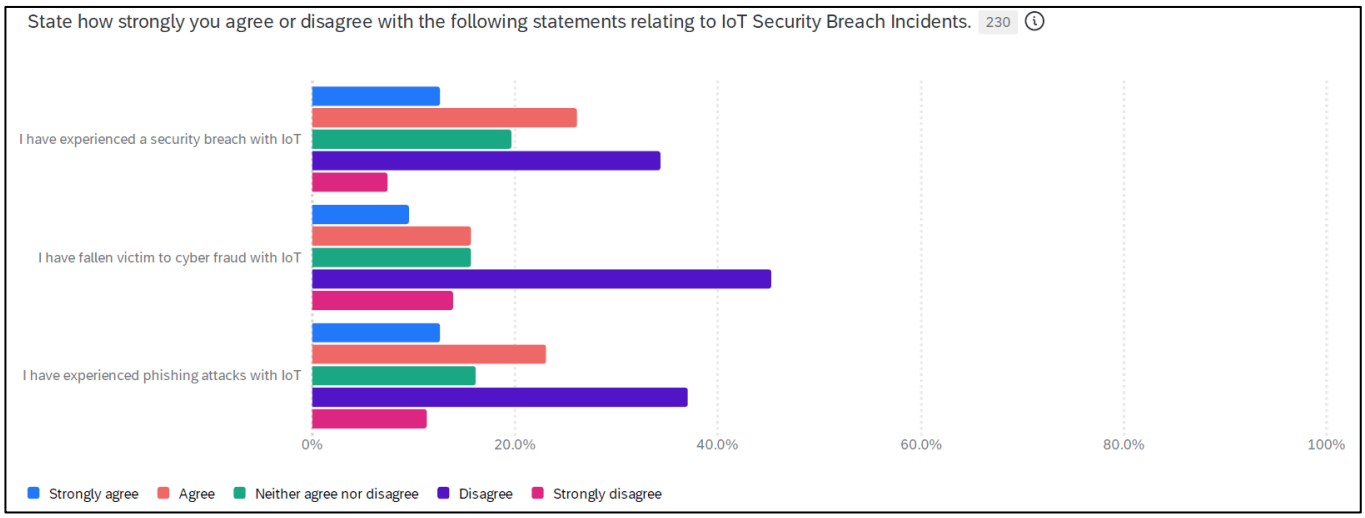

Figure 25: Qualtrics results summary - IoT security breach incidents

viii. Consumer IoT General Controllability

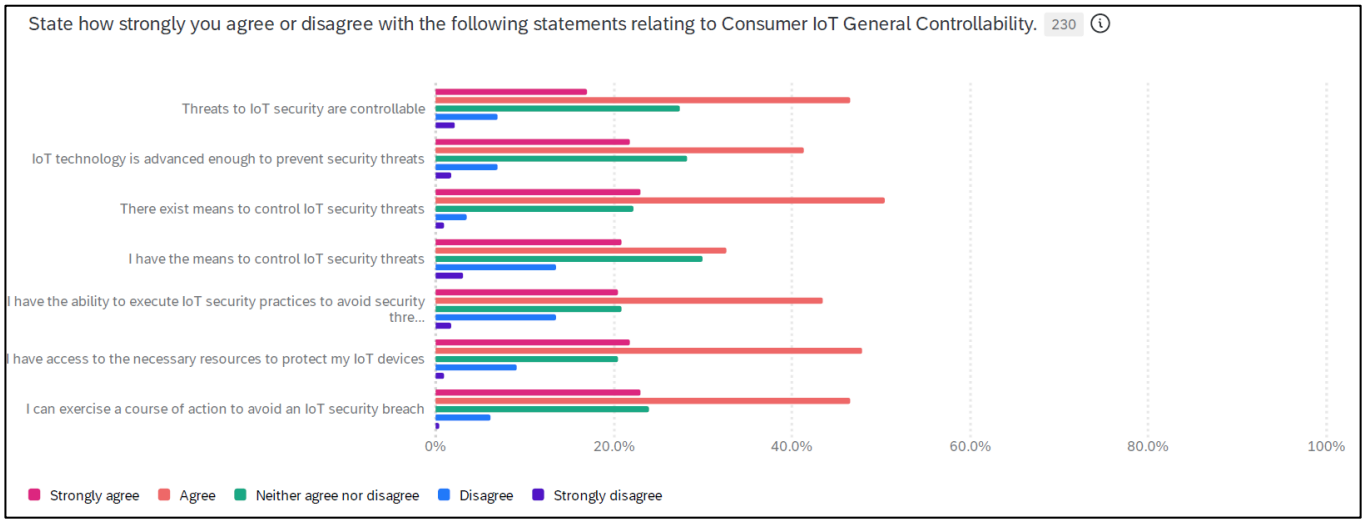

Figure 26: Qualtrics results summary - IoT general controllability

ix. Consumer IoT Security Self-Efficacy

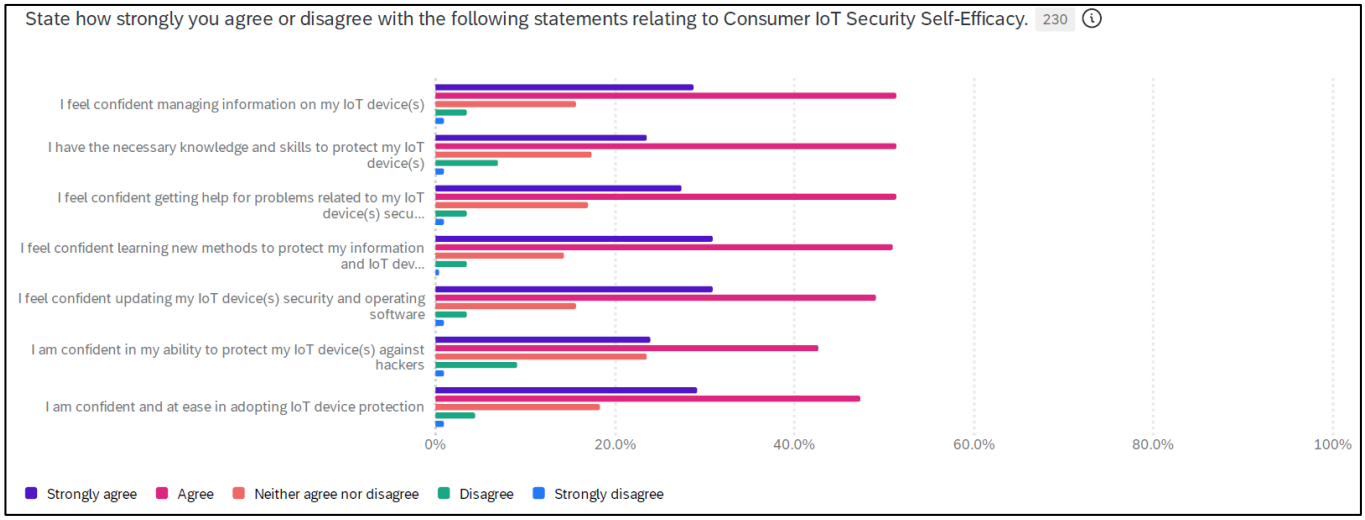

Figure 27: Qualtrics results summary - Consumer IoT security self-efficacy

x. Consumer IoT Security Technology Practices

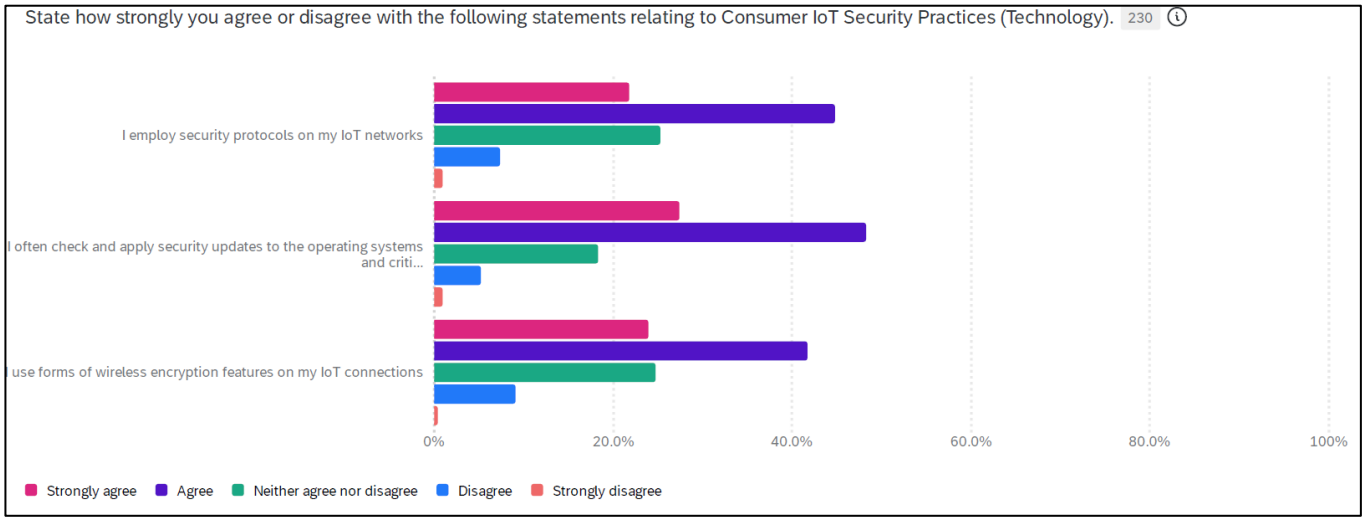

Figure 28: Qualtrics results summary - Consumer IoT security technology practices

xi. Behavioural Intention

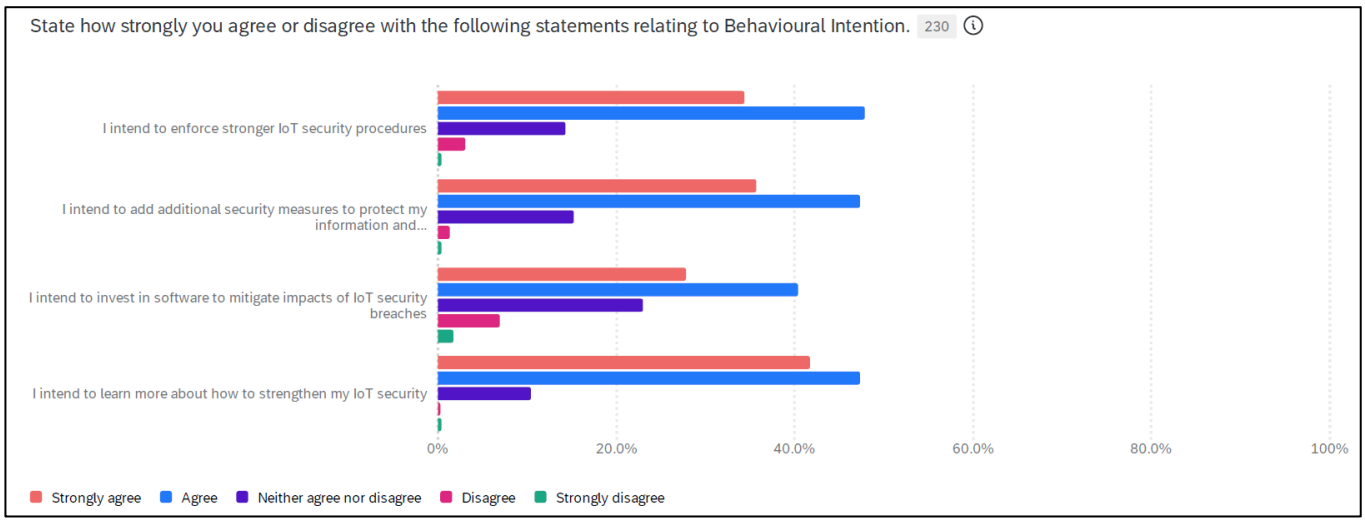

Figure 29: Qualtrics results summary - Behavioural intention

xii. IoT Security Behavioural Practices

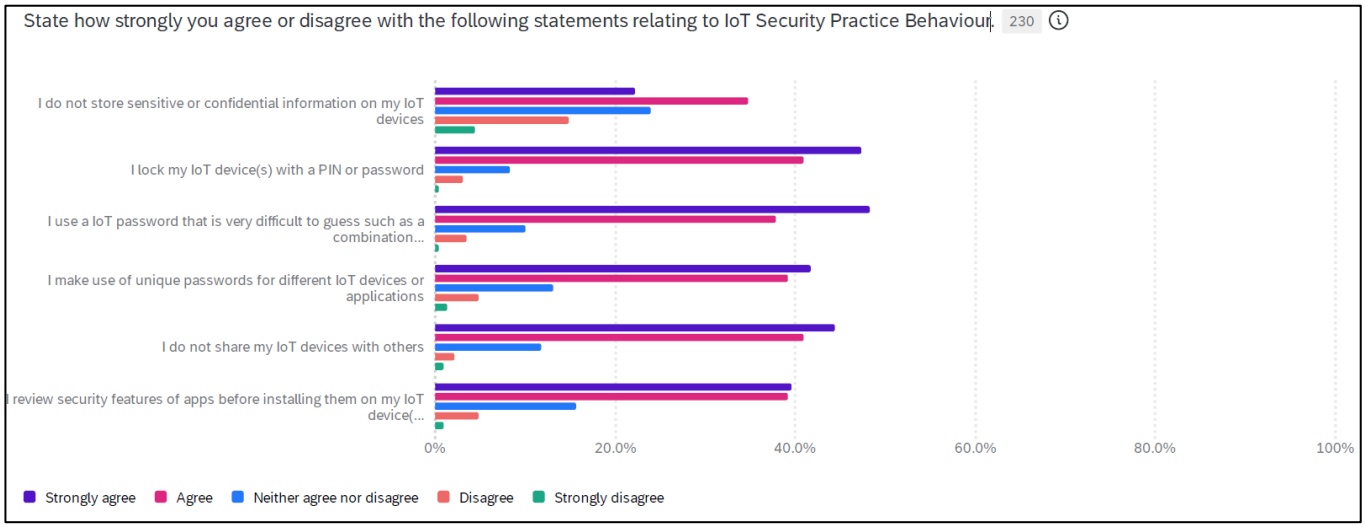

Figure 30: Qualtrics results summary - IoT security behavioural practices

Appendix 9: Graphical Model in SmartPLS 4

i. Factor Loadings, Path Coefficients and R-square

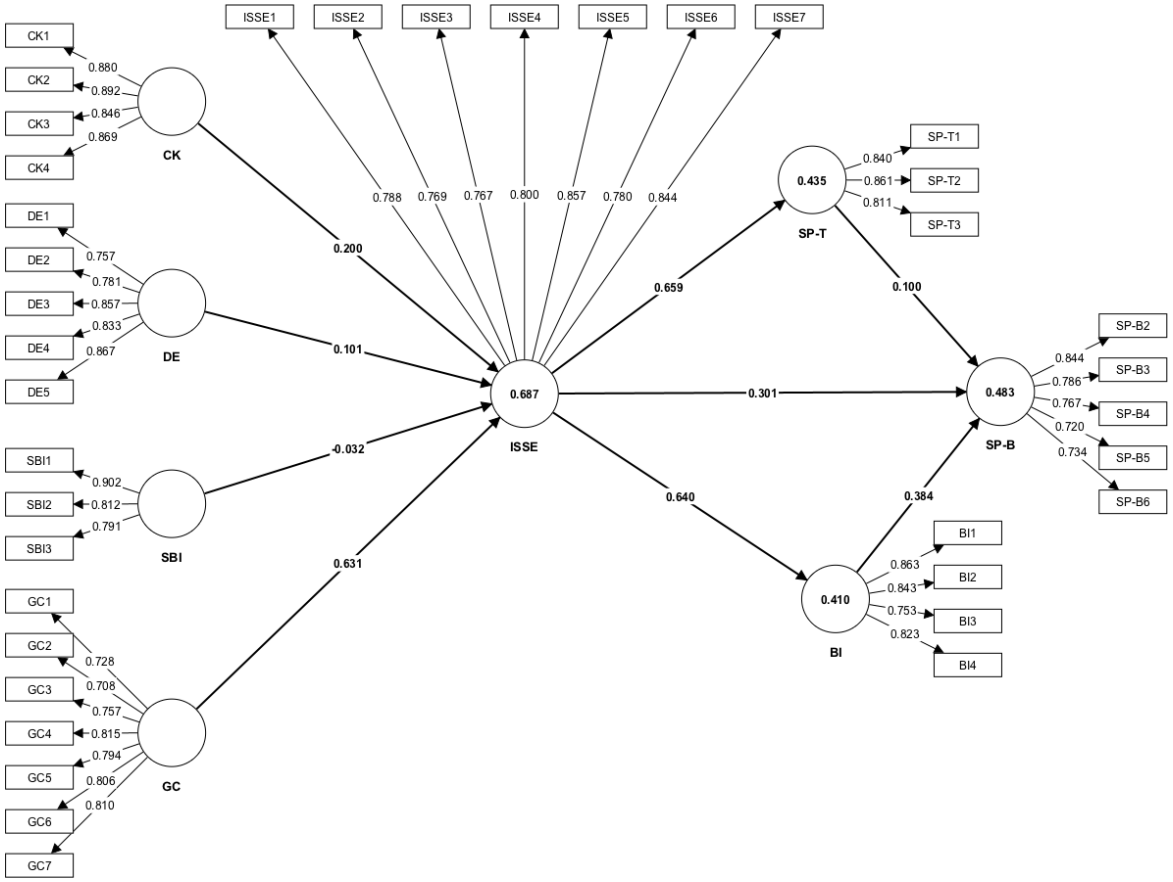

Figure 31: Factor loadings, path coefficients and R-square

ii. P-Values

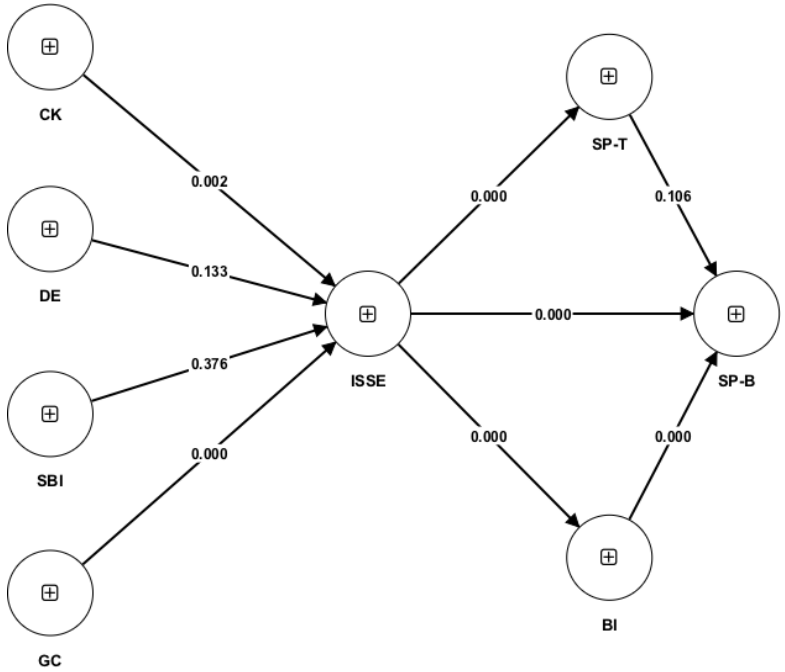

Figure 32: P-Values

iii. Path Coefficients and T-Values

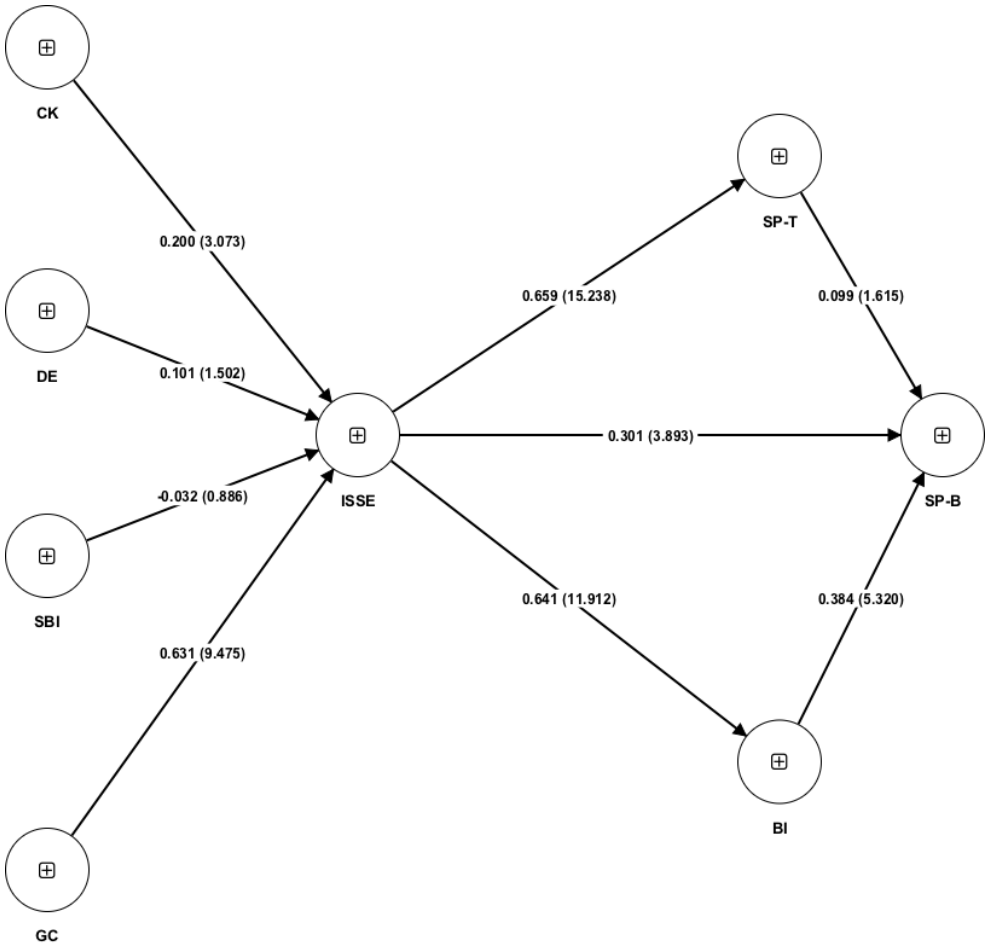

Figure 33: Path coefficients and T-Values