The Internet of Things: The Effects of Security Attitudes and Knowledge on Security Practices

Emergent Research Forum (ERF)

Zachary Singer
Texas Christian University
zsinger@textron.com

Beata Jones
Texas Christian University
b.jones@tcu.edu

Abstract

The paper examines the influence of the Internet of Things (IoT) users' security attitudes and security knowledge on their security practices, which has not been a subject of prior studies. Specifically, we focus on how knowledgeable individuals are about the security vulnerabilities present in IoT devices and how this knowledge affects their attitudes towards security and their willingness to own specific IoT devices. The researchers administered a survey to a convenience sample of 185 undergraduate business students investigating security vulnerabilities of three IoT devices—smart speakers, smart locks and IoT security cameras. This exploratory research aims to contribute to the existing literature in behavioral information security by providing preliminary insights into the relationship between IoT users' security attitudes, knowledge, and behaviors, with implications for the IoT device manufacturers and the information security scholars.

Keywords

Internet of Things, Security, User Behavior, User Knowledge, User Attitude

Introduction

The Internet of Things (IoT), the Internet-interconnected computing devices embedded in everyday objects, is becoming increasingly common in our daily lives. In 2018 alone, 23.14 billion "things" connected to the Internet were in use worldwide (Statista, n.d.). Today, 50% of businesses have an established IoT strategy or a pilot IoT project underway, and with $745 billion spending on the IoT across markets worldwide, there are more IoT devices on the way (IDC, n.d.). As technology continues to advance, it continues to affect more aspects of our lives. While the IoT devices aim to make our lives better and easier, what consumers often do not realize is that, with the rapidly growing network of these devices, a growing security risk is increasingly hard to ignore. The IoT 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 these devices.

Literature reports many instances of IoT device compromises or exploitations over the past few years. Common consumer devices, such as Amazon Echo (Greenberg, 2017) and the Nest Home Automation (Brandon, 2016) are examples of IoT devices that have been subject to cyber-attacks and exploitation by companies. We can no longer ignore the security issues of these devices. Our study seeks to answer the following 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 practices of IoT users regarding IoT device usage given their attitudes and knowledge of the security of those devices?
4. What are the practices of IoT users regarding IoT device usage after users become aware of historical security vulnerabilities and breaches of common IoT devices?

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

Literature Review

The Internet of Things and Security

While the expansive network that is the Internet of Things continues to flourish, the security surrounding that network is 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 step towards ensuring the protection of consumer data, it falls short in adequately addressing other vulnerabilities. A recent report revealed that 96% of corporations along with 90% of consumers believe that we need more IoT security regulations 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 exists for consumers in understanding IoT risks.

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). However, IoT manufacturers are focusing now 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).

The lack of formal regulation, paired with companies' desire to get their products to the market as quickly as possible, has already led to several instances of devices compromise. Amazon Echo is an example of an exploited IoT device. An individual could easily install malware on this Amazon device to turn it into a "personal eavesdropping microphone" without leaving a trace of its tampering (Greenberg, 2017). It would allow the hacker to listen to conversations around the Echo. Unfortunately, open placement of IoT devices in offices and hotel rooms makes tampering with them rather easy (Greenberg, 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 if they "purchased from trusted retailers" and "ensured their software was up-to-date" (Greenberg, 2017). Unfortunately, a software update does not fix this vulnerability, and, despite precautions, users with older Amazon Echoes are still be susceptible to this issue (Greenberg, 2017).

Homes do not seem to be safe either when considering IoT security vulnerabilities. Smart locks or locks that using a Bluetooth enabled device (such as a cellphone) fell prey to exploitation at a hacker convention known as DEF CON. There, two Mercurlite Security employees were able to break into 12 of 16 different types of smart locks with relative ease (Wollerton, 2016). The devices did not use encryption to store passwords. For about $100 investment, the hackers discovered all the passwords and unlocked the doors (Wollerton, 2016). In addition, a line of products from Nest has also run into their own set of security problems. One of Nest's products, a set of Bluetooth enabled security cameras, allows users to monitor easily their home from a distance. However, a security researcher found a way to exploit the Bluetooth connectivity and shut down the camera with a simple Bluetooth command, rendering their main purpose useless (Estes, 2017). It could give a burglar the time to enter a home undetected and allow a hacker to enter the home's network, if there are more connected devices on it (Estes, 2017). Alphabet did not fix this vulnerability until the above findings were published online (Estes, 2017).

Security Attitudes, Knowledge and Behaviors

Since the IoT devices are infiltrating all aspects of our lives, it is important to look at the current perceptions of the security of these devices among their users, as current security literature is lacking in this area. In the past, before the proliferation of the IoT devices, most studies found that security knowledge was not the issue in influencing an individual's security behavior. Partow-Navid and Slusky (2012) 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." That is, the compliance of security best practices is lower than an individual understanding of it (Partow-Navid and Slusky, 2012). Nowadays, however, consumers seem not to understand how to implement security best practices with their IoT devices, and they are often unaware of the risks that are involved with using them. Internet of Business (2017) determined that "48% of IoT users were not aware 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.

Most 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, push 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, while consumers at least acknowledge that they are aware of security vulnerabilities in IoT devices, they often choose to take on the consequences in favor of using the devices based on the utility they provide (IoT Security Foundation, 2017). However, as mentioned above (Internet of Business, 2017), consumers are largely unaware of what "security vulnerability" actually means. Making users aware of the specific incidents of IoT security compromises, such as those listed earlier, could potentially sway user attitudes enough to affect their behavior.

Theoretical Background

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) is what influence an individual's choice to engage in a behavior. In addition, the Unified Theory, 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 to examine how individuals behave when informed of IoT security vulnerabilities. Some studies previously mentioned in this paper have used one or both of these frameworks to study users through a variety of media, including social media sites and general online habits (e.g., Hazari & Brown, 2013). Figure 1 presents a research model for the study.

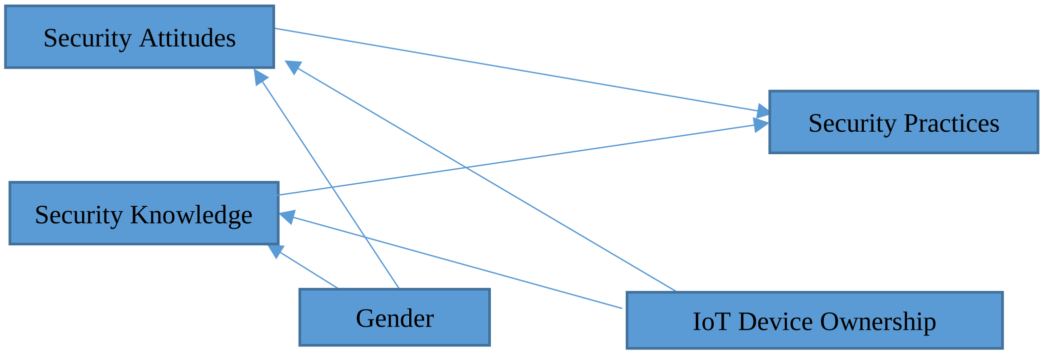

Figure 1 - Research Model

Methodology

The researchers gathered data from a convenience sample of 185 undergraduate business students at a private, southwestern university in the United States, across various demographic variables, such as age, gender, and education level, as presented in Table 1.

Age	**19 or Younger**	**20 or Older**	
	33%	67%	
Gender	**Male**	**Female**	
	54%	46%	
Year in College	**2nd**	**3rd or 4th**	**Not in College**
	78%	18%	4%
Number of IoT Devices Owned	**1-4**	**5-8**	**9+**
	48%	44%	8%

Table 1 – Demographic Data

The survey asked participants to respond to questions aimed to understand respondents' attitudes, knowledge, and behaviors towards current security practices and security vulnerabilities of the three IoT devices in the study: smart speakers, smart locks, and IoT security cameras. The survey used questions developed specifically for the study, and some questions were adapted to the context of the study from Hazari & Brown (2013). A majority of the questions used a seven-point Likert scale to determine the degree to which each respondent agreed with the statement presented. True/false questions and yes/no questions were also included in the survey. The researchers plan to use descriptive statistics, Cronbach's alpha to determine subscales' reliabilities, and Pearson correlations to analyze the data.

Conclusion

Relevance

Examining the IoT device users' security attitudes, knowledge and practices is an important research stream with implications for IoT device manufacturers and IS scholars alike. With the upcoming proliferation of IoT devices, device manufacturers will want to address appropriately their consumers' concerns. If the consumers are alarmed about security of IoT devices, manufacturers will need to put more effort into securing the devices before they bring them to market. If the consumers were concerned, but still willing to purchase the devices, perhaps there would be less sense of an urgency to address the device security issues. This study also lays a foundation for IS behavioral security scholars upon which others can build.

Limitations

A few limitations in the study are worth noting. The population of individuals surveyed was limited to business students at one university. While the focus of the survey was on students as they will be the largest consumers of IoT devices in the near future, the age range and education level of the students was narrow. Additionally, 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 and students' opinions and perceptions about IoT devices are likely to change in the near future.

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.

Capgemini. (2014, November). Securing the Internet of Things Opportunity: Putting Cybersecurity at the Heart of the IoT. Retrieved 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 from https://www.visioncritical.com/internet-of-things-stats/

Estes, Adam Clark. (2017, March 22). This Nest Security Flaw is Remarkably Dumb. Retrieved 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 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 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

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

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

IDC (n.d.). IDC Forecasts Worldwide Spending on the Internet of Things to Reach $745 Billion in 2019, Led by the Manufacturing, Consumer, Transportation, and Utilities Sectors, Retrieved from https://www.idc.com/getdoc.jsp?containerId=prUS44596319

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

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

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

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

Statista (n.d.) Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). Retrieved from: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

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.

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