THE INTERNET OF THINGS: SECURITY ATTITUDES, KNOWLEDGE, AND USER BEHAVIOR

by

Zachary Singer

Submitted in partial fulfillment of the

Requirements for Departmental Honors in

The Department of Business Information Systems and Supply Chain Management

Texas Christian University

Fort Worth, Texas

May 7, 2018

THE INTERNET OF THINGS: SECURITY ATTITUDES, KNOWLEDGE, AND USER BEHAVIOR

Project Approved:

Supervising Professor: Beata Jones, Ph.D.

Department of Information Systems and Supply Chain Management

Brad Harris, Ph.D.

Department of Management, Entrepreneurship, and Leadership

Abstract

The Internet of Things has expanded rapidly over the past five years and is expected to grow at an unprecedented pace over the next decade. Accompanying this growth is an increasing number of security vulnerabilities that are present in each one of these connected devices. This paper addressed five research questions aimed at understanding the security attitudes, knowledge, and practices of current Internet of Things device users. The focus was to understand how knowledgeable individuals currently were about the security vulnerabilities present in these devices and how this knowledge affected their attitudes towards security and their willingness to own specific Internet of Things devices. The paper identified literature discussing the current growth of the Internet of Things and highlighted various security vulnerabilities that had been discovered in various devices in the past. The paper also included literature assessing the current attitude and concerns of individuals towards the security of the Internet of Things. In addition to literature, a study was conducted that focused on answering the previously mentioned research questions and aimed to identify disconnects between individual's attitudes, knowledge, and practices regarding Internet of Things security and the willingness to own these devices.

Table of Contents

Introduction

The Internet of Things is defined as the interconnection via the Internet of computing devices embedded in everyday objects. These devices, commonly referred to as the IoT, are becoming increasingly common in many parts of our daily lives. In 2017 alone, 8.4 billion "things" will be in use worldwide that are connected to the Internet (Gartner, 2017). That number is an increase of 31 percent from 2016, and, by 2020, that number is expected to grow to 31 billion devices (Brandon, 2016). Currently, an average digital consumer owns approximately 3.64 connected devices (Buckle, 2017). As technology continues to advance and progress, it continues to affect more and more aspects of our day. Beginning first with the mass adoption of smart phones and traditional computers, the IoT has grown to include watches, TV's, and even household appliances. While these devices are primarily meant to make our lives better and easier, what consumers often don't realize is that, with the rapid growing network of connected devices, there is also a growing security risk that is becoming increasingly hard to ignore. Companies are entering unprecedented territory and many manufacturers are valuing the fast adoption of these devices over taking the time to secure them properly (Brandon, 2017). These devices are more vulnerable than ever, and most consumers have no inclination as to the types of risks they take on when they own or use many IoT devices.

Unfortunately, the United States government is far behind on producing effective legislation to help make the security of these devices more of a priority. Currently, the US Senate has introduced a bill, known as the Internet of Things Cybersecurity Improvement Act of 2017, that would require basic security for IoT devices supplied to the US government (US Senate, 2017). While a start, this bill would only apply to vendors who do business with government entities, and only requires minimal security for these devices; such as no hard-coded passwords

(passwords that cannot be changed) and no known security vulnerabilities (US Senate, 2017). Effects would likely affect the private sector as well, however, to this point, the amount of security that goes into IoT devices has been largely left up to the companies who manufacture them.

As a result, many instances have occurred where IoT devices have been compromised or exploited over the past few years. Common consumer devices, such as Fitbit (McGee, 2016), Amazon Echo (Greenburg, 2017), and the Nest Home Automation (Brandon, 2016) are just a few of the IoT devices that have been subjected to cyber-attacks. From learning the GPS location of a user to listening in on a conversation, the security of these devices is something that can no longer be ignored. One of the largest IoT compromises to date, the Distributed Denial of Service Attack on Dyn (an Internet performance management company) saw over 10s of millions of IoT devices taken over by a few individuals to flood the company with server requests. These requests all came in at one time and had the intent of halting their service (York, 2016). The attack caused much of the east coast to be without access to popular Internet sites such as Twitter, CNN, and PayPal for hours (Turton, 2016). While the intent of the attack was unknown, it showcased the potential for what IoT devices are capable of should certain security precautions not be taken. With many more devices on the way in the next few years, it becomes apparent that security should not be ignored.

The Internet of Things Revolution

There is no doubt that the Internet of Things will continue to grow at a rapid pace. Currently, there are 8.4 billion devices connected to the Internet, and that number is expected to increase to 31 billion in 2020 and to 74 billion in 2025 (Claveria, 2017). Additionally, there is not one specific sector or industry driving the growth, as the Internet of Things has permeated many aspects of an individual's day-to-day life. Wearable devices, including Fitbits and Apple Watches, are expected to grow from 125.5 million units shipped today to 240.1 million units in 2021 (Lamkin, 2017). The automotive industry, another sector affected by the IoT, is expected to see 75% of new cars in 2020 have some form of IoT capability built into them (Greenough, 2015). Apart from the consumer space, business to business products, such as industrial sensors, connected machines, and in-store analysis devices, are already integrated and in use among various enterprises, with approximately 2.5 billion of these devices already on the market (Moon, 2016). That number, as well, is expected to more than double, with an estimated 5.4 billion business-to-business devices connected to the IoT by 2020 (Moon, 2016).

There are many reasons as to why businesses and consumers alike have had such an aggressive adoption of these interconnected devices. For instance, this year 60% of global manufacturers will use analytics data from connected devices to analyze processes and identify optimization possibilities, something they were not capable of before the Internet of Things (IDC, 2017). In addition, that same data analysis will lead to 15% increases in productivity and supply chain performance for most companies (IDC, 2017). This is a huge benefit to businesses, allowing them to deliver products faster, cheaper, and to the right destinations.

Consumers are enjoying the benefits of multiple connected devices as well. For instance, individuals are finding it more convenient to move to connected television, with one study estimating that 168 million individuals in the United States alone will use a connected TV in 2017, up 10.1% from 2016 (eMarketer, 2017). This change has resulted from the consumer's expectation to have the ability to stream TV shows and other forms of media from the Internet to their television in addition to their traditional cable services (eMarketer, 2017).

Another popular IoT product, the "smart speaker", is a device that has already reached 24 million consumers in 2017, with the most popular speaker being Amazon's intelligent personal assistant, Echo (Voicebot, 2017). The Echo interacts with the consumer and gives them information regarding weather, traffic, and news, has the ability to play music, and can even control other connected devices in the home. It provides consumers with an easy ability to access information and will continue to be found in more households in the coming years (Voicebot, 2017).

While all these IoT devices are expected to continue to find their way into more businesses and households, this is not the only source of growth that we expect to see for the IoT. Many new products that do not already utilize the connectivity of the Internet will find ways to do so in the near future. In 2015, there were just under a million units of smart clothing sold worldwide. That figure included shoes and referenced various types of sensor clothing, with the ability to track anything from muscle activity to workplace safety (ReportBuyer, 2016). That figure is expected to grow exponentially to 24.75 billion by 2021, showcasing how much industries can grow with the influence of integrated connectivity (ReportBuyer, 2016). The smart refrigerator is another product that could find its way into households very soon, and it further showcases the unlimited potential for devices that are a part of the Internet of Things (Gilbert, 2016).

Today, 50% of businesses have an established IoT strategy or a pilot project for IoT integration underway, and with $737 billion being spent on the IoT across markets worldwide, there are plenty more connected devices on the way. According to GE, the IoT will add 10 to 15 trillion dollars to the global GDP by 2030, the current size of the Chinese economy, and we can expect all sorts of devices to contribute to that number in the coming years (IDC, 2017).

The Internet of Things and Security

While the expansive network that is the Internet of Things continues to flourish, the security surrounding that network has not. Currently, companies spend an average of only 11% of their IoT budget on securing their IoT devices. Of that 11%, data encryption remains the top method for securing these devices, with 67% of IoT manufacturers reporting data encryption as their primary method of security (Lohrmann, 2017). While encryption is a great step towards ensuring the protection of consumer data, it falls short in adequately addressing other vulnerabilities should these devices be compromised by hackers. Security has a long way to go to catch up to the current pace of IoT growth, but many companies are not sure what to do about it. A recent report revealed that 96% of corporations along with 90% of consumers believe that more IoT security regulations need to be put in place, and that the government should step in to do so (Gemalto, 2017). However, among consumers, only 14% believed that they were extremely knowledgeable when it came to understanding the security of these IoT devices (Gemalto, 2017). While consumers know security is important, a wide knowledge gap still seems to exist for consumers in truly understanding what risks become apparent with the Internet of Things.

A recent survey looked at the current security concerns of the consumer in relation to the IoT and found that 65% of consumers worry that a hacker could gain control of their IoT device, followed by 60% who worried about their data being leaked or stolen (Gemalto, 2017). At present, most companies are encrypting their data, but they are not taking steps to prevent the previously mentioned threats from happening. Instead, IoT manufacturers and retailers are focusing more on the rapid development of their IoT devices in order to reach the market faster at the expense of security. For instance, 80% of current IoT devices do not require a password that is complex enough to provide adequate protection. At the same time, six out of ten devices that provided a user interface were susceptible to a wide range of vulnerabilities in addition to having weak credentials (Patterson, 2017). Contributing to this issue is the fact that only 49% of IoT manufacturers release updates for their devices when vulnerabilities become known, and only 35% of these companies will bring in a security professional to identify the vulnerabilities of their products (Capgemini, 2016).

IoT Past Security Violations

The lack of formal regulation, paired with a company's desire to get their products out into the market as quickly as possible, has already led to a number of instances where devices were compromised or had the potential to be compromised. With the IoT continuing to spread rapidly, no industry is safe. One popular instance involved the Fitbit device, a wearable technology that tracks user information such as heart rate and level of exercise activity. In 2016, hackers were able to infiltrate the accounts of many customers and gain access to their information. While this hack was not a direct result of the device being a part of the Internet of Things, the information that was available to the perpetrators was greatly magnified because of the Fitbit's connectivity to the Internet. Hackers not only had access to customer information, but they also had access to things such as the user's GPS history; allowing them to see popular routes that the specific user might take on their evening run (McGee, 2016). Most individuals are unaware that this information could ever be made available, and it remains to be seen whether becoming aware of vulnerabilities such as this would keep customers from using these items. In addition, security breaches such as this are often as much a fault of the consumer as they are of the company, as the hacked accounts likely had very weak passwords (McGee, 2016). Knowledge of incidents such as this could not only caution consumers to be aware of security when purchasing IoT items, but it could also incentivize them to take more of a precaution when setting up their personal security; such as their password.

Another example of an exploited IoT vulnerability can be found with another popular consumer device, the Amazon Echo; a smart speaker product from Amazon that combines voice recognition with an "intelligent assistant”. A British researcher named Mark Barnes showcased in 2017 how an individual could easily install malware on this Amazon device to turn it into a “personal eavesdropping microphone” without leaving a trace that it had been tampered with (Greenburg, 2017). It would allow the hacker to listen to conversations around the Echo from the “safety of his own home”. Unfortunately, these devices are often left out in offices and hotel rooms, therefore, they are able to be tampered with quite easily (Greenburg, 2017). Amazon was able to fix this issue in their 2017 Echo models; however, any Echo purchased before that time remains vulnerable to the attack. When Amazon commented on the issue they ensured Echo users that their security would be fine as long as they “purchased from trusted retailers” and “ensured their software was up-to-date” (Greenburg, 2017). Unfortunately, a software update does not fix this vulnerability, and, despite these precautions, users with older Amazon Echoes would still be susceptible to this issue (Greenburg, 2017). Again, most users are unaware of both the security vulnerabilities of these devices as well as the lack of initiative on the part of companies to address them, and it is worth studying whether consumers would think twice before purchasing these items if they were first made aware of their vulnerabilities.

While the above instances were rather tame, there are other IoT devices that pose a much greater danger should they be compromised. As vehicles become more connected and society moves towards the mass adoption of driverless cars, they too will become vulnerable to being hacked and could be the targets for various attacks. Already, they pose a large security issue that is becoming harder and harder to ignore. Two researchers named Charlie Miller and Chris Valasek were able to hack into a standard Jeep SUV's Wi-Fi and subsequently move through the vehicle's Control Area Network to take over the main system (Drozhzhin, 2015). From there, they were subsequently able to control the vehicle, having the ability to make it speed up, slow down, or even veer off the road (Drozhzhin, 2015). In another example, a security firm named Trend Macro highlighted a little known hacking technique at DIVMA, a German security conference, which allowed hackers to exploit a car's internal network and interfere with the components that send messages within the vehicle. If a hacker were able to exploit this vulnerability, it would give them the ability to disable the airbags, disable the anti-lock brakes, unlock the car, and even allow them to steal the car (Greenburg, 2017). With autonomous vehicles beginning to become commercially available, this security concern in current transportation becomes a large issue. Many experts agree that autonomous vehicles becoming the normal mode of transportation is not a matter of "if" but a matter of "when" (Rainie, Anderson, 2017) and that "when" may be coming sooner than we think. Unfortunately, the security of these vehicles seems to lag behind their development, and, if potential consumers are made aware of this, it could cause the adoption rate of these vehicles to stall.

Homes do not seem to be safe either when considering IoT security vulnerabilities. “smart locks”, or locks that can be locked and unlocked through a Bluetooth enabled device (such as a cellphone) were recently exploited at a hacker convention known as DEF CON. There, Anthony Rose and Ben Ramsey, two Mercurlite Security employees, were able to break into 12 of 16 different types of smart locks with relative ease (Wollerton, 2016). They found that the passwords used to lock these devices were not encrypted, but rather stored in plain text. For about $100, they were able to hack these locks, discover the password, and unlock the door (Wollerton, 2016).

In addition, a line of products from Nest, the home automation system from Alphabet, has also run into its own set of security problems. One of Nest’s products, a set of Bluetooth enabled security cameras, allows users to easily monitor their home from wherever they may be. However, Jason Doyle, a security researcher, found a way to exploit that Bluetooth connectivity. Since these devices are connected to the Internet, a hacker could easily shut down the camera with a simple Bluetooth command, rendering their main purpose useless (Estes, 2017). It could give a burglar time to enter a home undetected and could even allow a hacker to enter the home’s network; if there are more connected devices on it (Estes, 2017). What’s more, even when Alphabet was made aware of this vulnerability, it was not a priority for them to fix it until these findings were published online (Estes, 2017).

To many individuals, the Internet of Things is seen as a great benefit that will improve our quality of life. Indeed, that does seem to be the main intention of a more connected lifestyle, yet the security vulnerabilities of these devices seem to be ignored in favor of the benefits they provide. Nowhere is this more prevalent than in the Medical Industry. St. Jude, a children’s research hospital, has created connected implantable cardiac devices for use in patients. These devices allow a doctor to monitor and control patient’s heart functions and prevent heart attacks (IoTforall, 2017). Unfortunately, it was recently discovered that even these devices have security flaws, and that a hacker with malicious intent could drain the battery or even administer incorrect pacing to these devices remotely (IoTforall, 2017). A larger focus on the security of these devices could eliminate the potential for these attacks to occur. There are IoT security concerns in all industries, and individuals are not currently considering the full, negative consequences of what could get hacked when using or purchasing these devices.

User Attitudes

Since all of the IoT devices are infiltrating many aspects of an individual’s life, it will be important to look at the current perception of the security of these devices. In the past, before the proliferation of many IoT devices, most studies found that security knowledge was not the issue in influencing an individual’s security behavior. In a 2012 study, Partow-Navid and Slusky discovered that “the major problem with security awareness is not due to a lack of security knowledge, but in the way individuals apply that knowledge in real-world situations” (Partow-Navid and Slusky, 2012). That is, the compliance of security best practices is lower than an individual’s understanding of it (Partow-Navid and Slusky, 2012). Unfortunately, in just the short span of five years, it seems as though this has changed. Now, consumers seem to not only not understand how to implement security best practices with their IoT devices, but they are often unaware of the risks that are involved with using them. In a survey conducted by the Internet of Business (2017), it was determined that “48% of IoT users were not aware of the fact that their IoT devices could be hijacked by hackers and used to initiate wide-scale cyber-attacks.” In addition, approximately four out of five respondents to their survey said that they have “not seen or read a news story that relates to IoT attacks” and, despite warnings, 78% of respondents have not seen their distrust in IoT security grow in the past year (Fearn, 2017). This is problematic, as it would suggest that there is not only a gap between user's knowledge of IoT security and their resulting behavior but also between their attitudes and understanding of the current security of these devices.

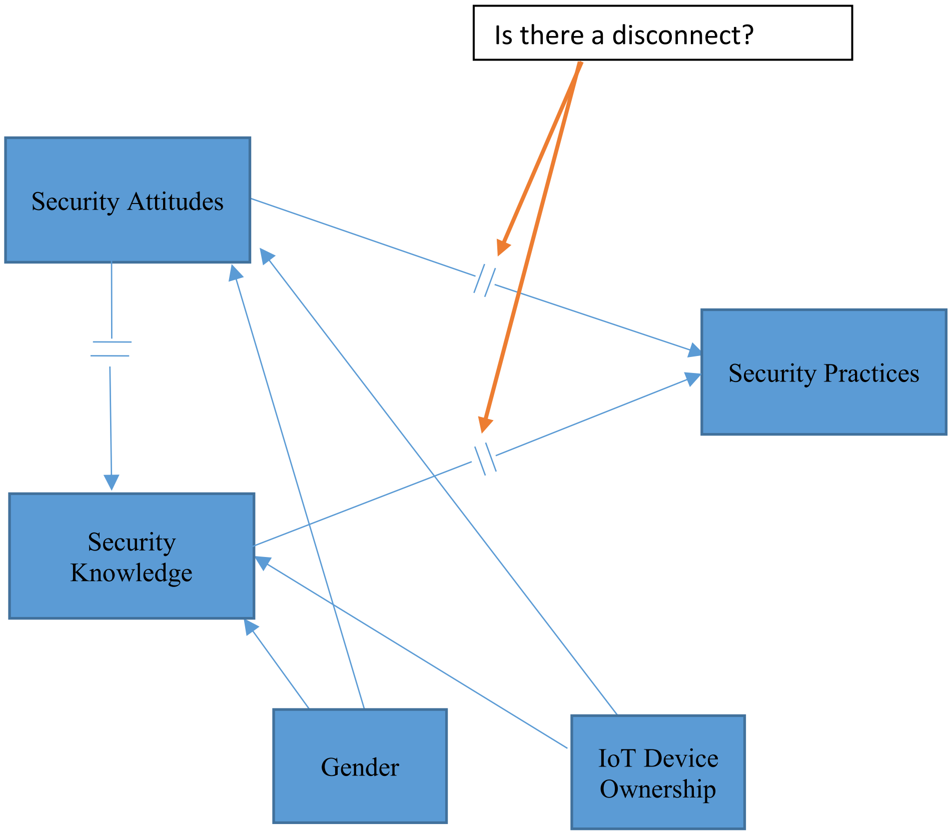
We have seen a similar attitude exhibited by consumers in the past in regards to giving up their privacy for the use of certain mobile applications. In a contradiction, a majority of consumers say that they have a problem with companies pulling personally identifiable information from them, especially without their knowledge. Yet, they are willing to provide this information to companies in order to use an application in lieu of their concern for giving up that information (Acquisti & Grossklags, 2005). In this case, the "performance expectancy" and the "social influence" of using specific mobile applications, such as Snapchat and Google Maps, pushes consumers to forgo their privacy concerns for the utility that comes from using the application (Venkatesh, 2003). In the mind of the consumer, the privacy risks are not enough to outweigh the use of the application. For the most part, it would seem as though IoT security would work the same way. Currently, the majority of consumers at least acknowledge that they are aware of security vulnerabilities in IoT devices, but they often choose to take on these consequences in favor of using these devices based on the utility they provide (IoT Security Foundation, 2017). However, as mentioned above (Internet of Business, 2017), they are largely unaware of what "security vulnerability" actually means. The consequences of security vulnerabilities in IoT devices have the potential to be far worse than their privacy counterparts. As a result, making users aware of the specific incidents of IoT security compromises, such as those listed earlier in this paper, could sway their attitudes enough to affect their behavior.

Theoretical Background

Thus far, it has been shown that individuals who hold a positive outlook about the security of IoT devices are more likely to engage with and feel secure in using these devices. The Theory of Reasoned Action (Ajzen and Fishbein, 1977) explains that an individual’s attitude towards a behavior in conjunction with subjected norms (the perceived social pressure to perform or not perform a behavior) are what influence an individual’s choice to engage in a particular behavior. In addition, the Unified Theory and Acceptance and Use of Technology (UTAUT), explains how age, gender, and experience can have an impact on the behavioral intentions of individuals as it relates to engaging with and using technology.

The following study uses the frameworks of both the Theory of Reasoned Action and UTAUT. The models will be applied to studying how individual behavior is influenced when individuals are made aware and forced to think about the security of various Internet of Things devices. With the rapid adoption of these devices and the inevitability of many more to become commercially available in the near future, it is necessary to look into the individual perception of security for these devices as well as the possible change in behavior that could result when users are made more aware of the vulnerabilities of these devices. Below is a model representation of the study followed by the research questions that the study will aim to answer.

Figure 1: Research Model



Research Questions:

1. What are the current attitudes of IoT users towards the current security of IoT devices?

2. What is the current knowledge of IoT users of the security, and lack thereof, of current IoT devices?

3. What are the current behaviors and practices of IoT users in regards to IoT device usage given their attitudes and knowledge of the security of those devices?

   3a. What are the behaviors and practices of IoT users in regards to IoT device usage after users are made aware of historical/actual security vulnerabilities and breaches of common IoT devices?

   3b. What are the behaviors and practices of IoT users in regards to IoT device usage after users are made aware of potential security vulnerabilities of common IoT devices?

4. How do Socio-demographic factors of IoT users affect attitude towards security, knowledge of security practices, and security-related behavior intentions on IoT devices.

5. Is there a disconnect between the IoT users' security attitudes, knowledge, and their security practices?

Methodology

This study surveys IoT device users across gender and IoT device ownership. It aims to study their attitudes, knowledge, and behavior as they relate to security in IoT devices. A copy of the survey has been included in the appendix.

Participants

Data will be gathered from a convenience sample of 150+ students attending Texas Christian University across various demographic variables such as age, gender, and education level. The participants will be Sophomore, Junior, and Senior business students. This study will be focused on the largest future consumer segment of IoT devices. These participants are considered representative of that segment.

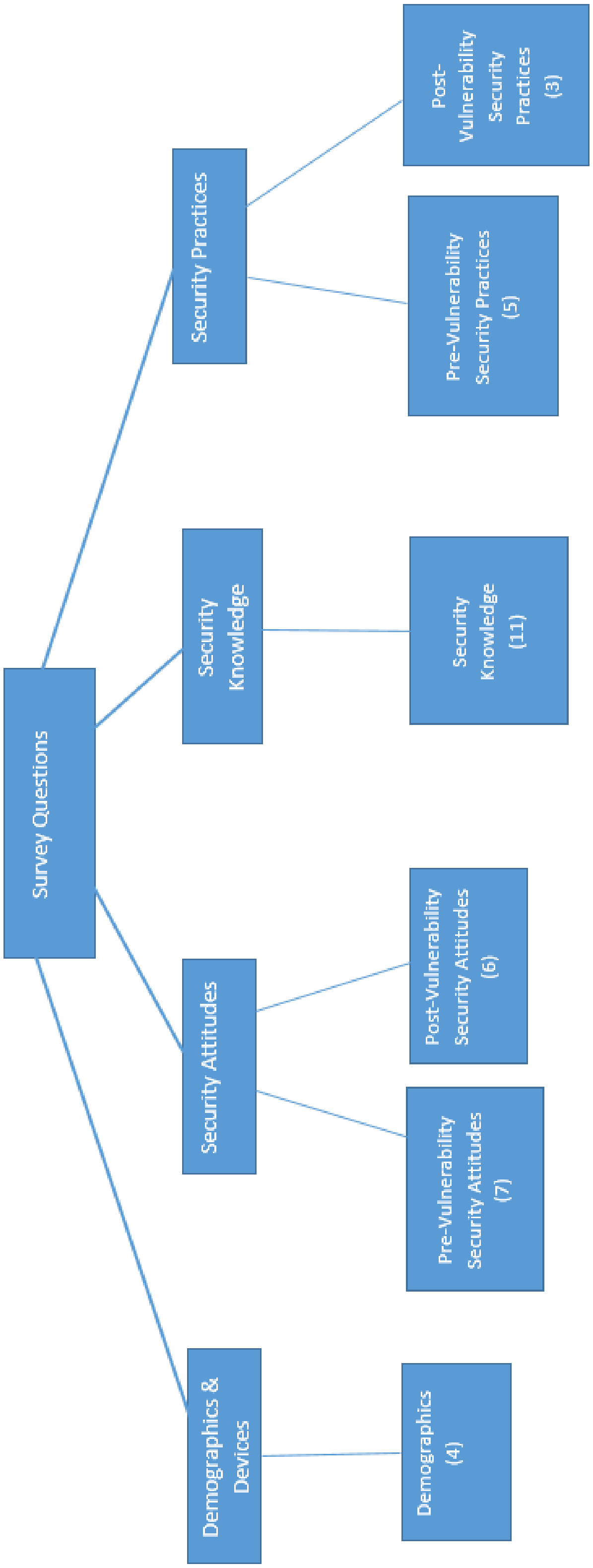
Procedure

In order to study the attitudes, knowledge, and behaviors towards the security of IoT devices of individuals, the investigators will conduct a survey in which participants will be asked to respond to questions that aim to understand their feelings towards current security practices and their responses to security vulnerabilities in IoT devices. Three IoT devices: smart speakers, smart locks, and IoT security cameras, will be used in the survey to showcase vulnerabilities present in IoT devices. The survey will be distributed online via email in business classes. The message associated with the survey will contain a brief description of the purpose of the survey and a link to the survey itself. The survey will be 33 questions and should not take more than 10 minutes to complete. Data will be gathered in March of 2018, and the responses will be organized using Qualtrics.

Measures

After completing a consent form and gathering demographic information, respondents will answer questions regarding their attitudes, knowledge, and behaviors towards the security of IoT devices. A majority of the questions asked in the survey use a seven-point Likert scale to determine the degree to which each respondent agrees with the statement presented. True/false questions and yes/no questions are also included in the survey.

Figure 2: Survey model


Survey Questions
Demographics & Devices
Security Attitudes
Security Knowledge
Security Practices
Demographics (4)
Pre-Vulnerability Security Attitudes (7)
Post-Vulnerability Security Attitudes (6)
Security Knowledge (11)
Pre-Vulnerability Security Practices (5)
Post-Vulnerability Security Practices (3)

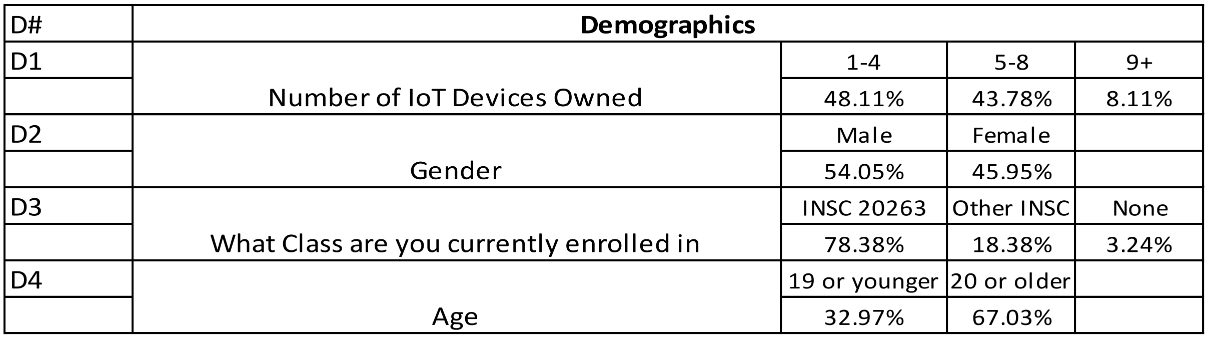
Analysis

After the surveys were administered, each response was checked for completeness and internal consistency. All incomplete and test surveys were removed from the analysis, leaving a total of 185 complete survey responses. For each subset of questions relating to attitudes, knowledge, and practices, a Cronbach Alpha analysis was run to test for internal consistency and reliability among the Likert Scale questions. The results for that analysis are included in the appendix. A summary of the findings, correlations, and disconnects are included in the following sections.

Demographics Data

Four demographic questions included in the survey gathered general information about respondents and were used to study potential correlations relating to gender and IoT device ownership. The questions collected information regarding the respondents' gender, whether or not they were enrolled in a specific business course, their age, as well as the specific IoT devices that they owned. A summary of their answers are included below with percentages of each answer out of 185 responses.

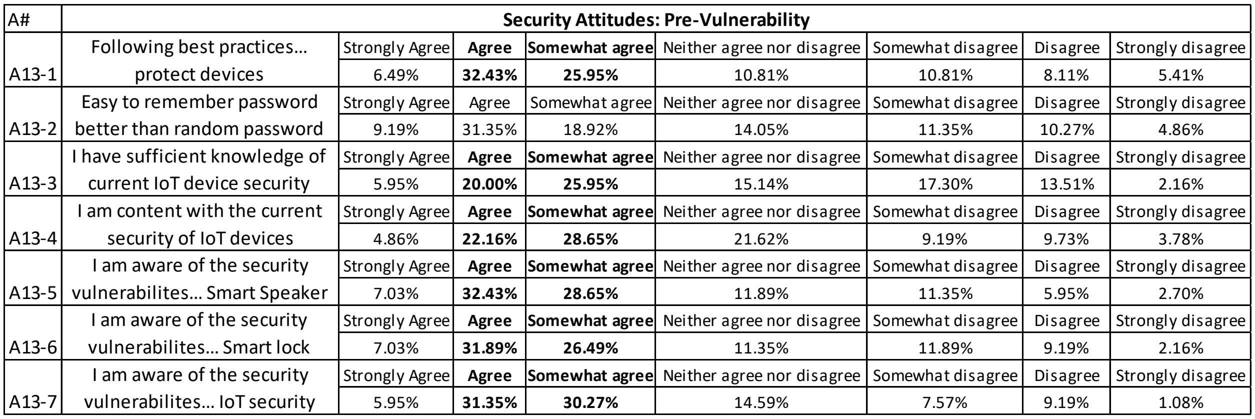
Demographics, Table 1



D#	Demographics			
D1	Number of IoT Devices Owned	1-4	5-8	9+
		48.11%	43.78%	8.11%
D2	Gender	Male	Female	
		54.05%	45.95%	
D3	What Class are you currently enrolled in	INSC 20263	Other INSC	None
		78.38%	18.38%	3.24%
D4	Age	19 or younger	20 or older	
		32.97%	67.03%	

The majority of respondents (92%) owned between 1-4 and 5-8 Internet of Things devices (D1). This aligned with the national average in the United States in 2017, which was approximately 3.64 IoT devices per individual (Buckle, 2017). The respondents were nearly half male and half female, and the majority of students surveyed (97%) were currently enrolled in a TCU INSC course.

Pre-Vulnerability Attitude Data, Table 2

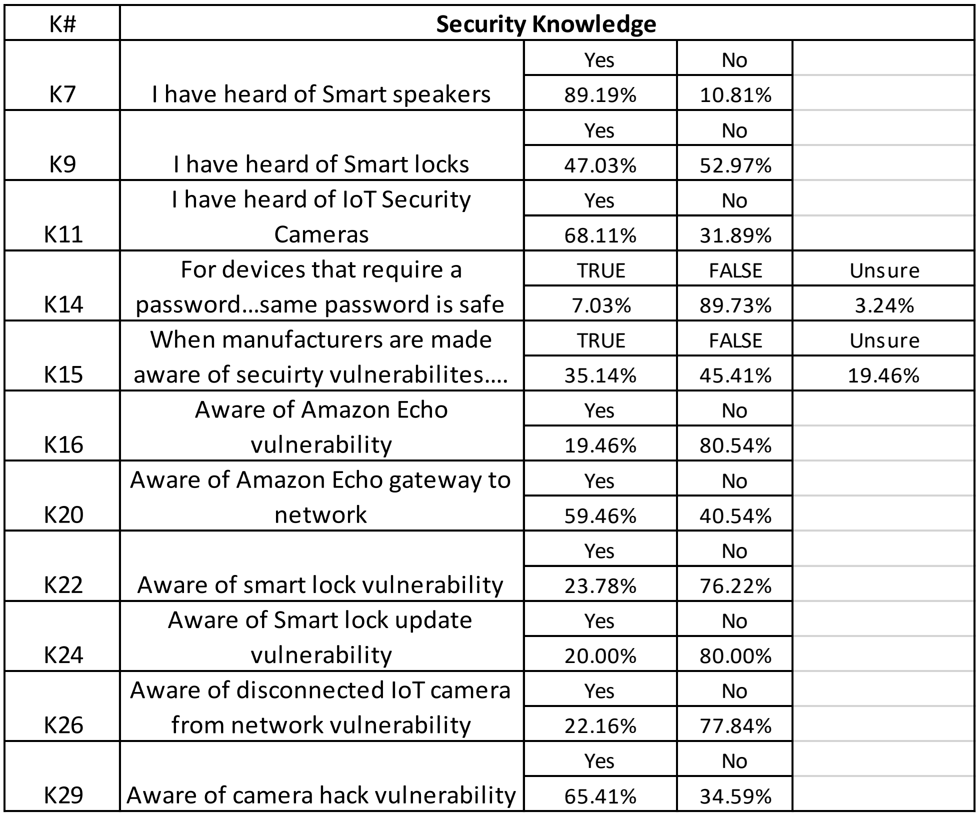


A#	**Security Attitudes: Pre-Vulnerability**							
A13-1	Following best practices… protect devices	Strongly Agree	**Agree**	**Somewhat agree**	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
		6.49%	**32.43%**	**25.95%**	10.81%	10.81%	8.11%	5.41%
A13-2	Easy to remember password better than random password	Strongly Agree	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
		9.19%	31.35%	18.92%	14.05%	11.35%	10.27%	4.86%
A13-3	I have sufficient knowledge of current IoT device security	Strongly Agree	**Agree**	**Somewhat agree**	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
		5.95%	**20.00%**	**25.95%**	15.14%	17.30%	13.51%	2.16%
A13-4	I am content with the current security of IoT devices	Strongly Agree	**Agree**	**Somewhat agree**	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
		4.86%	**22.16%**	**28.65%**	21.62%	9.19%	9.73%	3.78%
A13-5	I am aware of the security vulnerabilites… Smart Speaker	Strongly Agree	**Agree**	**Somewhat agree**	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
		7.03%	**32.43%**	**28.65%**	11.89%	11.35%	5.95%	2.70%
A13-6	I am aware of the security vulnerabilites… Smart lock	Strongly Agree	**Agree**	**Somewhat agree**	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
		7.03%	**31.89%**	**26.49%**	11.35%	11.89%	9.19%	2.16%
A13-7	I am aware of the security vulnerabilites… IoT security	Strongly Agree	**Agree**	**Somewhat agree**	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
		5.95%	**31.35%**	**30.27%**	14.59%	7.57%	9.19%	1.08%

Research Question 1: "What are the current attitudes of IoT users towards the current security of IoT devices?

In order to address this research question, respondents were asked about their current perceptions and opinions regarding their concern for the security of their IoT devices and how important they believe specific security practices are towards securing their devices. Based on the results, students initially did not show a high concern for the security of their devices. For instance, approximately 65% of students at least somewhat agreed with the statement, "Following best practices for security would completely protect my IoT devices" (A13-1). Often times, following best practices for security is not enough to keep devices secure, and a majority of students were unaware or believed that following best practices was enough to keep them safe. In addition, 60% of students claimed that using an easy to remember password was more convenient and outweighed the benefits of using a random password (13-2). Thus, students were initially not concerned about the security threats posed by poor security practices. Overall, a slight majority of respondents (56%) claimed that they were content with the current security of IoT devices, with an additional 22% claiming they were neither content nor discontent (13-4).

Knowledge Data, Table 3



K#	Security Knowledge			
K7	I have heard of Smart speakers	Yes	No	
		89.19%	10.81%	
K9	I have heard of Smart locks	Yes	No	
		47.03%	52.97%	
K11	I have heard of IoT Security Cameras	Yes	No	
		68.11%	31.89%	
K14	For devices that require a password...same password is safe	TRUE	FALSE	Unsure
		7.03%	89.73%	3.24%
K15	When manufacturers are made aware of secuirty vulnerabilites....	TRUE	FALSE	Unsure
		35.14%	45.41%	19.46%
K16	Aware of Amazon Echo vulnerability	Yes	No	
		19.46%	80.54%	
K20	Aware of Amazon Echo gateway to network	Yes	No	
		59.46%	40.54%	
K22	Aware of smart lock vulnerability	Yes	No	
		23.78%	76.22%	
K24	Aware of Smart lock update vulnerability	Yes	No	
		20.00%	80.00%	
K26	Aware of disconnected IoT camera from network vulnerability	Yes	No	
		22.16%	77.84%	
K29	Aware of camera hack vulnerability	Yes	No	
		65.41%	34.59%	

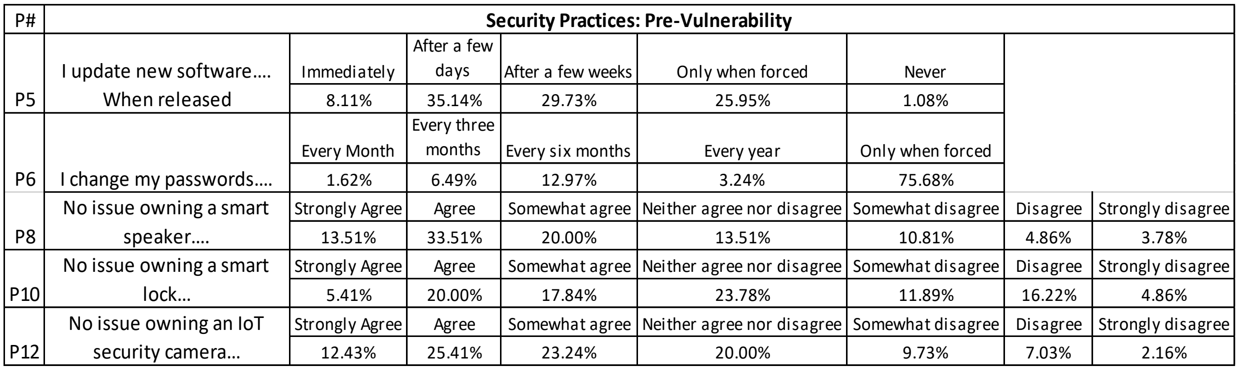
Research Question 2: What is the current knowledge, or lack thereof, of IoT users of the security of IoT devices?

Before understanding the knowledge each student had about the security vulnerabilities present in IoT devices, the survey first asked students if they were familiar with each of the IoT devices presented in the survey. While a majority of students were aware of the smart speaker (approximately 90%) and IoT security camera (approximately 70%), less than half (47%) were familiar with smart locks (K7, K9, K11). As such, a thorough description of all three devices was provided for students who may not have been aware of the devices before the survey so that they would still be able to answer questions relating to the device's security.

To assess the current security knowledge of students as it pertained to IoT devices, respondents were first presented with a security vulnerability that had already been discovered in a smart speaker, smart lock, and IoT security camera. After being made aware of the vulnerability, students were asked whether or not they were aware of the vulnerability. Only 20% of students were aware of the security vulnerability found in a smart speaker (K16), 24% aware of the vulnerability found in smart locks (K22), and 22% aware of the vulnerability found in an IoT security camera (K26), suggesting that students are not currently very knowledgeable about the security vulnerabilities present in IoT devices.

Students also were presented with a potential security vulnerability that could be exploited in the future, and respondents were asked again if they were aware of this vulnerability. While more students were aware of the future vulnerabilities for the smart speaker and IoT security camera (60% and 65% respectively) even fewer were aware of the second vulnerability presented in the smart locks (20%). Only a very small portion of respondents (11%) were aware of each pair of vulnerabilities present in each device.

Pre-vulnerability Practices Data, Table 4



P#	Security Practices: Pre-Vulnerability							
P5	I update new software…. When released	Immediately	After a few days	After a few weeks	Only when forced	Never		
		8.11%	35.14%	29.73%	25.95%	1.08%		
P6	I change my passwords….	Every Month	Every three months	Every six months	Every year	Only when forced		
		1.62%	6.49%	12.97%	3.24%	75.68%		
P8	No issue owning a smart speaker….	Strongly Agree	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
		13.51%	33.51%	20.00%	13.51%	10.81%	4.86%	3.78%
P10	No issue owning a smart lock…	Strongly Agree	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
		5.41%	20.00%	17.84%	23.78%	11.89%	16.22%	4.86%
P12	No issue owning an IoT security camera…	Strongly Agree	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
		12.43%	25.41%	23.24%	20.00%	9.73%	7.03%	2.16%

Research Question 3: What are the current behaviors and practices of IoT users in regards to IoT device usage given their attitudes and knowledge of the security of those devices?

To survey the current security practices of students as it related to owning IoT devices, students were first surveyed on general security practices. When new software becomes available from an IoT manufacturer, only 8.1% of students said they updated their software immediately (P5). In addition, when asked how often students changed their passwords for their IoT devices, a majority (approximately 75%) said they only will when forced to do so. Updating software when it released from a manufacturer is typically good practice, as is regularly updating passwords. These results indicate that currently a majority of students are not concerned with practicing good security habits with their IoT devices. They align with the previously surveyed security attitude and knowledge data, suggesting a general lack of concern for IoT security among students.

Students did not appear to have an issue owning the smart speaker or IoT security camera when considering their security. Approximately 67% of students had no issue owning a smart speaker (P8), and 61% had no issue owning an IoT security camera (P12). A slight minority felt comfortable owning a smart lock (44%); however, only 47% were initially familiar with the device, which likely contributed to this figure having been lower than the other two devices.

Post-Vulnerability Attitude Data, Table 5

A#	**Security Attitudes: Post-Vulnerability**							
A18	This information would affect my decision.... Smart speaker	Strongly Agree	**Agree**	**Somewhat agree**	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
		10.81%	**37.84%**	**25.95%**	14.05%	3.78%	6.49%	1.08%
A21	This information would affect my decision.... Smart speaker 2	Strongly Agree	**Agree**	**Somewhat agree**	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
		12.97%	**38.38%**	**24.32%**	13.51%	5.95%	3.24%	1.62%
A23	This information would affect my decision.... Smart lock	**Strongly Agree**	**Agree**	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
		29.73%	**37.84%**	18.38%	8.11%	2.70%	2.16%	1.08%
A25	This information would affect my decision.... Smart lock 2	**Strongly Agree**	**Agree**	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
		23.78%	**41.08%**	22.16%	7.57%	2.16%	2.70%	0.54%
A27	This information would affect my decision.... IoT security	Strongly Agree	**Agree**	**Somewhat agree**	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
		16.22%	**37.84%**	**28.11%**	9.73%	4.32%	3.24%	0.54%
A30	This information would affect my decision.... IoT security	**Strongly Agree**	**Agree**	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
		28.11%	**40.00%**	13.51%	10%	4.32%	3.78%	0.54%

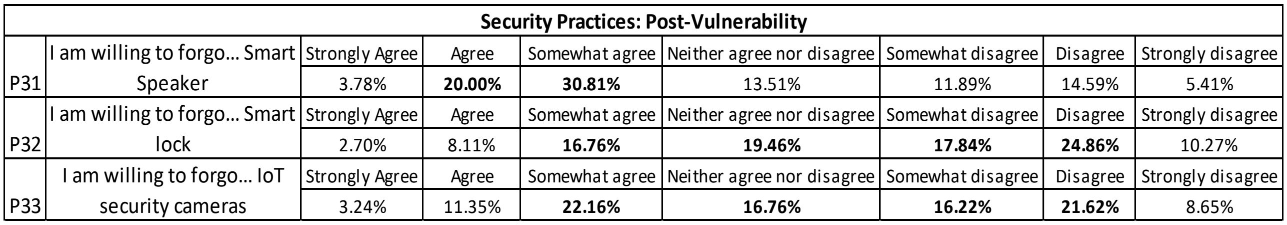
Research Question 3a: What are the attitudes and behaviors of IoT users in regards to IoT device usage after users are made aware of historical/actual security vulnerabilities and breaches of common IoT devices?

To answer this question, students were presented with a vulnerability either currently present or historically present in each one of the devices (The vulnerabilities presented in the survey are included with their questions in the appendix). After being made aware of the vulnerability, students were asked if the information would affect their decision to own or use the device when considering its security. Seventy-five percent of students said that it would affect their decision to own a smart speaker (A18), 86% said it would affect their decision to own a smart lock (A23), and 82% said it would affect their decision to own an IoT security camera (A27). At least three quarters of students admitted that they at least somewhat agree that the vulnerability would affect their decision to own or use each IoT device, suggesting that attitudes towards these devices were altered when students became aware of their security vulnerabilities. Students lack understanding of many of the vulnerabilities in these devices, and once they are made aware of them it has made them more hesitant to own the devices.

Research Question 3b: What are the attitudes and behaviors of IoT users in regards to IoT device usage after users are made aware of potential security vulnerabilities of common IoT devices?

Students also were presented with a security vulnerability in each device that had the potential to be exploited in the future (The vulnerabilities presented are included with their questions in the appendix). Once given this information, students were asked again if these vulnerabilities would affect their decision to own these devices when considering their security. In analyzing their responses, 76% of students said it would affect their decision to own a smart speaker (A21), 87% said it would affect their decision to own a smart lock (A25), and 82% said it would affect their decision to own an IoT security camera (A30). Again, these results would indicate that students' attitudes towards the security of these devices are affected when they are made aware of potential security vulnerabilities.

Post-Vulnerability Practice Data, Table 6:



Security Practices: Post-Vulnerability								
P31	I am willing to forgo… Smart Speaker	Strongly Agree	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
		3.78%	**20.00%**	**30.81%**	13.51%	11.89%	14.59%	5.41%
P32	I am willing to forgo… Smart lock	Strongly Agree	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
		2.70%	8.11%	**16.76%**	**19.46%**	**17.84%**	**24.86%**	10.27%
P33	I am willing to forgo… IoT security cameras	Strongly Agree	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
		3.24%	11.35%	**22.16%**	**16.76%**	**16.22%**	**21.62%**	8.65%

Students also were asked at the end of the survey if they would be willing to forgo the security vulnerabilities to own the devices. A majority of students said they would not be willing to forgo the security vulnerabilities presented in smart locks (53%), and a slightly smaller amount (46.5%) said they would not be willing to forgo the security vulnerabilities of an IoT security camera. Students' attitudes about the security of these IoT devices clearly were affected once they were made aware of the security vulnerabilities, and students' willingness to own the devices were also significantly affected. A large number of students (40%) said they would altogether not be willing to own the devices once made aware of their security vulnerabilities, suggesting that security may play an important role in a consumer's decision to own the device.

Research Question 4: How do Socio-demographic factors of IoT users affect their attitude towards security, knowledge of security practices, and security-related practices of IoT devices?

Tables 7, 8, 9, 10 and 11 show the correlations between demographic questions (D1 and D2) and each of the five subsets of questions specified in the survey model (Figure 2).

Pre-Vulnerability Attitudes, Table 7

Pre-Vulnerability Attitude – Demographics Correlation

		D1	D2			D1	D2
A13-1	Pearson Correlation	-.006	.014	A13-5	Pearson Correlation	**-.111***	-.045
	Sig. (2-tailed)	.873	.621		Sig. (2-tailed)	.026	.261
A13-2	Pearson Correlation	-.009	.007	A13-6	Pearson Correlation	.026	-.011
	Sig. (2-tailed)	.758	.781		Sig. (2-tailed)	.590	.783
A13-3	Pearson Correlation	**.080***	**-.074***	A13-7	Pearson Correlation	.078	.090
	Sig. (2-tailed)	.028	.012		Sig. (2-tailed)	.174	.053
A13-4	Pearson Correlation	.067	.029				
	Sig. (2-tailed)	.103	.365				

*. Correlation is significant at the 0.05 level (2-tailed).

Table 5 shows a significant correlation between demographic factors and questions A13-3 and A13-5. A positive correlation of .080 at the .05 significance level for question A13-3 shows that the more IoT devices a survey respondent owned, the more likely they were to believe that they had sufficient knowledge of the current security of IoT devices. Additionally, with a negative correlation of -.074 at the .05 level, men were more likely to believe that they were more knowledgeable about the security of IoT devices than were women. On a 7-point Likert scale, this difference translated to men rating their belief of their IoT security knowledge .76 points higher than women did on average. Lastly, another negative correlation resulted for pre-vulnerability attitudes of -.111 at the .05 level for question A13-5. This negative relationship revealed that those individuals who owned less IoT devices believed that they actually knew more about the specific security vulnerabilities present in a smart speaker than those who had more IoT devices. This correlation was a unique case and the only device in which this relationship occurred.

Post-Vulnerability Attitudes, Table 8

Post-Vulnerability Attitude – Demographics Correlation

	D1	D2		D1	D2
A18 Pearson Correlation	.017	-.035	A25 Pearson Correlation	.012	.014
Sig. (2-tailed)	.713	.336	Sig. (2-tailed)	.866	.815
A21 Pearson Correlation	-.061	-.030	A27 Pearson Correlation	**.141***	-.012
Sig. (2-tailed)	.276	.504	Sig. (2-tailed)	.021	.798
A23 Pearson Correlation	.045	.043	A30 Pearson Correlation	-.095	.011
Sig. (2-tailed)	.525	.440	Sig. (2-tailed)	.114	.814

*. Correlation is significant at the 0.05 level (2-tailed).

Table 6 shows only one significant relationship at the .05 level between post-vulnerability attitudes and the demographic factors analyzed. For question A27, a positive correlation of .141 indicates that individuals who own more IoT devices were more likely to say that, after being presented with a past security vulnerability, their decision to purchase or own an IoT security camera would be affected by the vulnerability.

Knowledge, Table 9

Knowledge – Demographics Correlation

	D1	D2		D1	D2
K16 Pearson Correlation	-.097	.112	K24 Pearson Correlation	.190	-.001
Sig. (2-tailed)	.494	.280	Sig. (2-tailed)	.240	.994
K20 Pearson Correlation	-.195	**-.195***	K26 Pearson Correlation	.136	**-.264***
Sig. (2-tailed)	.064	.020	Sig. (2-tailed)	.351	.023
K22 Pearson Correlation	-.002	.029	K29 Pearson Correlation	-.113	.025
Sig. (2-tailed)	.988	.814	Sig. (2-tailed)	.310	.773

*. Correlation is significant at the 0.05 level (2-tailed).

Analysis of the knowledge and demographic data from Table 9 shows one significant relationship. For each vulnerability that was presented for the IoT devices, women were more likely to have known the vulnerability existed than men were. This relationship was especially apparent for the specific vulnerabilities relating to smart speakers and IoT security cameras, where statistically significant negative correlations of -.195 and -.264 were present (K20 and

K26). This correlation was in direct contrast to the pre-vulnerability attitude question that showed men believed they knew more about the security vulnerabilities in IoT devices than women did.

Pre-Vulnerability Practice, Table 10

Pre-Vulnerability Practice – Demographics Correlation					
	D1	D2		D1	D2
P8 Pearson Correlation	**.114***	-.012	P12 Pearson Correlation	-.043	**-.071***
Sig. (2-tailed)	.003	.695	Sig. (2-tailed)	.268	.024
P10 Pearson Correlation	.009	.005			
Sig. (2-tailed)	.780	.856			

*. Correlation is significant at the 0.05 level (2-tailed).

Analyzing pre-vulnerability practice questions revealed a significant correlation between IoT device ownership and the willingness to own a smart speaker when considering its security. Specifically, individuals with more IoT devices were more likely to claim that they had no issuing owning a smart speaker than individuals with less IoT devices (P8). This relationship was expected, as individuals who own more IoT devices would likely be more comfortable with their security as a result of their willingness to own more devices. In this set of questions, a significant relationship relating to gender also existed. Women were more likely to agree with the statement, "I have no issue owning or using connected home security cameras when considering the security of the device" (P12) than men were before being presented with the security vulnerabilities.

Post-Vulnerability Practice, Table 11

Post-Vulnerability Practice – Demographics Correlation

	D1	D2		D1	D2
P31 Pearson Correlation	-.071	.011	P33 Pearson Correlation	-.078	.024
Sig. (2-tailed)	.058	.814	Sig. (2-tailed)	.110	.289
P32 Pearson Correlation	.079	**.058***			
Sig. (2-tailed)	.095	.041			

*. Correlation is significant at the 0.05 level (2-tailed).

For post-vulnerability practice questions, one statistically significant positive correlation between practice and gender existed. Specifically, men were more likely to agree with the statement, “I am willing to forgo the potential security risks of a smart lock for the benefit it provides” (P32) than women were.

5. Is there a disconnect between the IoT users' security attitudes, knowledge, and their security practices?

Tables 12, 13, 14, and 15 show results of correlations between attitude, knowledge, and practice questions. Questions were selected based on what would be expected to be common attitudes, common knowledge, and common practices as they relate to IoT device security. Therefore, the presence of a statistically significant correlation (or lack thereof) was used to identify disconnects between the three sections.

Table 12

A13-4 & Knowledge Disconnect Correlations

	K15	K16	K20	K22	K24	K26	K29
A13-4 Pearson Correlation	**.398***	-.473	.223	.196	.264	-.459	.088
Sig. (2-tailed)	.001	.163	.375	.592	.491	.189	.734

*. Correlation is significant at the 0.05 level (2-tailed).

Table 12 shows a positive, statistically significant correlation between questions A13-4 and K15. Specifically, users who disagreed with the statement “I am content with the current security of IoT devices” (A13-4) also tended to know that IoT devices manufacturers did not always take the necessary steps to fix security vulnerabilities in their devices when made aware of them (K15). This correlation can be expected; however, the lack of a correlation between question A13-4 and questions K16, K20, K22, K24, K26, and K29 could be identified as a possible disconnect for individual’s security attitudes and knowledge. This disconnect meant that individuals who were content with current IoT security were not necessarily aware or unaware of the vulnerabilities present in IoT devices.

Table 13

A13-4 & Practice Disconnect Correlations

	P8	P10	P12
A13-4 Pearson Correlation	**.351***	.126	.025
Sig. (2-tailed)	.000	.079	.767

*. Correlation is significant at the 0.05 level (2-tailed).

Table 13 addresses the possibility of disconnects between initial user practices and user attitudes as they relate to IoT device security. A statistically significant correlation exists between Questions A13-4 and P8 at the 0.05 level. Specifically, users who were content with current IoT security also had no issue owning a smart speaker when considering the security of the device. While this correlation would be expected, this same relationship was not observed for smart locks or IoT security cameras. This lack of a relationship would identify a possible disconnect between user attitudes and user's willingness to own an IoT device for devices that individuals are less familiar with. In this case, respondents were initially less familiar with smart locks and IoT security cameras than they were smart speakers.

Table 14

A13-4 & Practice Disconnect Correlations

	P31	P32	P33
A13-4 Pearson Correlation	.082	.049	**.213***
Sig. (2-tailed)	.302	.609	.031

*. Correlation is significant at the 0.05 level (2-tailed).

As shown above, Table 14 again addresses the possibility of disconnects between user attitudes and practices as it relates to IoT security; however, it focuses on the intended practices of individuals after they have been made aware of the security vulnerabilities present in each of the IoT devices. A statistically significant correlation was observed between questions A13-4 and P33, which indicated that users who were content with current IoT security were also willing to forgo the security vulnerabilities of an IoT security camera to use it for the benefit it provides.

This same relationship was not observed for smart speakers or smart locks, indicating that users who were content with current IoT security did not necessarily agree or disagree with the statement, “I am willing to forgo the potential security risks of a smart speaker (or smart lock) for the benefit it provides” (P32, P33). The lack of a relationship suggests a disconnect between how confident individuals are in the current security of IoT devices and their willingness to use those devices when presented with their vulnerabilities.

Table 15

Knowledge & Practice Disconnect Correlations

		K16	K20
P31	Pearson Correlation	-.025	-.009
	Sig. (2-tailed)	.165	.667
		K22	K24
P32	Pearson Correlation	-.004	-.003
	Sig. (2-tailed)	.811	.890
		K26	K29
P33	Pearson Correlation	**-.038***	-.031
	Sig. (2-tailed)	.044	.139

*. Correlation is significant at the 0.05 level (2-tailed).

Table 15 shows correlations between knowledge and practice questions and the potential for further disconnects. Each of the three practice questions listed in the table (one designated for each IoT device studied) is paired with both vulnerability questions that were presented for the device in the survey. As shown, a statistically significant correlation exists between questions K26 and P33; that is, individuals who were aware of the security vulnerability presented in IoT security cameras were more likely to agree with the statement, “I am willing to forgo the security vulnerabilities present in an IoT security camera for the benefit it provides” (P33). Either a positive or negative relationship would be expected between each pair of questions; however, the lack of this relationship between the other five pairs of questions suggests a disconnect between what individuals know about IoT device security and what devices they are willing to use.

Discussion

Due to a lack of statistically significant correlations between questions, at least somewhat of a disconnect exists between user IoT security attitudes and user IoT security knowledge. While 70% of students at least somewhat agreed with the statement, “I have sufficient knowledge of the current security of IoT devices” (A13-3), only 39.5% were aware of the security vulnerabilities in smart speakers, only 21.9% were aware of the vulnerabilities in smart locks, and only 43.8% were aware of the vulnerabilities in IoT security cameras. Students believed they were much more knowledgeable about the security of these devices than they actually were.

A lack of statistically significant relationships between attitude and practice questions (A13-4 and P12, P14, P31, P32) would suggest a disconnect is present here as well. Although 70% of students believed they understood and were content with current IoT security, only 55% were willing to own a smart speaker, 27.6% willing to own smart locks, and 36.8% willing to own an IoT security camera after learning about their security vulnerabilities. If a disconnect were not present, these figures would be expected to be relatively the same. In addition, only

71% of individuals who owned a smart speaker were willing to forgo the security vulnerabilities present in the device to use it, suggesting a good portion of individuals are no longer willing to own their smart speaker upon learning about its security vulnerabilities. This shift in attitude further illustrates a disconnect because both user attitude and practice have changed as a result of an awareness of the security vulnerabilities present in the devices.

Finally, due to a lack of statistically significant correlations between knowledge and practice questions, a final disconnect does seem to exist between IoT security practices and IoT security knowledge. At a specific question level, 67% of individuals said they had no issue owning a smart speaker when considering the security of the device, 43.3% had no issue owning smart locks, and 61.1% had no issue owning IoT security cameras before being presented with each devices' security vulnerabilities. However, after being made aware of the vulnerabilities, only 55% would be willing to own a smart speaker, 27.6% willing to own smart locks, and 36.8% willing to own an IoT security camera. This change in behavior indicates that user's practices are affected by their knowledge of the vulnerabilities in the devices, and therefore, a disconnect does exist due to their change in practices as a result of gaining this knowledge.

Limitations

A few limitations in the study exist that are worth noting. Specifically, the population of individuals surveyed was limited to students in the Neeley School of Business at TCU. While the focus of the survey was on students due to the fact that they will be the largest consumers of IoT devices in the near future, the age and education level of the students was narrow. Another limitation worth noting is the relatively recent growth of the Internet of Things. Since many IoT devices have only been around for five years or less, many students are still unaware of or do not own the devices themselves. With the continued rapid growth of the IoT, individuals will own many of these devices very soon, and students' opinions and perceptions about IoT devices are likely to change in the near future.

Implications

These results mean a good deal for individuals and businesses alike. A study performed by Ludwig Slusky and Parviz Partow-Navid in 2012 on student information security awareness and knowledge concluded, "Security awareness is not due to a lack of security knowledge, but in the way that students apply that knowledge in real-world situations. Simply, the compliance with information security awareness is lower than the understanding of it." (Partow-Navid and Slusky, 2012). While security awareness was not often due to a lack of security knowledge in 2012, the same cannot be said for 2018 and the security of the Internet of Things. The results of this study would indicate that security awareness is at least partially due to a lack of security knowledge. Most students in this study were not aware of the security vulnerabilities present in these devices and, while evidence showed that students' security awareness was lower than their understanding of it, their lack of security knowledge contributed to their lack of security awareness as well. The previous study was unable to take into account the Internet of Things (as it has only begun to grow rapidly in the past five years), and the many new connected devices and security vulnerabilities that have been created as a result. Students and individuals alike now need to not only ensure they are aware of potential security vulnerabilities in IoT devices but also ensure they are knowledgeable about the new vulnerabilities that each device presents. Since these security vulnerabilities affect the willingness of students to own these devices, learning about these vulnerabilities before purchasing future devices will be important.

Another study, performed two years ago by Brien Twomey, surveyed privacy concerns and attitudes of students as they related to mobile phone applications. One conclusion he was able to draw from his study stated, “Users say they are uncomfortable with companies taking their personally identifiable information, they are willing to provide that information despite their concerns” (Twomey, 2016). Students were reluctant to give up their information, but they were ultimately willing to do so in order to use applications like Google Maps and Snapchat. In the case of this study, students were willing to forgo security vulnerabilities to use IoT devices; however, the number of students willing to do so was a much smaller percentage than those who were willing to give up their privacy. While almost 90% of individuals were willing to give up their personal information in order to use Google Maps (Twomey, 2016), only 40% of individuals were willing to forgo security vulnerabilities presented in the three devices collectively. For manufacturers of IoT devices, this growing concern for security from consumers will have an impact on the future. As more and more consumers learn about the security vulnerabilities in these devices, it will force manufacturers to prioritize their security.

Future Research

The implications of this study are very interesting; especially as the Internet of Things continues to rapidly expand. As more and more devices get connected to the internet, more security vulnerabilities are created, and the ramifications of those vulnerabilities (should they be exploited) will continue to become more severe. For instance, if a hacker were able to take control of a self-driving car, they would potentially have the ability to control the entire vehicle. This exploit would be much more dangerous than if a hacker just broke into a smart speaker. As such, it will be interesting to see where individuals completely prioritize their security over using an IoT device. Specifically, at what threshold will the consequences of a potential hack be so severe that consumers refuse to use the device until changes are made or the major vulnerabilities are accounted for?

Appendix

Internet of Things Security Survey

Instructions: Read the following questions and answer truthfully.

1. An Internet of Things device (IoT) is defined as any device that is connected to the internet. How many devices do you own that are connected to the internet? (Check all that apply)

Tablet
Fitbit
Laptop
Smart Phone
Smart TV
Smart Watch
Desktop
Smart Speaker
Smart Thermostat (i.e. Nest)
Smart Lock
Streaming Device (i.e. Apple TV)
Connected Security Camera

2. What is your gender?
Male Female

3. How old are you?
Pull down menu with options from Under 18, 18, 19… Over 7

4. Which course are you enrolled in this semester?
INSC 20263 Other INSC Course Neither

5. I update new software from the manufacturers when it is released for an IoT device…
Immediately After a few days After a few weeks Only if forced Never

6. I change my passwords for these devices…
Every month Every three months Every six months Every year Never

7. The Amazon Echo is a smart speaker that is connected to a voice-controlled intelligence assistant. It processes voice requests and returns information related to news, weather, sports, etc.

Do you own, have heard of, or have used a smart speaker?
Yes No

8. I have no issue owning or purchasing a smart speaker when considering the security of the device
Strongly agree Agree Somewhat agree Neither agree nor disagree
Somewhat agree Disagree Strongly disagree

9. A Smart Lock is an electronic locking device that opens wirelessly from an authorized users' authentication. They are may be accessed via smartphone or other Bluetooth enabled devices.

Do you own, have heard of, or have used Smart Locks?
Yes No

10. I have no issue owning or using a “smart lock” when considering the security of the device
Strongly agree Agree Somewhat agree Neither agree nor disagree
Somewhat agree Disagree Strongly disagree

11. Internet of Things (IoT) Security Cameras define any camera that is connected to a network or the internet. These cameras are becoming increasingly popular in homes. Nest, a popular home automation company, is an example of a popular “IoT” security camera manufacturer.

Do you own, have heard of, or have used IoT security cameras?
Yes No

12. I have no issue owning or using connected home security cameras when considering the security of the device
Strongly agree Agree Somewhat agree Neither agree nor disagree
Somewhat agree Disagree Strongly disagree

13-1. Following best practices for security will completely protect my IoT devices
Strongly agree Agree Somewhat agree Neither agree nor disagree
Somewhat agree Disagree Strongly disagree

13-2. For IoT devices that require a password, the convenience of using an easy-to-remember password outweighs the benefit of having a random password
Strongly agree Agree Somewhat agree Neither agree nor disagree
Somewhat agree Disagree Strongly disagree

13-3. I have sufficient knowledge of the current security of IoT devices
Strongly agree Agree Somewhat agree Neither agree nor disagree
Somewhat agree Disagree Strongly disagree

13-4. I am content with the current security of IoT devices
Strongly agree Agree Somewhat agree Neither agree nor disagree
Somewhat agree Disagree Strongly disagree

13-5. I am aware of the security vulnerabilities that are present in a smart speaker.
Strongly agree Agree Somewhat agree Neither agree nor disagree
Somewhat agree Disagree Strongly disagree

13-6. I am aware of the security vulnerabilities that are present in smart locks
Strongly agree Agree Somewhat agree Neither agree nor disagree
Somewhat agree Disagree Strongly disagree

13-7. I am aware of the security vulnerabilities that are present in connected home security cameras
Strongly agree Agree Somewhat agree Neither agree nor disagree
Somewhat agree Disagree Strongly disagree

14. For devices that require a password, using the same password across multiple devices is safe
True False

15. When manufacturers are made aware of security vulnerabilities in their devices, they will always take the necessary steps to fix them
True False

16. Mark Barnes, a British Security Researcher, was able to easily install malware on an Amazon Echo that allowed him to stream audio from the device to his own server. It gave him the ability to listen to conversations near the Echo from the comfort of his own home. Amazon corrected the vulnerability on all Echo models sold in 2017. All models sold prior remain vulnerable.

I was aware of this security vulnerability.
Yes No

18. This information would affect my decision to purchase or own a smart speaker when considering the security of the device.
Strongly agree Agree Somewhat agree Neither agree nor disagree
Somewhat agree Disagree Strongly disagree

20. Since this device is connected to the internet, a hacker of the device could potentially have access to account information of the user or have the ability to attack other devices that are connected to the same network.

I was aware of this security vulnerability.
Yes No

21. This information would affect my decision to purchase or own a smart speaker when considering the security of the device.
Strongly agree Agree Somewhat agree Neither agree nor disagree
Somewhat agree Disagree Strongly disagree

22. Smart Locks are connected to a network. As a result, they are naturally prone to security risks. Security consultant Anthony Rose revealed security flaws in many Bluetooth-enabled Smart Locks in 2016. He was able to break into 12 of the 16 he tested.

I was aware of this security vulnerability.

Yes No

23. This information would affect my decision to own or use a smart lock when considering the security of the device.
Strongly agree Agree Somewhat agree Neither agree nor disagree
Somewhat agree Disagree Strongly disagree

24. LockState, a manufacturer of Smart Locks, issued an update for their internet-enabled smart locks in August 2017. The update broke 500 of their customer's locks and they had to be repaired or replaced. If a computer hacker were to alter a smart lock vendor's update system, they could disable a large majority of their customer's Smart Locks.

I was aware of this security vulnerability
Yes No

25. This information would affect my decision to own or use a smart lock when considering the security of the device.
Strongly agree Agree Somewhat agree Neither agree nor disagree
Somewhat agree Disagree Strongly disagree

26. In 2016, it was discovered that, by sending a Wi-Fi password parameter via Bluetooth, a Nest home security camera could be shut down for 60 to 90 seconds. A hacker would also have the ability to disconnect the camera from the network altogether.

I was aware of this security vulnerability.
Yes No

27. This information would affect my decision to own or use a connected home security camera when considering the security of the device.
Strongly agree Agree Somewhat agree Neither agree nor disagree
Somewhat agree Disagree Strongly disagree

29. In 2016, a mother had discovered that a hacker had gained control of a camera in one of her daughter's rooms. She found out that the hacker was able to take control of the camera through information shared by her daughter online while playing a video game. She had no knowledge that the camera had been compromised.

I was aware of this security vulnerability.
Yes No

30. This information would affect my decision to own or use a connected home security camera when considering the security of the device.
Strongly agree Agree Somewhat agree Neither agree nor disagree
Somewhat agree Disagree Strongly disagree

31. I am willing to forgo the potential security risks of a smart speaker for the benefit it provides

Strongly agree Agree Somewhat agree Neither agree nor disagree
Somewhat agree Disagree Strongly disagree

32. I am willing to forgo the potential security risks a Smart Lock for the benefit it provides.

Strongly agree Agree Somewhat agree Neither agree nor disagree
Somewhat agree Disagree Strongly disagree

33. I am willing to forgo the potential security risks of a connected security camera for the benefit it provides.

Strongly agree Agree Somewhat agree Neither agree nor disagree
Somewhat agree Disagree Strongly disagree

Cronbach Alpha Analysis

Attitude Subset Questions

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.712	.739	13

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Q131	58.4270	72.735	.072	.387	.733
Q132	58.3838	69.618	.173	.146	.720
Q133	57.4270	74.431	.019	.345	.738
Q134	58.2324	71.321	.151	.405	.719
Q135	56.9243	68.168	.293	.619	.701
Q136	57.0108	66.098	.362	.637	.691
Q137	56.9405	67.393	.346	.685	.694
Q18	56.6162	65.520	.453	.499	.680
Q21	56.5297	64.435	.519	.592	.672
Q23	56.0270	64.711	.542	.719	.671
Q25	56.0919	64.823	.579	.707	.669
Q27	56.3568	64.176	.589	.643	.666
Q30	56.1135	63.916	.539	.631	.669

Knowledge Subset Questions

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.714	.716	9

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Q7	2.9459	4.356	.175	.126	.720
Q9	3.3676	3.799	.323	.189	.704
Q11	3.1568	4.133	.173	.145	.730
Q16	3.6432	3.839	.439	.329	.681
Q20	3.2432	3.696	.392	.178	.689
Q22	3.6000	3.578	.569	.498	.655
Q24	3.6378	3.721	.516	.456	.667
Q26	3.6162	3.694	.507	.428	.668
Q29	3.4919	3.653	.438	.249	.679

Practice Subset Questions

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.806	.805	6

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Q8	19.6703	33.624	.564	.483	.776
Q10	18.8649	34.465	.487	.360	.793
Q12	19.5243	35.512	.479	.383	.794
Q31	18.9622	32.776	.602	.528	.767
Q32	18.1405	32.980	.601	.595	.767
Q33	18.4054	31.721	.652	.611	.755

References

Acquisti, A., & Grossklags, J. (2005). Privacy and Rationality in Individual Decision Making. IEEE Security & Privacy, 3(1), 26-33.

Ajzen, I., & Fishbein, M. (1977). Attitude-behavior relations: A theoretical analysis and review of empirical research. Psychological Bulletin, 84(5), 888-918.

Brandon, John. (2016, June 1). Security Concerns rising for the Internet of Things. Retrieved November 15, 2017. https://www.csoonline.com/article/3077537/internet-of-things/security-concerns-rising-for-internet-of-things-devices.html

Buckle, Chase. (2016, February 18). Digital consumers own 3.64 connected devices. Retrieved from Globalwebindex, from http://blog.globalwebindex.net/chart-of-the-day/digital-consumers-own-3-64-connected-devices/

Capgemini. (2014, November). Securing the Internet of Things Opportunity: Putting Cybersecurity at the Heart of the IoT. Retrieved November 27, 2017, from https://www.capgemini.com/wp-content/uploads/2017/07/securing_the_internet_of_things_opportunity_putting_cyber_security_at_the_heart_of_the_iot.pdf

Claveria, Kelvin. (2017, April 28). 13 Stunning Stats on the Internet of Things. Retrieved on November 15, 2017. https://www.visioncritical.com/internet-of-things-stats/

Drozhzhin, Alex. (2015, August 6). Black Hat USA 2015: The full story of how that Jeep was hacked. Retrieved October 21, 2017, from https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/

eMarketer (2017, July 26). 168 Million Will Watch Connected TV in the US This Year. Retrieved November 15, 2017, from https://www.emarketer.com/Article/168-Million-Will-Watch-Connected-TV-US-This-Year/1016233

Estes, Adam Clark. (2017, March 22). This Nest Security Flaw is Remarkably Dumb. Retrieved November 15, 2017, from https://gizmodo.com/this-nest-security-flaw-is-remarkably-dumb-1793524264

Fearn, Nicholas. (2017, February 1). Consumers unaware of the security risks posed by IoT devices, says report. Retrieved November 21, 2017, from https://internetofbusiness.com/consumers-security-risks-iot-devices/

Gartner, Inc. (2017, February 7). Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. Retrieved November 15, 2017, from https://www.gartner.com/newsroom/id/3598917

Gemalto. (2017, October 31). Gemalto survey confirms that Consumers lack confidence in IoT device security. Retrieved November 15, 2017, from https://www.gemalto.com/press/Pages/Gemalto-survey-confirms-that-Consumers-lack-confidence-in-IoT-device-security-.aspx

Gilbert, Ben. (2016, January 4). This is the refrigerator of the future. Retrieved on October 22, 2017, from http://www.businessinsider.com/the-refrigerator-of-the-future-2016-1?op=1

Greenberg, Andy. (2017, August 2). This hack lets Amazon Echo 'remotely snoop' on users. Retrieved on October 10, 2017. http://www.wired.co.uk/article/amazon-echo-alexa-hack

Greenberg, Andy. (2017, August 16). A Deep Flaw in your Car lets Hackers Shut Down Safety Features. Retrieved October 22, 2017, from https://www.wired.com/story/car-hack-shut-down-safety-features/

Greenough, John. (2015, February 19). The 'connected car' is creating a massive new business opportunity for auto, tech, and telecom companies. Retrieved October 21, 2017. http://www.businessinsider.com/connected-car-statistics-manufacturers-2015-2

Hazari, S., & Brown, C. (2013). An Empirical Investigation of Privacy Awareness and Concerns on Social Networking Sites. Journal of Information Privacy & Security, 31.

IDC (2017, January 4). Internet of Things Spending Forecast to Grow 17.9% in 2016 Led by Manufacturing, Transportation, and Utilities Investments, According to New IDC Spending Guide. Retrieved November 15, 2017, from https://www.idc.com/getdoc.jsp?containerId=prUS42209117

IoTforall. (2017, May 10). The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History. Retrieved November 15, 2017, from https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/

IoT Security Foundation. (2016, June). What do consumers think about IoT? Retrieved November 16, 2017, from https://www.iotsecurityfoundation.org/what-do-consumers-think-about-iot/

Lamkin, Paul. (2017, June 22). Wearable Tech Market To Double by 2021. Retrieved on November 27, 2017, from https://www.forbes.com/sites/paullamkin/2017/06/22/wearable-tech-market-to-double-by-2021/#b51c564d8f3e

Lohrmann, Dan. (2017, November 5). Lack of Trust in IoT Security Shows More Regulation Is Coming. Retrieved on November 15, 2017, from http://www.govtech.com/blogs/lohrmann-on-cybersecurity/lack-of-trust-in-iot-security-means-more-regulation-is-coming.html

McGee, Marianne Kolbasuk. (2016, January 11). Fitbit Hack: What are the lessons? Retrieved on October 10, 2017, from https://www.databreachtoday.com/fitbit-hack-what-are-lessons-a-8793

Moon, Bernard. (2016, March 10). Internet of Things & Hardware Industry Report 2016. Retrieved November 15, 2017, from https://www.slideshare.net/bernardmoon/internet-of-things-hardware-industry-report-2016

Patterson, Steven Max. (2017, August 21). How to improve IoT security. Retrieved on November 16, 2017, from https://www.networkworld.com/article/3217664/internet-of-things/how-to-improve-iot-security.html

Rainie, Lee. Anderson, Janna. (2017, June 6). The Internet of Things Connectivity Binge: What Are the Implications? Retrieved from Pew Research on October 22, 2017, from http://www.pewinternet.org/2017/06/06/the-internet-of-things-connectivity-binge-what-are-the-implications/

ReportBuyer. (2016, March 11). Smart Clothing and Body Sensors: Market Analysis and Forecasts. Retrieved on November 16, 2017, from https://www.prnewswire.com/news-releases/smart-clothing-and-body-sensors-market-analysis-and-forecasts-300267344.html

Slusky, L., & Partow-Navid, P. (2012). Students Information Security Practices and Awareness. Journal of Information Privacy and Security, 3.

Turton, William. (2016, October 21). This is Why Half the Internet Shut Down Today. Retrieved on October 21, 2017, from https://gizmodo.com/this-is-probably-why-half-the-internet-shut-down-today-1788062835

Twomey, Brien (2016, May 9). Mobile Apps: Privacy Attitudes, Knowledge, and User Practices. Retrieved August 21, 2017, from https://repository.tcu.edu/handle/116099117/11424

United States Senate (2017, August 1). Senators Introduce Bipartisan Legislation to Improve Cybersecurity of "Internet-of-Things" (IoT) Devices. Retrieved October 9, 2017, from https://www.warner.senate.gov/public/index.cfm/pressreleases?ID=06A5E941-FBC3-4A63-B9B4-523E18DADB36

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003, September). User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly, 27(3), 425-478.

Voicebot. (2017). Amazon Echo & Alexa Stats. Retrieved on November 15, 2017, from https://www.voicebot.ai/amazon-echo-alexa-stats/

Wollerton, Megan. (2016, August 9). Have a smart lock? Yeah, it can probably be hacked. Retrieved November 15, 2017, from https://www.cnet.com/news/have-a-smart-lock-yeah-it-can-probably-be-hacked/

York, Kyle. (2016, October 22). Dyn Statement on 10/21/2016 DDoS Attack. Retrieved from Dyn on October 21, 2017, from https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/