May 2020

CYBER SECURITY @ HOME: The Effect of Home User Perceptions of Personal Security Performance on Household IoT Security Intentions

Erica Mitchell
Syracuse University

ABSTRACT

This study explored potential human factors predictors of home user security intentions through the lens of past performance, perceived self-efficacy, and locus of control. While perceived self-efficacy and locus of control are elements in several organizational and individual security models, past performance has been less frequently studied. The variable, past performance, which has been referred to in other studies as prior experience, knowledge, and information security awareness, is usually a single question self-assessment of familiarity or comfort with technology. This study explores user technical prowess in further depth, using formal technical education, informal technical education, employment in an IT/CS field, and self-reported email and internet security measures as a measurement of technical ability. Security intentions were determined by best practices in hardware security, network security, and IoT device protection.

Studying IoT security in home users is important because there are 26.6 billion devices connected to the Internet already, with 127 devices are being added to the network every second, which creates a very large attack surface if left unsecured. Unlike organizations, with dedicated IT departments, home users must provide their own security within their network. Instead of building security around the user, this research attempts to determine what human factors variables effect intentions to use existing security technologies. Through an online survey, home users provided information on their background, device usage, perceived ability to perform security behaviors, level of control over their environment, current security intentions, and future security intentions.

Hierarchical linear regression, path modeling, and structural equation modeling determined that past performance was consistently the strongest predictor of security intentions for home users. Self-efficacy and locus of control had varying results among the disparate methods. Additionally, exposure to security concepts through the survey had an effect on user security intentions, as measured at the end of the survey.

This research contributed an initial model for the effects of past performance, self-efficacy, and locus of control on security intentions. It provided verification for existing self-efficacy and locus of control measurements, as well as comprehensive, modular security intentions survey questions. Additionally, this study provided insight into the effect of demographics on security intentions.

CYBER SECURITY @ HOME:

The Effect of Home User Perceptions of Personal Security Performance on Household IoT Security Intentions

Erica M Mitchell

B.S. United States Military Academy, 2001

M.S., Syracuse University, 2010

DISSERTATION

Submitted in partial fulfillment of requirements for a degree of
Doctor of Philosophy in Information Science and Technology

Syracuse University
May 2020

ACKNOWLEDGEMENTS

First and foremost, I thank my family. My mother, Pamela Quayson, has been my greatest supporter throughout my life. She is always ready to listen, give advice, and prod me when needed. My children, Chloe, Nathaniel, Lily and Noah (our guardian angel) didn't sign up for this, but have been (mostly) patient throughout the process. They have sacrificed their time with me for me to achieve of my goal of completing this PhD. Alexis, my little sister, has been an amazing sister and has helped me when she could. Jonathan has supported me and wrangled the kids and pets, keeping the household running through the dissertation process and my real-world work trips during that time.

Second, I want to thank my advisor and my committee. Joon, I appreciate the time, energy, and effort that you put into guiding me and preparing me for this. Scott, I appreciate your guidance and sanity checks, and to you I say Beat Navy! Jenny, you were my initial advisor and have pushed me to improve my statistics abilities while still being a friendly face. Yang, I appreciate your help and your work in the IoT field. Martha, thank you for pushing me to make the best possible product. Young, I appreciate you agreeing to chair the committee even though there was quite a gap between the initial request and the defense. Jeff, thank you for taking time to speak with me about statistics and being a part of the committee.

Last, I need to acknowledge the institutional support at both Syracuse University and West Point. Thank you to Steve and Jen at the iSchool for everything you do for the PhD students and candidates. Your passion for the job and support of the students is unmatched. Thank you to Sue Coreiri, who got me started on this journey when I was interested in a Master's degree many moons ago. To my fellow PhD students and those who have graduated, I appreciate the love and support during the program and hope that I have returned the favor.

At West Point, I have to thank the Army Cyber Institute for selecting me to do this program and providing overwhelming support throughout the whole process. COL (R) Greg Conti, I appreciate you selecting me as you were establishing the Army Cyber Institute and hope I have lived up to your expectations. COL Andrew Hall, thank you for believing in me and having the confidence that I would complete the program. Chris Hartley, thanks for staying on me to find out when I would finish and giving me the ability to ask for help. COL Jeff Erickson, thank you for giving me the time I needed to make the last push. Doug Fletcher, thank you for stepping up and taking on Jack Voltaic, so I could finish. There is no way I could have done both at the same time. Thank you Judy Esquibel, Austin Minter, Erik Korn, Patrick Bell, and Steve Whitham for your patience and hard work during this time.

Table of Contents

List of Tables viii
List of Figures x
Chapter 1: Introduction 1
1.1 Internet of Things (IoT) 1
1.2 Cyber Attack Lifecycle 4
1.3 Organizational Cyber Security Measures 8
1.4 Security Concerns Specific to Home IoT Devices 15
1.5 Research Problem 19
1.6 Contributions 23
Chapter 2 Literature Review 24
2.1 Psychological and Educational Theories 25
2.2 Protection Motivation Theory 27
2.2.1 Fear Appeals Model 30
2.2.2 Health Belief Model 30
2.2.3 Threat Control Model 32
2.3 Theory of Reasoned Action 33
2.3.1 Theory of Planned Behavior 33
2.3.2 Technology Adoption Model 34
2.3.3 Technology Threat Avoidance Theory 34
2.4 Knowledge Theories 35
2.5 Combined Theories 38
2.6 Usable Security, Mental Models, and the Internet of Things 39
2.7 NOAH for IoT Framework (Excerpted from (Mitchell & Park, 2017)) 44
2.9 Related Work Summary 52
Chapter 3: Research Methodology 56
3.1 Research Design 56
3.2 Participants 57
3.3 Variables 62
3.4 Data Processing 68
3.5 Analysis Methods 70
3.5.1 Validity and Reliability 71
3.5.2 Multiple Hierarchical Linear Regression 72

3.5.3 Partial Least Squares – Path Modeling 75
3.5.4 Structural Equation Modeling 76
Chapter 4 Survey Results 78
4.1 Respondents by Source 79
4.2 Demographics 80
4.3 IoT Non-Ownership 84
4.4 Past Performance 86
4.5 Security Intentions (Existing) 102
4.6 Locus of Control 104
4.7 Perceived Self-Efficacy 105
4.8 Security Intentions (Future) 105
Chapter 5 Quantitative Analysis 109
5.1 Variable Composition 111
5.1.1 Validity 112
5.1.2 Reliability 113
5.1.3 Past Performance 113
5.1.4 Locus of Control 116
5.1.5 Perceived Self-Efficacy 117
5.1.6 Security Intentions (Existing) 118
5.1.6 Security Intentions (Future) 119
5.2 Hierarchical Linear Regression 121
5.2.1 Security Intentions (Existing) Software Security Measures 123
5.2.2 Security Intentions (Existing) Network Protection Measures 127
5.2.3 Security Intentions (Existing) IoT Device Protection Measures 131
5.2.4 Security Intentions (Future) Security Changes 135
5.2.5 Security Intentions (Future) IoT Device Protection Measures 139
5.3 Demographic Mean Comparison 145
5.3.1 Age 145
5.3.4 Ethnicity 147
5.3.5 Annual Household Income 149
5.3.6 Gender 151
5.3.7 IoT Ownership 152
5.4 Survey Effects 154
5.5 Self-Reported Secure User Analysis 156
5.6 Partial Least Squares – Path Modeling 159

5.7 Structural Equation Modeling 175
5.8 Explanation of Findings 181
Chapter 6 Summary and Conclusion 184
6.1 Analysis of Survey Results 184
6.2 Implications 189
6.3 Limitations 191
6.4 Contributions 192
6.5 Future Work 193
6.6 Conclusion 195
Appendix A – Survey Instrument 197
Appendix B – Research Appeals 227
B.1 – Facebook Friends Appeal 227
B.2 – Facebook Military-Affiliated Groups Appeal 227
B.3 – LinkedIn Appeal 227
B.3 – 53listserv Appeal 228
Bibliography 230

List of Tables

Table 1 Facebook groups where research pleas were posted 59
Table 2 LinkedIn groups where research pleas were posted 60
Table 3 Past Performance Questions 64
Table 4 Locus of Control Questions 65
Table 5 Self-Efficacy Questions 66
Table 6 Security Intentions (Existing) Questions 66
Table 7 Security Intentions (Future) Questions 67
Table 8 Demographics Variables 80
Table 9 Demographic Summary Table 82
Table 10 Paired Samples Statistics 97
Table 11 Paired Samples Correlations 97
Table 12 Variable Descriptions 112
Table 13 Cronbach's Alpha for variables 113
Table 14 Summary Statistics for Past Performance 115
Table 15 Past Performance Eigenvalue and Percentage of Variance 115
Table 16 Exploratory Factor Analysis Factor Loadings for Past Performance 115
Table 17 Summary Statistics for Locus of Control 116
Table 18 Locus of Control Eigenvalue and Percentage of Variance 116
Table 19 Exploratory Factor Analysis Factor Loadings for Locus of Control 117
Table 20 Summary Statistics for Self-Efficacy 117
Table 21 Self-Efficacy Eigenvalue and Percentage of Variance 117
Table 22 Exploratory Factor Analysis Factor Loadings for Locus of Control 118
Table 23 Summary Statistics for Security Intentions (Existing) 118
Table 24 Eigenvalues and Variance for SINT_EX 119
Table 25 Exploratory Factor Analysis factor loading for SINT_EX 119
Table 26 Summary Statistics for Security Intentions (Future) 119
Table 27 Eigenvalues and Variance for SINT_FUT 120
Table 28 Exploratory Factor Analysis factor loadings for SINT_FUT 120
Table 29 Variance Inflation Factors for SINT_EX Security Software Regressions 124
Table 30 SINT_EX Security Software Model Summary 125
Table 31 Regression Results for Security Software 126
Table 32 Variance Inflation Factors in Security Intentions (Existing) Network Protections Regressions 128
Table 33 Network Protections Model Summary 129
Table 34 Regression Results for Network Protections 130
Table 35 Variance Inflation Factors for IoT Protections 132
Table 36 IoT Protections Model Summary 133
Table 37 Regression Results for IoT Protections 134
Table 38 Variance Inflation Factors for Future Changes 136
Table 39 Future Changes Model Summary 138
Table 40 Regression Results for Future Changes 139
Table 41 Variance Inflation Factors for Future IoT Changes 141
Table 42 Security Intentions (Future) IoT Changes Model Summary 143
Table 43 Regression Results for Future IoT Changes 144

Table 44 ANOVA comparing variables by age 146
Table 45 Comparison of Means by Age 147
Table 46 Analysis of Variance by Ethnicity 148
Table 47 Past Performance and Perceived Self-Efficacy by Race 149
Table 48 Analysis of Variance by Household Income 150
Table 49 Locus of Control by Household Income 150
Table 50 Analysis of Variance by Gender 151
Table 51 Perceived Self-Efficacy by Gender 152
Table 52 Locus of Control by Gender 152
Table 53 ANOVA of Effects of IoT Ownership on Variables 153
Table 54 Variance Inflation Factors 161
Table 55 Bootstrap Results 163
Table 56 Structural Model Summary 164
Table 57 Bootstrap Results for Inner Model 166
Table 58 Unidimensionality of Indicators 167
Table 59 Outer Model Summary Table 168
Table 60 Loadings and Crossloadings of the Outer Model 169
Table 61 Bootstrap Results for the Weights for Each Indicator 171
Table 62 Variance of Latent Variables 172
Table 63 Bootstrap Results for PLS-PM with Demographic Variables 173
Table 64 Loadings and Significance for SEM 177
Table 65 Latent Variable Correlations 178
Table 66 SEM Model Fit Indices 178
Table 67 SEM Error and Variance Values 179

List of Figures

Figure 1 Cyber Attack Lifecyle (Mandiant, 2017) 5
Figure 2 NOAH for IoT Framework 44
Figure 3 Survey Mechanics 57
Figure 4 Initial Analysis Diagram 71
Figure 5 Reasons IoT Devices Were Not Considered 85
Figure 6 Reasons IoT Devices Were Considered but not Installed 86
Figure 7 Formal IT/CS Education by Type 88
Figure 8 Certifications by Type 90
Figure 9 Formal and/or Informal IT/CS Education 92
Figure 10 IT/CS Degree or Certificate Recency 92
Figure 11 Participant Online Actions 96
Figure 12 Online Accounts and Passwords 97
Figure 13 IoT Device Protection Measures Count 104
Figure 14 Reasons for not making changes 107
Figure 15 Future IoT Security Intentions 108
Figure 16 Regression Coefficients 122
Figure 17 Q-Q Scatterplot for Security Intentions (Existing) Security Software Regressions 123
Figure 18 Residuals Scatterplot for Security Intentions (Existing) Security Software Regressions 124
Figure 19 Outliers in SINT_EX Security Software Regressions 124
Figure 20 Q-Q Scatterplot for Security Intentions (Existing) Network Protection Regressions 127
Figure 21 Residuals Scatterplot for Security Intentions (Existing) Network Protections Regressions 127
Figure 23 Outliers in Security Intentions (Existing) Network Protections Regressions 128
Figure 24 Q-Q Scatterplot for Security Intentions (Existing) IoT Protections 131
Figure 25 Residuals Scatterplot for IoT Protections 132
Figure 27 Outliers in IoT Protections 132
Figure 28 Q-Q Scatterplot for Security Intentions (Future) Changes 135
Figure 29 Residuals Scatterplot for Future Changes 136
Figure 30 Outliers in Future Changes 137
Figure 31 Q-Q Scatterplot for Security Intentions (Future) IoT Changes 140
Figure 32 Residuals Scatterplot for Future IoT Changes 141
Figure 33 Outliers in Future IoT Changes 142
Figure 34 Difference in IoT Protection Measures 154
Figure 35 Comparison of the Number of IoT Protective Measures 155
Figure 36 Comparison of Means of IoT Protection Measures 155
Figure 37 Comparison of Means of Self-Reported Secure Users and All Others 157
Figure 38 Structural Model 164
Figure 39 PLS-PM With Demographic Variables 174
Figure 40 Mahalanobis Distance 175
Figure 41 Structural Equation Model 180

Chapter 1: Introduction

Thirty years after reaching the home in 1990 via dialup connections (Zakon, n.d.), home broadband Internet reached 73% of the population of the United States by 2017 (Pew Research Center, 2017), where it has since plateaued (Pew Research Center, 2019). An additional 17% of Americans do not have broadband home access, but do have smartphone Internet access (Pew Research Center, 2019). What once required an expensive personal computer (PC) and home phone line for access, can now be accessed by mobile phones, tablets, and low-cost IoT devices, which can be purchased for as little as $6.99 (Amazon, 2020). With increased connectivity comes increased security and privacy risks for home users, who may not have the expertise or interest in securing their devices against attackers. With such a large quantity of connected devices, unsecured home devices pose risks not only to home users, but also to corporations, government entities, and national infrastructure, if attackers harness home devices into botnets to use them for distributed denial of service (DDoS) attacks on large organizations and infrastructure, or use an insecure IoT device as a gateway into an otherwise protected network (Newman, 2018).

1.1 Internet of Things (IoT)

Gartner defines the Internet of Things as a "network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment (Gartner, 2017)." The government defines IoT as "the concept of connecting and interacting through a network with a broad array of "smart" devices, such as fitness trackers, cameras, door locks, thermostats, vehicles, or jet engines" (United States

Government Accountability Office, 2017) and offers three categories of IoT: industry, consumer, and public sector.

According to the Institute of Electrical and Electronics Engineers (IEEE), the

> "Internet of Things envisions a self-configuring, adaptive, complex network that interconnects 'things' to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the thing's identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration (IEEE, 2015)."

All listed definitions share a common trait of previously non-networked physical devices being connected to the Internet. The Gartner definition is overly broad, avoiding differentiation between computers and other objects, while the government definition is both nonspecific by using the term "'smart' devices" and limiting by providing an example listing. The IEEE definition, while long, provides the most comprehensive definition of IoT. It seemingly excludes smartphones, stating that "service is exploited through the use of intelligent interfaces (IEEE, 2015)" when many smart devices are controlled remotely through smartphone applications. More directly, the FTC issued a report specifically excluding desktops, laptops, tablets, and smartphones from the Internet of Things (Federal Trade Commission, 2015). For the purposes of this paper, IoT devices exclude smartphones, tablets, and computers while recognizing that those devices can be used to control smart devices and typically house the applications required to do so. Despite the government definition including industry, which implies industrial control systems, those are outside of the scope of this paper. Industrial control systems are controlled

within the context of corporate or utility and therefore should have the organizational support that home IoT users lack.

IoT device vulnerability is attributable to four sources: software, hardware, network connectivity, and user configuration. In January of 2014, Bruce Schneier authored a prescient opinion piece highlighting the vulnerabilities of IoT devices, which are often unpatched, running older operating systems, have binary drivers, and may not have patches available, even if users were willing to install them (Schneier, 2014). There are significant passive attack vectors, such as eavesdropping, node destruction, node malfunction, node outage, and traffic analysis, as well as active attacks throughout the seven layers of the Open Systems Interconnection (OSI) model (Butun, Osterberg, & Song, 2019).

Attackers want control of IoT devices for three main reasons: using the device in a botnet to attack larger targets (Fruhlinger, 2018; Goodin, 2020), using access to the device to pivot to other portions of the user's network (Goodin, 2019), and more recently, financial gain through demanding ransom (Balaban, 2019). Less frequently, vigilantes compromise IoT devices and render them useless through destruction of software or hardware, better known as "bricking" them, to prevent their use by attackers (Laliberte, 2019).

As networking technology improves, the spread of IoT devices will continue, with low earth orbiting satellites and 5G mobile broadband expanding the availability of the Internet to areas that do not have broadband capability (Liberg, et al., 2019). The Internet of Things is a facilitator in globalization through technological interaction, whereby instant communication worldwide is possible and affordable (Bernard, 2020). The Cloud of Things is only as secure as its most insecure device, requiring participants to secure their individual devices for the security benefit of the herd (Brooks & McKnight, 2017).

1.2 Cyber Attack Lifecycle

In order to understand security concerns for IoT devices and home networks, it is important to first understand the cyber attack lifecycle, which is followed by attackers, regardless of target. The government definition of cyberspace is: "The interdependent network of information technology infrastructures, that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (Department of Homeland Security, 2017)" Cybersecurity is "the art of protecting networks, devices, and data from unauthorized criminal use and the practice of ensuring confidentiality, integrity, and availability of information (DHS CISA, 2019)." Information privacy is defined as "the right to have some control over how your personal information is collected and used (IAPP, 2020)."

While both concepts are important, and even overlap in some places, the scope of this research is examining security for home users. Privacy has a separate set of considerations and body of literature. The most important distinction is that a user's main influence over their privacy is determining how much information to share. Once a user's information is shared, the privacy and security of that information is controlled by the data recipient.

The extended definition of cybersecurity is:

> "strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. (Department of Homeland Security, 2017)"

The standard definition of a cyber attack is "an attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity (Department of Homeland Security, 2017)," while the extended definition is "the intentional act of attempting to

bypass one or more security services or controls of an information system. (Department of Homeland Security, 2017)"

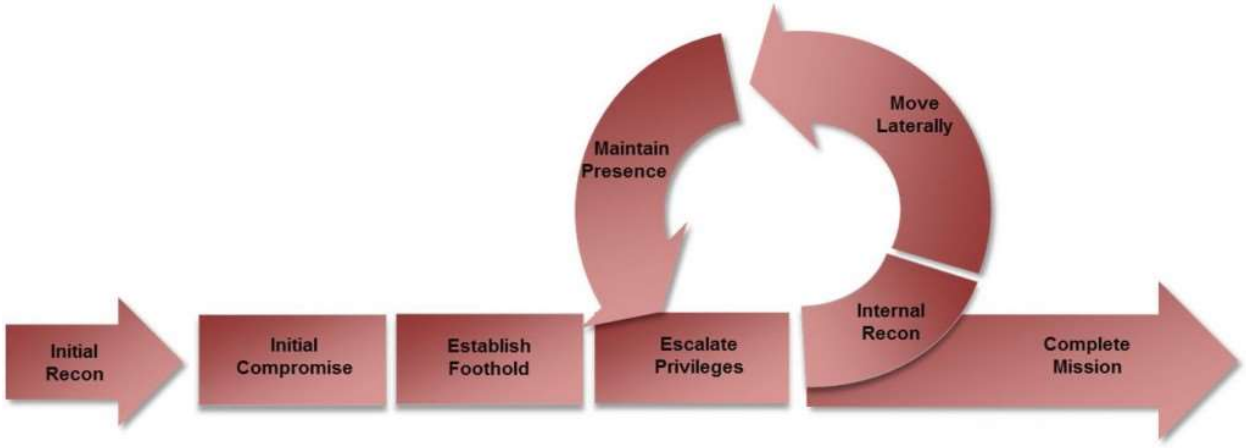

Figure 1 Cyber Attack Lifecyle (Mandiant, 2017)

The cyber attack lifecycle consists of initial reconnaissance, initial compromise, establishing a foothold, privilege escalation, internal reconnaissance, lateral movement, maintaining presence, and completing the mission.

Initial reconnaissance consists of collecting information on the company and/or employees of the company being targeted. This can be accomplished through physical methods, such as observing employees entering and exiting the building, dumpster diving for company information, and social engineering. Digitally, reconnaissance typically consists of scanning the network to enumerate the hardware on the network and open ports, which may provide information on the function of the server or computer and possible attack vectors. Scanning a network may be detected by organizations with more sophisticated security departments, so attacks on those organizations are performed over an extended time period with smaller data packets to prevent detection.

Initial compromise is when entry into the network is first achieved by a malicious attacker. This may involve gaining access to a server directly, but most often involves gaining

access to the most insecure device on the network, which may be a computer, printer, or IoT device. This may be accomplished through an attack on the server directly, exploiting open ports or outdated software. It may also be accomplished through user compromise, such as a phishing attack where the user opens a malicious attachment or provides their credentials to an external website. For IoT devices, there are at least eight ways to penetrate the device itself (Dunlap, 2019) and there is also the ability to intervene in the communication between the device and the app that controls it (Ashford, 2019).

Establishing a foothold consists of depositing software on the infected network to provide a backdoor into the system. The software allows the attacker to continue to re-access the system at the conclusion of their initial session. One example of establishing a foothold may be the creation of a user account that appears legitimate within the company, but that the attacker has sole control over. At this time, the attacker may also download software to assist in the next several steps of the attack lifecycle.

Escalating privileges is when the attacker uses various exploits to escalate privileges from basic user access to elevated, administrative privileges. This may be accomplished through performing actions as the SYSTEM account, cracking administrative passwords, or passing password hashes. Typically, as part of this step, consistent with establishing a foothold, the attacker will build an administrator account that is named to blend in with existing accounts.

Internal reconnaissance consists of performing reconnaissance using compromised user credentials or surreptitiously created credentials to determine what data exists in the network, where it is stored, what hardware assets are on the network, network topology, and access control lists for network devices and data storage. This information is recorded to speed the process of exploiting the network to exfiltrate target information or to gain control over particular assets.

Lateral movement means pivoting from the initial entry point into other parts of the network and to other networks through trust relationships between the networks. For example, during the Target breach, attackers initially gained entry into a heating, venting, and air conditioning (HVAC) contractor's computer, which was used to log in to Target contractor management website, from which the attacker pivoted to the point of sale (POS) system network for Target (Krebs, 2015).

Maintaining presence consists of emplacing backdoors and malicious software in several locations, allowing the attacker to re-establish presence if their presence is discovered and eradicated. This may also consist of hiding malicious software within commonly used files, such as Microsoft Word documents and Adobe Portable Data Filler (pdf) files, to trigger the emplacement of another backdoor when opened. Often malicious software uses reverse shells to bypass network security, making it seem like the connection is originating from inside of the network, rather than being connected to by outside parties.

Completing the mission can consist of exfiltrating targeted data, damaging or deleting targeted data, and/or damaging equipment. Most often, the attackers leave their backdoors in place, even when the mission is complete to prevent repeating the steps listed above should a new mission arise. An example is the series of attacks on Saudi oil companies. First, there was the Shamoon virus that deleted data and destroyed hard drives, which was followed by another attack using an unnamed software that may have been intended to cause an explosion (Perlroth & Krauss, 2018). It appears that the same attackers were behind both attacks, so the new software may have been implanted using backdoors emplaced during the initial attack.

Understanding the cyber attack lifecycle is critical to hardening systems to prevent or disrupt an attack. This research is primarily focused on studying home user personal security

performance measures, to determine how best to enable them to prevent initial compromise, keep attackers from establishing a foothold, prevent privilege escalation, reduce internal reconnaissance efficacy, and prevent lateral movement within their home network.

1.3 Organizational Cyber Security Measures

Information assurance or defensive cyber measures in general are widely varied and can be divided into administrative, network level, and host level. Administrative defensive cyber measures include understanding the organization's function and how data supports it, using DNS reputation services, monitoring, inventorying hardware and software, establishing security boundaries, securing data at all times, user training, penetration testing, and having a cyber incident response plan (National Security Agency Information Assurance Division, 2015). Network mitigations include firewalls, demilitarized zones (DMZs), access control lists (ACLs) on routers and firewalls, virtual private networks (VPNs), segregating networks and functions, and honeypots (United States Computer Emergency Readiness Team, 2016). Host level mitigations include application whitelisting, anti-virus and anti-malware software packages, controlling administrative privileges, limiting workstation to workstation communication, secure baseline configurations, applying patches in a timely fashion, and host intrusion prevention rules (National Security Agency Information Assurance Division, 2015). Additionally, a 99 page guide to industrial control system cyber security assessments was published in 2016 (National Security Agency, 2016).

Understanding the organization's function and how data supports it means evaluating the overall organization and how that data needs to move between functions. By understanding what data is accumulated and how it is processed, an organization can take steps to secure that data and ensure that it is not vulnerable to attackers.

Domain Name Service (DNS) reputation services inspect hyperlinks to ensure that they are legitimate. This is most often offered by an outside company that provides the service to several organizations and is constantly updating their intelligence, on which the system is based.

Network monitoring and monitoring logs allows for system and network administrators to determine the network and computer baseline. When there is an anomalous traffic pattern, the administrators can inspect the logs and dissect the attack or attempted attack. If it is caught early enough, the administrators may be able to better secure their network to prevent an attack. However, once inside the network, attackers often delete logs or portions of logs to obscure malicious activity. In the event of real-time reporting, administrators may receive so many alerts that malicious intrusions are masked by other alerts or may reduce altering thresholds (Critical Start, 2019).

Inventorying hardware and software prevents attackers from emplacing new devices on the network by ensuring that administrators recognize what belongs and take action to block or remove that which does not. Inventorying software simplifies the application whitelisting process, while inventorying hardware can assist in configuring port security. Network administrators may also use port security to prevent new devices being added to the network without an administrator granting permission.

Establishing security boundaries means determining the security levels for various segments of the network. For example, a business that offers free customer Wi-Fi will not want customers to be able to access their internal documents. In a company with trade secrets, the network storage location on which they are contained, will be segregated logically from the rest of the network to prevent intellectual property theft. On airplanes that offer WiFi access to

customers, the internal aircraft systems should be segregated to prevent a user from accessing flight controls (Higgins, 2019).

Securing data at all times means securing data in motion as well as data at rest through the use of encryption. Products such as Microsoft Bitlocker encrypt the entire hard drive, so if the computer is stolen, the thief cannot gain access to the data without a password. Securing data in motion involves encryption of the conveyance, whether that is an SD card, USB drive, email or any other form factor for moving data. Digitally signing a document provides verification that it came from the sender, but no protection preventing others from reading the document, while encrypting the document verifies the sender and keeps the content confidential, allowing only the sender and recipients to read it.

User training can expose users to possible attack vectors and through education, organizations may prevent some users from making security mistakes that allow an attacker access. User education may focus on what is contained in an acceptable use policy or may provide helpful tips, such as how to identify a phishing email and what to do if they receive one. User education may be required in an organizational environment, but there are no mechanisms to provide education to home users or require their compliance with best practices.

Penetration testing may be executed by a third-party company or using an internal penetration tester to test the security of the network. There are red teams, also known as black box penetration testers, with no insider knowledge of the company, and blue teams, who are given access to the internal workings of the company and provide mitigation feedback. The purpose of this is to proactively test the network and determine security flaws and mitigate them prior to an attack.

Cyber incident response plans provide guidance for recovery from incidents such as disasters, breaches, or data loss. The plans provide guidance for operating in austere conditions, recovering data, and restoring consumer confidence. They also attempt to provide risk assessments concerning the likelihood of an incident and cost of recovery from it. In some cases, it may also include cyber insurance coverage, depending on the reliance of the company on online presence and customer confidence.

Firewalls are typically the first line of defense in a defense in depth strategy and are used to direct and filter traffic (Bradley, 2019). A firewall is typically placed between a border router and the rest of the network. The firewall usually has at least two networks behind it, a demilitarized zone (DMZ) network and the internal organizational network. At a basic level, the firewall tries to prevent attackers from reaching the internal network, while allowing any visitors access to the DMZ, where public-facing servers are located. Through the use of access control lists (ACLs), the firewall can block traffic from known malicious internet protocol addresses (IPs), as well as prevent spoofed traffic from entering the internal network with non-routable IPs (Rubens, 2018).

The DMZ is a less heavily protected network, where servers, such as web servers and mail servers, that visitors communicate with are placed. While it is not placed directly on the Internet, it has minimal protections thus allowing visitors to reach the servers there. The servers themselves are hardened against attacks since they are less protected than those in the internal network. The DMZ can be set up as a side network on a single firewall, or may be configured with dual firewalls, requiring all traffic to pass through the DMZ to get to the internal network.

Access control lists exist on firewalls, routers, and layer three switches, which operate at the transport layer of the Open Systems Interconnection (OSI) model. They can be used to route

and filter traffic appropriately. An ACL statement is typically formatted as [action] [source] [destination]. The action is “allow” or “deny”, while the source and destination can be individual internet protocol addresses (IPs), subnets, or “any”. By default, ACLs are configured to deny access to any IP. Due to application from the top of the list when applying an appropriate rule, the ordering of the statements in the ACL is as important as having the correct statements. If the first statement in the ACL is “deny any any”, then no traffic will pass through that hardware, while if the first statement is “permit any any”, all traffic will be allowed to pass through the router despite any statements to restrict traffic further down in the list. ACLs can be used to block traffic from entire lists of IPs and ports, thus blocking malicious traffic based on where it originated or what protocol it is using. The downside to ACLs is that they are static, must be updated frequently, and minor changes can prevent network traffic from being routed appropriately if a statement is placed in the wrong position or if a statement is accidentally deleted or disabled (Franklin, 2019).

Virtual Private Networks (VPNs) allow organizations to create encrypted tunnels, through which multiple physical locations can communicate through encrypted tunnels or employees can connect securely from remote locations. For the employee or alternate location, it allows full access into the internal network from outside of the organization. Encryption makes it harder for an attacker to intercept the data being passed between the internal and external location.

Segregating networks and functions is often achieved with virtual local area networks (VLANs) and the appropriate access control lists to restrict traffic. For example, in a large corporation, there may be three main functions: finance, manufacturing, and human resources. The average worker in the manufacturing department does not need access to the finance

department's records and information. Using the principle of least privilege, the manufacturing department would be placed in a VLAN with access to only their own information. If the manufacturing manager needed access to a folder in the finance department, that individual may be granted access to only the files or folders required. With a layer three switch, each port can be configured for the VLAN it belongs to, allowing employees from each department to use the same hardware, but remain virtually segregated based on their department (Cisco, 2018). As an added security measure, the switch can be configured with port security to prevent a manufacturing employee from switching his computer to a finance VLAN port to gain access to their files.

Honeypots are virtual networks that appear to be insecure, which are used to lure potential attackers and determine what their methods are. While a honeypot does not actually prevent being attacked, it can serve as an early warning that a network is being targeted and can provide intelligence about the attackers to allow the internal network to be protected (Fruhlinger, 2019).

Application whitelisting determines what programs (by name, file type, and/or location) a computer will execute, rather than attempting to block known bad applications by name or signature (Sedgewick, Souppaya, & Scarfone, 2015). While it is time-consuming to configure, it is one of the most robust protections against malicious software on a computer. It can prevent execution by files that should not be executable, such as word documents and pdf files. Once configured, it remains relatively static, but in the event a program does not function properly, it can be configured to allow that file to execute. Properly configuring the whitelist requires clean computers that have not been infected with malicious software.

Antivirus software alone is no longer an effective protection, but developers have added a cloud intelligence component to their antivirus protection, allowing for real-time updates to virus signatures (Raghunarayan, 2018). Additionally, there are software companies offering anti-malware packages, which search for rootkits, ransomware, adware, and other malware. Advanced versions may also provide real-time detection of patterns that indicate malicious software, by running the file in a sandbox to observe its behavior, even if there is no signature for that exact file.

Controlling administrative privileges also falls under the principle of least privilege. Elevated privileges should only be given to administrators and should only be used on an as needed basis, meaning that an administrator should log in to their unprivileged account for routine use and should elevate privileges as needed to perform their tasks. There should never be an email account associated with a privileged user account, as email is a vector for an attacker to gain credentials using a phishing attack.

Limiting workstation to workstation communication not only assists with the segregating of networks and functions, but also prevents a pass the hash attack, which allows for a hash of a user's credentials to be used to allow access to another computer. An attacker can then pivot through the network using that hash, which is much more damaging if it is a hash of administrator credentials.

Secure baseline configurations are used to develop a uniform secure computer image, which ensures that only patched, secure computers are placed on the network and allows for infected machines to be wiped and reloaded quickly. They are also updated with all patches up to the point the image was made, reducing the amount of time spent patching a computer.

A significant source of intrusions is unpatched software, which makes it important to patch operating systems and other software as soon as the patches become available. When software manufacturers announce patches, they are also announcing exploitable flaws that exist in unpatched software, providing attackers with information on how to compromise computers. With Windows 10 Home Edition in 2015, Microsoft made patching mandatory for home users, but Pro and Enterprise users either receive patches through their organization or opt-in to Microsoft patches (Gibbs, 2015). In an Enterprise environment, there are several options for centrally managing and deploying patches, rather than patching each computer individually.

Host intrusion prevention server (HIPS) rules are centrally managed for an Enterprise network and are designed to blacklist malicious software and signatures. The updates are sent to the individual hosts, allowing for the machines to be protected even if the server goes down. However, one drawback to the system is that if the HIPS server rules are compromised by an attacker, it will be proliferated to all managed hosts in the network. Additionally, it is trivial for an attacker to make a minor change to malicious software, resulting in a new signature.

While these are organizational security measures, many can be adapted to the home network to further the goal of reducing an attackers' ability to compromise a user's home network, establish a foothold, escalate privileges, and move laterally. Determining how to motivate the user to perform home equivalents of organizational security measures will reduce the attack footprint, thus improving collective cyber security.

1.4 Security Concerns Specific to Home IoT Devices

Given the numerous threats to their devices, home users should want to protect their devices and online presence, but their attempts to do so appear to be mixed, with some unconcerned about password security, while others attempt to follow best practices (Olmstead &

Smith, 2017). When searching for “home internet security best practices”, Google returns several websites, each of which are primarily focused traditional organizational computing (Google, 2017). For example, 2014 NSA guidance, published by the Department of Defense Chief Information Officer, includes three tips out of twenty-six that are specific to home entertainment devices (NSA, 2014), while a subsequent report reduces the number of tips for home entertainment devices to two (NSA, 2016). Home entertainment devices are only one form of many varieties of IoT devices and are the only ones that are addressed in either report. In 2018, Best Practices for Keeping Your Home Network Secure, had specific “computing and entertainment device recommendations” (National Security Agency, 2018). Over time, the guidance given to home users to secure their networks has increased and incorporated more IoT device recommendations.

While home users cannot be expected to have organizational level cybersecurity measures in place, but there are several recommendations for commonly available home user security precautions. CSO Online offers eight tips for securing IoT devices at home and in the workplace: don’t connect if you don’t need to, create a separate network, pick good passwords and a different password for each device, turn off Universal Plug and Play (UPnP), make sure you have the latest firmware, be wary of cloud services, keep personal devices out of the workplace, and track and assess devices (Drolet, 2016). While the last two suggestions are directed to organizations, they may be applied in the home user context as well.

There are many devices that can connect to the Internet, but just because it is possible, does not mean that it is prudent to do so. Many smart appliances, including at least one toaster, were part of the Mirai botnet (Blue, 2016) that disrupted DNS on the East Coast in 2016. While

notifications that toast is ready are convenient, they are likely not worth the security gap created by having an insecure device on the network.

Several routers offer the option of a guest network, allowing the home user to segment computers from other devices, as well as allowing for visitors to connect to the Internet without receiving access to the home network. While this is an excellent solution to segment less secure devices, the user must ensure that their router's guest network still offers encryption. Having an open Wi-Fi network invites intruders (Hoffman, 2015), who have an easier route to the more secure home network once connected to the guest network.

Picking good passwords and multiple passwords is difficult for users to do, based on complexity guidance, frequency of change, and the number of accounts that home users have across the Internet. Fortunately, password complexity and frequency of change guidance has been updated to encourage longer, more user-friendly passwords with no timeline for change requirements (Sophos, 2016). Additionally, given the potential for password sharing within a household to manage smart devices, users must ensure that they do not reuse a password for a sensitive account on their devices. It is especially important that users change their default username and password on their routers to prevent attackers from compromising their network, due to default usernames and passwords being readily available on the Internet. Password vaults are another security measure that could reduce the mental burden on users to remember several long, complex, frequently changing passwords, reducing their requirement to remember a single password to access the others within the vault.

Universal Plug and Play (UPnP), allows users to quickly configure their devices to connect to the Internet through the router by forwarding ports (Hoffman, 2016; List, 2019). The main vulnerability is that anything connected to the network is deemed trustworthy and may then

request that port forwarding. Given the inherent vulnerability in IoT devices, an attacker could gain access to the IoT device and use it to open ports, allowing for an attacker to establish a foothold on the network.

Having the latest firmware can reduce the vulnerability of devices on the network to hacking. However, not all devices have upgradeable firmware, which can leave vulnerable, unpatched devices on the network for years with no support. Some devices automatically check for updates and prompt the user to install the latest firmware, but many require the user to manually check for updates, either on the device or online. There are also free services that will perform the website check for users and email them when the page has changed. It requires the user to perform an initial setup, where a user must enter the website for firmware updates for their particular device model (VisualPing, 2017).

Due to their minimal computing power, many IoT devices rely on cloud services to function, as they do not have significant onboard storage or processing power. However, by sending data to the cloud, the user is opening an avenue into their network, which can be exploited. Some devices offer encryption between the device and the controller, but it is not configured by default.

Keeping personal devices out of the workplace was advice intended to protect the organization, but can be applied in the home network as well. When hosting visitors, keep them in the guest network, instead of the trusted network. Compartmentalizing trusted devices from untrusted will improve the security of the network, as well as protecting the data stored on traditional computing devices. Due to their limited security features, IoT devices should also be placed into the untrusted guest network, instead of the trusted network.

The recommendation to track and assess devices was organizational advice, however, home routers have the capability to do so as well. Not only can users view devices connected to their network, they can also restrict connectivity by media access control (MAC) address, preventing new devices from being introduced to the network without administrator approval, similar to how port security works on a corporate network's wired routers and switches. Home routers also have logging capability, allowing the home network manager to monitor for anomalous network traffic. Additionally, home network users can configure timers in their routers, restricting IoT device traffic when they are home with no need to remotely manage their devices.

1.5 Research Problem

Cybersecurity is a complex, multi-billion dollar industry for organizations, but there is little support for home users. While the number of personally-owned IoT devices is increasing, security support for home users is not, creating a security gap that is being exploited by attackers. IoT devices have been used to generate malicious botnets, which have been used to disrupt the Internet.

Household IoT devices are always connected to the Internet, provide little to no direct feedback, are infrequently monitored remotely, and consistently connected to a power source, making them a target for attackers to use them in botnets (Palmer, 2018). With an estimated 26.6 billion IoT devices connected to the Internet in 2019 (Maayan, 2020), a more than fivefold increase from the 5.2 billion home user IoT devices connected to the Internet in 2017 (Gartner, 2017), IoT devices have already surpassed the 3.365 billion personal computers (PCs) that were sold between 2006-2016 (Dunn, 2017). While PC sales have decreased between one and ten percent year over year since 2012, IoT device installations grew by 750 million between 2014

and 2015, and by 1 billion between 2015 and 2016 (Columbus, 2016), and by 21.4 billion between 2017 and 2019 (Gartner, 2017; Maayan, 2020). At an estimated rate of 127 devices connecting per second (Maayan, 2020), over 4 billion new IoT devices will be added by the end of 2020.

While many devices generate small quantities of network traffic to connect to the controller and to send information to the cloud, IP cameras can produce significant network traffic. For example, Nest recommends a minimum upload speed of 2 Mbps for their indoor and outdoor cameras (Nest, 2017), but bandwidth calculations for a single 5MP camera, using H.264 encoding, streaming high quality video, at 30 fps requires 24.06 Mbps of bandwidth (Securitybros, 2017). One hundred thousand cameras can potentially generate 2.4 Tbps of traffic if aggregated and directed at a single source. The Mirai botnet attack and related attacks prior to it generated 620 Gbps to 1.5 Tbps of network traffic, which enabled the attackers to disrupt each website they targeted (Department of Homeland Security, 2016). While the most highly publicized incidents have been directed at civilian websites, the greatest threat from botnets are attacks targeting the government, military, or critical infrastructure.

There is no infrastructure in place, nor any federal laws or regulations requiring home users to secure their network or requiring manufacturers to provide security measures in their devices intended for home use. The IoT Cybersecurity Improvement Act of 2017, would have required that devices purchased for federal government use " (1) do not contain known security vulnerabilities or defects; (2) rely on software or firmware components capable of accepting properly authenticated and trusted updates from the vendor; (3) rely only on non-deprecated industry-standard protocols and technologies for certain functions; and (4) do not include fixed

or hard-coded credentials (Warner, 2017).” The bill was not passed, but the requirements would have been beneficial for both federal government entities and home users.

National Institute of Standards and Technology (NIST) has a Cybersecurity for IoT Program, which “supports the development & application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed (NIST, 2020).” Their stakeholders are government, industry, international bodies, and academia, with users being noticeably absent (NIST, 2020). As part of the program, NIST has developed two frameworks: draft recommendations for IoT manufacturers (Fagan, Megas, Scarfone, & Smith, 2020) and considerations for managing IoT cybersecurity and privacy risks (Boeckl, et al., 2019). Neither document focuses on home user security protections, with the former targeting manufacturers and the latter targeting the organizational cybersecurity workforce. California passed Assembly Bill 1906, which took effect January 1, 2020, requiring manufacturers to provide “a reasonable security feature or features” for connected devices, with a specific focus on authentication (California Assembly, 2018).

Insecure IoT devices pose a threat not only to the home user whose network it resides on, but also to the organizations that are targeted by botnets. While those botnets are currently used to perform DDoS attacks, in the future they could be used to harness computing power for any number of uses, including cracking cryptographic algorithms. Studying home user’s security behaviors and motivations, to determine how to increase their security can reduce the number of unsecured devices available to attackers and improve cybersecurity for everyone.

Home users do not typically receive security feedback from their IoT devices to determine whether they have been hacked or not. Encouraging users to secure their devices will improve the security of the Internet for everyone, because of the threat of IoT devices being used

in a botnet to attack larger targets. Additionally, with the option to work from home, a corporate or government network could be attacked through an employee's more easily accessed home network.

This study intends to explore IoT security's relationship to locus of control, self-efficacy, and past performance by answering the following question: How does a user's locus of control, self-efficacy, and past performance influence home IoT security intentions? This is an important question because there are no safeguards in place for users as there are in a corporate environment. Those who choose to secure their IoT devices and home networks are either committing to research how to secure those devices or are already familiar with cyber security through formal or informal education and exposure. One would also expect that they are confident in their ability to secure the network and their belief that the network is something that they can control. Exploring how those three elements interrelate can help researchers determine how to increase user propensity to secure their home network with existing tools and methods.

Internal locus of control means that a person believes that they can control things within their environment, while external locus of control is the belief that things happen to them, which they do not control. Perceived self-efficacy is the belief that the person can accomplish a given domain-specific task. Past performance, for this study, is the measure of formal education, informal education, IT/CS-related employment, and self-reported internet and email security behaviors.

The hypothesis for this study is: *Home users' perception of self-efficacy, increased past performance, and internal locus of control in computing environments will increase their intentions to make their home IoT environments more secure.*

1.6 Contributions

This study looked deeply into human factors in security intentions for home IoT users in the specific context of locus of control, self-efficacy, and past performance. While it was guided by theory, to reduce interaction effects, it focused solely on those three concepts, which appear in several theories, as outlined in the literature review. It also contributed a valid and reliable test instrument for measuring past performance, which measures respondents' exposure to cybersecurity and internet and email security habits. While the Security Behavior Intentions Scale (SeBIS) measures individual security intentions, the SeBIS focuses on device securement, software updates, password management, and proactive awareness. In the IoT environment, those are not necessarily the priority and, in some cases, they are not possible. Additionally, the Human Aspects of Information Security Questionnaire (HAIS-Q) evaluates organizational user security behaviors. However, given the organizational context, it focuses on compliance with policy, rather than a personal, internal drive to protect a home network. While some of the self-efficacy questions refer to information security policy, this study focused on home users with no organizational support. This instrument explores what constructs cause users to put forth the effort to secure their home network without any external influence or support. Understanding what motivates a user allows future research to focus on ways to influence human factors that encourage security intentions.

Chapter 2 Literature Review

Most academic IoT-specific security research is focused on technical systemic solutions to IoT security. At best, there is mention of a user role in securing the Internet of Things, but those references generally absolve the user of any expectations or responsibility. However, there is a large body of literature pertaining to organizational computer users relating to technology adoption, coping with threats, and user security behaviors.

User behaviors differ greatly in the home context from the organizational context. Whereas organizations have acceptable use policies and security control mechanisms, such as minimum password complexity or two-factor authentication requirements, home users have greater autonomy over their security mechanisms. A home user may choose convenience over security, which can result in many insecure behaviors. For example, a home user can decide to leave the default administrator password on their home router, which allows any attacker to gain full control of their home network. They may also choose to just use the router out of the box, without taking advantage of available security mechanisms, such as restricting users, not broadcasting the SSID for passers-by to see, or not requiring any authentication to connect to the Wi-Fi.

Security is also unique in that it is invisible, users of IoT devices receive no feedback relating to security efficacy, and even home personal computers (PCs) that don't have updated security software will not provide efficacy feedback. Organizations have various forms of monitoring, logging, and real-time updates in some cases, allowing system administrators potential early warning of intrusions. On the other hand, a home user may be breached and may not realize it, unless the attacker has done something noticeable, such as adjusting a Nest thermostat (Maher, 2019) or installing software on a computer that leaves a trace.

Organizations also have the benefit of dedicated security personnel, who are responsible for researching, installing, maintaining, and monitoring security hardware and software, while home users may be technological novices. Not only do home users not have access to organizational level software suites, but they may also receive pop-up ads offering protection, which may instead be malicious software.

Several main theories, and their derivatives, may influence user security behaviors from diverse fields including psychology, healthcare, and human-computer interaction. The scope for this literature review is human factors research that influenced the variable selection, technology-related studies focused on human factors in security, IoT specific studies, and user technology mental models.

2.1 Psychological and Educational Theories

Wigfield and Eccles' (2000) Expectancy-Value theory, based on Atkinson's motivational determinants of risk-taking behavior (Atkinson, 1957), includes previous achievement-related experiences as an influence on achievement motivation, in the context of mathematical achievement motivation in children. While the full theory measures many more items, the inclusion of past performance components allows an analysis of ability and domain-specific education in relation to the belief structures locus of control and self-efficacy. Past performance is evaluated through previous achievement-related experiences, which effect the child's interpretation of experience, including locus of control. The interpretations of experience effect the child's goals, including their self-concept of their abilities, which in turn drives their expectation of success (Wigfield & Eccles, 2000).

Locus of control (Rotter, 1966) is part of the broader social learning theory (Rotter, 1954) and focuses on an individual's perception of whether what happens to them can be controlled.

Those with internal locus of control feel that they have control over their circumstances and what happens, while those with external locus of control feel that they have little to no control over what happens to them and are less invested in their experiences.

Locus of control was examined in early studies of information systems (Schneiderman, 1979; Zmud, 1979; Simes & Sirsky, 1985; Meinert, Festervand, & Lumpkin, 1991), but primarily in the context of user satisfaction and human-computer interaction. Schneiderman (1979) and Simes and Sirsky (1985) found that locus of control effected user satisfaction with human-computer interaction, while Meinert, Festervand, & Lumpkin (1991) found that there was no statistically significant relationship between locus of control and user satisfaction.

Self-efficacy is a construct from social cognitive theory that assesses individuals' personal beliefs in their ability to complete a task (Bandura, 1977). Computer self-efficacy is the individuals' perception of their ability to use a computer, and in the initial development of the construct, computer self-efficacy accounted for 22.5% of the variance in computer usage and 24% of the variance in outcome expectations – performance (Compeau & Higgins, 1995).

In later work, Bandura clarified that self-efficacy constructs should be intentional about being specific enough to measure the desired construct, as self-efficacy is domain specific (Bandura, 2006). Additionally, the work cautions to avoid conflating self-efficacy with security intentions, encouraging terms like "will" be reserved for intentions, while self-efficacy should use words like "can". Bandura (2006) also warned that self-efficacy must be differentiated from locus of control, due to its focus on the respondents' belief of whether they control their own outcomes or whether their outcomes are externally controlled, while self-efficacy focuses on the ability to perform the specific task(s).

2.2 Protection Motivation Theory

Protection Motivation Theory (PMT) is a health-based theory based on threat appraisal and coping-appraisal (Floyd, Prentice-Dunn, & Rogers, 2000). PMT is based on fear appeals and how they influence individual's behaviors (Rogers & Deckner, 1975). It has since been updated to include reward and self-efficacy factors (Rogers, 1983). This theory has environmental inputs and intrapersonal inputs, which then go through the cognitive mediating processes, evaluating a maladaptive response (threat appraisal) and adaptive response (coping appraisal). With the addition of fear, the threat appraisal and coping appraisal determine the protection motivation. Based on that protection motivation, the user will then decide to perform a maladaptive response (not to protect their system) or an adaptive response (self-protection) (Floyd, Prentice-Dunn, & Rogers, 2000).

Hanus and Wu (2016) conducted a study focused on home users (students) to determine the impact of users' security awareness on desktop security behavior, viewed through a PMT lens. In their survey, they measured threat awareness, countermeasure awareness, perceived severity, perceived vulnerability, self-efficacy, response efficacy, response cost, and desktop security behavior and analyzed the results using partial least squares structural equation modeling (PLS-SEM). Threat awareness was expected to effect perceived severity and vulnerability, while countermeasure awareness was expected to effect self-efficacy, response efficacy, and response cost (Hanus & Wu, 2016). Countermeasure awareness items were Likert scale questions in which users self-reported their familiarity with installing system updates, antivirus software, firewalls, and data backup. Self-efficacy, perceived severity, perceived vulnerability, response cost, and response efficacy were both independent and dependent variables. The path coefficient for countermeasure awareness to self-efficacy was 0.487 and for

self-efficacy to desktop security behavior was 0.522, with desktop security behavior having an R^2 value of 0.461 (Hanus & Wu, 2016).

Torten, Reaiche, & Boyle (2018) used the constructs from Hanus & Wu (2016) to study information security professionals, instead of students, using the same model. Their analysis was performed with partial least squares path modeling (PLS-PM). Countermeasure awareness still had a significant large effect on self-efficacy, while the R^2 for self-efficacy increased to 0.317. The overall R^2 value for desktop security behavior increased to 0.619 (Torten, Reaiche, & Boyle, 2018).

Woon, Tan, and Low (2005) studied home wireless security in the context of PMT. They measured knowledge through a quiz and then measured perceived vulnerability, perceived severity, response efficacy, self-efficacy, and response cost. Their study showed a high correlation between knowledge and self-efficacy. Self-efficacy had the highest effect on recommended behavior.

Anderson & Agarwal (2010) proposed the Individual Security Motivation Model, which is based in PMT and proposes that there is a difference between intentions to protect one's own computer and the Internet as a whole. In the paper Anderson & Agarwal briefly discuss that there are similarities to the theory of planned behavior and the theory of reasoned action (Anderson & Agarwal, 2010). The first study tested the effect of security behavior self-efficacy on attitude toward security-related behavior, resulting in a path coefficient of 0.32. Attitude toward security-related behavior had a significant relationship to both intentions to perform security-related behavior to protect the Internet and separately to protect one's own computer. The effect on intentions to perform security-related behavior (one's own computer) was far stronger (0.61)

than the effect on intentions to perform security-related behavior (Internet) (0.15) (Anderson & Agarwal, 2010).

Egelman and Peer (2015a) based the Security Behavior Intentions Scale (SeBIS) primarily on PMT. To develop the scale, they determined best practices and had users rate their agreement with statements. The final four constructs were device securement, password generation, proactive awareness, and updating (Egelman & Peer, 2015). In a follow-up experiment, Egelman & Peer (2015b) measured the Big Five personality traits and their effects on privacy preferences and behaviors, then measured decision-making psychometrics against privacy preferences and behaviors. Decision-making psychometrics generated a higher R^2, with awareness having the highest R^2 of 0.27 (Egelman & Peer, 2015).

Egelman & Peer's (2015a, 2015b) SeBIS scale was used to test the variance in cyber security behavior intentions based on demographics, personality traits, risk-taking preferences, and decision-making styles. Gender had a significant effect in passwords, awareness, and updating, while age and role had no effect (Gratian, Bandi, Cukier, Dykstra, & Ginther, 2018). Race, education, and household income were not evaluated.

Jansen & van Schaik (2018) used a modified PMT to study precautionary online behavior in an online banking context. Analyzing the results using partial least squares path modeling (PLS-PM), response efficacy, self-efficacy, and locus of control had the highest effect on precautionary online behavior. Precautionary online behavior had an R^2 of 0.66 with locus of control having a path coefficient of 0.15 and self-efficacy having a path coefficient of 0.26 (Jansen & van Schaik, 2018).

Tsai et al. (2016) studied security intentions from a PMT perspective. Using multiple regression to analyze three models, their respective adjusted R^2 values were 0.29, 0.433, and

0.432. Self-efficacy had a slight positive B value in the first model (0.06), but a stronger negative B value in the second and third models (-0.10) (Tsai, et al., 2016).

2.2.1 Fear Appeals Model

Specifically, in the cybersecurity space, a fear appeals model (FAM) based on PMT has been proposed which focuses on autonomous users in a decentralized IT environment, a closer approximation to home users. Fear appeals are designed to express a threat, then provide mitigation instructions and their value to the user (Johnston & Warkentin, 2010). For example, for a home user, they could be warned about phishing attempts, then provided with a lesson on how to identify phishing attempts, and an explanation of how not falling victim could prevent their computer being compromised or their bank account being emptied.

FAM measures perceived threat severity and perceived threat susceptibility, which in turn influence response efficacy and self-efficacy. According to the model, social influence is unrelated to threat severity, susceptibility, response efficacy, and self-efficacy, but influences behavioral intent. In the Johnson & Warkentin (2010) study, response efficacy and self-efficacy significantly influence behavioral intent. Social influence had no statistically significant relationship with behavioral intent or the other variables (Johnston & Warkentin, 2010). The result of experimental testing showed an R^2 of 0.271 and that the correlation of perceived threat susceptibility and response efficacy and self-efficacy (0.187) were statistically significant (Johnston & Warkentin, 2010). The study from which the self-efficacy questions were adapted, was a health study, which measured self-efficacy as ability, ease, and convenience to perform a prevention task (Witte, Cameron, McKeon, & Berkowitz, 1996).

2.2.2 Health Belief Model

The Health Belief Model (HBM) is derived from PMT and the Expectancy-Value theory, and was used to measure user security behaviors starting in 2009 (Ng, Kankanhalli, & Xu, 2009). In their study, Ng et al. (2009) studied how Perceived Susceptibility, Perceived Benefits, Perceived Barriers, Cues to Action, General Security Orientation, Self-Efficacy, Perceived Severity effected Computer Security Behavior. Unlike the Johnston and Warkentin (2009) study, there was no social element.

Williams, Wynn, Madupalli, Karahanna, & Duncan (2014) developed the Security Belief Model, which was an adapted Health Belief Model specifically geared toward information systems. In the study, years of computer experience, years of total experience, work in IT department, use PC regularly at work, have internet access at work, and position were used to measure computer experience and work experience. Computer experience and work experience were control variables, as opposed to independent variables (Williams, Wynn, Madupalli, Karahanna, & Duncan, 2014). The model explained 43% of variance in security behavior intentions, but self-efficacy was not statistically significant.

Another study using HBM evaluated the effect of Perceived Vulnerability, Perceived Severity, Perceived Benefits, Perceived Barriers, Self-Efficacy, and Cues to Action on Computer Security Usage with Age, Gender, Education, and Prior Experience as moderating variables (Claar & Johnson, 2012). Prior Experience measured frequency, recency, and severity of a computer security problem. Through multiple regression, the relationship of vulnerability, barriers, and self-efficacy to computer security usage were found to be significant. The authors used two different models, with the first having an R^2 of 0.14 and the second an R^2 of 0.304.

More recently, an HBM study targeted farmers and those in the agriculture business to evaluate the effect of perceived susceptibility, perceived severity, perceived benefits, self-

efficacy, and cues to action on cyber security behavior, with gender, age, and education as moderating variables (Geil, Sagers, Spaulding, & Wolf, 2018). This differed from the Claar & Johnston (2012) study in that it did not use prior experience as a variable, although it did have items that measured whether respondents were affected by a computer security incident and the recency of the event. Barriers, benefits, and self-efficacy were the most influential variables.

White (2015), in studying the effect of education and prevention on security for home computers, showed that education increases preventative behavior. The study also attempted to quantify prior experience, but in this case, that meant prior experience with security incidents, not prior IT or security-related experience. However, the education level of the participants and their exposure to security education had a positive effect on security behaviors (White G. L., 2015). In an updated study, computer security education was added as a moderating variable on the effect of protective behavior (White, Ekin, & Visinescu, 2017).

Anwar et al. (2017) studied gender differences in cybersecurity behavior. Additionally, their model added computer skills and experience with cyber security practice to their model and determined that there were significant differences between the genders in five variables: computer skill, prior experience, cues to action, security self-efficacy, and self reported cyber security behavior (Anwar, et al., 2017).

2.2.3 Threat Control Model

The threat control model addresses locus of control and self-efficacy in predicting a user's security behaviors (Workman, Bommer, & Straub, 2008). In a factor analysis of the model, self-efficacy, response efficacy, and locus of control were the top three influences on user security intentions. Locus of control had a large, significant negative effect on omissive

behavior: subjective, while self-efficacy had a significant negative effect on subjective omissive behavior and objective omissive behavior.

2.3 Theory of Reasoned Action

According to the theory of reasoned action (Fishbein & Azjen, 1975), our behaviors are influenced by attitudes and subjective norms. Attitudes are comprised of evaluation and strength of a belief, while subjective norms are comprised of normative beliefs and motivation to comply. One critique of the theory of reasoned action is that its predictive power sharply decreases in situations where additional information, resources, or experience are required to complete the behavior (Sheppard, Hartwick, & Warshaw, 1988). Measuring past performance to determine user education and comfort with technology and security is intended to fill this gap.

2.3.1 Theory of Planned Behavior

The theory of planned behavior is situation dependent and examines environmental effects on perceived behavioral control (Ajzen, 1991). Attitude toward the behavior, subjective norm, and perceived behavioral control are inputs to the intention to perform a behavior and the actual behavior is the output (Ajzen, 1991). Subjective norms and perceived behavioral control consider external influence, in the case of subjective norms, and environmental factors, such as availability of a career path, are included in perceived behavioral control. While an individual may feel strongly that they control their fate overall, they may also believe that they cannot complete a behavior due to other limitations. For example, five years ago, a female military member may have had significant tactical proficiency and been in excellent physical shape, but felt that she would never complete Ranger school, due to gender restrictions preventing attendance.

The theory of planned behavior has a strong basis in Bandura's self-efficacy theory and attempts to predict behavior from participant intention and perceived behavioral control (Ajzen, 1991). Within the theory of planned behavior, the term perceived behavioral control is based on Bandura's self-efficacy construct. The word confident was used synonymously with perception of self-efficacy, asserting that if intentions remained constant, a person confident that they can master an activity would be more likely to persevere (Ajzen, 1991). Ajzen (1991) acknowledges that perceived behavioral control alone may not be enough if the individual lacks sufficient information about the behavior.

2.3.2 Technology Adoption Model

Taylor & Todd (1995) used an augmented TAM to evaluate the role of past experience in behavioral intention. In their study, perceived behavioral control, of which past experience is a component, had a path coefficient to behavioral intention of 0.50 for experienced users compared to 0.16 for inexperienced users (Taylor & Todd, 1995).

In a study of IoT users, that was focused on security deBoer et al. (2019) found that past performance influenced IoT usage. With use as the dependent variable, six moderating variables, and one dependent variable, their model was able to explain 18% of variance in IoT use. Their past performance equivalent, was a construct labeled IoT skills, which included mobile skills, information navigation skills, social skills, and creative skills, and had path coefficient of 0.38 to perceived ease of use and 0.21 to perceived usefulness. The effect of IoT skills on use was not directly tested.

2.3.3 Technology Threat Avoidance Theory

Liang and Xue (2009) proposed that technology adoption and threat avoidance are two separate phenomena, with technology adoption unable to fully explain user threat avoidance

behaviors. Their theory is based on cybernetic theory (Weiner, 1948), which posits that human behavior is self-regulated through feedback loops (Carver & Scheier, 1982). The technology threat avoidance theory (TTAT) is based on the positive feedback loop, whereas the technology adoption model is based on the negative feedback loop. When malicious software is introduced, the user will perform a threat appraisal, determining impacts of infection, and coping appraisal, which either focuses on solving the problem or changing the user's perspective of the problem (Liang & Xue, 2009). In the threat appraisal context, self-efficacy is referred to as "confidence in taking the safeguarding measure" and influences user perceptions of the overall efficacy of protective measures (Liang & Xue, Avoidance of Information Technology Threats: A Theoretical Perspective, 2009). When empirically tested, perceived self-efficacy had a significant relationship to avoidance motivation (Liang & Xue, 2010).

Chen & Liang (2019) expanded TTAT with the addition of wishful thinking to extend TTAT. The study focused on coping behavior and included wishful thinking as a moderating variable. Self-efficacy was an independent variable, with perceived avoidability as the dependent variable. Self-efficacy explained 25% of the variance in perceived avoidability, had a negative relationship with perceived threat, a positive relationship with avoidance motivation, and a statistically insignificant relationship to wishful thinking (Chen & Liang, 2019).

2.4 Knowledge Theories

The knowledge, attitude and behavior (KAB) model, also known as Information Security Awareness (ISA) was developed as a global model to evaluate a user's awareness in particular regions, their attitude toward security, and their self-reported security behaviors (Kruger & Kearney, 2006).

Parsons, McCormac, Butavicius, Pattinson, & Jerram (2014), developed the hypothesis that as users' domain specific knowledge increases, their attitude toward information security should also increase, which in turn should generate more risk-averse security behavior. The Human Aspects of Information Security Questionnaire (HAIS-Q) was designed to measure password management, email use, internet use, social networking site use, mobile computing, information handling, and incident reporting (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014). Survey responses were analyzed using multiple regression and a significant relationship was found between knowledge of policy and procedures, attitude towards policy and procedures, and self-reported behavior.

Whitty, Doodson, Creese, & Hodges (2015) focused on the effect of cyber security knowledge, age, locus of control, self-monitoring, lack of premeditation, urgency, sensation seeking, and lack of perseverance on password sharing. Participants rated their own knowledge on a five-point Likert scale "very unknowledgeable" to "very knowledgeable", with 91% rating themselves as average or above (Whitty, Doodson, Creese, & Hodges, 2015). Age, self-monitoring, and lack of perseverance were the only statistically significant predictors. However, cyber security knowledge had the highest *B* despite not being statistically significant.

While not based in theory, Cain, Edwards, & Still (2018) conducted a cyber hygiene study evaluating the effect of knowledge on cyber hygiene behaviors. In their paper, they argue that self-report is a valid measure for the subject area. However, with technical measures, a user may think that they have performed the task sufficiently and be incorrect, such as believing they have a secure password when they do not (Egelman, Harbach, & Peer, 2016). However, in both studies users were likely to report negative security behavior.

The cyber hygiene study was exploratory and attempted to collect more information on typical security behaviors, technology usage, and social media usage. Their analysis of age difference determined that the oldest age group had more secure behaviors, but that there was no difference in other age groups. They found no differences between groups between age and knowledge; gender and behaviors; having been attacked and knowledge; training and behavior; and training and knowledge, however there were significant differences between genders' knowledge. Additionally, self-proclaimed experts had less secure behaviors and less cyber hygiene knowledge (Cain, Edwards, & Still, 2018).

Continuing to evaluate differences in individual users, but still within an organizational context, Hadlington, Popovac, Janicke, Yevseyeva, & Jones (2019) added work locus of control to the evaluation of ISA. Work locus of control, work identity commitment, and reconsideration of work commitment were all entered into the hierarchical regression simultaneously. Work locus of control was the only significant predictor of the three and had a large negative effect on ISA scores at -39.6%. (Hadlington, Popovac, Janicke, Yevseyeva, & Jones, 2019). The study also explored the relationship between gender and HAIS-Q scores, with women scoring consistently higher, but with a small effect size.

While focused on cybersecurity professionals, Ben-Asher & Gonzalez (2015) evaluated the effect of domain specific knowledge on an intrusion detection task. Using skills evaluations for theoretical knowledge and a work history, including education, certification, and work time for practical knowledge, the team determined actual experience levels. There was no difference in performance among experts and novices and the two groups had similar levels of confidence in detecting an attack (Ben-Asher & Gonzalez, 2015).

Zimmerman & Renaud (2019) propose a shift from “human as problem” to “human as solution”, of which a pillar is to encourage learning and communicate and collaborate. Security awareness is an important aspect of this and employees are encouraged complete training in mixed groups across departments (Zimmerman & Renaud, 2019).

2.5 Combined Theories

The Unified Theory of Acceptance and Use of Technology (UTAUT) and UTAUT2 combined elements of TAM, TPB, and TRA to determine what had the most predictive power in order to be retained in the model (Venkatesh, Speier, & Morris, 2002).

Theory of planned behavior and threat control model were combined with organizational narcissism to determine what factors influence organizational users’ risky security behaviors (Cox, 2012). Locus of control and self-efficacy were combined into Perceived Behavioral Control. Attitude toward behavior and subjective norms were evaluated for their effect on intended behavior, while perceived behavioral control was evaluated for its effect on intended behavior and actual behavior. Perceived self-efficacy had a high loading, while locus of control had a low loading (Cox, 2012).

Herath et al. (2014) proposed combining PMT, TTAT, and TAM into a single model and examined implementation of email security services with that model. The experiment tested risk perception, email screening self-efficacy, adoption intention, and attitude (usefulness, ease of use, responsiveness, and privacy concern). In that study, perception of self-efficacy influenced the intention to adopt eAuth, an email security authentication service (Herath, et al., 2014). Email screening self-efficacy had a small significant effect on intention to adopt the software, with all of the independent variables explaining 31% of the total variance in intention to adopt.

Goal achievement (Batra & Ahtola, 1991) includes two categories: hedonic goals and utilitarian goals. Hedonic goals are achieved through enjoyment of using the device, software, or security measures, while utilitarian goals are achieved by the outcome of the use of the device, software or security measures (Batra & Ahtola, 1991). These measures of efficacy have been combined to attempt to measure how a user will perceive the usefulness of a product, to include applications for home users (Jang J. , Shin, Aum, Kim, & Kim, 2016), which combined locus of control with goal achievement theory.

In information science, experiential locus of control has been divided into hedonic goals, utilitarian goals, and autonomy (Jang J. , Shin, Aum, Kim, & Kim, 2016). Hedonic goals refer to the internal motivation of users to enjoy their experience, while utilitarian motivation aligns with external motivation for functionality and ability to use the software or device. Autonomy has been explained as both system and user autonomy, with the authors hypothesizing that lower user autonomy positively affects the user's external locus of control (Jang J. , Shin, Aum, Kim, & Kim, 2016). This study has experiential locus of control as the dependent variable, with variables comprising hedonic goals and utilitarian goals.

2.6 Usable Security, Mental Models, and the Internet of Things

Challenges with securing Internet of Things devices are managing multiple devices, safety, understanding interaction between devices, lack of manufacturer support, and home user configuration of devices (Fu, et al., 2017). While most of the IoT literature attempts to solve the technical problems, this white paper offers suggestions for improving home user understanding and ability to manage their own security configurations, while also providing recommendations for manufacturers to make their devices easier for home users to control and configure.

End users have a very different understanding of how IoT devices function and communicate with each other, thus making it more difficult for them to understand how to secure those same devices (Zeng, Mare, & Roesner, 2017). Their research focused on how users interact with their smart homes, their technology mental models, their threat mental models, mitigation strategies, multi-user interactions, and other concerns. The most important lesson from this research is the effect that user mental models have on their threat models and security behaviors (Zeng, Mare, & Roesner, 2017). By not understanding how security works, users tend to make bad decisions based on erroneous assumptions (Wash, 2010). In his study, Wash (2010) compared best practices with users' mental models of viruses and hackers. None of the participants in the study could conceive of a botnet only wanting to use the computing power of their device to attack another computer, but that has become far more common.

More recently, there was a study focused on a new 6 item scale for measuring end user security attitudes, meant to extend SeBIS (Faklaris, Dabbish, & Hong, 2019). The 6 items are device-neutral and use general language to measure security, such as "I seek out opportunities to learn about security measures that are relevant to me (Faklaris, Dabbish, & Hong, 2019)." The generality allows it to be used for multiple environments, but may prevent the instrument from measuring the differences in technical ability based on platform.

Another recommendation from tangential research is for systems to be "understandable through study and observation (Rader & Slaker, 2017)." While the research was focused on folk models of sensor data collected, the lesson regarding user understandability of the data collected can be applied to all IoT devices, not just wearables. Smart home IoT devices provide little feedback to the user to allow them to understand how the device interacts with the Internet and home network, and what data is transmitted, stored remotely, or stored locally.

Using Discrete Choice Theory, Molin, Meeuwisse, Pieters & Chorus, (2018) studied the relationship between technical measures, perceived security, perceived usability, utility, and choice. Their experiment offered three different packages with varying levels of security measures and has users evaluate those packages for security, user-friendliness, and asks for their preference (Molin, Meeuwisse, Pieters, & Chorus, 2018). There was a small negative correlation of -0.143 between security and usability. One limitation of this study is that the security measures were evaluated as packages, rather than individual items. This does not evaluate whether users may tolerate higher security in some technical measures, but want lower security in others.

Dhillon, Oliveira, Susarapu, & Caldeira (2016), adapted value focused thinking, based on Keeney's (1992, 1999) work, to consider the relationship between information security and usability. The authors' began with interviews with users to determine their priorities. Starting with 150 items, measuring 24 constructs, their survey and factor analysis reduced the model to 24 items spanning 4 constructs. Of the initial items, only 12 items, measuring 2 constructs were included in their security-related survey . Maximize security & privacy spanned 8 items and maximize disaster recovery spanned 4 items. However, the final 4 constructs, maximize ease of use, enhance system related communication, maximize standardization and integration, and maximize system capability, are not directly security constructs (Dhillon, Oliveira, Sasrapu, & Caldeira, 2016). The study does not provide specific data on the loadings or correlations of the two security-related constructs.

Egelman, Harbach, & Peer (2016) combined survey feedback with an examination of the relationship between self-reported security behaviors and actual security behaviors. For awareness, participants were asked to identify a phishing website, of which 3.1% were

successful. For securement, they attempted to crack user passwords, with an 85.3% success rate. For updating, users participated in a survey in which they provided their user-agent string from a Mac. Lastly, to test securement, Android phone users were tested to see if they used a PIN, pattern, or slide to unlock (Egelman, Harbach, & Peer, 2016).

Emerging IoT research focuses heavily on providing security for both organizational and home contexts, but are focused on the technological aspects of security and/or privacy. Guomopoulos & Mavrommarti (2020) are testing a framework for pervasive computing applications designed to allow users to configure their smart environments. Using the end user development framework to amalgamate commercially available devices, they focused on user mental models of construction to develop a smart environment. TAM3 was the theoretical background, which evaluates computer self-efficacy. Interestingly, this study evaluated locus of control with external locus of control treated as a positive attribute, through measuring whether the user felt they had enough technical support to complete the task (Goumopoulos & Mavrommati, 2020).

Hochleitner et al. (2012) focused on understandable and usable interfaces, with concern for "psychological acceptability" in security feedback mechanisms. In order to make it easier for the user to perform tasks, they wanted the interface to match user mental models, as well as to provide feedback from the system to the user (Hochleitner, Graf, Unger, & Tscheligi, 2012).

Technical researchers are focusing on defining the attack surface of IoT (Rizvi, Orr, Cox, Ashokkumar, & Rizvi, 2020), technical vulnerabilities (Butun, Osterberg, & Song, 2019; Jurcut, Ranaweera, & Xu, 2020; Yang, Wu, Yin, & Zhao, 2017), and defining a new four layer hierarchical information security model specific to IoT (Yin, Fang, Gou, Sun, & Tian, 2020).

Outside of the scope of this document, but deserving of a brief mention, are research studies concerning IoT privacy. IoT privacy scholars are exploring co-designing smart home privacy mechanisms (Yao, Basdeo, Kaushik, & Wang, 2019), making the user a part of the process instead of designing a system then testing it on the user later, and designing privacy-aware internet of things applications (Perera, et al., 2020) within the construct of a privacy by design framework. One study monitored traffic within 3 residences to determine what private data was being transmitted and where, surprising the European residents with the amount of data that was transported outside of the GDPR area (Seymour, Kraemer, Bims, & van Kleek, 2020).

In an empirical study, Hsu and Lin (2016), explored the determinants of IoT service adoption from a network externality perspective. The study developed its measurement instrument from some of the same literature included here, but study measured concern for information privacy, with security being relegated to the data recipient, not the user (Hsu & Lin, 2016). Kim, Park, and Choi (2017) studied the adoption of an IoT smart home service through the lens of the value-based adoption model. However, neither study had a security component and neither used locus of control, self-efficacy, or past performance.

Other researchers have used TAM and TPB to study the effect of privacy controls, among other variables, on intention to use IoT devices (Guhr, Werth, Blacha, & Brietner, 2020). Zheng et al. (2018) studied user perceptions of smart home privacy in an exploratory, qualitative study that examined the users' mental models of how their devices work, what data they collect, as well as their feeling about their data being exposed, privacy concerns, and whether they were willing to take additional steps to protect their privacy.

2.7 NOAH for IoT Framework (Excerpted from (Mitchell & Park, 2017))

"While there are organizations using IoT devices on their corporate networks, this version of the NOAH Framework is intended to focus on the household as the unit of measure. The larger NOAH Framework can address organizational uses of IoT devices and would have the same considerations, while a household deciding to implement IoT would have far different considerations within the same general framework categories.

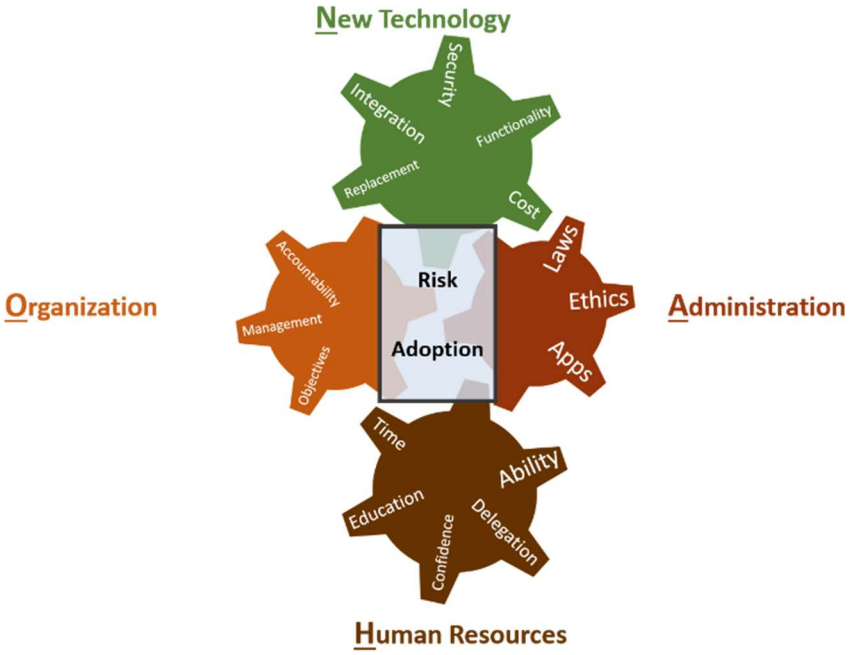

Figure 2 NOAH for IoT Framework

IoT devices give households the ability to run many aspects of their household remotely. When a household is considering IoT technologies, they must consider the purpose of their devices. The household may need something to make it look like they are home due to frequent travel, remote control of thermostat settings due to an irregular schedule, or monitoring of the home to prevent burglary. Whatever the purpose, incorporating IoT in the home should be a planned process in order to establish a secure and reliable computing environment.

A simple example case would be that of a traveler who wants to make it appear that someone is home. They have very little background in IT and want a simple deterrent. The user wants to make the lights turn off and on at random times.

Most IoT devices are designed to work out of the box, with little to no intervention from the user. However, management typically involves downloading an app or going to a website and using an account to manage the devices remotely. In a short period of time, a user with little to no IT experience can get their devices online and meeting their household needs. This functionality is important, as users are less likely to adopt technology if it is difficult or time-consuming to configure it (Rogers E. , 1999). In our example scenario, the user has very little IT background, so difficult installation or multiple or complicated applications will not work for this user.

Another concern within functionality are vigilante acts, such as "bricking" IoT devices, which will eliminate the functionality of a given device (Laliberte, 2019). The malicious software (malware) does not discriminate based on the device's function, so if a healthcare IoT or industrial IoT device is rendered unusable, it may have grave consequences. A pacemaker or insulin pump becoming inoperative can kill the device's users, while industrial IoT devices that no longer function could cause power outages or water system failures. For ordinary consumer devices, if it happened soon after being connected to the network, the consumer may be able to return it for a refund, otherwise, they would have no recourse. Even if they were able to determine the source of the software and the person behind it lives in the United States, the dollar value of an IoT device would not likely be enough for law enforcement to intervene. While the creator of the BrickerBot malware pledged to discontinue the vigilante campaign in December

2017 (Mathews, 2017), Silex malware emerged in 2019 performing a similar function (Cimpanu, 2019).

IoT devices ship with default administrator usernames and passwords, a vulnerability exploited by Mirai botnet software. Attackers used IoT devices to perform DDoS attacks on many websites and Dyn, the company that handles domain name system (DNS) resolution for servers hosted on the East Coast. The largest attack made Twitter, Netflix, and other websites unavailable (Woolf, 2016). After the release of the source code, subsequent variants have been observed targeting Enterprise IoT devices (Nigam, 2019). Depending on the device, there are various security options, but a review of Nest thermostat installation, welcome, and set-up guides, offers no information on how to securely configure your device (Nest, n.d.). Security is only discussed is in the set-up guide in the context of knowing the Wi-Fi password. When establishing a Nest account, it does require a moderately strong password (minimum of eight characters with at least one each upper case, lower case, and special characters). Meanwhile, older Foscam IP cameras phone home to the company and other cameras, even when peer to peer (P2P) traffic is turned off in configuration settings (Krebs, 2016). Whether this is due to insecure coding practices or something more malicious, it highlights the lack of transparency by IoT manufacturers concerning their products.

The example user would need to evaluate whether the firmware can be updated, if the manufacturer offers technical support, whether the device or manufacturer have had past security breaches, if directions are provided for a secure installation, and whether there are analog options, such as light timers, that can meet the user's needs.

IoT devices are highly proprietary, making integration into a home network difficult unless a user only purchases a single brand. Otherwise, each brand has a different app to manage their devices (App My Home, n.d.). However, Amazon's Alexa works with most newer IoT devices, allowing voice control of various IoT devices in the home. While present in the home, a user can centrally manage their devices, but when not physically present must use the Amazon app, if they have iOS, or a third-party workaround for Android (Lloyd, 2017). The example user would need to evaluate which devices appeal to them and what accessories may be required for each device.

The cost of IoT devices limits the population that will utilize them, as well as the number and type of devices an individual will use. Ranging from approximately thirty to fifty dollars for smart lightbulbs and outlets to hundreds of dollars for thermostats and locks to thousands for a smart refrigerator, they are expensive to introduce and require dedicated Internet access in the home to function as intended (Home Depot, n.d.). Anyone who tethers Internet service through their cell phone provider can only utilize IoT devices when their mobile device is present and receiving service in the home. There are hidden costs that must be considered, such as the cost of mitigations, the value of the user's time, and the difference in cost between any analog options and the IoT option.

Like all other technology, IoT devices will need to be replaced. Given the lack of maturity in the IoT market, it is unclear how long these devices will last and what will trigger a need for replacement for a user. Some manufacturers claim that smart lightbulbs can last up to 22.8 years, based on 3 hours of use per day. (Home Depot, n.d.) Based on their lifetime calculations, the lightbulb lasts 24,983 hours. Even if left on continuously, the lightbulb should last 2.85 years. Some devices have upgradeable firmware, but many others do not. If a device is

determined to be a security risk, a user must decide whether to replace it immediately or accept risk and wait until it no longer functions. Users must consider the maturity of the technology, as WiFi products will likely be supported long-term, while newer technologies, such as ZigBee may not.

Each household is a separate organization with its own mores and standards, so NOAH for IoT focuses on accountability from the IoT manufacturers themselves. Many of the lower cost products on the market are unsupported. The manufacturers make them, but provide little in the way of support or software updates, leaving a user vulnerable to attackers. Devices are still proprietary with no standards for use of ports, configurations, user-adjustable attributes, maintenance, support, or responsibility when there is a vulnerability.

Management of IoT devices in the household has an added layer of complication in that many of those who would procure, install, and maintain the equipment are not trained in information technology and even more do not fully understand cybersecurity. The management of devices is further complicated by the need for multiple applications, as mentioned in the New Technology section.

Each household may also have different objectives. Some may want to use smart devices for security purposes, such as monitoring the home while away, making it appear that someone is there. Others may want smart devices to reduce energy consumption, allowing for monitoring and managing of ambient temperature and device energy utilization. Yet another group may want smart devices for convenience sake, with learning devices adjusting to their schedules and smart refrigerators providing them with a grocery list. Another possible audience would be those with disabilities who use smart devices to allow for independent living. Each household should

evaluate their needs and wants before installing a slew of smart devices that introduce vulnerabilities into their home network. In other words, just because something can be automated and connected to the Internet doesn't mean it should be.

The United States has a complicated patchwork of federal, state, and local laws. With the rise of telecommunications then Internet, geographical boundaries have been blurred. In 2018, the General Data Protection Regulation took effect in the European Union (Official Journal of the European Union, 2016). Some IoT devices are constantly listening and logging users' behaviors, which raises several legal issues. Companies have navigated the legal system to protect themselves, although there are current challenges to a company's duty to provide information on their users. So far, there has been no legal precedent to determine whether a host is required to notify guests that they have IoT devices in their home and that those devices may possibly record their image or audio. There has also been no precedent to determine what data a host can collect from visitors to their network or what responsibility they may have if their network has been hacked and a visitor's data is compromised. However, there has been legal precedent allowing a company to be held liable for its product being used to commit privacy violations. (Sieniuc, 2016)

Ethical standards vary by region, religion, and any other number of factors. However, IoT does not have any clear ethical boundaries yet. Nanny cams have become popular to watch visitors to a home without their knowledge. There should be clear limitations to device placement (no bathrooms, private changing areas, etc.), as well as a duty to warn to allow individuals to opt out of entering a home with cameras. With the existing insecurity of IoT devices, there are questions relating to a homeowner's liability, legally and morally, if their in-home cameras were used to monitor another individual for nefarious purposes, such as stalking

or finding someone in witness protection. The vigilante botnets present further ethical concerns. While the individuals responsible may feel they are serving the greater good by diminishing the devices available to attackers, those same attackers could seize their botnet. BrickerBot prevents the devices from working again, even with a factory reset, depriving an end user of the use of their personal property.

Using another definition of administration, there are considerations for who will be managing the various hardware and software within the home. Typically, younger users are expected to be the IT savvy members of a household, but parents may want to monitor the same individuals who are likely to have the most ability to install and configure these devices. Depending on the number of different types of devices and different brands, a single household may be juggling multiple applications, hubs, and interface devices. The more complex the system is, the more difficult it will be for a household to manage installation, configuration, and security for the system.

In this context, human resources refers primarily to whomever manages and uses the system. In a household, there may also be users who are non-participants in using the devices, such as small children and those who choose not to use them. While they are still affected by the choices that the users and administrators of the devices make, they do not fit within the Human Resources context of the framework; their issues are considered in the Administration portion of the framework.

The first component of human resources is time. Time to set the devices up can be a predictive measure of how securely the system will be configured. The longer it takes to configure it, the less likely a user will securely configure it.

The technical education level of the person responsible for the installation will influence the security of the configuration. Users with higher levels of technical education will be more likely to attempt to securely configure their devices. Technical education includes, but is not limited to, online programming classes, learning to program, hands-on time with various hardware and software, structured degree programs, and professional certification courses.

A user's confidence in their technical skills may also be a deciding factor. Even those who have technical education may not feel comfortable with what they learned or may have academic knowledge, but not hands-on knowledge of how to configure devices. Those with more confidence are more likely to continue to work on their configuration and make it more secure.

Delegation refers to the ability of multiple users in the household to control the devices. Some devices allow for multiple user accounts to manage the same devices, which is a more secure installation, while others link devices to a single account, requiring the household to share passwords. Given a user's propensity to re-use passwords, requiring devices to be linked to a single account, will make the primary account holder vulnerable to other household members having access to their other accounts.

Risk overlaps all areas of the framework. From a New Technology standpoint, every device introduces its own risks, which are difficult for a user to evaluate. Manufacturers do not publish the ports their devices communicate on, what information is locally stored, and what information traverses the router. The user manuals also do not provide information on possible risks or ways to reduce them. From an organization standpoint, the interaction of the devices with each other and with any required hubs adds to the level of risk within the system. As entropy increases, management becomes more difficult and users seek ways to simplify how they

manage their devices. From an administration standpoint, there may be some liability on the part of the device owner should their devices cause harm to someone else. The new Amazon Echo Look, has a camera that will use machine learning to increase their ability to personalize your experience (Barrett, 2017). Based on their stated use case, taking pictures of you to determine your best outfit option, the device will likely be in a bedroom. If that camera, or any others, are insecure and a third-party posts nudes of a visitor to the home, the owner of the insecure network may be liable for the damages if the visitor did not consent to being recorded. Lastly, the operator of the network introduces risk and non-participant members of the household are subject to risk. A child with an Internet-connected baby monitor may be at risk of being verbally abused by a complete stranger (Owens, 2016).

Adoption is another area that overlaps the four main components of NOAH for IoT. As technology changes on a near constant basis, there is always a question of when to adopt and commit to purchasing a device. The decision-maker must weigh several factors to determine when and what to adopt. While one decision-maker may choose devices that don't require a hub, another may already have a hub and adopt only devices that work with it. Administratively, the decision-maker must decide how they are going to use the technology to determine if it is worth adopting. Lastly, the installer will have to determine if they are able to install those devices. If they do not have the technological acumen to install them, the household will be unable to adopt the selected devices. (Mitchell & Park, 2017)"

2.9 Related Work Summary

While the concepts of locus of control and self-efficacy in information security are mature and present in many theories, they have not been consistent, in their significance or

direction. In most models listed above, they are studied in the context of threats (vulnerability, susceptibility, and/or severity) and other external factors, including benefits, costs, barriers, cues to action, and social influence. The interaction effects of these other elements may be the reason for the contradictory findings among studies.

The human factors empirical studies in this section have almost exclusively focused on traditional computing, with the exception of Cain, Edwards, & Still (2019). The IoT empirical studies have focused on technical measures, instead of human factors, except for Goumopoulos & Mavrommati (2020), who focused on end user development for IoT usage, not security.

Twenty-nine human factors empirical studies were evaluated, with eighteen focusing on individual users and eleven focusing on organizational users. They had two to nineteen independent variables and one to eight dependent variables. The adjusted R^2 range for the computer security or use dependent variable was from 0.045 to 0.777. Interestingly, the model with the fewest variables, two independent and one dependent, had the highest R^2 at 0.777. The analysis methods used in those studies were Partial Least Squares (Path Modeling and Structural Equation Modeling), regression, ANOVA, correlation, and means and t-tests. Fifteen of the studies evaluated self-efficacy with coefficients ranging from -0.29 to 0.565 and two that were not significant. Five studies included locus of control with coefficients from -0.990 to 0.15 and one not significant result. Past performance was included in ten studies, with a coefficient range of 0.185 to 0.603 on security intentions and a 0.487 to 0.563 range of effect on self-efficacy with three not significant results. Rhee, Kim, and Ryu's (2009) study tested an approximation of all three variables in my research, but their past performance approximation measured computer experience and was not detailed or security specific. Additionally, the studies tested existing

intentions and behaviors, but none of them tested future changes that respondents intended to make.

Most of the recent IoT scholarship is focused on technical solutions for privacy and security. While technical solutions are important, the complexity of securing disparate brands in a rapidly evolving space with little supply chain control, makes a single solution difficult to achieve. My research focuses on human factors that can be leveraged to motivate users to secure their devices and networks with existing, available technologies. This research focuses on why home users make the security choices they do, while the majority of the most recent research focuses on how to secure IoT.

The role of past performance in user security behaviors is less mature, but that may be explained by it being known by different variable names, including past experience and knowledge. Given the dearth of secure IoT configuration information available on the Internet or in manufacturer documentation, users may not have the enough knowledge or information to perform the security behaviors they intend to. IoT courses and certification programs are new, compared to traditional cyber security, and targeted toward IT security professionals (Cert Nexus, 2020). Cisco introduced IoT certification courses in 2015 (Cisco, 2015), but competitors have since developed their own IoT curricula (Wouk, 2019).

Locus of control appears in social learning theory, experiential locus of control, and threat control model. Psychological locus of control research focuses on locus of control as the dependent variable to determine what shapes the individual's internal or external locus of control, while much of the information systems research uses locus of control as an independent variable to explain users' actions.

In the information systems and security field, self-efficacy presents in various forms in theory of planned behavior, theory of reasoned action, protection motivation theory, fear appeals model, goal achievement, and the combined TAM and TTAT.

Past performance is a consideration in Expectancy-Value theory, while there are at least two studies attempting to quantify the role of education in security behaviors. Varying past performance measures appear as prior experience in the health belief model and security belief model, knowledge in the Knowledge Attitude Belief model, and countermeasure awareness in some versions of the protection motivation theory.

Security Intentions is known by many names throughout the various theories concerning information security, including security behavior intentions (Williams, Wynn, Madupalli, Karahanna, & Duncan, 2014), desktop security behavior, ISSP compliance behavioral intention (Infinedo, 2012), and avoidance behavior (Liang & Xue, Avoidance of Information Technology Threats: A Theoretical Perspective, 2009).

Kritzinger & von Solms (2010) proposed an E-Awareness model, which would force home users to participate in cyber awareness training before being allowed to get on the Internet. This would place the responsibility of information security on the ISP providing Internet access, rather than the user (Kritzinger & von Solms, 2010).

Due to the inconsistency of effect of locus of control and perceived self-efficacy, along with the limited study of past performance, this study will focus on the effect of locus of control, perceived self-efficacy, and past performance on home user security intentions. The models were decomposed, removing any other independent variables, such as threat avoidance, coping appraisal, cues to action, response efficacy, response cost, social influence, and benefits.

Chapter 3: Research Methodology

Chen and Liang (2019) used a series of vignettes to test users' responses to placing themselves in computer security scenarios. Respondents answered online survey questions to measure the variables perceived susceptibility, perceived severity, perceived effectiveness, perceived costs, self-efficacy, social influence, risk tolerance, wishful thinking, and avoidance motivation. Egelman, Harbach, & Peer (2016) conducted a series of surveys, but also independently verified security behaviors through password cracking and observing how users secured their mobile devices. For this exploratory survey, there was no independent verification of security behaviors, as related to security intentions, nor were there vignettes to place respondents into scenarios.

Linear regression (Woon, Tan, & Low, 2005; Ng, Kankanhalli, & Xu, 2009; Claar & Johnson, 2012; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014;Whitty, Doodson, Creese, & Hodges, 2015; Egelman & Peer, 2015; Tsai, et al., 2016; Geil, Sagers, Spaulding, & Wolf, 2017; Gratian, Bandi, Cukier, Dykstra, 2018; Hadlington, Popovac, Janicke, Yevseyeva, & Jones, 2019), Partial Least Squares Path Modeling (Workman, Bommer, & Straub, 2008; Rhee, Kim, & Ryu, 2009; Johnson & Warkentin, 2010; Cox, 2012; Chen & Liang, 2019; Hanus & Wu, 2016; Torten, Reaiche, & Boyle, 2018; Jansen & van Schaik, 2018), and Structural Equation Modeling (Bulgurcu, 2010; Infinedo, 2012; Hanus & Wu, 2016; deBoer et al., 2019) were used to analyze the resultant data in prior studies.

3.1 Research Design

This survey was designed to measure locus of control, past performance, self-efficacy, and security intentions in IoT home users over the age of 18. Past performance was designed to

consider general technical measures, such as information technology/computer science (IT/CS) education, as well as security specific measures, such as security certifications. Self-efficacy also measures both technical and security specific domains. Security intentions are the network and device protection measures participants self-report they are currently using, as well as those they intend to use in the future to improve their security. Age, ethnicity, gender, household income, and overall education level are control variables.

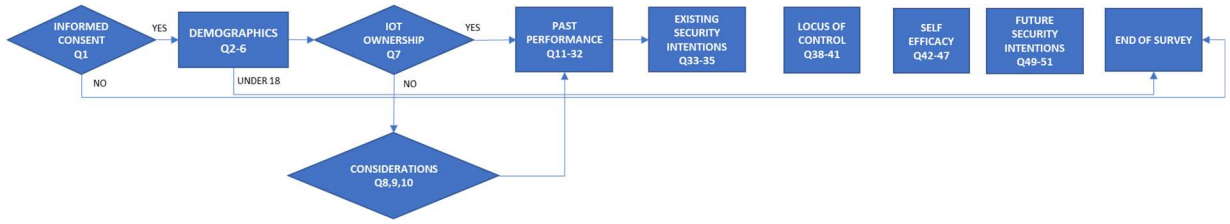

Figure 3 Survey Mechanics

3.2 Participants

Participants were recruited through Facebook, LinkedIn, and 2 email distribution lists, called listservers (listservs) for information management professionals, with the survey open February 22 through March 5, 2018. Those who received the initial invitation to participate were asked to pass on the link to their networks, which is a form of snowball sampling.

As a convenience sample, participants opted-in to participate and all who did so were included in the survey. The target audience were IoT device owners, but those who did not own IoT devices were asked follow-up questions to explore their reasoning for not owning them. There were 528 respondents through Facebook, 98 respondents through the listservs, and 13 respondents through LinkedIn, for a total of 639 respondents, 569 of whom completed the survey.

On Facebook the research plea was posted on my personal Facebook wall, where it had the potential to reach 557 friends, as well as multiple Facebook groups, ranging from hundreds to

thousands of members. Each of the groups in Table 1 have varying degrees of affinity and likelihood of participation in the survey. However, there is overlap between the various groups, as evidenced by my membership in all of them. For example, West Point Class of 2001 has a membership of 703, while all members of WPW (West Point Women) Class of 2001, with a membership of 103, are all eligible to be members of the broader West Point Class of 2001 group. Therefore, without completing a significant membership analysis, it is impossible to determine the actual reach of the research pleas posted.

Additionally, there was no method, at the time, in Facebook to track the number of views of a post. It is unclear how many of the various groups' membership saw the research plea. The algorithm Facebook uses to determine what each user sees on their timeline is not publicly available, therefore it is not possible to determine the possibility that any given member of any group would see the post on their own timeline. The Facebook groups and their membership numbers can be viewed in Table 1.

Facebook	
Group Name	Members
Personal Wall	557
African American Army Officers	9926
WPW Class of 2001	103
SVO at Syracuse University Social Group	83
West Point Class of 2001	703
West Point Forum	1338
West Point Women	3344
Veteran 2 Veteran Info	473751
Army Women Officers Mentorship	9874
Formation 22	25858
All About Leader Self Development	139
African American Female Army Officers	2069
West Point African American Women	269
Single Parent Army Officers	89
Women's Mentorship Network	2944
Army Signal Officer Network	1321
USMA Careers and Networking	10664
USMA DC '01 +/- 4	88
An Officer and a Mommy	335
The Officer's Club	3705
The Unarmed Forces	1117
Academy Women	860
Veterans 2 Federal Government Jobs	49721
West Point African American Army Officers	728
The Legacy of the Long Gray Line	2206
Total	601792

Table 1 Facebook groups where research pleas were posted

On LinkedIn, the research plea was posted to my personal profile, where it was expected to reach 577 individuals, many of whom are members of the cybersecurity community. The 53listserv is a community of current and former Army information systems managers, while the Functional Area (FA) 26B listserv is a listserv of current Army information systems managers only. There are hundreds of members on each listserv, with the 53listserv including those who have left the military to work in the defense industry, as well as corporate information technology. However, there is significant overlap between the 26B listserv and the 53listserv,

with the main difference being the exclusion of former Army information systems managers on the 26B listserv. Some of the members of the listservs are also in the Facebook groups listed above and are Facebook friends.

LinkedIn	
Group Name	Members
Contacts	577
Cyber Security Forum Initiative - CSFI	92176
Cyber Law and Information Security	11260
CuseConnect - Syracuse University Students/Alumni	15604
Global B2B Defence	19903
Syracuse University Alumni Network	39749
US Army	47495
Bronze Star Medal Recipients Association	11135
Georgia Tech Cybersecurity Leadership Program	37
Institute for National Security and Counterterrorism (INSCT)	906
Iraq War Veterans	31309
Joint Service Academy Network - New York Metro	800
Military Officers of the United States of America	15844
Ringknockers	5821
Service Academy Business Network	3436
Signal Corps Regimental Affiliation	2935
Syracuse University - School of Information Studies	4458
Syracuse University iSchool Information Management	271
US Military Tech and Comms	916
USMA Tech	1022
United States Military Academy (USMA) at West Point	3805
West Point Alumni Group	3761
West Point Association of Graduates LI Discussion Group	17162
West Point Class of 2001	395
West Point Women	875
Total	331652

Table 2 LinkedIn groups where research pleas were posted

Response rates are difficult to determine due to the nature of the sampling methodology. Facebook, LinkedIn, and the listservs do not provide information on who has seen the research plea, unless the people who viewed it choose to leave an attributable response, such as a reaction

(like, love, etc.), a comment, or chose to share it. To improve response rates, I shared the information publicly, allowing anyone on Facebook to view the research plea and allowing those in my friends list to share it without requiring additional interaction, such as commenting or sending a message. Because it is a snowball sample as well, it is difficult to view all shares, depending on the methodology the sharer uses. For example, on Facebook, the sharer can share through Facebook Messenger, where the share would no longer be traceable. Individuals may also copy and paste the link once they enter the survey and send it out from there, preventing tracing the number of potential participants who have seen the plea.

Traditional response rate calculations cannot be accurately applied in this scenario, as there is no way to measure the number of people who were exposed to the survey appeal. Users may not have read the email that was sent out over the two listservs, members of groups may not have read the appeal posted within those groups, and those who are linked to me on social media may not have received the appeal in their feeds.

Typically, snowball sampling is reserved for hard to reach populations, where you start with members of the population, who then provide contact information for others meeting the same criteria. The challenge with home users is that there is no central organization through which to arrange the survey. Traditional mail-in surveys are time-consuming and expensive, while not guaranteeing that those contacted are in the targeted audience of home users.

The LinkedIn response rate was low compared with that of Facebook and the two listservs. While a case can be made that LinkedIn is not used as much, that would likely not account for such a sharp drop in participants. Revisiting the post determined that instead of hyperlinking the survey in the preview window at the bottom of the post, the platform hyperlinked the syr.edu website from my email address. Anyone who clicked at the bottom of

the post, instead of clicking on the specific survey hyperlink in the main body of the post, was redirected to the syr.edu main page, from which there was no way to navigate to the survey, which was hosted on an entirely different website. While I received no feedback from users concerning this problem, I have many contacts that are on both LinkedIn and Facebook and I assume that those who are on both platforms chose to use the Facebook survey link instead.

3.3 Variables

The following charts show which questions tested each variable. Not every participant received each question, as some questions are situation dependent. For example, if a user responds "no" to question 11, asking if they have any formal education, they will not view questions 13, 14, 15, 16, or 19, which are designed to measure the amount and types of formal education they have. Some questions were also mutually exclusive, such as questions 49 and 50. Answering "yes" to question 48, concerning whether the user planned to make any changes to their security settings, directed the user to question 49, while answering "no" directed the user to question 50. Answers to question 50 were then used to determine why the respondent was not planning to make any security changes. Question 51 asked what IoT device changes the user planned to make, regardless of their answer to Question 48.

There were no users under 18, but the survey was designed to eliminate them if they answered under 18 to age range question. Those who did not own IoT devices provided demographic information, then were directed to alternate questions concerning their consideration of IoT devices and reasoning for not incorporating them into their home network. The alternate questions did not have any bearing on the measured variables, but were collected for exploratory purposes to determine the course of future research concerning non-adopters. The alternate questions are not included in the tables below that map survey questions to variables.

After the alternate questions, the non-IoT owners were then asked the rest of the survey questions.

Past Performance		
Item	Question Number(s)	Question
PP1	Q12,18	Informal IT Education
PP2	Q11,13,14,15,16,19	Formal IT Education
PP3	Q17	Job in IT/CS-related field/work on computers[1]
PP4	Q20	What kinds of devices are connected to the Internet in your home?
PP5	Q21	Approximately how many IoT devices do you have in your home? (Excludes computers and smartphones)
PP6	Q22	Do you own your router or is it provided by your Internet provider?: personally owned, Internet provider owned, other
PP7	Q23	Did you set up your router yourself?: yes, no
PP8	Q24	Have you logged in to the router provided by your Internet provider?: yes, no
PP9	Q25	Who set up your router?: someone else who resides in the home; commercial third party, i.e.. Geek Squad; No one, it worked out of the box; Other
PP10	Q26	Do you know how to log in to the Internet provider-owned router?
PP11	Q27	What do you do on the Internet?
PP12	Q28	Approximately how many online accounts do you have?
PP13	Q29	Approximately how many unique passwords do you have?
PP14	Q30	When using the Internet, do you: check for encryption when performing secure transactions, use strong passwords, use the same password on multiple sites, use a password vault, check the reputation of shopping sites, log out of secure sites when finished, close the browser when finished with a secure site?: always...never
PP15	Q31	When checking email, do you: open emails from people you don't know, open attachments from people you don't know, click on links in emails, use digital signatures/encryption, log out when finished, close the browser when finished?: always...never

Table 3 Past Performance Questions

The questions listed above in Table 3 are designed to determine the respondent's past performance. The questions attempt to determine technical and security ability in a meaningful way. Previous studies have attempted to quantify past performance as knowledge (Cain,

[1] Adapted from White, et al. (2017).

Edwards, & Still, 2018; Ben-Asher & Gonzalez, 2015; Whitty, Doodson, Creese, & Hodges, 2015; Hadlington, Popovac, Janicke, Yevseyeva, & Jones, 2019; Gratian, Bandi, Cukier, Dykstra, & Ginther, 2018) or prior experience (Taylor & Todd, 1995) with measurements such as length of computer experience or knowledge of specific security tasks. This study explored several different options for constitution of knowledge. Formal education measured high school and below classes, college classes, certifications, degrees, and recency of degrees or certificates. Informal education determined whether respondents learned from friends/relatives, looking up solutions to IT problems, reading books related to IT/CS, hands-on tinkering, self-taught programming, and an option to provide a free text "other" answer.

Locus of Control			
Item	Question	Measure	Adapted from:
LOC1	Q38	Keeping my home network safe is: beyond my control…within my control	Workman, et al. (2008), who adapted from Rotter (1971) and modified according to Harrington's (1996) guidelines
LOC2	Q39	I believe that it is within my control to protect myself from information security violations at home: disagree…agree	
LOC3	Q40	The primary responsibility for protecting my home network belongs to: my Internet provider…myself	
LOC4	Q41	Taking necessary security measures is entirely under my control: disagree…agree	Tsai, et al. (2016), but listed as a self-efficacy measure

Table 4 Locus of Control Questions

The locus of control questions in Figure 7 were adapted from Workman, et al. (2008) and Tsai, et al. (2016), as were the self-efficacy questions in Figure 8. The locus of control questions tested whether the respondents had an external or internal locus of control, with internal scoring highest on the Likert scale. The self-efficacy questions measured whether the respondents were confident in their ability to protect their home network, implement preventative security measures, and stop information security violations. Additionally, question 45 measured anxiety concerning online security issues.

Self-Efficacy			
Item	Question	Measure	Adapted from:
SEFF1	Q42	I feel comfortable taking measures to protect my home network: disagree…agree	Tsai, et al. (2016), who adapted from Anderson and Agarwal (2010)
SEFF2	Q43	I have the resources and the knowledge to protect my home network: disagree…agree	
SEFF3	Q44	Protecting my home network is: hard…easy	
SEFF4	Q45	I feel nervous when I think about online security issues: agree…disagree	
SEFF5	Q46	I have the skills to implement preventative measures to keep stop people damaging my home network: disagree…agree	Workman, et al. (2008), who adapted from Rotter (1971) and modified according to Compeau and Higgins (1995) guidelines
SEFF6	Q47	My skills to stop information security violations on my home network are: inadequate…adequate	

Table 5 Self-Efficacy Questions

Security intentions (existing) were measured by security software, network protection measures, and IoT device protection measures. Each question provided a list of potential security measures for its respective domain that were adapted from best practices (NSA, 2014; National Security Agency Information Assurance Division, 2015a; National Security Agency Information Assurance Division, 2015b).

Security Intentions (Existing)		
Item	Question	Measure
SINTEX1	Q33	Which of the following security software do you use?
SINTEX2	Q34	Which of the following network protection methods do you use?
SINTEX3	Q35	Which of the following IoT device protection measures do you use?

Table 6 Security Intentions (Existing) Questions

Security intentions (future) questions shown in Figure 10 were partially adapted from Tsai et al. (2016) and Liang & Xue (2010), with the remaining measures based on best practices (NSA, 2014; National Security Agency Information Assurance Division, 2015a; National Security Agency Information Assurance Division, 2015b).

Security Intentions (Future)			
Item	Question	Measure	Adapted from:
SINTF1	Q49	Thinking of your future actions, indicate the degree to which you agree or disagree with the following statements regarding your likelihood of implementing security measures to protect your home network.	Tsai, et al. (2016), who adapted from Anderson and Agarwal (2010), Liang and Xue (2010)
		1. I am likely to take security measures to protect the Internet.	
		2. I will upgrade my security measures to protect myself better online.	
		3. I will change my passwords more often.	
		4. I will use passwords that are harder to guess.	
		5. I will change my browser security settings to a higher level.	
		6. I will learn how to be more secure online.	
		7. I will keep guests and IoT devices on a separate guest network.	
		8. I will not use default passwords.	
		9. I will limit connections to my router by MAC address.	
		10. I will use WEP encryption	
		11. I will use WPA2 encryption.	
		12. I will limit the number of connections to my router.	
		13. I will change the WiFi password to a mix of letters, numbers, and special characters.	
		14. I will change the IP address range and default gateway to random numbers (avoiding .1, .100, and .254).	
		15. I will turn off remote router management.	
		16. Other	
SINTF2	Q51	In the future, I plan to make the following IoT device changes:	
		1. Buy only devices with upgradeable firmware.	
		2. Place IoT devices on a separate guest network.	
		3. Replace insecure IoT devices, even if they are still functional.	
		4. Check for firmware updates regularly.	
		5. Update firmware when available.	
		6. Review router logs.	
		7. Use encryption when available.	
		8. Check shodan.io to see if any of my devices are vulnerable.	
		9. Find other alternatives for devices that don't need to connect to the Internet.	
		10. Other	

Table 7 Security Intentions (Future) Questions

The survey was piloted to ensure that the language was understandable for participants. While there are some technical questions regarding security measures in the test, explanations and examples were provided for those questions.

3.4 Data Processing

There were 639 total respondents, of whom 569 completed the survey, for a completion percentage of 89.05%. Columns included start date and end date, from which the completion time was calculated. Start date, end date, and recorded date were deleted from the processed data set, while completion time was retained. Empty columns, such as Recipient Last Name, Recipient First Name, Recipient Email, and External Reference were all deleted. Additionally, columns containing identifying information, such as latitude, longitude, and IP address were deleted to protect the confidentiality of participants. The distribution and user language columns were deleted as all of the answers were “anonymous” and “EN” respectively. The 15 digit response ID was replaced with a sequential Participant ID, providing each response with a number from 1 to 639.

Those who did not complete the survey were removed from the results by filtering on completion percentage, keeping only results with a value of 100. Having a value of 100 does not mean that all questions are answered, but does mean that the respondent clicked through the entire survey through the last question. On this survey, the only questions that were required were the survey consent and the selection of an age, to ensure that no one under the age of 18 could participate.

For questions with checkboxes, the responses were provided in a single column, with commas separating the values. While using checkboxes provided greater fidelity in fewer overall

survey questions, using the information required breaking the comma separated values into usable information. Each check was assigned a value from 1 to 14, depending on the number of options available on each question. An equal number of columns were created to hold a value for each possible answer. For a smaller subset of questions, an additional column was added to total the values in each separate column. For the majority of questions, the value in each column was binary, with a 1 for yes and 0 for no. However, for one question, the responses were weighted based on the increasing difficulty to attain the education listed.

For checkbox questions with 9 or fewer options, no additional substitution was required. However, for questions with 10 options, using Excel to separate out each number caused issues with the formulas used to do so. In that case, I used find and replace to change all instances of the number 10 to roman numeral X. Two questions had 14 options, at which point changing all answers to the letters A through O in reverse sequential order prevented inadvertent changes, such as 14 being changed to 1D, when attempting to change the number 4 to D had the changes been made in sequential order.

Once the data was transformed in a way that it could be processed, I used the if, iserror, and find functions of Excel to divide the checkbox questions into their individual answers. The command “=IF(ISERROR(FIND("1",G2)),0,1)” instructs Excel to look in cell G2 for the number one and if it is present, to place a one in the cell in which the formula appears. If it is not present, Excel will place a zero in that cell.

Likert items were auto-numbered using Qualtrics. However, they were not always auto-numbered in 1-5 or 1-7 order. Some of the questions were sequentially numbered 8-14, 15-21, 18-24, 20-26, or 22-28. When cleaning the data, those answers were changed back to 1-7, using

find and replace in Excel. Inexplicably, question 47 was auto-numbered 1-5,11,12, requiring 11 to be re-coded as 6, 12 to be re-coded as 7, etc.

For questions that were negatively worded, the answers were reverse-coded to ensure that the responses are positive and on the same scale as those items that were positively worded. Questions thirty and thirty-one would have typically had some elements reversed based on the wording of the question. However, the answer scale was reversed and went from Always to Never instead of Never to Always, so the positively worded questions were reversed, while the negatively worded questions were not.

Processing the Excel spreadsheet for import into SPSS was a three step process. First, all columns that were calculated were copied and pasted back into place as a number. Then, columns that held multiple answers separated by commas and text boxes were deleted, as they were irrelevant to the numerical analysis. For reverse coded questions, the original columns were also deleted.

3.5 Analysis Methods

Prior to conducting analysis, the data was processed, as described above and imported into SPSS 26 and Intellectus statistics for analysis. Descriptive statistics were run on a per question basis, in order to ensure all data is within appropriate parameters, as well as to illustrate trends by question. Means and standard deviations are provided for continuous data, while frequencies and percentages are used for categorical data. In some cases, categorical data is converted to and analyzed as continuous data.

3.5.1 Validity and Reliability

Exploratory factor analysis can be used to determine the influence of each question on user security intentions (Fabrigar & Wegener, 2012). This allows for the questions with low loadings to be excluded and focus on the influence of those that have the most impact.

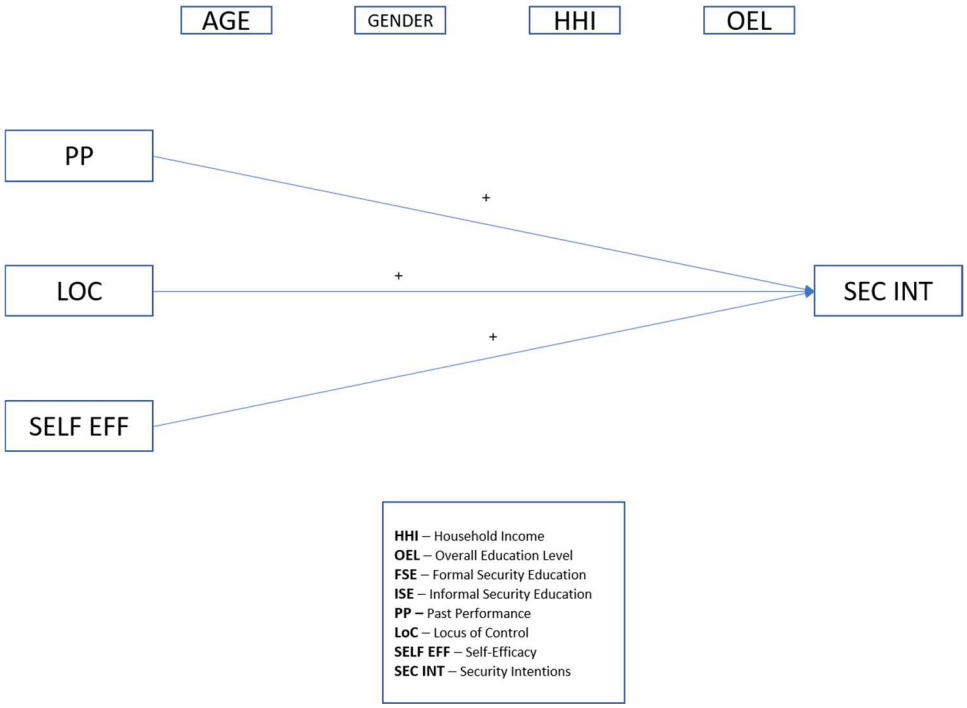

Figure 4 Initial Analysis Diagram

While locus of control and self-efficacy questions are primarily adapted from prior studies, past performance only had one question from a prior study and security intentions had six items from a prior study out of twenty-six. In order to test the correlation to various past performance factors, there are a significant number of questions relating to the participant's formal education, informal education, and Internet security habits. Those that had the least effect on the participant's security intentions were removed from consideration, thus providing a smaller pool of questions to be used in future studies and in the analysis of this study. Additionally, the questions were on different scales and had to be analyzed individually rather than as a combined variable.

3.5.2 Multiple Hierarchical Linear Regression

In order to examine the research question, five multiple hierarchical linear regressions will be conducted to determine the effects of locus of control, perceived self-efficacy, and past performance on home user security intentions. Five analyses are appropriate because there are five items measuring security intentions, each on different scales. Multiple linear regression was selected to assess the relationship among nominal, ordinal, or continuous predictor variables on a continuous criterion variable. For this study, the independent variables are locus of control, perceived self-efficacy, and past performance, with security intentions as the dependent variable.

Research Question: Do locus of control, perceived self-efficacy, and past performance predict security intentions?

H_0: Locus of control, perceived self-efficacy, and past performance do not predict security intentions.

H_1: Locus of control, perceived self-efficacy, and past performance predict security intentions (existing) security software usage.

H_2: Locus of control, perceived self-efficacy, and past performance predict security intentions (existing) network protection measures.

H_3: Locus of control, perceived self-efficacy, and past performance predict security intentions (existing) IoT protection measures.

H_4: Locus of control, perceived self-efficacy, and past performance predict security intentions (future) security changes.

H_5: Locus of control, perceived self-efficacy, and past performance predict security intentions (future) IoT protection changes.

Past performance is based on six items on the survey. Due to the items being scored on different scales, the individual questions for questions 13, 15, 17(reversed), and 18, were used as predictors, while questions 30 and 31 are both Likert scale questions on the same scale and were combined into a single variable. Question 13 measured formal education and is categorical. Question 15 measures progressive information technology and security education through measuring weighted certification counts. Question 17 is also ordinal with participants measured on how much IT/CS is required in their job, if they have had an IT/CS-related job in the last three years, or do not have a job that requires IT. Question 18 is also a categorical variable, measuring informal education, which was a count of the number of answers selected. Mean scores for questions 30 and 31 were also used as predictors to measure past performance.

Locus of control is a continuous variable calculated by the mean score of four Likert scale survey questions (Questions 38-41). Perceived self-efficacy is also a continuous variable and will be calculated from the mean of six survey questions (Questions 42-47). For the multiple linear regression, the security intentions dependent variable was first divided into existing and future. The security intentions (existing) dependent variable was further separated into security software (Q33), network protection (Q34), and IoT protection (Q35). Security intentions (future) was divided into changes (Q49) and IoT changes (Q51). Question 33 was measured as a count of number of types of security software self-reported by the user. Question 34 and 35 will also be counts of types of network protection measures and IoT device protection measures respectively. Security intentions (future) was measured by a mean score of responses to question 49 and a count of IoT device protection types in Question 51. The number of respondents who answered

question 49 were greatly reduced, because only respondents who answered yes to question 48, which asked whether they intended to make changes, were shown question 49. All respondents were shown question 49, which asked what IoT changes they intended to make.

To ensure validity of the model, the assumptions of normality of residuals, homoscedasticity of residuals, absence of multicollinearity, and lack of outliers will be assessed. Normality of residuals assumes that residuals of the regression model follow a normal distribution. A Q-Q scatterplot of the residuals tested for normality (DeCarlo, 1997; Bates, Machler, Bolker, & Walker, 2015; Field, 2013). The assumption of homoscedasticity of residuals is that there is no relationship between the residuals and the fitted values, which will be examined with a scatterplot of the residuals and the fitted values (Bates, Machler, Bolker, & Walker, 2015; Field, 2013; Osborne & Waters, 2002). The absence of multicollinearity was assessed using variance inflation factors (VIF), where values over 10 would have suggested the presence of multicollinearity (Menard, 2009). Lastly, lack of outliers will be determined by a studentized residual that exceeds the .999 quantile of a t-distribution with n-1 degrees of freedom (Field, 2013; Stevens, 2009).

The hypothesis was tested using hierarchical multiple linear regression, where predictors were added in sequence to understand the effect that each independent variable has on each dependent variable being measured. They were evaluated to determine their predictive value. The F-test was used to determine whether the independent variables predicted the dependent variable. R-squared was reported to determine the amount of variance in the dependent variable can be accounted for by the independent variables. The t-test will determine the significance of each predictor and beta coefficients were used to quantify the magnitude of prediction for each predictor.

3.5.3 Partial Least Squares – Path Modeling

For partial least squares path modeling (PLS-PM), the research question remains the same, but the hypotheses are slightly different. Due to the ability of PLS-PM to aggregate the dependent variables into latent variables, the dependent variable is only divided into security intentions existing and future variables.

Research Question: Do locus of control, perceived self-efficacy, and past performance effect security intentions?

H_0: Locus of control, perceived self-efficacy, and past performance do not effect security intentions.

H_6: Locus of control, perceived self-efficacy, and past performance effect security intentions (existing).

H_7: Locus of control, perceived self-efficacy, and past performance effect security intentions (future).

As a non-parametric test, PLS-PM does not assume normality of distribution and does not require any assumption tests.

The data was evaluated by a measurement (outer) model and a structural (inner) model. For the outer model, validity was tested based on whether the construct was reflective or formative. For reflective factors, loadings and communalities, unidimensionality of indicators, crossloadings and bootstrapped loadings were explored. A Cronbach's alpha and Dustin-Goldstein rho above 0.7 were considered unidimensional. The loading and communalities were examined to determine if at least 50% of variance can be explained, with loadings greater than or equal to 0.707 and communalities greater than or equal to 0.50. Crossloadings exist when an

indicator variable has a higher loading on a different latent variable. Significance of bootstrapped loadings were determined with a 95% confidence interval.

Multicollinearity and bootstrapped weights were evaluated for formative indicators. A variance inflation factor (VIF) over ten would indicate multicollinearity in the model (Menard, 2009). Bootstrapped weights for formative indicators were also determined with a 95% confidence interval.

The R^2 value, average variance extracted (AVE), goodness of fit index (GoF), and bootstrapped regression coefficients were examined for the structural model. Endogenous latent variables were examined to determine if at least 20% of their variance was explained by each independent variable. Each reflective indicator was evaluated to determine if it had an AVE greater than or equal to 0.50.

3.5.4 Structural Equation Modeling

Structural equation modeling (SEM) tests whether the latent variables, security intentions (existing) and security intentions (future) are adequately described by past performance, locus of control, and self-efficacy. The research question and hypotheses remain the same as PLS-PM.

Research Question: Do past performance, locus of control, and self-efficacy effect security intentions?

H_0: Past performance, locus of control, and self-efficacy do not effect security intentions.

H_6: Locus of control, perceived self-efficacy, and past performance effect security intentions (existing).

H_7: Locus of control, perceived self-efficacy, and past performance effect security intentions (future).

The assumptions of multivariate normality, outliers, and absence of multicollinearity were tested. Multivariate normality assumes that each linear combination of variables follows a univariate normal distribution, which was tested by plotting Mahalanobis distances and comparing them to a Chi-square distribution (Field, 2013). An outlier is a Mahalanobis distance exceeding the 0.999 quantile of the Chi-square distribution (Kline, 2015). Multicollinearity was tested by calculating the R^2 values of the variables and creating a correlation matrix of the variables. An R^2 exceeding 0.90 would be considered high collinearity (Kline, 2015), as would a determinant of the correlation matrix of less than 0.00001 (Field, 2013).

The model was evaluated using the Chi-square goodness of fit test, model fit, and examining the R2 values between indicator variables and their latent variables (Hooper, Coughlan, & Mullen, 2008). The model was considered a good fit if there was a non-significant Chi-square result at a significance level of 0.05. Additionally, root mean square error of approximation (RMSEA), comparative fit index (CFI), Tucker-Lewis index (TLI), and standardized root mean square residual (SRMR). An RMSEA less than 0.10 was considered adequate and less than 0.08 was considered an excellent fit; a CFI value above 0.90 was considered an acceptable fit and greater than 0.95 was considered a good fit; a TLI value exceeding 0.95 was considered an excellent fit; and an SRMR less than 0.08 was considered adequate and below 0.05 was excellent (Hooper, Coughlan, & Mullen, 2008). An R^2 below 0.20 was indicative of possibly not describing the latent construct and was considered for removal.

For subsequent regressions, the unstandardized estimate was used as the Beta coefficient, while the z statistic and p-value were used to determine the significance of the direct effect. Mediation was then assessed by evaluating direct, indirect, and total effects.

Chapter 4 Survey Results

From February 22, 2018 to March 5, 2018, a 52 question survey measuring locus of control, perceived self-efficacy, past performance, and security intentions, was conducted via Qualtrics, an online survey platform, with a total of 637 respondents, of whom 569 completed the survey, for an 89.32% completion rate. The survey utilized a snowball sampling methodology, resulting in this method of calculating completion rate. While one would typically measure completion rate by the number of participants who completed the survey divided by those identified to participate in the survey, that calculation is impossible in this situation for the reasons listed below.

Due to the limitations of social media and emails sent to list servers, there is no way of definitively quantifying the number of potential participants who viewed the research plea. At the time of this survey, Facebook did not show analytics concerning the number of people who viewed a post. Additionally, when an email is sent to a list server, it is sent to a central email address. Once the central email address receives the email, it sends it to member email addresses based on their delivery preferences. There was no way to request a read or delivery receipt and notices that an email is invalid would have been sent to the listserv email address, not the message originator's email address. For the 53listserv, available options are receiving each email as it is sent or receiving a daily digest of all emails that were sent that day. Either way, even if a user received the email, it may not have been viewed depending on whether they opened it, or in the case of an email digest, whether they read the email in its entirety.

The user survey collected a wide variety of variables to understand what affects user IoT security intentions. The research question asked: How does user locus of control, self-efficacy,

and past performance in security measures influence home security intentions? My hypothesis was that internal locus of control, higher perceived self-efficacy, and higher past performance would result in increased security intentions.

In this section, the results for each question are reported for all participants who completed the survey. Survey results from those who did not finish are not included in this section.

4.1 Respondents by Source

The research plea was posted to Facebook and LinkedIn, as well as emailed out to two list servers based on Information Systems Management affinity groups. The results can be seen in Figure 10. The Facebook research plea produced the most respondents, with 528, of whom 464 completed the survey, for a completion rate of 87.88%. The email plea resulted in far fewer respondents with 98, of whom 93 completed the survey, for a completion rate of 94.90%. LinkedIn produced the fewest respondents, with 13, of whom 12 completed the survey, for a completion rate of 92.31%.

Of the three sources, Facebook provided the most value, despite having the lowest completion rate. Email had the highest completion rate, likely because the targeted respondents have an affinity for information security, as that is, or was previously, their primary occupation. LinkedIn had a high completion rate, but a low participation rate of 2.03%, providing 13 out of a total of 639 participants.

LinkedIn had a low participation rate, which may have been due to a technical limitation how hyperlinks are treated in their posts. The research pleas were nearly identical across all platforms, with only the name of the platform and universal resource locator (URL) changed

based on the platform the plea was shared on. The survey link was approximately halfway through the post and I included my syr.edu email address, as the point of contact, near the end of the post. Facebook allowed for users to click on the link and go directly to the survey. The email had the hyperlink in the body, allowing users to go straight to the survey. However, LinkedIn instead provided a clickable link to the Syracuse University main website, http://www.syr.edu, based on the included contact email address, rather than the survey hyperlink. The 13 people who attempted the survey had to copy and paste the link into their browser to complete the survey, rather than clicking the hyperlink.

4.2 Demographics

The demographic items collected for the survey instrument were age, education level, ethnicity, household income, and gender. The available options, as well as method of input are listed below in Table 8.

Demographics Variables		
Variable	Options	Input
Age	<18, 18-24, 25-34, 35-44, 45-54, 55-64, 65-74, 75-84, 85+	Radio button
Overall Education Level (OEL)	<High School, High School Graduate, Some College, 2 year degree, 4 year degree, Professional Degree, Doctorate	Radio button
Ethnicity	White, Black or African American, American Indian or Alaska Native, Asian, Native Hawaiian or Pacific Islander, Other	Checkbox
Household Income (HHI)	<$10K, $10-19,999, $20-29,999, $30-39,999, $40-49,999, $50-59,999, $60-69,999, $70-79,999, $80-89,999, $90-99,999, $100-149,999, $150K+	Radio button
Gender	Male, Female, Nonbinary	Radio button

Table 8 Demographics Variables

Ethnicity was the only question that allowed for multiple inputs via checkbox. All other questions required the selection of a single answer. In post hoc processing, those who selected multiple races were reassigned a code of 7 for multi-racial for analysis.

Household income was collected in $10,000 increments, up to $150,000. Household income was used instead of individual income because Internet of Things devices tend to be a household purchase, as opposed to an individual purchase. While there are some exceptions, such as video game consoles, many IoT devices are intended for household usage, such as Amazon Echos, smart doorbells, and cameras.

A nonbinary option was included in gender, resulting in four respondents who identified as nonbinary and an additional four respondents that left gender blank while answering all other demographic questions. Based on a population estimate that 0.6% of the population is transgender (Flores, Herman, Gates, & Brown, 2016), 3.4 of the respondents would be expected to be transgender. Another estimate of 390 out of 100,000 (Meerwijk & Sevelius, 2017), would mean .039% of the general population or 2.22 respondents to the survey would be expected to be transgender. While transgender and nonbinary are not synonymous, estimates of the nonbinary population have been conducted as a subpopulation of the transgender community, with 35% self-reporting as nonbinary (James, et al., 2016).

The ages of the survey respondents, as shown in Figure 13 below, included twenty respondents over the age of 65, who finished the survey. The perception of technology participation is that it is primarily the domain of younger people, but there were almost an equal amount of participants between the ages of 18 and 24 as there were over 65. One reason for this may be that people in the 18-24 age bracket are more likely to be living in someone else's space, such as a college dorm and that they are also likely to have a lower household income, due to being in school or at the beginning stages of a career. On the other hand, participants over the age of 65 may be more likely to own IoT devices to assist with independent living and because they may have adult children who gift them devices.

Variable	*n*	%	Variable	*n*	%
Age			**Annual HHI**		
18-24	22	3.87	>$10,000	3	0.53
25-34	154	27.07	$10,000-$19,999	3	0.53
35-44	218	38.31	$20,000-$29,999	6	1.05
45-54	86	15.11	$30,000-$39,999	14	2.46
55-64	69	12.13	$40,000-$49,999	16	2.81
65-74	18	3.16	$50,000-$59,999	25	4.39
75-84	2	0.35	$60,000-$69,999	32	5.62
			$70,000-$79,999	36	6.33
Education			$80,000-$89,999	38	6.68
< High School	1	0.18	$90,000-$99,999	46	8.08
HS graduate	4	0.7	$100,000-$149,999	179	31.46
Some college	18	3.16	$150,000+	166	29.17
2 year degree	18	3.16	Missing	5	0.88
4 year degree	183	32.16			
Professional degree	304	53.43	**Gender**		
Doctorate	40	7.03	Male	322	56.59
Missing	1	0.18	Female	239	42
			Nonbinary	4	0.7
Ethnicity			Missing	4	0.7
White	407	71.53			
Black	106	18.63	**IoT Ownership**		
Am. Ind./AK native	1	0.18	Yes	445	78.21
Asian	20	3.51	No	124	21.79
Other	20	3.51			
Multi-racial	14	2.46			
Missing	1	0.18			

Table 9 Demographic Summary Table

Overall education levels for the participants in this study were high with 92.62% of respondents having a 4 year degree or higher, compared to 30.69% of the United States population (US Census Bureau, 2016), and 39.2% of the United States internet user population (Ryan, 2018). There were forty respondents with doctoral degrees, three hundred and four with a professional degree, and one hundred and eighty-three with a 4 year degree. By contrast, there were only eighteen respondents with a 2 year degree, eighteen with some college, four high

school graduates, and one respondent who is not a high school graduate, for a total of forty one respondents with a 2 year degree or below.

Survey respondents were primarily white at 71.53% of respondents, followed by black at 18.63%, Other (including Hispanic) at 3.51%, Asian at 3.51%, American Indian or Alaska Native at 0.18%, Native Hawaiian or Pacific Islander at 0.53%, and 2.46% who selected more than one race. Respondents were able to select more than one ethnicity, resulting in a percentage greater than 100%. The accidental exclusion of Hispanic as an option was noticed by at least eleven respondents, who selected Other and typed variations of Hispanic or Latinx in. There were two respondents who typed "American" in the other box and one respondent who typed "mixed". The sample of white respondents is aligned with that of computer and internet users in 2016 in America, while black respondents were overrepresented, and Asian and Hispanic respondents were underrepresented (Ryan, 2018). Due to the exclusion of the Hispanic category, it is impossible to know how many other respondents of Hispanic origin may have chosen not to select other.

Survey participants had a high annual household income, with 60.63% of respondents having an annual household income above $100,000. There were slightly more respondents in the $100,000-149,999 category (179) as there were whose household income was below $89,999 (173). Only 13.53% of respondents self-reported household income below the United States median household income of $60,293 (US Census Bureau, 2018). Internet usage penetrates higher income households at a greater rate (Ryan, 2018), but this survey overrepresents high income household and underrepresents lower income households.

Respondents were given three choices for gender: male, female, or nonbinary. Males are overrepresented at 56.59% compared to their US population representation of 49.02%, while

females are underrepresented at 42% for survey respondents, as opposed to comprising 50.98% of the US population. The nonbinary respondents provided another data point for estimating their representation within the United States population. Gender was not included in the Census Bureau Computer and Internet Usage survey to determine if technology is adopted equally across genders (Ryan, 2018).

4.3 IoT Non-Ownership

Prior to measuring the variables outlined in 4.3, survey participants were asked whether they owned IoT devices. Those who did not were provided with a follow-up question whether they had considered owning IoT devices or not. 136 respondents answered no to the IoT ownership question, while only 135 of those respondents answered the follow-up question about whether they had considered it or not. Of the 135, 58% answered no, while the other 42% answered yes.

Seventy-eight respondents selected no when asked if they had considered IoT devices. When asked to provide reasons why they had not, they selected a total of 113 reasons for not considering them, as respondents were able to select multiple answers. Figure 5 shows the reasons they were not considered and the number of respondents selecting each option.

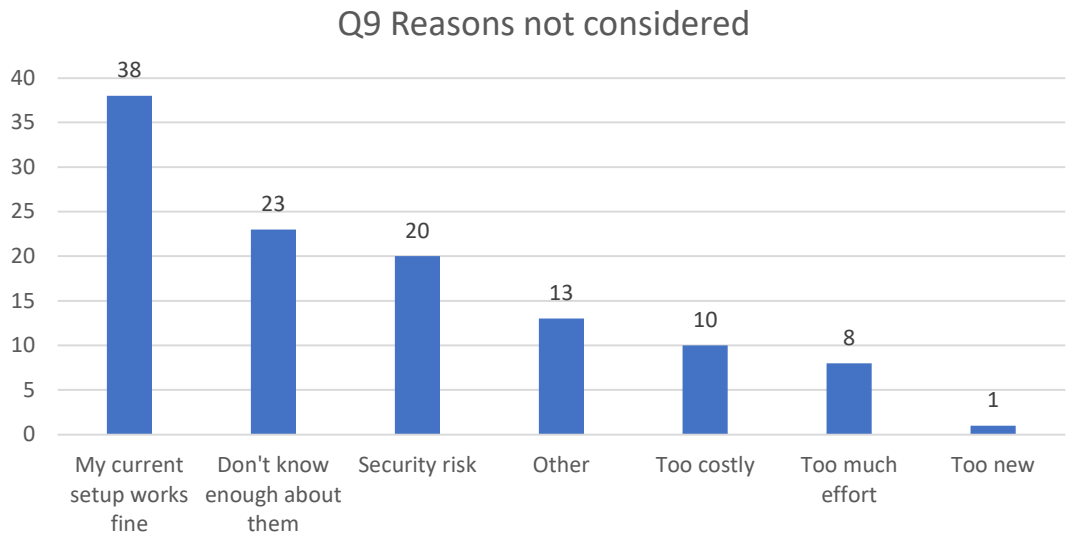

Figure 5 Reasons IoT Devices Were Not Considered

Among all respondents, having an acceptable existing configuration was the leading reason that IoT devices had not been considered with thirty-eight respondents, followed by not knowing enough about them with twenty-three respondents, while only twenty respondents viewed them as a security risk. Among the thirteen respondents that selected Other, five believed that because they were renting, they could not have IoT devices, two hadn't thought of it, two did not elaborate in the text box, one questioned why they should get them, one said they didn't need them, one did not have the network capability for them, and one said they believe they are counterproductive. Ten respondents viewed them as too costly, eight believe they require too much effort, and one respondent felt they are too new.

Fifty-seven respondents had considered IoT devices, but ultimately had not installed any, providing ninety-six reasons why they had not, averaging 1.68 reasons each. Their responses are visualized in Figure 18 below.

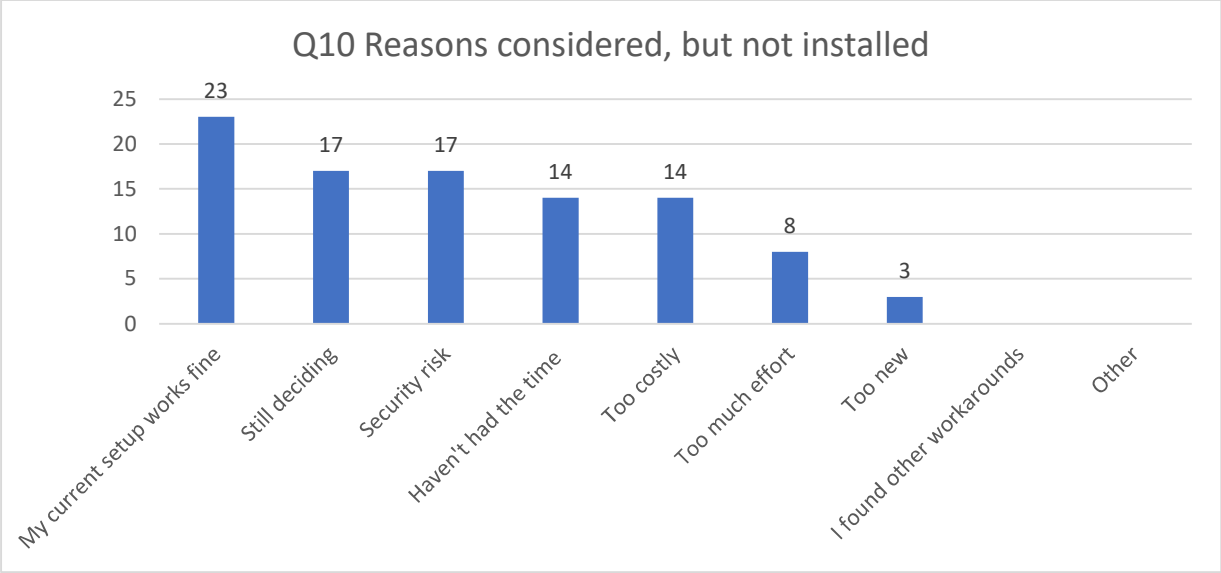

Figure 6 Reasons IoT Devices Were Considered but not Installed

Like those who had not considered IoT devices at all, the respondents' leading answer was that their existing configuration met their needs satisfactorily with twenty-three responses, followed by those that are still deciding with seventeen responses and those that view them as a security risk with seventeen responses as well. Not having the time and cost each had fourteen responses, while the devices being viewed as requiring too much effort had eight responses. Three respondents viewed the devices as being too new, while no respondents selected that they had found other workarounds or Other.

4.4 Past Performance

Questions 11-26 measured respondents' self-reported past performance. Only the questions used for the past performance variable are reported here.

62.21% of respondents reported having formal information technology or computer science education, compared to 37.79% without it. Attempting to compare the survey respondents to the United States population uncovered the dearth of reporting of formal

information technology and computer science formal education, as well as the disparity between states in their K-12 computer science curriculum (Google, 2018).

Unfortunately, even in collegiate computer science education, security is most frequently an elective and not a required course (Cable, 2019). By not requiring security courses or teaching secure coding in the curriculum, software development focuses on usability rather than security.

College courses were the most frequently selected option by respondents, with two hundred and thirty-six self-reporting that they took IT/CS related courses in college. Of those who took college courses, fourteen completed a minor in an IT/CS field, sixty-nine completed a bachelor's degree, eighty-five completed a master's degree, ten completed a graduate certificate, and seven completed a PhD. 13.09% of those who completed a four year degree, determined by totaling all respondents with a 4 year degree or higher degree, completed that degree in an IT/CS field, while 17.5% of those who completed a doctorate did so in an IT/CS field. Only 2.66% of those who completed a bachelor's degree had a minor in Information Technology or Computer Science.

Certification courses were the second most frequently selected formal education, with 123 respondents reporting that they completed at least one certification course. One hundred and five respondents reported completing high school classes and below.

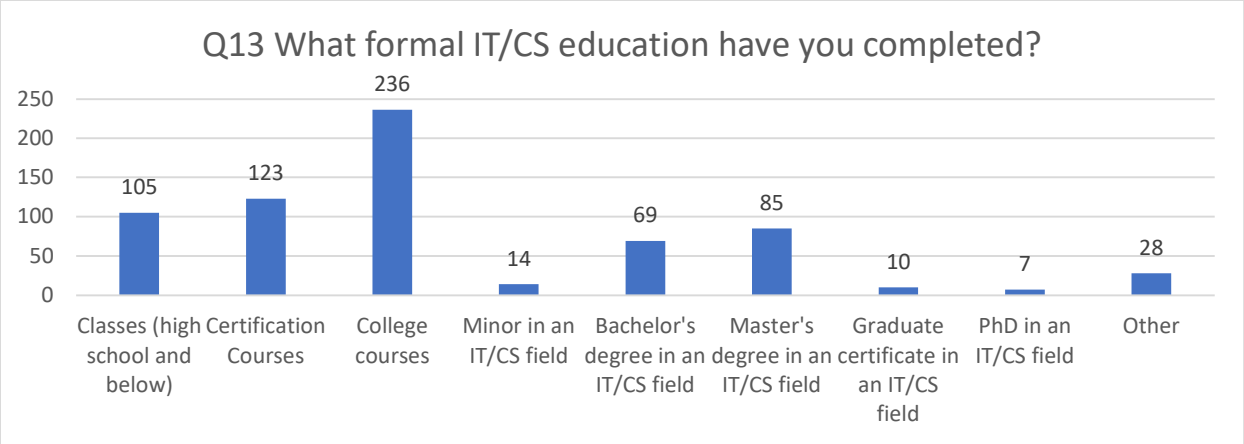

Figure 7 Formal IT/CS Education by Type

Among those who obtained degrees in IT/CS fields, there were no respondents who did their bachelor's, master's degrees and PhD all in IT/CS fields. Twenty-eight respondents did their bachelor's and master's degrees, three respondents did their bachelor's, master's, and a graduate certificate, and three did their master's and PhD in IT/CS fields. Based on their responses, it appears most common for students to get a bachelor's in a non-IT/CS field and then return for a master's degree in an IT/CS field, as fifty-seven of the respondents did. It is unusual that there were no respondents who completed their bachelor's through PhD in the same field and that there were four respondents who only did their PhD in an IT/CS field.

Respondents who selected other and provided a written response cited military training, on the job training and experience, online training, and an associate's degree. The associate's degree was used as an example, but then was not included on the list of formal education options. The military respondents primarily attended Signal Corps basic branch training, but there was at least one respondent who attended the specialty Telecommunications Engineer course. Some of the respondents didn't specify which military training course they attended.

Among the ninety respondents who had taken classes in high school, the range was from one to fifteen classes pertaining to IT/CS, with two being the most common. Thirty-six

respondents have two classes relating to computer security, while twenty-five had one, and seventeen had three. Six respondents had four, two had five, three had six, and one had fifteen.

Question 15 asked respondents what certifications they had and provided radio buttons to select multiple options. This question was weighted with values assigned to the certifications based on difficulty to obtain them and relevance to security. Basic IT certifications were assigned a value of one point, basic security certifications two points, intermediate IT certifications three points, intermediate security certifications four points, advanced IT certifications five points, and advanced security certifications were assigned a value of six points.

Four hundred and forty-six respondents (78.38%) had no certifications. The remaining one hundred and twenty-three respondents held a total of 295 certification levels, resulting in an average of 1.48 certification levels each, with a range from one to six. The question did not give the respondents the ability to provide the count of how many certifications they had at each level, but instead how many skill levels they have certifications in.

Among those with certifications, the number of respondents with each type of certification decreased as difficulty level increased, except for advanced security certifications. While difficulty of the material may be one reason for this, higher level certifications generally require more prerequisites, in the form of additional certification tests, time working in the field, and recommendations from colleagues who already hold the higher certification (ISC2.org, n.d.) (Cisco, n.d.).

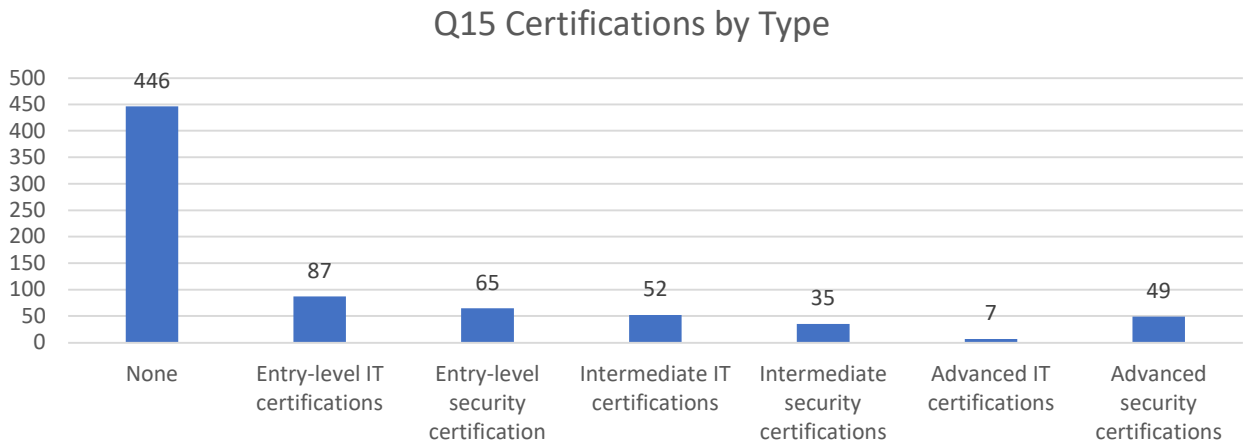

Figure 8 Certifications by Type

Three hundred and thirty-three respondents (58.52%) did not take any IT/CS courses in college. The remaining two hundred and thirty-six respondents took one to thirty IT/CS courses. Those who did not take any IT/CS courses were removed from Figure 9.

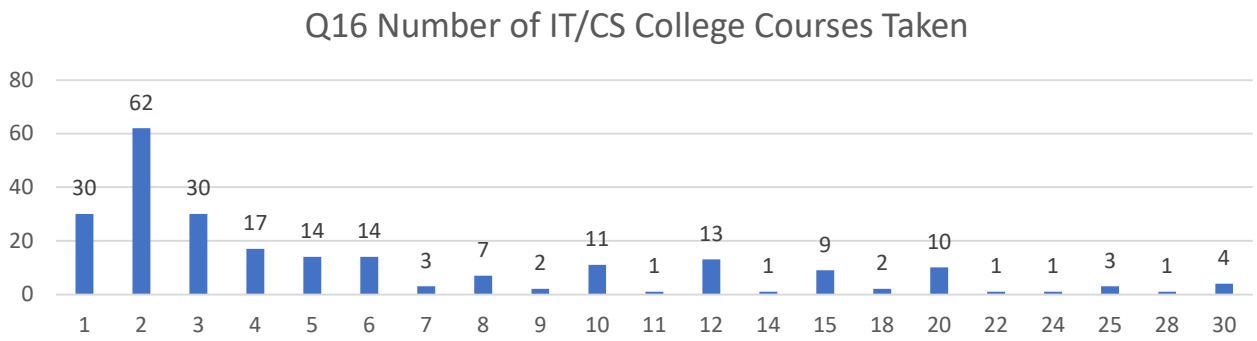

Figure 9 Number of IT/CS College Courses

With those who did not take a class removed, 58.9% of the remaining respondents did not take sufficient classes for an IT/CS minor, which normally requires approximately five courses. On the other end of the spectrum, twenty of the remaining respondents (8.48%) took twenty to thirty courses, indicating completing a bachelor's and taking additional graduate level courses.

Four hundred and forty-one respondents (77.5%) self-reported informal IT/CS education, while one hundred twenty-eight respondents (22.5%) reported that they had no informal IT/CS education. Three hundred and nineteen respondents (56%) had both formal and informal IT/CS

education, one hundred and fifty-seven (28%) had either formal or informal IT/CS education, while ninety-three had neither (16%).

Of those with informal education, three hundred and fifty-six have looked up solutions to IT/CS problems on the Internet, three hundred and twelve have tinkered with computers or other devices, two hundred and forty-four have learned programming, two hundred and forty have learned from friends and relatives, while two hundred and one have read books on IT/CS topics. There was an average of 3.11 types of informal IT/CS education per respondent.

Three hundred and fifty-one respondents (61.69%) do not currently work in an IT/CS-related field, nor have they in the last three years. The second highest number of participants, one hundred and thirty-four, currently hold positions that require IT/CS work more than fifty percent of the time. Twenty-eight respondents (4.92%) perform IT/CS work for thirty to fifty percent of their job, while thirty-seven respondents (6.5%) spend less than 30% of their work time on IT/CS-related tasks. Nineteen respondents (3.34%) do not currently work in an IT/CS-related field, but have in the last three years.

Ninety-three, or 16.34%, of respondents had no formal or informal IT/CS education, while three hundred and nineteen had both formal and informal IT/CS education. While states are making progress in improving access to computer science education at the K-12 level (Ascione, 2018), that will not provide IT/CS education for those who have already completed high school. Eighty-six of the ninety-three who had no formal or informal IT/CS education also do not work in an IT/CS-related job. 15.11% of all respondents have no obvious method of learning how to secure their personal network and devices with no formal or informal IT/CS education, and no exposure to organizational information security policies or on the job training.

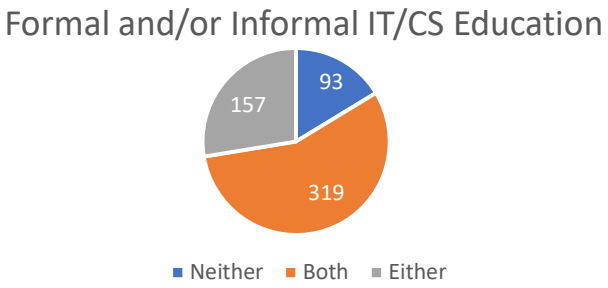

Figure 9 Formal and/or Informal IT/CS Education

Of those who had either IT/CS degrees or certificates, their most recent degree or certificate was awarded from 1971 to 2018. 47.76% of all respondents who reported the year of their most recent degree or certificate had earned it in the three years prior to the survey, 57.46% in the five years prior, and 70.9% in the ten years prior. Figure 10 shows the distribution of degrees or certificates by year.

Figure 10 IT/CS Degree or Certificate Recency

Overall, respondents had 6.36 connected device types per household. This question did not ask how many devices per type there were. Computers, smartphones, and tablets have the most household saturation with 98.07%, 96.13%, and 85.06% respectively, but they are not IoT devices per the selected definition. 79.09% of respondents have home automation devices, with smart outlets, thermostats, and lightbulbs given as examples for that category. 56.77% had E-readers, 46.22% had fitness trackers, and 37.43% had media devices that connect to the Internet,

such as Smart TVs, Fire Sticks, and connected DVD/Blu-Ray players. 34.45% have video game systems, 32.34% have monitoring devices, such as baby monitors or nanny cameras, 29.17% have smartwatches, such as Apple Watch and Samsung Galaxy Gear, and 11.25% have do-it-yourself lightweight computing, such as Raspberry Pi or Arduino systems. Security system devices, medical devices, and smart appliances were the least common devices at 9.14%, 5.45%, and 5.10% respectively. 10.72% of respondents selected Other.

Respondents were asked how many IoT devices they had in their home. Answers ranged from zero to forty-five devices, with 12.30% having zero, 49.56% having between one and five, 27.24% with six to ten, and 10.90% with eleven or more. There was one respondent each with forty-five devices, forty devices, thirty devices, twenty-seven devices, and twenty-two devices. Among those with eleven or more devices, twelve was most common with twelve respondents, followed by fifteen devices selected by eleven respondents, and twenty devices reported by eight respondents.

While forty-five devices may seem excessive now, there are many ways that could become a more common number in the future. To illustrate a scenario where forty-five devices may be reasonable, assume a family of four with two adults and two school-aged children are living in a 1300 square foot, 3 bedroom, 2 bathroom house. A home of that size has approximately twenty-three electrical receptacles, for a total of forty-six outlets, based on the National Electrical Code (National Fire Protection Association, 2020). Smart outlet devices can purchased for as little as $8.99 individually or $29.99 for four, equating to $7.50 each (Amazon, 2020). That same home would have at least eight light fixtures, where smart lightbulbs could be used in place of standard bulbs at a cost of $13.99 individually or $39.99 for a four pack, equating to $10.00 each (Amazon, 2020). The house may contain one to four smart televisions,

depending on the parents' stand on technology in the children's rooms. Even if the televisions are not smart, they may have a media player or fire stick to stream to the non-smart televisions. The home may also have a smart thermostat. Because there are children in the home, there may be one or two video game consoles, which are also connected to the Internet. There is likely at least one additional smart device to control the various devices around the home, such as a Google Home or Amazon Alexa. To protect and monitor the home, there may also be a smart doorbell with camera and two cameras inside the home. In this scenario, there are up to sixty-three IoT devices not including any smart appliances, medical devices, smartwatches, or fitness trackers. Even if the household only used smart outlets for half of their outlets, that would still be forty potential IoT devices.

Only seventy people responded that they had zero IoT devices, yet one hundred and thirty-six respondents answered no to question eight, which asked if they owned IoT devices. The other sixty-six respondents who self-reported having no IoT devices in question eight had between one and fifteen IoT devices in their household. This may indicate that the respondent does not own the devices, but they are present and in the possession of another member of the household. Depending on the types of devices within the household, there may be privacy and agency implications for the non-owner resident, such as the children in the example above.

Question 22 asked respondents who owned their as an exploratory question. 53.36% of respondents owned their router, 44.63% have ISP-owned routers, 4.53% had both personally-owned and ISP-owned routers, and 2.01% selected Other. ISP-owned routers typically are installed by the ISP and have some default security mechanisms built in, such as complex randomized passwords. However, ISP-owned routers may also be using the customer's home

Wi-Fi network as a public Wi-Fi hotspot, allowing unknown parties to connect to their router (Hayes, 2014).

67.83% of respondents set their routers up themselves, while 32.17% did not. This question does not necessary indicate technical prowess, as it does not delve into what settings they used, or even how long the router setup may have taken. Such follow-up questions in the future may help to determine whether it was configured securely or just configured to function as quickly as possible.

Of the two hundred and sixty-six respondents who have ISP-owned routers, they were asked whether they had logged into the router. While an overwhelming majority had at 81.58%, there was a sizeable minority that had not. Forty-nine respondents had no configuration control over their router, as it was installed by the ISP and has never received any further configuration from the user.

Routers were most frequently configured by a commercial third party, if not configured by the respondent with 39.34%, followed by the least secure answer “no one, it worked out of the box” at 19.12%, and 18.03% selected “someone else who resides in the home”. 23.5% of respondents selected other, of whom four of the respondents did not have a router, one had a friend set it up, one had a landlord set it up, and the remainder who provided a reason listed some variation of their ISP. In the future, the ISP needs to be added as a selection.

Those who had not logged in to their ISP-owned router were asked if they knew how in Question 26. Of the forty-nine respondents, 75.51% did not know how to log in to the router, while 24.49% knew how and chose not to.

Respondents overwhelmingly perform the following actions online: check email (99.47%), perform searches (97.36%), shop online (96.49%), use social media (95.08%), watch

videos (94.02%), communicate anonymously (93.32%), bank online (92.97%), and read news (92.79%). Conducting research is close behind at 86.99%, with a sharp drop to 51.32% for chat, 50.79% for playing games, 46.92% comment on news and blog posts, while only 7.73% communicate secretly. Email is consistent with prior results; online banking, online shopping, and research have expanded; while chat has experienced a small amount of growth (Furnell, Bryant, & Phippen, 2007).

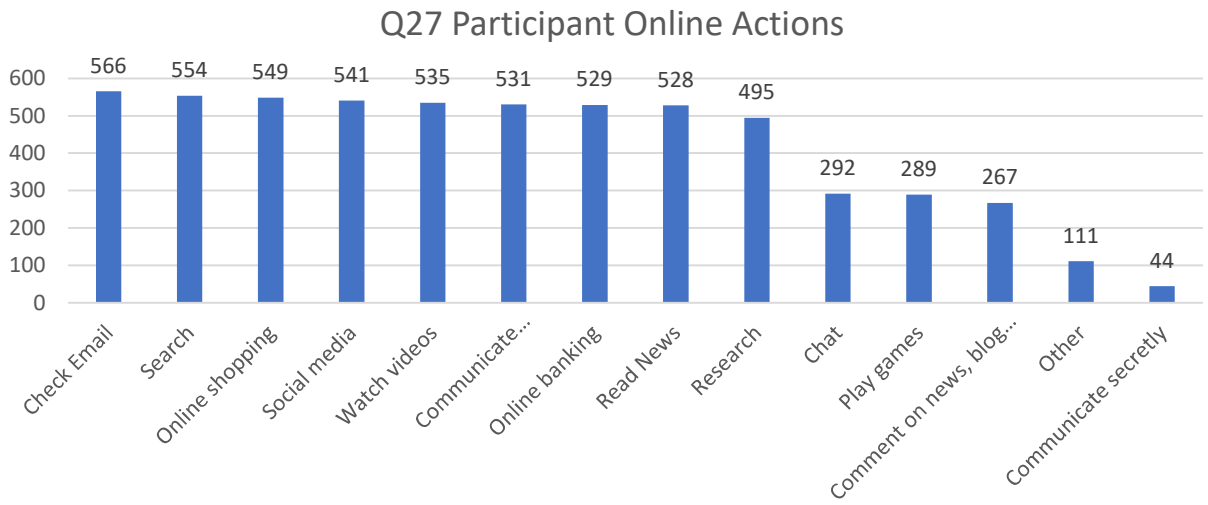

Figure 11 Participant Online Actions

Question 28 asked respondents how many online accounts they had, with answers provided as a selection of ranges: 1-5, 6-10, 11-20, 21-30, and more than 30. Question 29 asked the participants how many unique passwords they had, with answers also provided as a selection of ranges: 1-5, 6-10, 11-15, 15-20, or more than 20. Due to the two questions having two different sets of answers, the only way to compare them directly was to process them after the survey was complete to get them on the same range. In Question 28, the ranges 21-30 and more than 30 were combined into a single answer of more than 20, while in Question 29, the ranges 11-15 and 15-20 were combined into a single answer. Because the answers are based on ranges, it is more difficult to determine if there is a one to one ratio between accounts and passwords.

However, there were one hundred and ninety-eight respondents (34.86%) who the same range of accounts as they had of passwords.

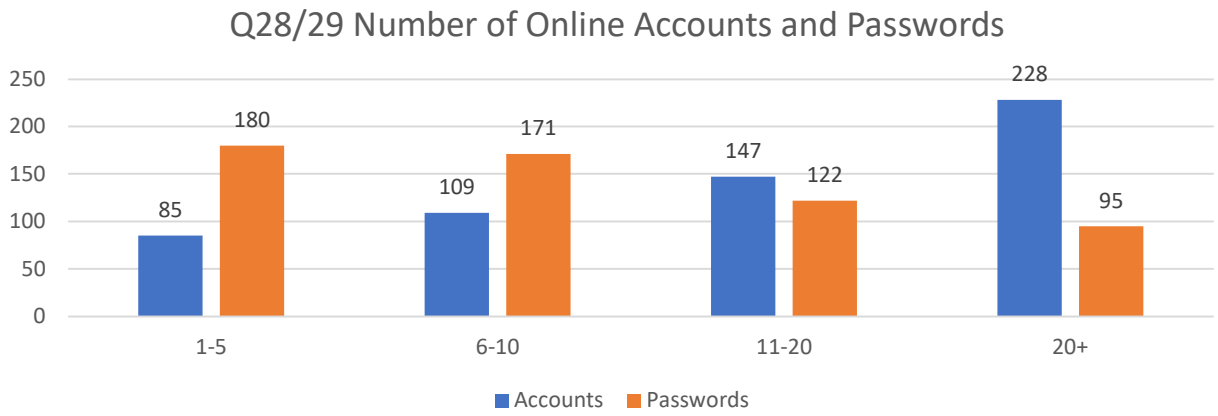

Figure 12 Online Accounts and Passwords

As seen in Figure 12, there is an inverse relationship between the number of accounts and the number of passwords. If users had a unique password for each account, there would be a correlation of 1 between the two questions and their means would be the same. As seen in Figure 41, there is a .6796 difference between the two means, with the mean for number of accounts higher than the mean for number of passwords, and the standard errors for both are .04567 and .04497 respectively. There is only a correlation of .432 (p=.000) between the answers to the two questions, as seen in Figure 42, which indicates a relationship, but not a direct correlation.

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	Q28_scale	2.9120	568	1.08834	.04567
	Q29_scale	2.2324	568	1.07178	.04497

Table 10 Paired Samples Statistics

Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	Q28_scale & Q29_scale	568	.432	.000

Table 11 Paired Samples Correlations

Question 30 answered a series of questions about participants' online security past performance. The answers were on a Likert scale from always to never. Originally, it appeared that these questions had an opposite effect from the education questions. However, the reason for that initial appearance was that the answers range from positive effect to negative effect, whereas the other Likert scale questions ranged from negative to positive. Therefore, when reverse coding negatively worded questions and leaving positively worded questions untouched, it produced an opposite effect.

Overall, respondents' self-reporting positive security behaviors outnumbered those reporting negative security behaviors on every question but the one asking if they used a password vault. For the other questions, 45.76% to 77.74% self-reported positive security behaviors, while 7.24% to 22.08% selected the neutral response, and 13.60% to 38.16% self-reported negative security behaviors.

Checking for encryption when performing secure transactions allows the user to ensure that their information is encrypted while passing over the network, where an attacker can steal the information, and to ensure that they are performing a transaction with the website that they intend to. Two hundred and twenty-six respondents (39.93%) always check, while one hundred and seventy-four (30.74%) check for encryption most of the time. Forty-one (7.24%) answered that they check approximately half of the time, eighty-one (14.31%) selected sometimes, while forty-four (7.77%) never check.

Using strong passwords had the most positive responses, with 77.74% of respondents selecting either Always or Most of the Time. For this question, a strong password was defined as a password with "at least 2 upper case, 2 lower case, 2 numbers, 2 special characters, total of at least 14 characters." This question also had the least negative responses with those selecting

sometimes or never totaling 13.60%. The twenty respondents who selected never when asked about using strong passwords are particularly concerning. The survey question description is more stringent than typical web-based account requirements, but similar to corporate password complexity requirements.

Nine of the twenty respondents (45%) who selected that they never use strong passwords have neither formal nor informal IT education, nor an IT/CS-related job. Eleven of fifty-seven respondents (19.30%) who self-reported sometimes using strong passwords have neither formal nor informal IT education, nor hold an IT/CS job. However, twenty-two of the two hundred and sixty-three respondents (8.37%) who always use strong passwords also have no IT education or a job related to IT/CS.

As a follow up to Questions 28 and 29, participants were asked whether they used the same passwords on multiple sites. From the comparison of number of accounts to the number of passwords, it was clear that respondents were re-using passwords across multiple accounts, which was confirmed by the answers to Question 30. While thirty-four respondents (5.99%) said they always re-used passwords, one hundred and forty-nine (26.23%) selected most of the time, for a total of 32.33% with negative password behavior. Another one hundred and twenty-five respondents (22.08%) selected about half the time, while two hundred and six (36.27%) selected sometimes. Only fifty-three respondents (9.33%) selected never. 5.28% of respondents had over 20 online accounts and between one to five passwords, indicating that a breach on any of their accounts would likely lead to a compromise on several other accounts. This aligned closely with the respondents who self-reported that they always re-use passwords.

Based on the number of users that re-use passwords, password vaults might reduce password re-use, but respondents aren't using them. A password vault is software that stores a

password for each account that a user has, while the user only has to memorize a single password or can use a simpler PIN or password in conjunction with a two factor authentication method.

Respondents overwhelmingly do not use password vaults, with three hundred and forty-one (60.04%) responding that they never use a password vault, while fifty-nine respondents (10.39%) self-reported using a password vault most of the time, and twenty-five (4.40%) reported using a password vault about half of the time. Online shopping was self-reported by 96.49% of respondents, making it a sizeable threat vector. However, the percentage of those who practice the security behavior of checking the reputation of shopping sites most or all of the time is only 52.83%, while 38.16% check either sometimes or never. When online shopping, users voluntarily supply enough information for a malicious actor to steal funds from the credit card or account they chose to use for their purchase.

One hundred and fifty-nine respondents (27.99%) self-reported always logging out of secure sites when finished and one hundred and forty (24.65%) reported doing so most of the time. The question does not address whether they are the only people with access to their device, as anyone with physical access can perform tasks under their account if it is already logged in. On a home computer or mobile phone that no one else has physical access to, this is not a security risk. 10.25% log out about half of the time, while 19.61% log out either sometimes or never.

Two hundred and six respondents (36.27%) self-reported that they always close their browser when finished with secure sites, one hundred and forty-three (25.17%) selected most of the time, and fifty-nine (10.39%) reported that they close the browser when finished about half of the time. This security measure protects the user from someone using the back button from returning to a secure session or from credentials being cached in the browser until it is closed.

One hundred and twenty-two respondents (21.48%) sometimes close their browser when finished, while thirty-five (6.16%) never do.

Question 31 was used to determine the respondents' past performance in email security. While their Internet security measures were mildly positive, respondents' email security measures were significantly positive. For the first three questions, concerning opening emails from unknown senders, opening attachments from unknown senders, and clicking on links in emails, the respondents' overwhelmingly chose sometimes or never. The following two questions, concerning logging out when finished and closing the browser, had much more mixed results. That may be due to respondents' being the only users with physical access to the computer or device on which they check their email.

50.89% of respondents never open emails from people they don't know, while 43.59% sometimes open emails from people they don't know. 2.49% open them about half the time, 2.14% most of the time, and 0.89% open emails from people they don't know always. Results for opening attachments from unknown senders are even more positive. 92.16% of respondents never open attachments from unknown senders, 6.24% do sometimes, 1.07% about half of the time, while those who selected most of the time (0.18%) and always (0.36%) were less than 1%.

Respondents reported clicking on links in emails, as shown in Figure 45, by choosing never (31.55%), sometimes (55.97%) about half of the time (7.66%), most of the time (4.28%), or always (0.53%). When answering whether they log out when finished with email, it was a much wider distribution of answers. Like Internet usage, if the respondent is the only person with physical access to the device, logging out is not necessary.

Like logging out when finished, closing the browser is more important when on a shared device, not on devices dedicated to the respondent alone. Over half of respondents selected

always (32.09%) or most of the time (19.86%), while a little under half selected about half of the time (10.82%), sometimes (28.19%), or never (9.04%).

4.5 Security Intentions (Existing)

84.6% of survey respondents are responsible for maintaining the Internet in their home, while 16.4% are not. When asked what security software was being used, 9.14% of respondents were unsure and 5.45% reported using no security software. Of the remaining respondents who are using security software and know what security software they are using, antivirus (70.37%), malware protection (52.88%), and a personal firewall (47.12%) are the most common security software packages in use by respondents. Application whitelisting (9.05%), monitoring software (7.41%), other (6.58%) were selected at a much lower rate.

While thirty-one respondents selected none for security software used, an additional eighty-one respondents did not select any options for security software, including other, for a total of one hundred and twelve respondents (19.68%) that are not using security software. Two software types (22.67%) were most common, followed by three (21.44%), then one (18.98%). Those with four or more software types totaled 8.08%. Those who selected unsure were treated as having zero security software in the analysis. While each individual type of security software has a different level of efficacy, information security focuses on the concept of defense in depth, encouraging more layers that an attacker must traverse to get to their goal. Therefore, the number of types of each protective measure is a better indicator of each respondent's level of security.

Of the 569 respondents to this question, twenty-four (4.22%) selected none of the above and seventy-two (12.65%) failed to provide an answer. Using encryption (72.94%), changing WiFi passwords (62.21%), and changing default passwords (52.22%) were the only three that more than half of the respondents used. The three least used are review router logs (17.34%),

limit connection by MAC address (14.16%), and change the IP address range (13.53%). No answer and none of the above were counted as having zero network protection measures.

Of the remaining 473 respondents, who selected at least one network protection measure, there were 1730 network protection measures in place, with an average of 3.66 network prevention measures per person. Two (19.33%) was the most common number of network protection measures, followed by zero (16.87%), then three (14.13%).

Update firmware when available (49.03%), use encryption (when available) (42.68%), and check for firmware updates (38.98%) are the most selected IoT device protection measures. However, one of the major weaknesses of IoT devices is that many of them do not have updateable firmware or use encryption. However, only 20.46% of respondents committed to buying only devices with upgradeable firmware and 8.99% are willing to replace insecure devices, so those intentions to perform the top three IoT device protective measures may not be executable with the respondents' current hardware.

Of the 567 respondents to the question, 444 had at least one IoT device protection measure. With a total of 1082 reported protection measures, the 444 respondents average 2.44 device protection measures each. Figure 26 shows the number IoT device protection measures respondents self-reported.

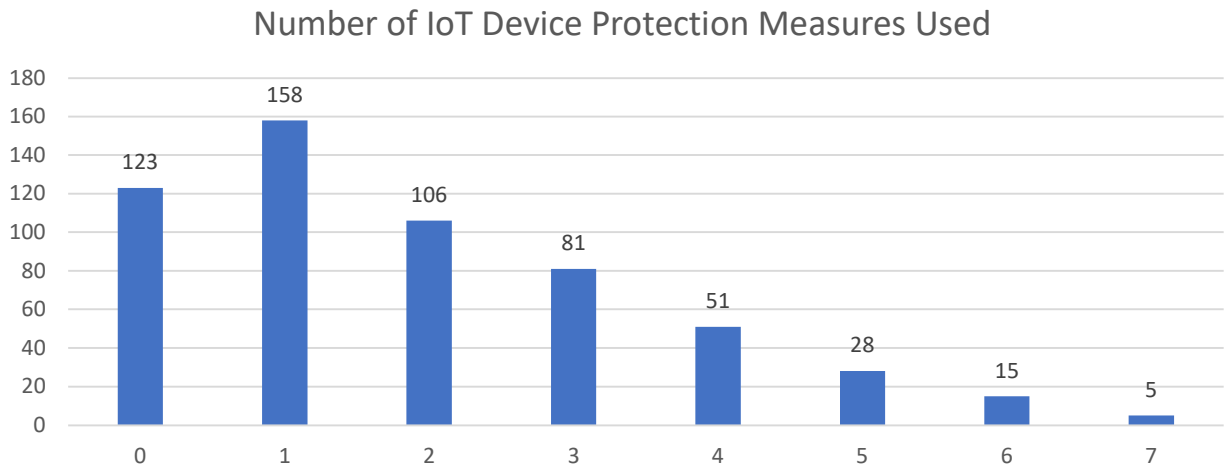

Figure 13 IoT Device Protection Measures Count

Respondents were concerned with self-protection on the Internet, with 444 respondents (78.45%) ranging from somewhat concerned to very concerned. Of the remaining respondents, 22 (3.89%) were neutral, while 100 respondents (17.67%) ranged from somewhat unconcerned to very unconcerned.

When asked about bad experiences on the Internet, 141 respondents (24.78%) had no negative consequences, while the remaining 468 (75.22%) had at least one, for a combined total of 698 negative consequences. Malware infections (280) and hacked accounts (206) were the most common, followed by identity theft (113), having someone pose as them on social media (49), and any other negative consequence (50).

4.6 Locus of Control

Locus of control answers are mostly positive, with 86.4% of respondents exhibiting an internal locus of control concerning their Internet safety, while only 10% demonstrated an external locus of control. The results for self-protection from information security violations at home were even stronger with 90.5% of respondents in agreement that it is within their control to protect themselves from information security violations at home. Fewer respondents felt that

they were primarily responsible for home network protection, with 84.2% believing they were primarily responsible. 89% believed that taking necessary security measures is within their control. The highest number of respondents selected “agree” followed by “somewhat agree”, with “strongly agree” having slightly fewer responses.

4.7 Perceived Self-Efficacy

Perceived self-efficacy responses were not nearly as consistent, as those for locus of control. While respondents had positive responses to comfort taking measures to protect their home network (81.9% agree) and resources and knowledge to protect their home network (71.4%), responses varied markedly on the four subsequent questions. When asked if protecting their home network was hard or easy, 45.3% chose hard, while only 35.7% chose easy. 19% remained neutral. However, anxiety about online security issues was high among respondents with 52.8% agreeing that they feel nervous when thinking about online security issues, compared to 32.3% who disagreed. More respondents agreed that they had the skills to implement preventative measures (61.3%) than did not (28.6%). Additionally, more respondents also rated their skills to stop information security violations as adequate (58.4%) than did not (34.1%).

4.8 Security Intentions (Future)

Security intentions (future) was measured by Likert items requesting respondents indicate the degree to which they agree with the statement given. Additionally, respondents were asked which IoT device protection measures they intended to use in the future.

Question 49 measured users’ likelihood to take action to either protect the Internet or protect themselves. While the answers are similar, there is a slightly different number of each

response. On the positive end of the spectrum, the number of people taking action for self-protection were slightly lower than those protecting the Internet for agree and strongly agree.

Those who selected somewhat agree to strongly agree for changing passwords more often (70.61%) and using passwords that are harder to guess (77.19%) far exceeded those who chose neutral or negative behaviors.

Fewer respondents were committed to increasing their browser security settings at 60.46%. However, respondents overwhelmingly committed to learning to be more secure online at 86.31%. 64.15% of respondents selected a form of agree to keeping guests and IoT devices on a guest network, while 92.75% agreed not to use default passwords.

Respondents have the intention to change their WiFi passwords to more secure passwords (75.19%), while fewer have the intent to change their IP address range and default gateway (50%).

Two hundred ninety-seven respondents answered no to the question, “Will you make any changes to your home network or IoT devices after completing this survey?”, while another sixty-eight respondents skipped the question. Of those sixty-eight respondents who skipped the question, only two of them answered the question about what future IoT device changes they intended to make. However, all of them clicked through to the end of the survey.

The reasons respondents selected for why they don’t intend to change their security are shown in Figure 32. 122 respondents felt their network was already secure enough, while 77 believed their system works just fine as it is, 58 don’t know how to make changes, 46 selected Other, 43 believed selected nothing has happened to them yet, 31 selected that no one wants to get into their network, 23 have someone else manage their home network, while only 22 felt that changing their security configuration is too hard.

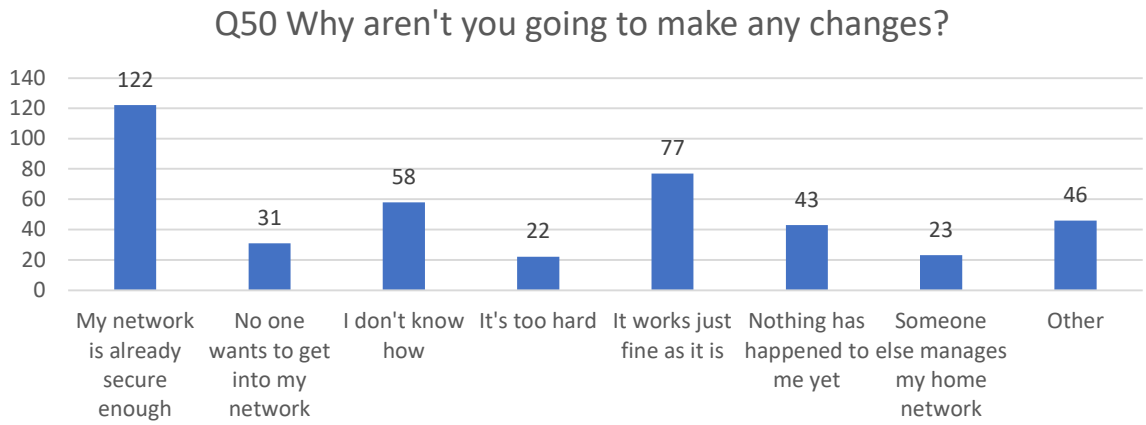

Figure 14 Reasons for not making changes

Through a survey configuration error, those who said they had no intention to make changes in the future were still asked in the future what changes they planned to make to their IoT devices. Even after answering that they planned to make no changes, and providing reasons why, those respondents selected changes that they intend to make. Two hundred twenty-three respondents selected five hundred thirty changes they would make with a mean of 2.3767 changes per person. This number is far below the Security Intentions (Future) average of those who intended to make changes to their network at 5.2303 per person, but well above the zero that would be expected after they expressed that they would not be making changes.

Respondents were able to choose from a range of possible security measures, such as using encryption, purchasing only devices with upgradeable firmware, upgrading firmware, and replacing outdated insecure devices. Using encryption when available had the most responses with eighty-nine, followed by updating firmware when available with eighty-two, and checking for firmware updates regularly was third highest with seventy-five responses. Checking shodan.io was fourth with fifty-six users committing to doing so, followed by only buying devices with upgradeable firmware with fifty-one responses, and reviewing router logs with forty-five. The bottom four options were finding other alternatives that don't need to connect to

the Internet with forty-three responses, place IoT devices on a guest network with forty-two responses, followed by replacing insecure IoT devices even if they are still functional with twenty-four, and other was last with twenty-three responses.

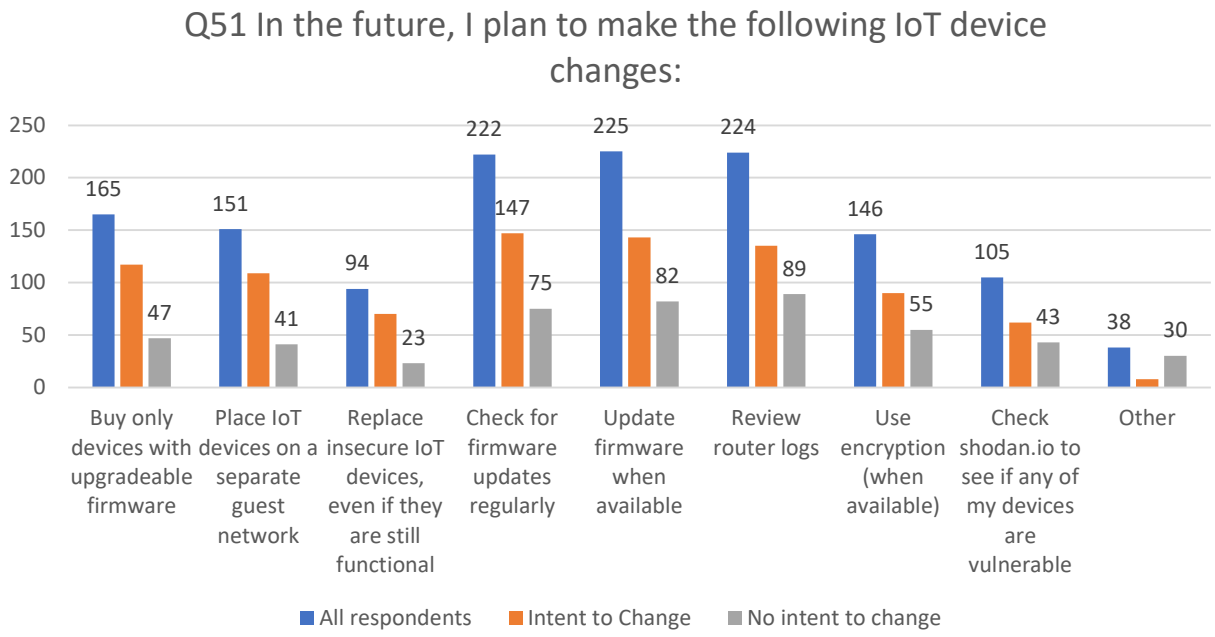

Figure 15 Future IoT Security Intentions

Chapter 5 Quantitative Analysis

In this data set, there are two latent dependent variables, security intentions (existing) and security intentions (future), and 3 independent variables, past performance, locus of control, and self-efficacy. Security intentions (existing) is further divided into security software, network protection measures, and IoT protection measures. Security intentions (future) is comprised of security changes and IoT changes. Past performance incorporates IT/CS related employment, formal education, informal education, internet and email security, and certifications. Self-efficacy and locus of control are not divided into individual questions.

Four of the five elements of security intentions are ratio variables, because there is an absolute zero, or absence of security intentions, and the intervals are equal. A person with two network protection measures has twice as many as a person with one (Warne, 2018). However, the security intentions (future) security changes variable is interval data, as respondents were asked to answer how likely they were to implement each measure, rather than just select those they plan to implement.

IT/CS employment is interval data, assigning value to employment that requires working on a computer, ranging from not working on a computer to working on a computer more than half of the time. Formal education, informal education, and certification count are all ratio data. Internet and email security questions are interval data.

With more than one independent variable and more than one dependent variable, there are two main options, analyzing dependent variables separately with univariate methods, or using a multivariate method, such as structural equation modeling (Warne, 2018). Another text recommended a Spearman rank-order correlation (Creswell, 2009), but that would not provide the same fidelity of information as multiple regression, path modeling or structural equation

modeling. However, Creswell (2009) did recommend multiple regression for two or more independent variables and a single dependent variable.

Given this study's exploratory nature, hierarchical linear regression provided the opportunity for an in-depth look into the relationships between each component of past performance with each component of security intentions, as well as the aggregate effect of past performance. The past performance variables were different types of measures, on different scales, so they could not be combined into a single measure. Hierarchical linear regression also allowed analysis of the overall effect of past performance without the measurements being on the same scale, as well as allowed for exploration of interactions between the independent variables and any indication of a Simpson's paradox (Warne, 2018), where the direction of the effect changes depending upon the addition of other independent variables.

Based on the studies analyzed in the literature review, ten used regression and eleven used partial least squares. The challenge with partial least squares methods is that variables that are on different scales are group together in latent variables, allowing insight only into the whole variable and not the individual components.

However, after reviewing the results of the hierarchical linear regression, which did not show interaction amongst the elements of past performance, locus of control, and self-efficacy, it was important to explore the latent variable constructs of past performance, security intentions (existing) and security intentions (future) to determine the overall effect of the different variables. Partial least squares path modeling is typically used for exploratory studies, when attempting to assess relationships between latent variables.

Structural equation modeling was one of the other options available for analyzing multiple independent variables and multiple dependent variables. While structural equation

modeling is typically used for confirming existing models, it was worth investigating whether the results would be similar to the hierarchical linear regressions and the path modeling analyses.

5.1 Variable Composition

Initially, there were four variables to be measured: past performance, locus of control, perceived self-efficacy, and security intentions. However, only locus of control and perceived self-efficacy had established scales that required only minor alterations to be subject matter specific. Past performance and security intentions were newly developed with minimal items that have been used previously in survey instruments. The past performance variable measured technical education, informal education, and attitudes toward security in typical Internet usage.

Variable Acronym	Group	Variable Description
PP	Past Performance	All elements of past performance
PP_ITCSJob	Past Performance	Whether the respondent has a job that is related to information technology or computer science
PP_FormalEd	Past Performance	Dummy count of types of formal education
PP_InfEd	Past Performance	Dummy count of types of informal education
PP_Likert	Past Performance	Internet and Email security questions
PP_CertCount	Past Performance	Weighted Certificate Scores
LofC	Locus of Control	Respondent belief concerning whether they control their environment or it is controlled externally
SEFF	Self-Efficacy	Respondents' perception of their ability to perform security tasks
SINTEX	Security Intentions (Existing)	Existing Security Intentions (Inclusive of SecSoftware, NetworkPro, and IoTPro)
SINTEX SecSoftware	Security Intentions (Existing)	Security software that respondents self-report currently using
SINTEX_NetworkPro	Security Intentions (Existing)	Network protection measures that respondents self-report currently using
SINTEX_IoTPro	Security Intentions (Existing)	IoT protection measures that respondents self-report currently using
SINTFUT	Security Intentions (Future)	Security changes respondents self-reported they were going to make (inclusive of Changes and IoTChanges)
SINTFUT_Changes	Security Intentions (Future)	(Optional) Changes to network and software respondents intended to make
SINTFUT_IoTChanges	Security Intentions (Future)	Changes to IoT protections respondents intended to make

Table 12 Variable Descriptions

Security intentions variables were the dependent variables, while past performance, locus of control, and self-efficacy were the independent variables. Self-efficacy was also tested as a moderating variable between past performance and security intentions.

5.1.1 Validity

Exploratory factor analysis (EFA) was conducted for past performance, self-efficacy, locus of control, security intention (existing), and security intentions (future). The assumption of multivariate normality was assessed using Mahalanobis distances, plotted against the quantiles of a Chi-Square distribution. All five latent variables met the multivariate normality assumption.

Pearson correlations were calculated to determine intercorrelations for the items comprising each latent variable, all of which exceeded 0.30, making them suitable for factor analysis. The determinant of the correlation table was then calculated to ensure that it exceeds .00001, indicating there is no multicollinearity.

Using the Kaiser Criterion, all factors with an Eigenvalue greater than one are retained.

5.1.2 Reliability

Cronbach's alpha is used to determine the internal consistency of questions to ensure that variables are being accurately measured (Cortina, 1993). By comparing the questions in each block, the questions can be reduced to those that show the most internal consistency, reducing the time participants spend answering similar survey questions. By reducing the number of questions and time to complete the survey, more participants are likely to complete the entire survey. Typically, a Cronbach's alpha above 0.7 is considered acceptable for reliability, in that the questions are measuring the variable they are intended to.

Scale	No. of Items	α
Past_Performance	5	0.72
Locus_of_Control	4	0.79
Self-Efficacy	6	0.87
SINTEX	3	0.75
SINTFUT	17	0.88

Table 13 Cronbach's Alpha for variables

5.1.3 Past Performance

The past performance scale was designed to measure pertinent IT/CS and security education. Formal and informal education were separated from the user's current individual security practices. It is possible to have learned the best security practices, but to not put them in practice due to a myriad of reasons. Due to the changing nature of technology, security

knowledge is ephemeral and can quickly become stale if not used and refreshed on a regular basis, resulting in outdated security practices.

While up to nine questions were asked quantifying education, including job-related education, six had the highest internal consistency, resulting in a Cronbach's alpha of 0.72. Three of the six results counted the number of varying types of formal education, number of IT certifications, number of types of informal education, while the fourth measured whether they have a job that requires computer work. The question about IT/CS accounts for possible on the job training, including organizationally required mandatory computer security training. The fifth and sixth questions asked for the respondents' internet and email security past performance.

For Question 15, the certifications were weighted based on difficulty and subject specificity. A basic IT certification is worth one point, while a basic security certification is worth two, an intermediate IT certification worth three points, an intermediate security certification worth four points, an advanced IT certification worth 5 points and an advanced security certification worth 6 points. This question was focused more on the diversity of education than on the number of total certifications that had been earned. For example, there was no mechanism for a respondent to report multiple certifications at the same difficulty level in the same subject.

Questions 30 and 31 were Likert scale items requesting participants self-report their internet and email security past performance. These were on a scale of 1-5 points, while the remainder of the survey was on a 1-7 scale of Likert items. Question 30 focused on secure Internet usage past performance and Question 31 focused on secure email past performance.

Table 14 displays the summary statistics for the past performance variables. For PP_Cert_Count, skewness is greater than 2 in absolute value, therefore the variable is

asymmetrical about its mean. Due to the kurtosis being greater than or equal to 3, then the variable's distribution is markedly different than a normal distribution.

Variable	*M*	*SD*	*n*	SE_M	Min	Max	Skewness	Kurtosis
PP_Cert_Count	1.48	3.72	569	0.16	0.00	21.00	2.90	8.27
PP_FormalEd	1.33	1.54	569	0.06	0.00	7.00	1.33	1.21
PP_InfEd	2.41	1.83	569	0.08	0.00	6.00	0.03	-1.43
PP_ITCSJob	2.25	1.71	569	0.07	1.00	5.00	0.79	-1.21
PP_Likert	3.58	0.61	544	0.03	1.92	5.00	-0.12	-0.51

Table 14 Summary Statistics for Past Performance

The χ^2 goodness of fit being significant shows that this model may not be the strongest predictor and that other factors may need to be added to improve the model fit.

Factor	Eigenvalue	% of variance	Cumulative %
1	2.33	46.63	46.63

Note: $\chi^2(5) = 48.13$, $p < .001$

Table 15 Past Performance Eigenvalue and Percentage of Variance

The loading for PP_Likert is poor, which would typically warrant removal from the scale. However, it was left in because removal reduced the predictive power of the model and further regression analysis revealed that PP_Likert was extremely important in modeling past performance's relationship to security intentions.

	Factor loading	
Variable	1	Communality
PP_FormalEd	0.88	0.77
PP_InfEd	0.60	0.36
PP_Cert_Count	0.73	0.54
PP_ITCSJob	0.71	0.50
PP_Likert	0.40	0.16

Table 16 Exploratory Factor Analysis Factor Loadings for Past Performance

Due to the items being on different scales, it was imprudent to combine them into a single variable. Therefore, the two Likert items were combined into a single item, while the other four

were maintained separately. They were handled as five separate items in the hierarchical regression analysis.

5.1.4 Locus of Control

The locus of control scale consists of four Likert scale questions designed to measure whether respondents have an internal locus of control, where they believe that they are in control of their own environment, or an external locus of control, where things happen to them. While the means are consistent among items on the scale, the kurtosis of Q39 is slightly above 3, indicating that question does not have a normal distribution.

Variable	*M*	*SD*	*n*	SE_M	Min	Max	Skewness	Kurtosis
Q38	5.44	1.24	567	0.05	1.00	7.00	-1.12	1.21
Q39	5.64	1.23	566	0.05	1.00	7.00	-1.56	3.27
Q40	5.59	1.55	563	0.07	1.00	7.00	-1.45	1.26
Q41	5.65	1.23	565	0.05	1.00	7.00	-1.45	2.53

Table 17 Summary Statistics for Locus of Control

The χ^2 goodness of fit shows that this model is a good fit.

Factor	Eigenvalue	% of variance	Cumulative %
1	2.02	50.50	50.50

Note: $\chi^2(2) = 2.42$, $p = .298$.

Table 18 Locus of Control Eigenvalue and Percentage of Variance

While all loadings are acceptable to good, communality is below the 0.40 threshold for Q40. However, Q40 remained in the model because when it was removed, the predictive power of the model decreased.

	Factor loading	
Variable	**1**	**Communality**
Q38	0.73	0.54
Q39	0.78	0.61
Q40	0.58	0.34
Q41	0.73	0.53

Table 19 Exploratory Factor Analysis Factor Loadings for Locus of Control

Because these items were all on the same 7 point Likert scale, they were combined into a single item by adding the values for each question and calculating the mean of all four values.

5.1.5 Perceived Self-Efficacy

Self-Efficacy was measured through a series of questions to determine the respondents' level of confidence in their ability to secure their home network and devices. The means for these questions vary much more widely than those of locus of control, with a range from 3.76 to 5.40. All data is normally distributed.

Variable	***M***	***SD***	***n***	SE_M	**Min**	**Max**	**Skewness**	**Kurtosis**
Q42	5.40	1.44	564	0.06	1.00	7.00	-1.16	0.84
Q43	4.89	1.64	567	0.07	1.00	7.00	-0.72	-0.31
Q44	3.93	1.51	568	0.06	1.00	7.00	0.10	-0.67
Q45_R	3.76	1.68	566	0.07	1.00	7.00	0.33	-0.91
Q46	4.60	1.63	565	0.07	1.00	7.00	-0.46	-0.76
Q47	4.42	1.79	566	0.08	1.00	7.00	-0.44	-1.04

Table 20 Summary Statistics for Self-Efficacy

The model is not a good fit, based on χ^2 being significant.

Factor	**Eigenvalue**	**% of variance**	**Cumulative %**
1	3.55	59.14	59.14

Note: $\chi^2(9) = 81.57$, $p < .001$.

Table 21 Self-Efficacy Eigenvalue and Percentage of Variance

Q45_R, which asked about respondent anxiety in securing their network and was reverse coded, had low factor loadings and low communality. Like other items, removing Q45_R reduced the predictive power of the model. Therefore, it was placed back in the model.

	Factor loading	
Variable	**1**	**Communality**
Q42	0.81	0.65
Q43	0.90	0.82
Q44	0.69	0.48
Q45_R		0.08
Q46	0.89	0.78
Q47	0.86	0.74

Note: Factor loadings < .32 are suppressed.

Table 22 Exploratory Factor Analysis Factor Loadings for Locus of Control

These items were all on a 7 point Likert scale and were combined into a single mean, like the four items in locus of control.

5.1.6 Security Intentions (Existing)

Due to the inability to evaluate users' self-reported security measures, the term security intentions was used for self-reported current security configuration. This variable measured security software usage, network protection measures, and IoT device protection measures. The network protection mean was higher while the means for IoT protection and security software were closer in value.

Variable	*M*	*SD*	*n*	SE_M	Min	Max	Skewness	Kurtosis
SINTEX_IoTPro	1.93	1.69	569	0.07	0.00	8.00	0.90	0.35
SINTEX_NetworkPro	3.04	2.55	569	0.11	0.00	11.00	0.84	0.11
SINTEX_SecSoftware	1.65	1.41	569	0.06	0.00	6.00	0.51	-0.33

Table 23 Summary Statistics for Security Intentions (Existing)

A Chi-squared value could not be calculated to determine the goodness of fit.

Factor	Eigenvalue	% of variance	Cumulative %
1	1.71	56.84	56.84

Table 24 Eigenvalues and Variance for SINT_EX

All three measures had strong loadings, but IoT protection measures had a low communality. Usually that would result in removal, but exploratory factor analysis requires at least three measures with loadings above 0.32, thus requiring the measure to remain.

	Factor loading	
Variable	1	Communality
SINTEX_SecSoftware	0.75	0.56
SINTEX_NetworkPro	0.91	0.83
SINTEX_IoTPro	0.56	0.31

Table 25 Exploratory Factor Analysis factor loading for SINT_EX

These items were not combined, in order to determine the relationship between the independent variables and each classification of security intention. Each variable is a count of the number of security measures by type.

5.1.6 Security Intentions (Future)

The mean of the 16 item Likert scale was taken as a measure of SINTFUT_Changes. The number of respondents who committed to making changes (n=245) was far lower than the number of respondents for the other variables, due to the question being optional. Only respondents who answered yes to Q48, asking if they planned to make changes, were able to view Q49.

Variable	*M*	*SD*	*n*	SE_M	Min	Max	Skewness	Kurtosis
SINTFUT_Changes	5.24	0.88	245	0.06	1.73	7.00	-0.47	0.82
SINTFUT_IoTChanges	2.59	2.44	569	0.10	0.00	9.00	0.91	-0.05

Table 26 Summary Statistics for Security Intentions (Future)

The model was not a good fit for the data, based on the χ^2 being significant, as shown in Table 27.

Factor	Eigenvalue	% of variance	Cumulative %
1	6.18	36.37	36.37
2	1.20	7.08	43.46

Note: $\chi^2(103) = 150.65$, $p = .002$.

Table 27 Eigenvalues and Variance for SINT_FUT

The factor loadings were low on Q49_10 and SINTFUT_IoTChanges, while the communality was low for Q49_1, Q49_7, Q49_8, Q49_10, and Q49_11. Removing all six items would result in a sharp decrease in the ability to explain variance in security intentions (future).

	Factor loading		
Variable	**1**	**2**	**Communality**
Q49_1	0.46		0.24
Q49_2	0.64		0.44
Q49_3	0.75		0.67
Q49_4	0.69	0.38	0.63
Q49_5	0.69	0.41	0.65
Q49_6	0.65		0.46
Q49_7	0.60		0.36
Q49_8	0.37		0.14
Q49_9	0.59	0.33	0.45
Q49_10			0.07
Q49_11	0.51		0.33
Q49_12	0.63	0.32	0.50
Q49_15	0.67		0.49
Q49_16	0.73		0.53
Q49_17	0.70		0.49
Q49_13	0.73	-0.59	0.88
SINTFUT_IoTChanges			0.06

Table 28 Exploratory Factor Analysis factor loadings for SINT_FUT

All 16 items in Q49 were combined into a single variable, SINTFUT_Changes, while SINTFUT_IoTChanges was kept as a separate variable.

5.2 Hierarchical Linear Regression

Performing a hierarchical linear regression allows the regression to be run by building upon each variable. Past performance cannot be simplified to a single variable, so the hierarchical linear regression allows the regression to be run with the five past performance items and determine the effect of past performance on each security intentions variable.

For the three security intentions (existing) items, a three-step hierarchical regression was performed. The first step measured the effect of the five past performance items, while the second step added perceived self-efficacy, and the third step measured the added effect of locus of control. Neither security intentions (future) item were tested against the security intentions (existing) items because future intentions cannot effect existing intentions.

For the two security intentions (future) items, a four-step hierarchical regression was performed. The first three steps were identical to those for the security intentions (existing) items, while the fourth step added the three security intentions (existing) items to determine the effect of current security intentions on future security intentions.

The statistically significant effects are shown in Figure 34. PP_ITCSJob was not statistically significant in any of the five hierarchical linear regressions. PP_CertCount was only significant for SINTEX_NetworkPro. PP_Likert had the greatest weight amongst independent variables, but was not statistically significant for SINTFUT_IoTChanges.

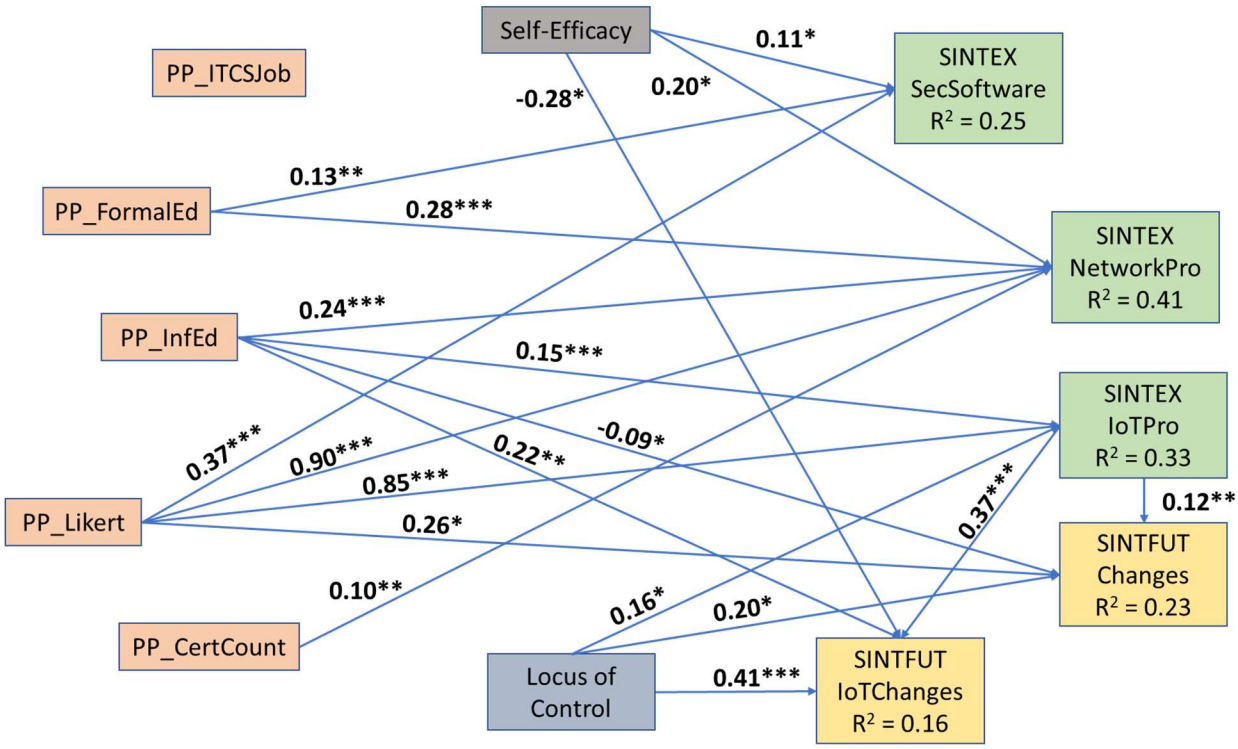

Figure 16 Regression Coefficients

The assumptions for linear regression are that the data is normal, homoscedastic, not multicollinear, and have few or no outliers. For each model, normality was tested using a Q-Q scatter plot, which compares the distribution of the residuals with a normal distribution. The plotted points should follow a mostly straight line, which represents the theoretical quantiles of a normal distribution.

To evaluate homoscedasticity, model residuals were plotted against predicted model values (Osborne & Walters, 2002). To meet the assumption, the points should appear randomly distributed with a mean of zero and not resembling a curve.

Variance Inflation Factors (VIFs) were used to detect the presence of multicollinearity between predictor variables in the model, which can occur when there is a high degree of correlation between predictors. High multicollinearity decreases the statistical power of the model (Yoo et al., 2014), and decreases the reliability of the regression coefficient for the

variable. Variance Inflation Factors greater than 10 indicate high multicollinearity, while VIFs greater than 5 are concerning.

To identify outliers, studentized residuals were calculated and plotted against the observation numbers. Each regression has those outliers identified and plotted.

5.2.1 Security Intentions (Existing) Software Security Measures

Security Intentions (Existing) Software Security Measures, the dependent variable, is comprised of a count of the number of different security software packages that respondents are using and is labeled SINTEX_SecSoftware in the dataset. In Step 1 of the regression, PP_FormalEd, PPInfEd_Count, PP_ITCSJob, PP_Cert_Count, and PP_Likert were the predictor variables entered into the null model. In Step 2, Perceived_Self_Efficacy was added, while in Step 3, Locus_of_Control was added.

The Q-Q scatterplot in Figure 87 below shows a mostly straight line through all three steps of the regression, indicating normality.

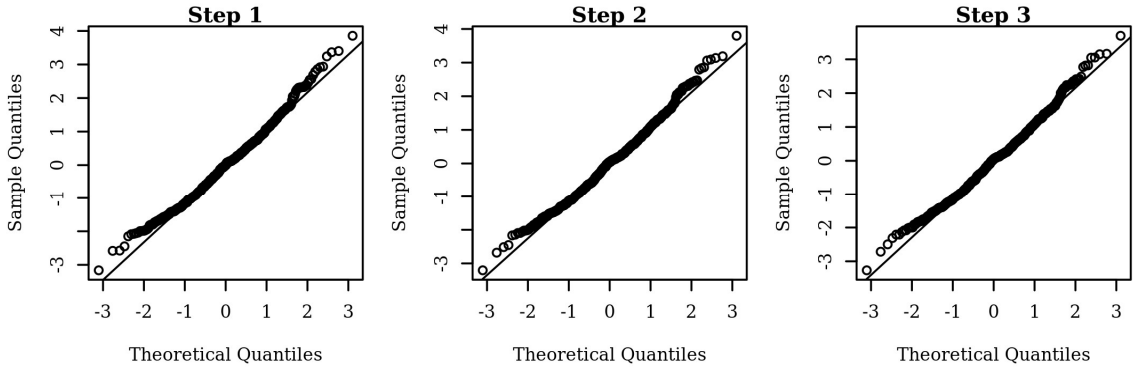

Figure 17 Q-Q Scatterplot for Security Intentions (Existing) Security Software Regressions

The residuals scatterplot in Figure 36 shows data with a mean of zero and no curvature, thus indicating the data meets the homoscedasticity assumption.

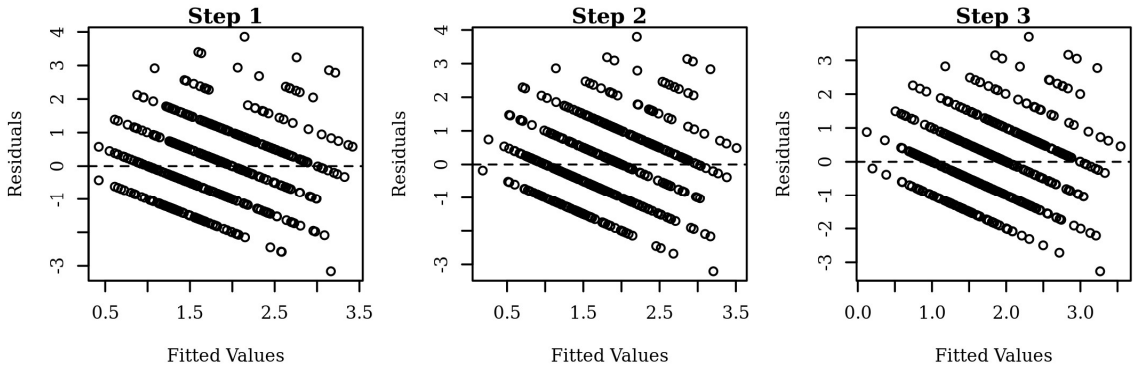

Figure 18 Residuals Scatterplot for Security Intentions (Existing) Security Software Regressions

The Variance Inflation Factors (VIFs) in the chart below are all below 5 for Steps 1-3 of the regression.

Variable	VIF	Variable	VIF	Variable	VIF
Step 1		Step 2		Step 3	
PP_FormalEd	2.49	PP_FormalEd	2.49	PP_FormalEd	2.51
PP_InfEd	1.53	PP_InfEd	1.58	PP_InfEd	1.58
PP_ITCSJob	1.77	PP_ITCSJob	1.79	PP_ITCSJob	1.79
PP_Cert_Count	1.94	PP_Cert_Count	1.95	PP_Cert_Count	1.96
PP_Likert	1.2	PP_Likert	1.41	PP_Likert	1.42
		Perceived_Self_Efficacy	1.49	Perceived_Self_Efficacy	2.09
				Locus_of_Control	1.65

Table 29 Variance Inflation Factors for SINT_EX Security Software Regressions

One observation with a Studentized residual greater than 3.11 in absolute value, the 0.999 quartile of a *t* distribution with 524 degrees of freedom, had significant influence on the results of the model.

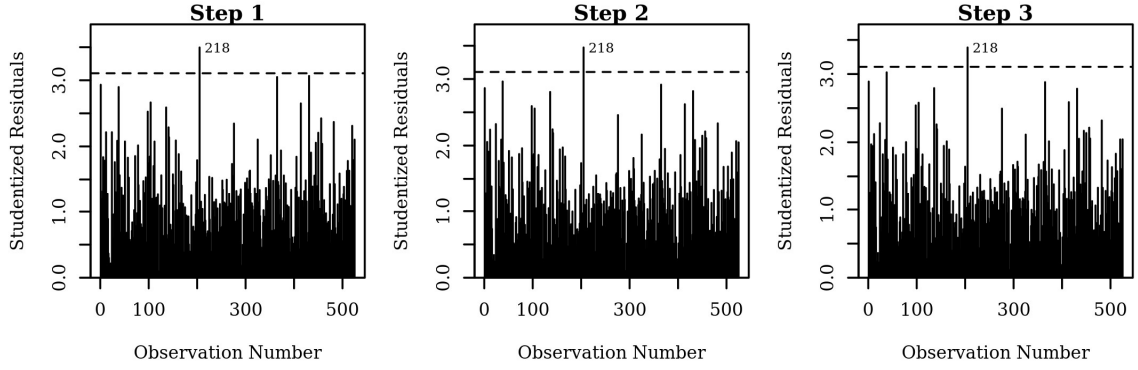

Figure 19 Outliers in SINT_EX Security Software Regressions

The *F*-test for Step 1 was significant, F (5,519) = 32.27, p<.001, $\Delta R^2 = 0.24$, indicating the five measured items explained 23.72% of the variation in SINTEX_SecSoftware. The Step 2 *F*-test was also significant, $F(1,518)=10.12$, $p=.002$, $\Delta R^2 = 0.01$, indicating that Perceived_Self_Efficacy accounted for 1.46% of the variation in SINTEX_SecSoftware.

The *F*-test for Step 3 was not significant, $F(1,157)=1.59$, $p=.207$, $\Delta R^2 = 0.00$, demonstrating that Locus_of_Control did not account for any additional variation in the model. Together, past performance and perceived self-efficacy accounted for 25.18% of the variation in SINTEX_SecSoftware.

Model	R^2	df_{mod}	df_{res}	F	p	ΔR^2
Step 1	0.24	5	519	32.27	< .001	0.24
Step 2	0.25	1	518	10.12	0.002	0.01
Step 3	0.25	1	517	1.59	0.207	0

Table 30 SINT_EX Security Software Model Summary

Significant past performance predictors in the model were PP_FormalEd, $B = 0.13$, $t(517) = 2.63$, $p = .009$; PP_InfEd, $B = 0.12$, $t(517) = 3.51$, $p < .001$; and PP_Likert, $B = 0.37$, $t(517) = 3.85$, $p < .001$. Perceived_Self_Efficacy, $B = 0.11$, $t(517) = 2.01$, $p = .045$, was also a significant predictor.

The hypothesis for this regression was:

H_1: Locus of control, perceived self-efficacy, and past performance predict security intentions (existing) security software usage.

H_1 is partially supported. Three of five past performance variables (formal education, informal education, and internet and email security) and perceived self-efficacy were statistically significant predictors, while locus of control was not.

Variable	*B*	*SE*	CI	β	*t*	*p*
Step 1						
(Intercept)	-0.55	0.30	[-1.14, 0.04]	0.00	-1.82	.070
PP_FormalEd	0.13	0.05	[0.03, 0.23]	0.15	2.54	.011
PP_InfEd	0.13	0.03	[0.07, 0.20]	0.19	4.06	< .001
PP_ITCSJob	0.02	0.04	[-0.05, 0.10]	0.03	0.61	.543
PP_Cert_Count	0.01	0.02	[-0.02, 0.05]	0.04	0.72	.474
PP_Likert	0.49	0.09	[0.32, 0.66]	0.23	5.59	< .001
Step 2						
(Intercept)	-0.73	0.30	[-1.33, -0.13]	0.00	-2.41	.016
PP_FormalEd	0.13	0.05	[0.03, 0.22]	0.15	2.53	.012
PP_InfEd	0.12	0.03	[0.05, 0.18]	0.17	3.48	< .001
PP_ITCSJob	0.01	0.04	[-0.06, 0.09]	0.02	0.31	.753
PP_Cert_Count	0.01	0.02	[-0.03, 0.04]	0.02	0.46	.646
PP_Likert	0.38	0.09	[0.19, 0.56]	0.18	3.99	< .001
Perceived_Self_Efficacy	0.15	0.05	[0.06, 0.24]	0.15	3.18	.002
Step 3						
(Intercept)	-0.95	0.35	[-1.64, -0.26]	0.00	-2.72	.007
PP_FormalEd	0.13	0.05	[0.03, 0.23]	0.16	2.63	.009
PP_InfEd	0.12	0.03	[0.05, 0.18]	0.17	3.51	< .001
PP_ITCSJob	0.01	0.04	[-0.06, 0.09]	0.02	0.33	.739
PP_Cert_Count	0.01	0.02	[-0.03, 0.04]	0.02	0.39	.696
PP_Likert	0.37	0.09	[0.18, 0.55]	0.17	3.85	< .001
Perceived_Self_Efficacy	0.11	0.06	[0.00, 0.22]	0.11	2.01	.045
Locus_of_Control	0.08	0.06	[-0.04, 0.20]	0.06	1.26	.207

Table 31 Regression Results for Security Software

The internet and email security Likert questions have the greatest influence with a *B* value of 0.37, followed by formal education with *B* value of 0.13, informal education with a *B* value of 0.12, and perceived self-efficacy with a *B* value of 0.11. The unstandardized regression equation to predict Security Intentions (Existing) Security Software is:

SINTEX_SecSoftware = 0.13*PP_FormalEdCount + 0.12*PP_InfEd + 0.01*PP_ITCSJob + 0.01*PP_Cert_Count + 037*PP_Likert + 0.11*Perceived_Self_Efficacy + 0.08*Locus_of_Control - 0.95.

5.2.2 Security Intentions (Existing) Network Protection Measures

Security Intentions (Existing) Network Protection Measures, the dependent variable, is comprised of a count of the number of different network security measures that respondents self-reported and is labeled SINTEX_NetworkPro in the dataset. In Step 1 of the regression, PP_FormalEd, PPInfEd, PP_ITCSJob, PP_Cert_Count, and PP_Likert were the predictor variables entered into the null model. In Step 2, Perceived_Self_Efficacy was added, while in Step 3, Locus_of_Control was added.

The Q-Q scatterplot in Figure 20 below shows a mostly straight line through all three steps of the regression, indicating normality.

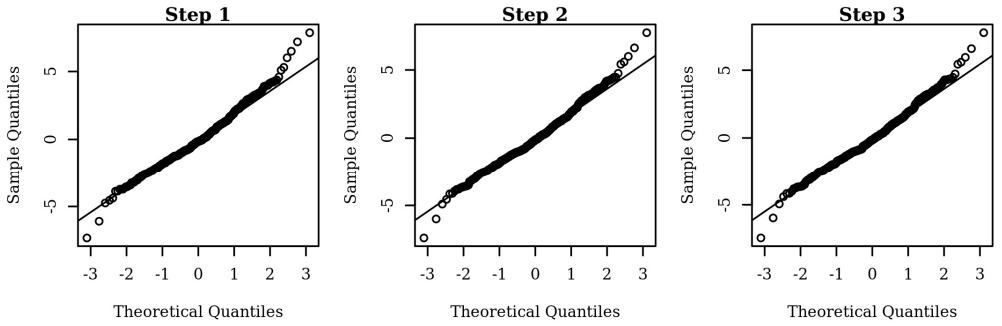

Figure 20 Q-Q Scatterplot for Security Intentions (Existing) Network Protection Regressions

The residuals scatterplot in Figure 21 shows data with a mean of zero and no curvature, thus indicating the data meets the homoscedasticity assumption.

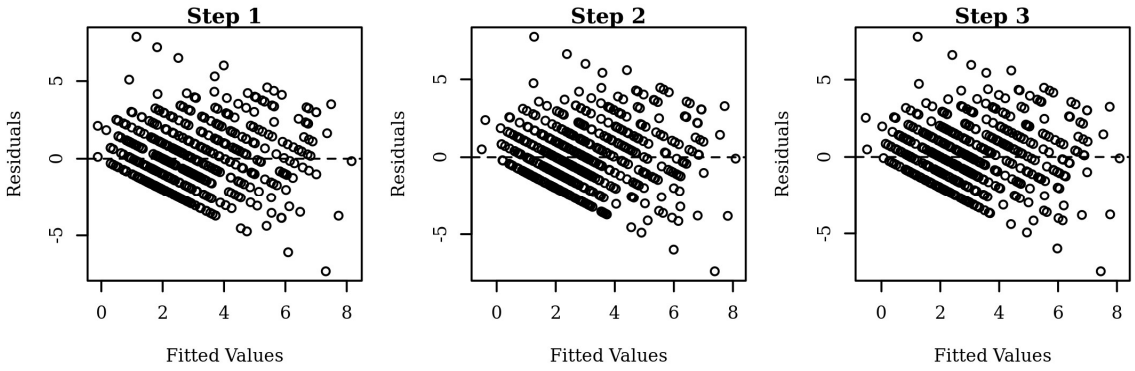

Figure 21 Residuals Scatterplot for Security Intentions (Existing) Network Protections Regressions

The Variance Inflation Factors (VIFs) in the chart below are all below 5 for Steps 1-3 of the regression.

Variable	VIF	Variable	VIF	Variable	VIF
Step 1		Step 2		Step 3	
PP_FormalEd	2.49	PP_FormalEd	2.49	PP_FormalEd	2.51
PP_InfEd	1.53	PP_InfEd	1.58	PP_InfEd	1.58
PP_ITCSJob	1.77	PP_ITCSJob	1.79	PP_ITCSJob	1.79
PP_Cert_Count	1.94	PP_Cert_Count	1.95	PP_Cert_Count	1.96
PP_Likert	1.2	PP_Likert	1.41	PP_Likert	1.42
		Perceived_Self_Efficacy	1.49	Perceived_Self_Efficacy	2.09
				Locus_of_Control	1.65

Table 32 Variance Inflation Factors in Security Intentions (Existing) Network Protections Regressions

Five observations were considered outliers with Studentized residuals greater than 3.11, the 0.999 quartile of a *t* distribution with 524 degrees of freedom. Figure 23 shows those observations.

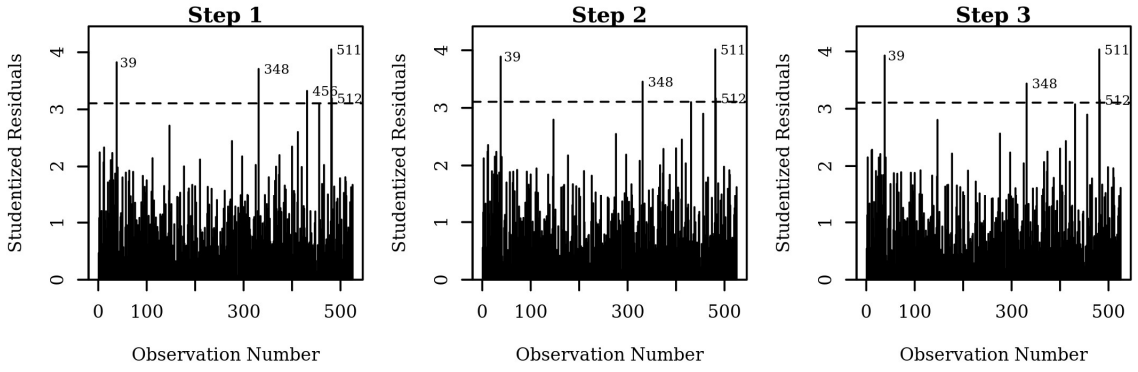

Figure 22 Outliers in Security Intentions (Existing) Network Protections Regressions

The *F*-test for past performance was significant, $F(5,519)=70.42$, p<.001, $\Delta R^2 = 0.40$, indicating that the past performance items account for 40.42% of the variation in SINTEX_NetworkPro. The *F*-test for Step 2 was also significant, $F(1,518)=8.37$, $p=.004$, $\Delta R^2 = 0.01$, indicating that Perceived_Self_Efficacy explained 0.95% of the variation in SINTEX_NetworkPro. Again, the *F*-test for Step 3 was not significant, $F(1,517)=0.61$, $p=.436$, $\Delta R^2 = 0.00$, indicating that Locus_of_Control does not add to the predictive power of the model.

Past performance and perceived self-efficacy accounted for a total of 41.37% of the variation in SINTEX_NetworkPro.

Model	R^2	df_{mod}	df_{res}	F	p	ΔR^2
Step 1	0.40	5	519	70.42	< .001	0.40
Step 2	0.41	1	518	8.37	.004	0.01
Step 3	0.41	1	517	0.61	.436	0.00

Table 33 Network Protections Model Summary

PP_FormalEd, $B = 0.28$, $t(517) = 3.20$, $p = .001$, PP_InfEd, $B = 0.24$, $t(517) = 4.06$, $p < .001$, PP_Cert_Count, $B = 0.10$, $t(517) = 3.02$, $p = .003$, and PP_Likert, $B = 0.90$, $t(517) = 5.35$, $p < .001$, were the past performance significant predictors. Perceived_Self_Efficacy was a significant predictor, $B = 0.20$, $t(517) = 2.02$, $p = .044$. Locus_of_Control did not have a significant effect on SINTEX_NetworkPro.

The hypothesis for this regression was:

H_2: Locus of control, perceived self-efficacy, and past performance predict security intentions (existing) network protection measures.

H_2 was partially supported. Past performance variables, excluding past performance (IT/CS job), and perceived self-efficacy were significant predictors, while locus of control was not.

Variable	*B*	*SE*	CI	β	*t*	*p*
Step 1						
(Intercept)	-2.35	0.53	[-3.39, -1.31]	0.00	-4.44	< .001
PP_FormalEd	0.28	0.09	[0.10, 0.45]	0.17	3.15	.002
PP_InfEd	0.27	0.06	[0.15, 0.38]	0.19	4.58	< .001
PP_ITCSJob	0.13	0.07	[-0.00, 0.26]	0.09	1.96	.050
PP_Cert_Count	0.11	0.03	[0.04, 0.17]	0.16	3.29	.001
PP_Likert	1.09	0.16	[0.79, 1.40]	0.26	7.05	< .001
Step 2						
(Intercept)	-2.65	0.54	[-3.70, -1.60]	0.00	-4.95	< .001
PP_FormalEd	0.28	0.09	[0.10, 0.45]	0.17	3.15	.002
PP_InfEd	0.24	0.06	[0.12, 0.35]	0.17	4.04	< .001
PP_ITCSJob	0.11	0.07	[-0.02, 0.24]	0.08	1.70	.090
PP_Cert_Count	0.10	0.03	[0.04, 0.16]	0.14	3.07	.002
PP_Likert	0.91	0.17	[0.58, 1.24]	0.22	5.45	< .001
Perceived_Self_Efficacy	0.24	0.08	[0.08, 0.41]	0.12	2.89	.004
Step 3						
(Intercept)	-2.89	0.62	[-4.11, -1.67]	0.00	-4.67	< .001
PP_FormalEd	0.28	0.09	[0.11, 0.45]	0.17	3.20	.001
PP_InfEd	0.24	0.06	[0.12, 0.35]	0.17	4.06	< .001
PP_ITCSJob	0.11	0.07	[-0.02, 0.24]	0.08	1.71	.088
PP_Cert_Count	0.10	0.03	[0.03, 0.16]	0.14	3.02	.003
PP_Likert	0.90	0.17	[0.57, 1.23]	0.21	5.35	< .001
Perceived_Self_Efficacy	0.20	0.10	[0.01, 0.39]	0.10	2.02	.044
Locus_of_Control	0.08	0.11	[-0.13, 0.29]	0.03	0.78	.436

Table 34 Regression Results for Network Protections

The internet and email security questions had the greatest influence on network security protections, with a *B* value of 0.90, followed by PP_FormalEd, with a *B* value of 0.28, PP_InfEd, with a *B* value of 0.24, and perceived self-efficacy with a *B* value of 0.20. The unstandardized regression equation is:

PP_NetworkPro_Count = 0.28*PP_FormalEd + 0.24*PP_InfEd + 0.11*PP_ITCSJob + 0.10*PP_Cert_Count + 0.90*PP_Likert + 0.20*Perceived_Self_Efficacy + 0.08*Locus_of_Control – 2.89.

5.2.3 Security Intentions (Existing) IoT Device Protection Measures

Security Intentions (Existing) IoT Device Protection Measures, the dependent variable, is comprised of a count of the number of different network security measures that respondents self-reported and is labeled SINTEX_IoTPro in the dataset. In Step 1 of the regression, PP_FormalEd, PPInfEd, PP_ITCSJob, PP_Cert_Count, and PP_Likert were the predictor variables entered into the null model. In Step 2, Perceived_Self_Efficacy was added, while in Step 3, Locus_of_Control was added.

The Q-Q scatterplot in Figure 24 shows a mostly straight line through all three steps of the regression, indicating normality.

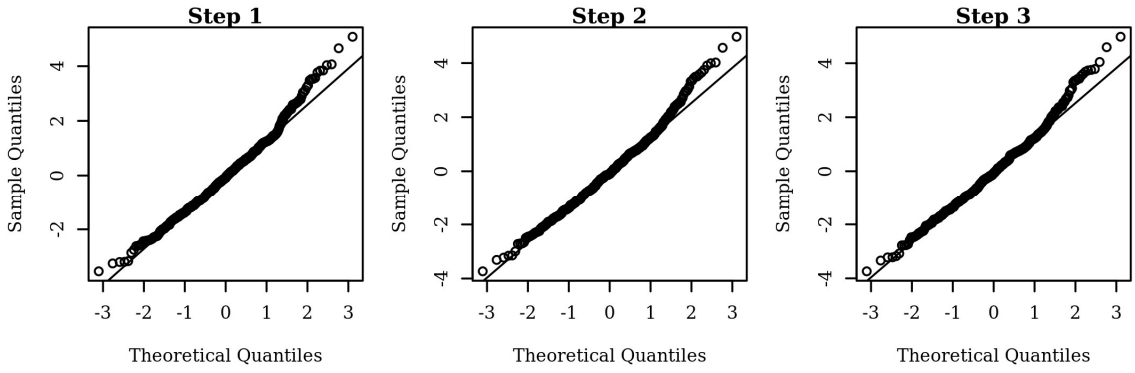

Figure 23 Q-Q Scatterplot for Security Intentions (Existing) IoT Protections

The residuals scatterplot in Figure 25 shows data with a mean of zero and no curvature, thus indicating the data meets the homoscedasticity assumption.

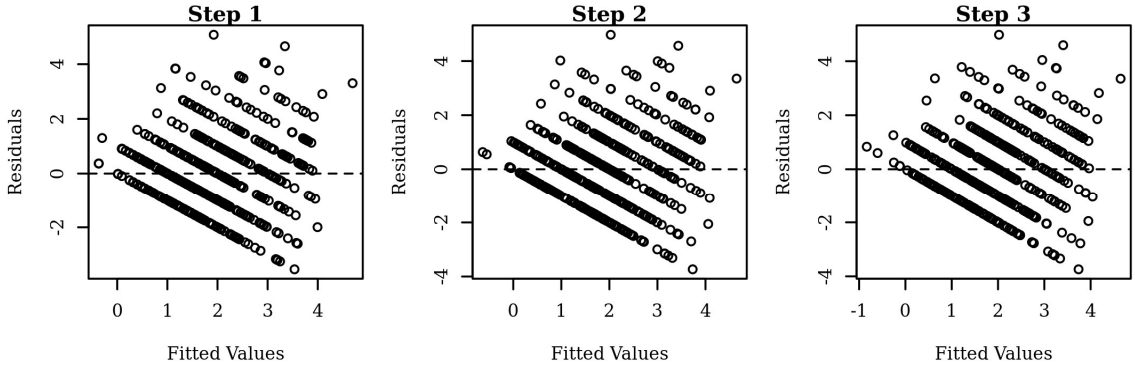

Figure 24 Residuals Scatterplot for IoT Protections

The Variance Inflation Factors (VIFs) in the chart below are all below 5 for Steps 1-3 of the regression.

Variable	VIF	Variable	VIF	Variable	VIF
Step 1		Step 2		Step 3	
PP_FormalEd	2.49	PP_FormalEd	2.49	PP_FormalEd	2.51
PP_InfEd	1.53	PP_InfEd	1.58	PP_InfEd	1.58
PP_ITCSJob	1.77	PP_ITCSJob	1.79	PP_ITCSJob	1.79
PP_Cert_Count	1.94	PP_Cert_Count	1.95	PP_Cert_Count	1.96
PP_Likert	1.2	PP_Likert	1.41	PP_Likert	1.42
		Perceived_Self_Efficacy	1.49	Perceived_Self_Efficacy	2.09
				Locus_of_Control	1.65

Table 35 Variance Inflation Factors for IoT Protections

Two observations with a Studentized residual greater than 3.11 in absolute value, the 0.999 quartile of a *t* distribution with 524 degrees of freedom, had significant influence on the results of the model.

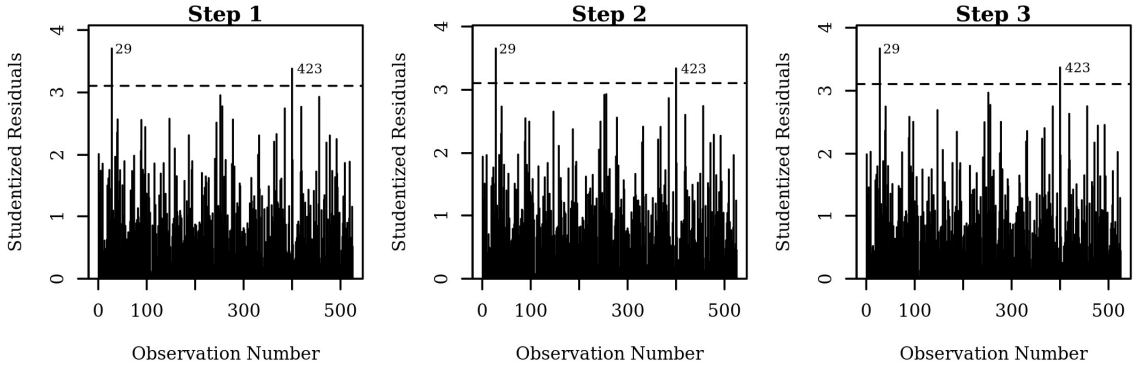

Figure 25 Outliers in IoT Protections

The *F*-test for Step 1 was significant, F (5, 519) = 47.40, $p < .001$, $\Delta R^2 = 0.31$. This model indicates that adding PP_FormalEd, PP_InfEd, PP_ITCSJob, PP_Cert_Count, and PP_Likert explained an additional 31.35% of the variation in SINTEX_IoTPro. The *F*-test for Step 2 was significant, F (1, 518) = 7.86, $p = .005$, $\Delta R^2 = 0.01$. This model indicates that adding

Perceived_Self_Efficacy explained an additional 1.03% of the variation in SINTEX_IoTPro. The *F*-test for Step 3 was significant, F (1, 517) = 4.44, p = .036, ΔR^2 = 0.01. This model indicates that adding Locus_of_Control explained an additional 0.58% of the variation in SINTEX_IoTPro. Past performance, perceived self-efficacy, and locus of control together account for 32.96% of the variation in SINTEX_IoTPro.

Model	R^2	df_{mod}	df_{res}	F	p	ΔR^2
Step 1	0.31	5	519	47.40	< .001	0.31
Step 2	0.32	1	518	7.86	.005	0.01
Step 3	0.33	1	517	4.44	.036	0.01

Table 36 IoT Protections Model Summary

The two significant past performance predictors were PP_InfEd, B = 0.15, t(517) = 3.59, p < .001 and PP_Likert, B = 0.85, t(517) = 7.15, p < .001. A one unit increase in PP_InfEd will increase SINTEX_IoTPro by 0.15 units, while a one unit increase of PP_Likert will increase SINTEX_IoTPro by 0.85 units. Perceived_Self_Efficacy did not significantly predict SINTEX_IoTPro in the third step of the model, but did during the second step. Locus_of_Control significantly predicted SINTEX_IoTPro, B = 0.16, t(517) = 2.11, p = .036. A one unit increase in Locus of Control increases SINTEX_IoTPro by 0.16 units.

The hypothesis for this regression was:

H_3: Locus of control, perceived self-efficacy, and past performance predict security intentions (existing) IoT protection measures.

H_3 was partially supported. Past performance (informal education), past performance (internet and email security), and locus of control were significant predictors, while perceived self-efficacy was not.

Variable	*B*	*SE*	CI	β	*t*	*p*
Step 1						
(Intercept)	-2.33	0.37	[-3.07, -1.60]	0.00	-6.23	< .001
PP_FormalEd	0.07	0.06	[-0.05, 0.19]	0.06	1.09	.277
PP_InfEd	0.17	0.04	[0.09, 0.25]	0.18	4.06	< .001
PP_ITCSJob	0.05	0.05	[-0.05, 0.14]	0.05	0.98	.325
PP_Cert_Count	0.04	0.02	[-0.00, 0.09]	0.09	1.79	.074
PP_Likert	1.00	0.11	[0.78, 1.21]	0.36	9.08	< .001
Step 2						
(Intercept)	-2.54	0.38	[-3.28, -1.79]	0.00	-6.69	< .001
PP_FormalEd	0.07	0.06	[-0.06, 0.19]	0.06	1.07	.285
PP_InfEd	0.15	0.04	[0.07, 0.23]	0.16	3.53	< .001
PP_ITCSJob	0.03	0.05	[-0.06, 0.13]	0.04	0.73	.469
PP_Cert_Count	0.04	0.02	[-0.01, 0.08]	0.08	1.57	.118
PP_Likert	0.87	0.12	[0.64, 1.10]	0.32	7.37	< .001
Perceived_Self_Efficacy	0.17	0.06	[0.05, 0.28]	0.12	2.80	.005
Step 3						
(Intercept)	-3.00	0.44	[-3.86, -2.14]	0.00	-6.86	< .001
PP_FormalEd	0.08	0.06	[-0.04, 0.20]	0.07	1.24	.215
PP_InfEd	0.15	0.04	[0.07, 0.23]	0.16	3.59	< .001
PP_ITCSJob	0.04	0.05	[-0.06, 0.13]	0.04	0.76	.448
PP_Cert_Count	0.03	0.02	[-0.01, 0.08]	0.07	1.45	.146
PP_Likert	0.85	0.12	[0.61, 1.08]	0.31	7.15	< .001
Perceived_Self_Efficacy	0.09	0.07	[-0.05, 0.22]	0.06	1.24	.214
Locus_of_Control	0.16	0.08	[0.01, 0.31]	0.10	2.11	.036

Table 37 Regression Results for IoT Protections

The unstandardized regression equation for Security Intentions (Existing) IoT Protection Measures is:

SINTEX_IoTPro = 0.08*PP_FormalEd + 0.15*PP_InfEd + 0.04*PP_ITCSJob + 0.03*PP_Cert_Count + 0.85*PP_Likert + 0.09*Perceived_Self_Efficacy + 0.16*Locus_of_Control – 3.00.

5.2.4 Security Intentions (Future) Security Changes

Security Intentions (Future) Security Changes, the dependent variable, is comprised of a count of the number of changes the respondents plan to make to their existing security configuration, labeled SINTFUT_Changes in the dataset. In Step 1 of the regression, PP_FormalEd, PPInfEd_Count, PP_ITCSJob, PP_Cert_Count, and PP_Likert were the predictor variables entered into the null model. In Step 2, Perceived_Self_Efficacy was added, in Step 3, Locus_of_Control was added, while in Step 4, SINTEX_SecSoftware, SINTEX_NetworkPro, and SINTEX_IoTPro were added.

The Q-Q scatterplot in Figure 28 shows a mostly straight line through all four steps of the regression, indicating normality.

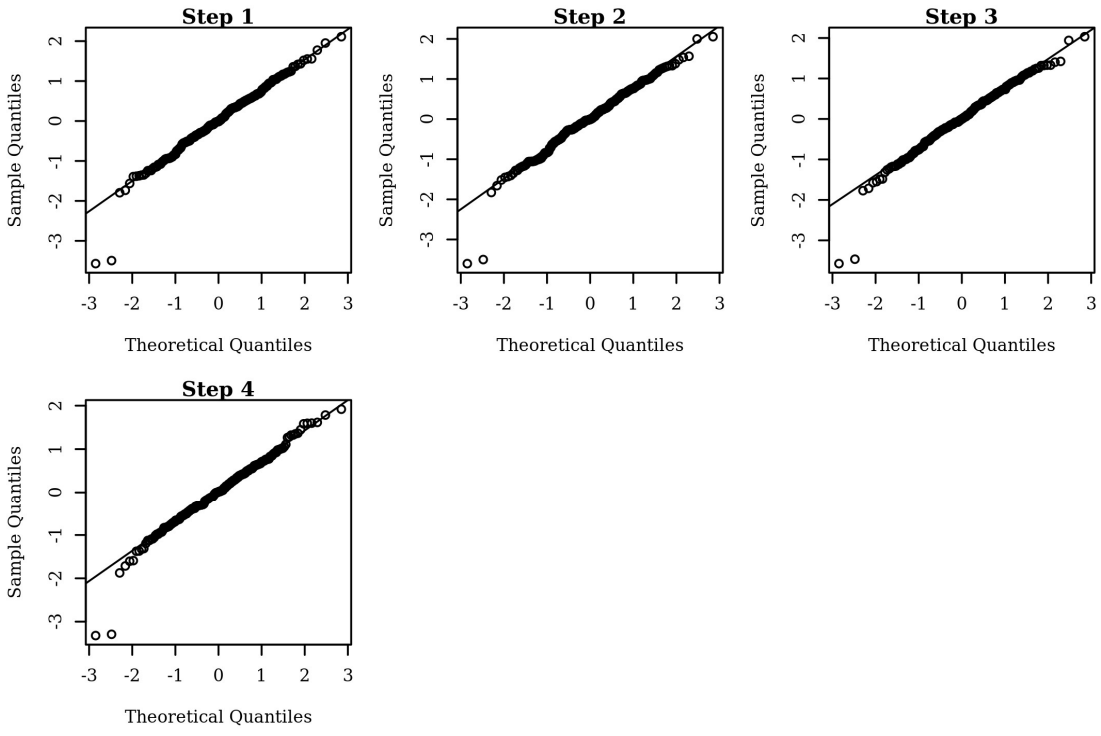

Figure 26 Q-Q Scatterplot for Security Intentions (Future) Changes

The residuals scatterplot in Figure 29 shows data with a mean of zero and no curvature, thus indicating the data meets the homoscedasticity assumption.

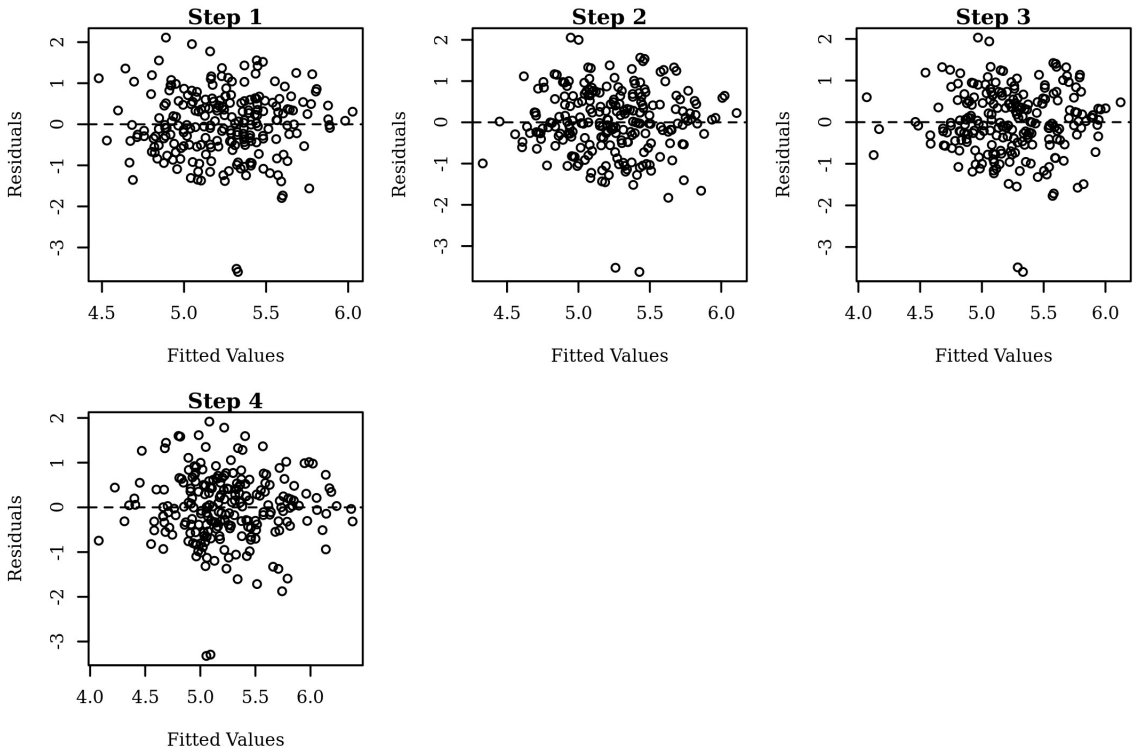

Figure 27 Residuals Scatterplot for Future Changes

The Variance Inflation Factors (VIFs), shown in the chart below, are all below 5 for Steps 1-4 of the regression.

Variable	VIF	Variable	VIF	Variable	VIF
Step 1		**Step 3**		**Step 4**	
PP_FormalEd	2.21	PP_FormalEd	2.24	PP_FormalEd	2.29
PP_InfEd	1.47	PP_InfEd	1.52	PP_InfEd	1.66
PP_ITCSJob	1.72	PP_ITCSJob	1.72	PP_ITCSJob	1.73
PP_Cert_Count	1.75	PP_Cert_Count	1.78	PP_Cert_Count	1.83
PP_Likert	1.14	PP_Likert	1.24	PP_Likert	1.48
Step 2		Perceived_Self_Efficacy	1.72	Perceived_Self_Efficacy	1.76
PP_FormalEd	2.22	Locus_of_Control	1.45	Locus_of_Control	1.46
PP_InfEd	1.51			SINTEX_SecSoftware	1.79
PP_ITCSJob	1.72			SINTEX_NetworkPro	2.5
PP_Cert_Count	1.78			SINTEX_IoTPro	1.45
PP_Likert	1.23				
Perceived_Self_Efficacy	1.3				

Table 38 Variance Inflation Factors for Future Changes

Two observations with a Studentized residual greater than 3.13 in absolute value, the 0.999 quartile of a *t* distribution with 227 degrees of freedom, had significant influence on the results of the model.

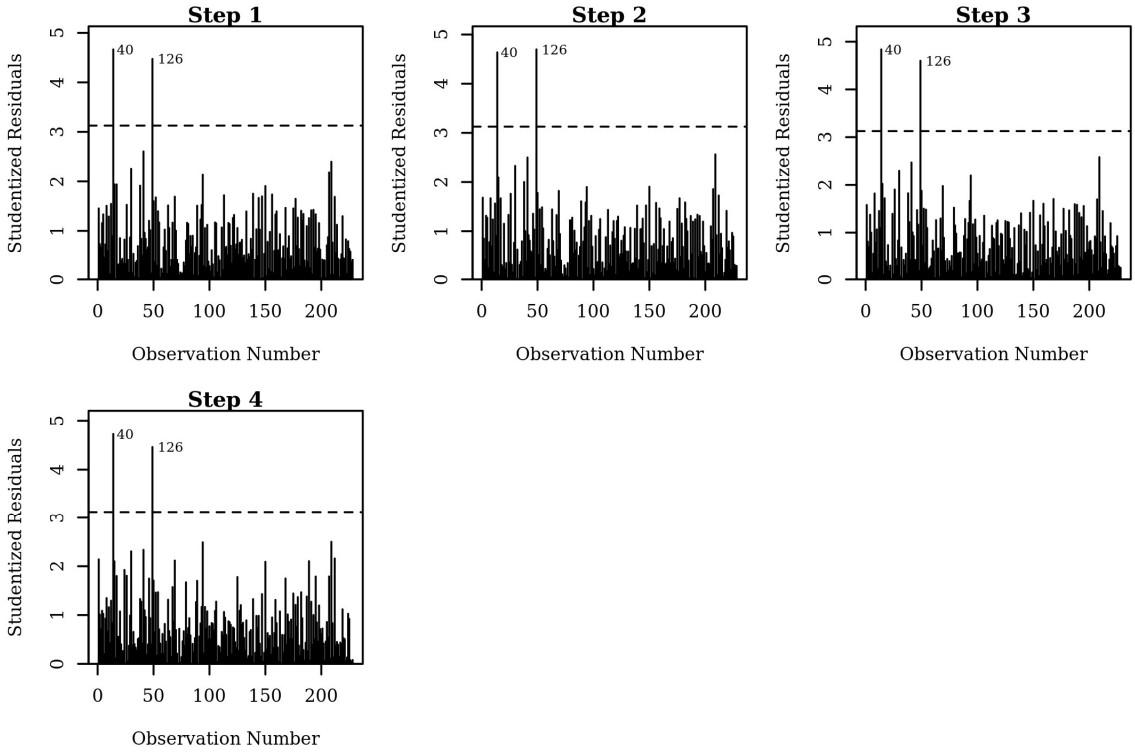

Figure 28 Outliers in Future Changes

The *F*-test for Step 1 was significant, F (5,222) = 6.08, $p < .001$, $\Delta R^2 = 0.12$. This model indicates PP_FormalEd, PP_InfEd, PP_ITCSJob, PP_Cert_Count, and PP_Likert explains 12.05% of the variation in SINTFUT_Changes. The *F*-test for Step 2 was significant, F (1, 221) = 6.82, $p = .010$, $\Delta R^2 = 0.03$. This model indicates that adding Perceived_Self_Efficacy explained an additional 2.63% of the variation in SINTFUT_Changes. The *F*-test for Step 3 was significant, F (1, 220) = 8.84, $p = .003$, $\Delta R^2 = 0.03$. This model indicates that adding Locus_of_Control explained an additional 3.30% of the variation in SINTFUT_Changes. The *F*-test for Step 4 was significant, F (3, 217) = 4.89, $p = .003$, $\Delta R^2 = 0.05$. This model indicates that adding SINTEX_SecSoftware, SINTEX_NetworkPro, and SINTEX_IoTPro explained an

additional 5.20% of the variation in SINTFUT_Changes. Past performance, perceived self-efficacy, locus of control, and security intentions (existing) accounted for a total of 23.18% of the variance in SINTFUT_Changes.

Model	R^2	df_{mod}	df_{res}	F	p	ΔR^2
Step 1	0.12	5	222	6.08	< .001	0.12
Step 2	0.15	1	221	6.82	.010	0.03
Step 3	0.18	1	220	8.84	.003	0.03
Step 4	0.23	3	217	4.89	.003	0.05

Table 39 Future Changes Model Summary

PP_InfEd significantly predicted SINTFUT_Changes, B = -0.09, $t(217)$ = -2.34, p = .020, indicating that a one-unit increase of PP_InfEd will decrease the value of SINTFUT_Changes by 0.09 units. Locus_of_Control significantly predicted SINTFUT_Changes, B = 0.20, $t(217)$ = 2.79, p = .006. SINTEX_IoTPro significantly predicted SINTFUT_Changes, B = 0.12, $t(217)$ = 2.92, p = .004.

The hypothesis for this regression was:

H_4: Locus of control, perceived self-efficacy, past performance, and security intentions (existing) predict security intentions (future) security changes.

H_4 was partially supported. Past performance (informal education), locus of control, and security intentions (existing) IoT protection measures were significant predictors.

Variable	*B*	*SE*	CI	β	*t*	*p*
Step 1						
(Intercept)	3.56	0.35	[2.86, 4.25]	0.00	10.02	< .001
PP_FormalEd	-0.03	0.06	[-0.15, 0.08]	-0.06	-0.59	.553
PP_InfEd	-0.04	0.04	[-0.11, 0.04]	-0.08	-1.01	.311
PP_ITCSJob	-0.05	0.04	[-0.13, 0.04]	-0.09	-1.06	.288
PP_Cert_Count	0.03	0.02	[-0.01, 0.08]	0.12	1.39	.166
PP_Likert	0.52	0.10	[0.32, 0.72]	0.35	5.13	< .001
Step 2						
(Intercept)	3.25	0.37	[2.52, 3.97]	0.00	8.78	< .001
PP_FormalEd	-0.04	0.06	[-0.16, 0.07]	-0.07	-0.74	.459
PP_InfEd	-0.05	0.04	[-0.13, 0.02]	-0.11	-1.44	.152
PP_ITCSJob	-0.05	0.04	[-0.13, 0.04]	-0.09	-1.13	.259
PP_Cert_Count	0.03	0.02	[-0.02, 0.07]	0.09	1.07	.286
PP_Likert	0.45	0.10	[0.25, 0.66]	0.30	4.33	< .001
Perceived_Self_Efficacy	0.14	0.05	[0.03, 0.25]	0.18	2.61	.010
Step 3						
(Intercept)	2.51	0.44	[1.65, 3.38]	0.00	5.72	< .001
PP_FormalEd	-0.03	0.06	[-0.14, 0.08]	-0.05	-0.51	.609
PP_InfEd	-0.05	0.04	[-0.12, 0.02]	-0.10	-1.36	.175
PP_ITCSJob	-0.05	0.04	[-0.13, 0.03]	-0.10	-1.19	.234
PP_Cert_Count	0.02	0.02	[-0.02, 0.07]	0.08	0.99	.325
PP_Likert	0.42	0.10	[0.22, 0.62]	0.28	4.10	< .001
Perceived_Self_Efficacy	0.05	0.06	[-0.07, 0.17]	0.07	0.83	.405
Locus_of_Control	0.22	0.07	[0.07, 0.36]	0.22	2.97	.003
Step 4						
(Intercept)	3.04	0.46	[2.14, 3.94]	0.00	6.66	< .001
PP_FormalEd	-0.05	0.06	[-0.17, 0.06]	-0.09	-0.97	.332
PP_InfEd	-0.09	0.04	[-0.16, -0.01]	-0.18	-2.34	.020
PP_ITCSJob	-0.05	0.04	[-0.13, 0.03]	-0.10	-1.30	.195
PP_Cert_Count	0.02	0.02	[-0.03, 0.07]	0.07	0.89	.374
PP_Likert	0.26	0.11	[0.05, 0.48]	0.17	2.40	.017
Perceived_Self_Efficacy	0.02	0.06	[-0.10, 0.14]	0.03	0.34	.736
Locus_of_Control	0.20	0.07	[0.06, 0.34]	0.20	2.79	.006
SINTEX_SecSoftware	0.02	0.06	[-0.09, 0.13]	0.03	0.34	.734
SINTEX_NetworkPro	0.05	0.04	[-0.02, 0.12]	0.13	1.35	.179
SINTEX_IoTPro	0.12	0.04	[0.04, 0.21]	0.21	2.92	.004

Table 40 Regression Results for Future Changes

5.2.5 Security Intentions (Future) IoT Device Protection Measures

Security Intentions (Future) IoT Device Protection Measures, the dependent variable, is comprised of a count of the number of changes the respondents plan to make to their IoT device

configurations, labeled SINTFUT_IoTChanges in the dataset. In Step 1 of the regression, PP_FormalEd, PPInfEd, PP_ITCSJob, PP_Cert_Count, and PP_Likert were the predictor variables entered into the null model. In Step 2, Perceived_Self_Efficacy was added, in Step 3, Locus_of_Control was added, while in Step 4, SINTEX_SecSoftware, SINTEX_NetworkPro, and SINTEX_IoTPro were added.

The Q-Q scatterplot shows a mostly straight line through all four steps of the regression, indicating normality.

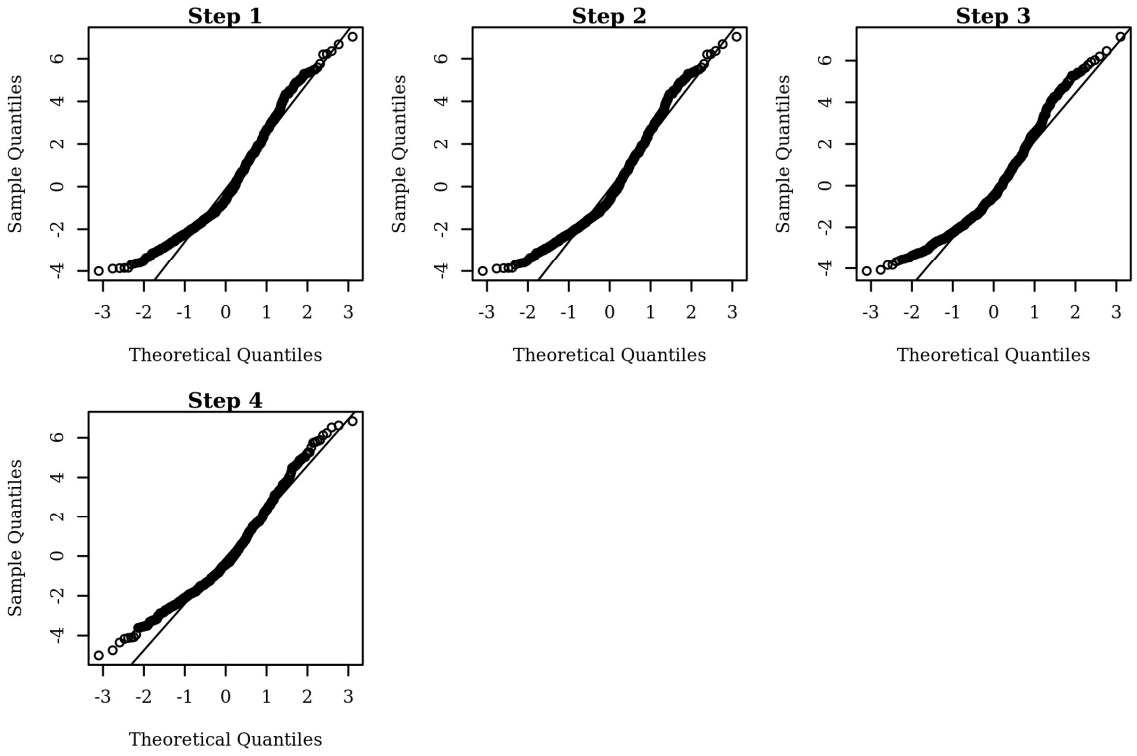

Figure 29 Q-Q Scatterplot for Security Intentions (Future) IoT Changes

The residuals scatterplot in Figure 32 below shows data with a mean of zero and no curvature, thus indicating the data meets the homoscedasticity assumption.

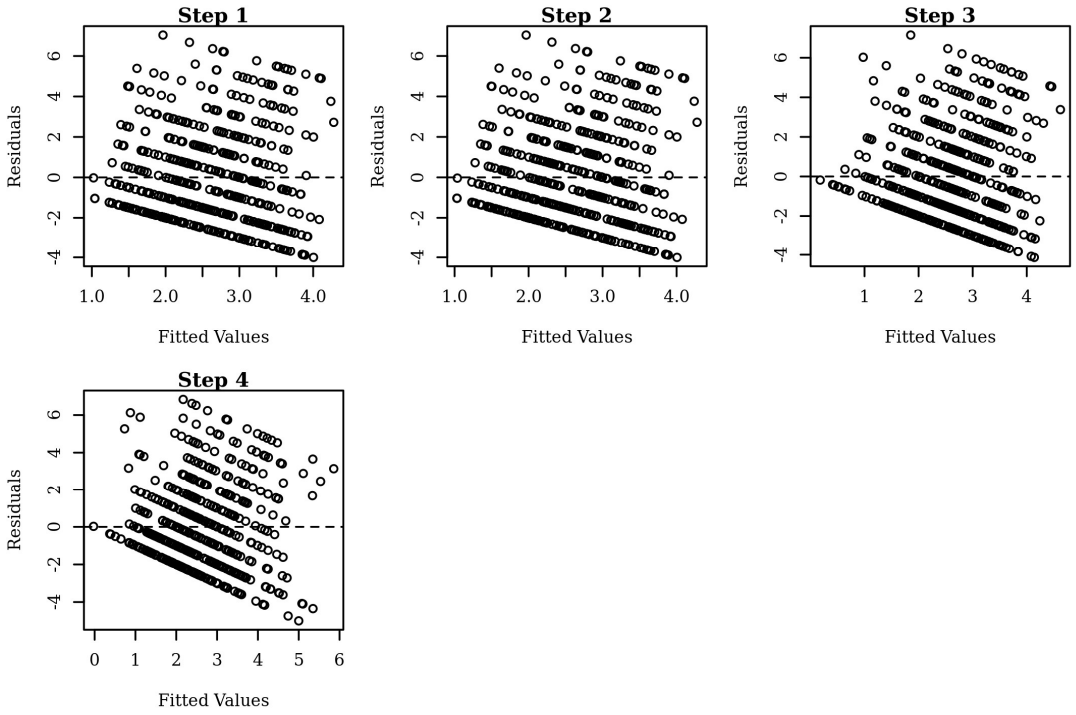

Figure 30 Residuals Scatterplot for Future IoT Changes

The Variance Inflation Factors (VIFs), shown in the chart below, are all below 5 for Steps 1-4 of the regression.

Variable	VIF	Variable	VIF	Variable	VIF
Step 1		Step 3		Step 4	
PP_FormalEd	2.49	PP_FormalEd	2.51	PP_FormalEd	2.57
PP_InfEd	1.53	PP_InfEd	1.58	PP_InfEd	1.66
PP_ITCSJob	1.77	PP_ITCSJob	1.79	PP_ITCSJob	1.8
PP_Cert_Count	1.94	PP_Cert_Count	1.96	PP_Cert_Count	2
PP_Likert	1.2	PP_Likert	1.42	PP_Likert	1.6
Step 2		Perceived_Self_Efficacy	2.09	Perceived_Self_Efficacy	2.11
PP_FormalEd	2.49	Locus_of_Control	1.65	Locus_of_Control	1.67
PP_InfEd	1.58			SINTEX_SecSoftware	1.87
PP_ITCSJob	1.79			SINTEX_NetworkPro	2.49
PP_Cert_Count	1.95			SINTEX_IoTPro	1.61
PP_Likert	1.41				
Perceived_Self_Efficacy	1.49				

Table 41 Variance Inflation Factors for Future IoT Changes

No observations with a Studentized residual greater than 3.11 in absolute value, the 0.999 quartile of a *t* distribution with 524 degrees of freedom, had significant influence on the results of the model.

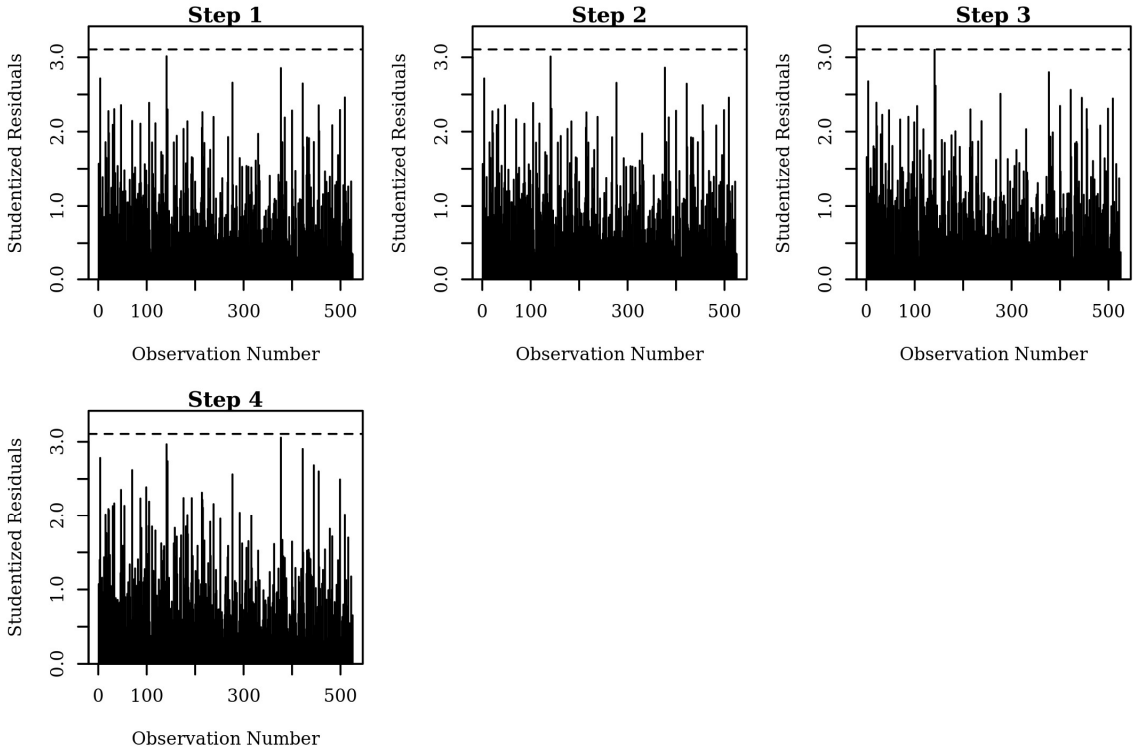

Figure 31 Outliers in Future IoT Changes

The *F*-test for Step 1 was significant, F (5, 519) = 9.30, $p < .001$, $\Delta R^2 = 0.08$. This model indicates that adding PP_FormalEd, PP_InfEd, PP_ITCSJob, PP_Cert_Count, and PP_Likert explained 8.22% of the variation in SINTFUT_IoTChanges. The *F*-test for Step 2 was not significant, F (1, 518) = 0.00, $p = .953$, $\Delta R^2 = 0.00$. This model indicates that adding Perceived_Self_Efficacy did not account for a significant amount of additional variation in SINTFUT_IoTChanges. The *F*-test for Step 3 was significant, F (1, 517) = 14.17, $p < .001$, $\Delta R^2 = 0.02$. This model indicates that adding Locus_of_Control explained an additional 2.45% of the variation in SINTFUT_IoTChanges. The *F*-test for Step 4 was significant, F (3, 514) = 10.96, $p < .001$, $\Delta R^2 = 0.05$. This model indicates that adding SINTEX_SecSoftware,

SINTEX_NetworkPro, and SINTEX_IoTPro explained an additional 5.37% of the variation in SINTFUT_IoTChanges. Past performance, locus of control, and security intentions (existing) account for 16.04% of the variance in SINTFUT_IoTChanges.

Model	R^2	df_{mod}	df_{res}	F	p	ΔR^2
Step 1	0.08	5	519	9.30	< .001	0.08
Step 2	0.08	1	518	0.00	.953	0.00
Step 3	0.11	1	517	14.17	< .001	0.02
Step 4	0.16	3	514	10.96	< .001	0.05

Table 42 Security Intentions (Future) IoT Changes Model Summary

PP_InfEd significantly predicted SINTFUT_IoTChanges, $B = 0.22$, $t(514) = 3.15$, $p = .002$. Perceived_Self_Efficacy significantly predicted SINTFUT_IoTChanges, $B = -0.28$, $t(514) = -2.45$, $p = .014$. This indicates that on average, a one-unit increase of Perceived_Self_Efficacy will decrease the value of SINTFUT_IoTChanges by 0.28 units. Locus_of_Control significantly predicted SINTFUT_IoTChanges, $B = 0.41$, $t(514) = 3.28$, $p = .001$. This indicates that on average, a one-unit increase of Locus_of_Control will increase the value of SINTFUT_IoTChanges by 0.41 units. SINTEX_IoTPro significantly predicted SINTFUT_IoTChanges, $B = 0.37$, $t(514) = 4.91$, $p < .001$.

The hypothesis for this regression was:

H_5: Locus of control, perceived self-efficacy, past performance, and security intentions (existing) predict security intentions (future) IoT changes.

H_5 was partially supported. Past performance (informal education), perceived self-efficacy, locus of control, and security intentions (existing) IoT protection predicted security intentions (future) IoT changes.

Variable	*B*	*SE*	CI	β	*t*	*p*
Step 1						
(Intercept)	-0.03	0.63	[-1.27, 1.21]	0.00	-0.05	.963
PP_FormalEd	-0.02	0.11	[-0.22, 0.19]	-0.01	-0.17	.868
PP_InfEd	0.29	0.07	[0.15, 0.43]	0.22	4.15	< .001
PP_ITCSJob	0.09	0.08	[-0.07, 0.25]	0.06	1.11	.266
PP_Cert_Count	-0.05	0.04	[-0.12, 0.03]	-0.07	-1.24	.214
PP_Likert	0.51	0.19	[0.15, 0.87]	0.13	2.75	.006
Step 2						
(Intercept)	-0.04	0.65	[-1.31, 1.23]	0.00	-0.06	.955
PP_FormalEd	-0.02	0.11	[-0.23, 0.19]	-0.01	-0.17	.868
PP_InfEd	0.29	0.07	[0.15, 0.43]	0.22	4.08	< .001
PP_ITCSJob	0.09	0.08	[-0.07, 0.25]	0.06	1.10	.271
PP_Cert_Count	-0.05	0.04	[-0.12, 0.03]	-0.07	-1.24	.214
PP_Likert	0.51	0.20	[0.11, 0.90]	0.13	2.51	.012
Perceived_Self_Efficacy	0.01	0.10	[-0.19, 0.20]	0.00	0.06	.953
Step 3						
(Intercept)	-1.44	0.74	[-2.89, 0.01]	0.00	-1.94	.052
PP_FormalEd	0.01	0.10	[-0.19, 0.22]	0.01	0.14	.889
PP_InfEd	0.29	0.07	[0.16, 0.43]	0.22	4.20	< .001
PP_ITCSJob	0.09	0.08	[-0.06, 0.25]	0.07	1.17	.241
PP_Cert_Count	-0.06	0.04	[-0.13, 0.02]	-0.08	-1.46	.145
PP_Likert	0.43	0.20	[0.04, 0.82]	0.11	2.17	.031
Perceived_Self_Efficacy	-0.23	0.12	[-0.46, -0.00]	-0.12	-1.97	.050
Locus_of_Control	0.48	0.13	[0.23, 0.73]	0.20	3.76	< .001
Step 4						
(Intercept)	-0.16	0.76	[-1.64, 1.33]	0.00	-0.21	.834
PP_FormalEd	-0.04	0.10	[-0.24, 0.17]	-0.02	-0.35	.726
PP_InfEd	0.22	0.07	[0.08, 0.36]	0.16	3.15	.002
PP_ITCSJob	0.08	0.08	[-0.08, 0.23]	0.05	0.99	.321
PP_Cert_Count	-0.07	0.04	[-0.14, 0.00]	-0.11	-1.86	.063
PP_Likert	0.06	0.21	[-0.35, 0.46]	0.01	0.28	.781
Perceived_Self_Efficacy	-0.28	0.12	[-0.51, -0.06]	-0.14	-2.45	.014
Locus_of_Control	0.41	0.12	[0.16, 0.65]	0.17	3.28	.001
SINTEX_SecSoftware	0.15	0.11	[-0.06, 0.36]	0.08	1.39	.165
SINTEX_NetworkPro	0.01	0.06	[-0.11, 0.13]	0.01	0.17	.865
SINTEX_IoTPro	0.37	0.08	[0.22, 0.52]	0.25	4.91	< .001

Table 43 Regression Results for Future IoT Changes

The unstandardized regression equation for SINTFUT_IoTChanges is:

SINTFUT_IoTChanges = -0.04*PP_FormalEd + 0.22*PP_InfEd + 0.08*PP_ITCSJob – 0.07*PP_Cert_Count + 0.06*PP_Likert – 0.28*Perceived_Self_Efficacy + 0.41*Locus_of_Control + 0.15*SINTEX_SecSoftware + 0.01*SINTEX_NetworkPro + 0.37*SINTEX_IoTPro.

5.3 Demographic Mean Comparison

Several publications have indicated that there are differences in information security behavior based on demographic variables, as discussed in the Literature Review. I collected the respondents' demographic characteristics to determine whether there are differences based on gender, race, age, education level, and/or household income. I also included IoT ownership to determine if there are significant differences between respondents, based on IoT ownership. General education level had no statistically significant effect on any of the measured variables.

In this section, only those variables with statistically significant differences ($p < .05$) will be discussed further. Unfortunately, due to the small size of some groups within the demographics variables, there was not a large enough sample size for each group to perform a regression analysis of the effect on each variable. For example, there were too few respondents over the age of 75 to have sufficient cases for a regression.

5.3.1 Age

Respondent age had a statistically significant effect on Locus of Control, Security Intentions (Existing) Security Software, and Security Intentions (Existing) Network Protection Measures. Variables that did not have a statistically significant effect were removed from Table 41.

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Locus_of_Control	Between Groups	13.538	6	2.256	2.173	0.044
	Within Groups	568.897	548	1.038		
	Total	582.435	554			
SINTEX_SecSoftware	Between Groups	32.487	6	5.414	3.238	0.004
	Within Groups	936.442	560	1.672		
	Total	968.929	566			
SINTEX_NetworkPro	Between Groups	119.444	6	19.907	3.142	0.005
	Within Groups	3547.7	560	6.335		
	Total	3667.15	566			

Table 44 ANOVA comparing variables by age

The youngest respondents, 18-24 year olds, had the lowest locus of control scores, indicating greater external locus of control, while 25-34 year olds had a 13.50% increase in locus of control. 45-54 year old respondents had the highest locus of control scores, 15.29% higher than 18-24 year olds. As seen in Figure 92, 45-54 year olds have the highest mean in all categories, while 18-24 year olds and 75-84 year olds have the lowest in all categories. The prior cyber hygiene study that collected data on similar variables treated everyone over 55 as a monolith (Cain, Edwards, & Still, 2018), but the data collected in this study showed sizeable differences between 55-64 year olds, 65-74 year olds, and 75-84 year olds. While there were only two respondents in the 75-84 year old category, this study provides insight into the age group that others have not.

Variable		18-24	25-34	35-44	45-54	55-64	65-74	75-84	Total
Locus of Control	**Mean**	**4.9773**	**5.6490**	**5.5974**	**5.7382**	**5.5076**	**5.2206**	**5.2500**	**5.5856**
	Std. Error of Mean	0.26569	0.08445	0.06699	0.10966	0.12613	0.25714		0.04352
	N	22	151	213	85	66	17	1	555
	Std. Deviation	1.24621	1.03770	0.97774	1.01103	1.02467	1.06023		1.02534
	Variance	1.553	1.077	0.956	1.022	1.050	1.124		1.051
SINTEX_SecSoftware	**Mean**	**0.9545**	**1.8693**	**1.6843**	**2.1163**	**1.9275**	**1.8333**	**0.5000**	**1.8016**
	Std. Error of Mean	0.20255	0.10272	0.09552	0.13172	0.14790	0.21768	0.50000	0.05495
	N	22	153	217	86	69	18	2	567
	Std. Deviation	0.95005	1.27058	1.40704	1.22156	1.22857	0.92355	0.70711	1.30839
	Variance	0.903	1.614	1.980	1.492	1.509	0.853	0.500	1.712
SINTEX_NetworkPro	**Mean**	**1.8636**	**3.4052**	**2.7097**	**3.5930**	**3.2029**	**2.2222**	**1.5000**	**3.0388**
	Std. Error of Mean	0.43790	0.20621	0.17508	0.28235	0.29313	0.37535	1.50000	0.10690
	N	22	153	217	86	69	18	2	567
	Std. Deviation	2.05393	2.55064	2.57904	2.61839	2.43492	1.59247	2.12132	2.54540
	Variance	4.219	6.506	6.651	6.856	5.929	2.536	4.500	6.479

Table 45 Comparison of Means by Age

5.3.4 Ethnicity

Ethnicity had a statistically significant effect on every variable, excluding Past Performance Likert scores, Locus of Control, and Security Intentions (Future) IoT Changes.

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
PP_FormalEd	Between Groups	59.580	5	11.916	5.181	.000
	Within Groups	1287.975	560	2.300		
	Total	1347.555	565			
PP_InfEd	Between Groups	50.065	5	10.013	3.051	.010
	Within Groups	1838.090	560	3.282		
	Total	1888.155	565			
PP_Cert_Count	Between Groups	402.594	5	80.519	6.053	.000
	Within Groups	7448.763	560	13.301		
	Total	7851.357	565			
PP_ITCSJob	Between Groups	64.986	5	12.997	4.556	.000
	Within Groups	1597.388	560	2.852		
	Total	1662.375	565			
Perceived_Self_Efficacy	Between Groups	18.445	5	3.689	2.339	.041
	Within Groups	866.021	549	1.577		
	Total	884.466	554			
SINTEX_SecSoftware	Between Groups	22.938	5	4.588	2.720	.019
	Within Groups	944.552	560	1.687		
	Total	967.490	565			
SINTEX_NetworkPro	Between Groups	165.158	5	33.032	5.306	.000
	Within Groups	3486.270	560	6.225		
	Total	3651.428	565			
SINTEX_IoTPro	Between Groups	36.610	5	7.322	2.614	.024
	Within Groups	1568.563	560	2.801		
	Total	1605.173	565			
SINTFUT_Changes	Between Groups	10.382	5	2.076	2.435	.036
	Within Groups	202.988	238	.853		
	Total	213.371	243			

Table 46 Analysis of Variance by Ethnicity

While they had smaller sample sizes, respondents in the American Indian/Alaska Native, Asian, Other, and Multi-racial categories had higher means than white respondents or African-Americans in all categories, except perceived self-efficacy, where African-Americans had a higher mean than Asians.

		White	Black or African-American	American Indian or Alaska Native	Asian	Other	Multi-racial	Total
PP_FormalEd	Mean	1.3160	0.9717	3.0000	1.6500	2.2500	2.6429	1.3322
	Std. Error of Mean	0.07472	0.12173		0.44883	0.49137	0.47587	0.06491
	N	405	106	1	20	20	14	566
	Std. Deviation	1.50375	1.25324		2.00722	2.19749	1.78054	1.54436
	Variance	2.261	1.571		4.029	4.829	3.170	2.385
PP_InfEd	Mean	2.4938	1.8774	3.0000	2.4500	2.5000	3.5000	2.4028
	Std. Error of Mean	0.09201	0.17204		0.39387	0.32847	0.35933	0.07684
	N	405	106	1	20	20	14	566
	Std. Deviation	1.85170	1.77121		1.76143	1.46898	1.34450	1.82808
	Variance	3.429	3.137		3.103	2.158	1.808	3.342
PP_Cert_Count	Mean	1.4247	0.7830	16.0000	2.6000	3.5000	3.0000	1.4841
	Std. Error of Mean	0.17798	0.26028		0.98782	1.34849	1.57243	0.15669
	N	405	106	1	20	20	14	566
	Std. Deviation	3.58177	2.67975		4.41767	6.03062	5.88348	3.72776
	Variance	12.829	7.181		19.516	36.368	34.615	13.896
PP_ITCSJob	Mean	2.2025	1.9811	5.0000	2.6500	3.6500	2.9286	2.2509
	Std. Error of Mean	0.08432	0.15516		0.39918	0.39918	0.49685	0.07210
	N	405	106	1	20	20	14	566
	Std. Deviation	1.69697	1.59750		1.78517	1.78517	1.85904	1.71530
	Variance	2.880	2.552		3.187	3.187	3.456	2.942
Perceived_Self_Efficacy	Mean	4.4184	4.5175	6.5000	4.4833	4.9167	5.3077	4.4820
	Std. Error of Mean	0.06417	0.12426		0.20974	0.24348	0.30067	0.05363
	N	396	105	1	20	20	13	555
	Std. Deviation	1.27693	1.27327		0.93799	1.08889	1.08407	1.26353
	Variance	1.631	1.621		0.880	1.186	1.175	1.597

Table 47 Past Performance and Perceived Self-Efficacy by Race

5.3.5 Annual Household Income

Annual Household Income only had a statistically significant effect on Locus of Control.

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Locus_of_Control	Between Groups	23.700	11	2.155	2.082	.020
	Within Groups	556.703	538	1.035		
	Total	580.403	549			

Table 48 Analysis of Variance by Household Income

Participants with a household income of $10,000-19,999 have the highest locus of control mean, while those with a household income below $10,000 have the lowest. Those with a household income of $100-149.999K have the second highest locus of control mean, 1.95% below those with a household income of $10,000-19,999. There are no obvious linear trends with the means for locus of control. However, there is a significantly lower mean among those with a household income from $50-59.999K, 12.35% lower than those in $40-49.999K income bracket and 8.77% below those in the $60-69.999K income bracket.

Locus of Control by HHI					
HHI	Mean	N	Std Dev	Median	Variance
<$10K	4.388888888888890	3	0.673575314054564	4.500000000000000	0.454
$10-19.999K	5.833333333333330	3	0.381881307912987	5.750000000000000	0.146
$20-29.999K	5.597222222222220	6	1.479880500681150	6.250000000000000	2.190
$30-$39.999K	5.232142857142860	14	1.186722562168780	5.250000000000000	1.408
$40-49.999K	5.677083333333330	16	0.989703940018877	5.875000000000000	0.980
$50-59.999K	4.970000000000000	25	1.229667976867470	5.000000000000000	1.512
$60-69.999K	5.447916666666670	32	1.162001039487750	5.500000000000000	1.350
$70-79.999K	5.437500000000000	36	0.928468400877796	5.500000000000000	0.862
$80-89.999K	5.651315789473690	38	0.910782767147657	5.750000000000000	0.830
$90-99.999K	5.695652173913040	46	1.017776775731000	6.000000000000000	1.036
$100-149.999K	5.718632958801500	178	0.943927400126974	6.000000000000000	0.891
>$150K	5.560240963855420	166	1.090115773437380	5.750000000000000	1.188
Total	5.577856719952640	563	1.038185573531390	5.750000000000000	1.078

Table 49 Locus of Control by Household Income

5.3.6 Gender

Gender had a statistically significant effect on all variables, excluding Security Intentions (Future) Changes and Security Intentions (Future) IoT Changes.

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
PP_FormalEd	Between Groups	84.103	2	42.051	18.852	.000
	Within Groups	1249.119	560	2.231		
	Total	1333.222	562			
PP_InfEd	Between Groups	129.679	2	64.839	20.764	.000
	Within Groups	1748.719	560	3.123		
	Total	1878.398	562			
PP_Cert_Count	Between Groups	424.748	2	212.374	16.024	.000
	Within Groups	7421.990	560	13.254		
	Total	7846.739	562			
PP_ITCSJob	Between Groups	93.023	2	46.511	16.573	.000
	Within Groups	1571.595	560	2.806		
	Total	1664.618	562			
PP_Likert	Between Groups	4.375	2	2.187	5.728	.003
	Within Groups	204.693	536	.382		
	Total	209.068	538			
Perceived_Self_Efficacy	Between Groups	59.924	2	29.962	20.043	.000
	Within Groups	820.697	549	1.495		
	Total	880.621	551			
Locus_of_Control	Between Groups	8.335	2	4.168	3.996	.019
	Within Groups	571.511	548	1.043		
	Total	579.846	550			
SINTEX_SecSoftware	Between Groups	83.592	2	41.796	26.696	.000
	Within Groups	876.748	560	1.566		
	Total	960.340	562			
SINTEX_NetworkPro	Between Groups	237.550	2	118.775	19.528	.000
	Within Groups	3406.155	560	6.082		
	Total	3643.705	562			
SINTEX_IoTPro	Between Groups	44.933	2	22.466	8.093	.000
	Within Groups	1554.502	560	2.776		
	Total	1599.435	562			

Table 50 Analysis of Variance by Gender

Men had a 17.2% higher perception of self-efficacy than women, while nonbinary respondents had the highest perceived self-efficacy, with a score .3% higher than men. When comparing median scores, men were 20% higher than women and equal to nonbinary respondents.

Self-Efficacy by Gender					
Gender	Mean	N	Std Dev	Median	Variance
Male	4.861283643892340	322	1.178918904593700	5.000000000000000	1.390
Female	4.022175732217580	239	1.236692415863140	4.000000000000000	1.529
Nonbinary	4.875000000000000	4	0.936650850004853	5.000000000000000	0.877
Total	4.506430678466070	565	1.270162815151090	4.666666666666670	1.613

Table 51 Perceived Self-Efficacy by Gender

Nonbinary respondents had the highest locus of control means at 5.75 and second highest locus of control medians at 5.875, with men second in locus of control means at 5.69, 1% behind nonbinary respondents and highest in locus of control medians at 6. Women were lower with a mean of 5.42, 5.7% lower than nonbinary respondents, and a median of 5.5.

Locus of Control by Gender					
Gender	Mean	N	Std Dev	Median	Variance
Male	5.689771547248180	321	1.019560473320420	6.000000000000000	1.040
Female	5.422245467224550	239	1.042946396956710	5.500000000000000	1.088
Nonbinary	5.750000000000000	4	1.136515141415490	5.875000000000000	1.292
Total	5.576832151300240	564	1.036906336436100	5.750000000000000	1.075

Table 52 Locus of Control by Gender

5.3.7 IoT Ownership

IoT Ownership had a statistically significant effect on all measured variables, excluding Past Performance Certifications and Security Intentions (Future) Changes.

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
PP_FormalEd	Between Groups	12.877	1	12.877	5.440	.020
	Within Groups	1337.455	565	2.367		
	Total	1350.332	566			
PP_InfEd	Between Groups	68.306	1	68.306	21.128	.000
	Within Groups	1826.583	565	3.233		
	Total	1894.889	566			
PP_ITCSJob	Between Groups	13.798	1	13.798	4.707	.030
	Within Groups	1656.121	565	2.931		
	Total	1669.919	566			
PP_Likert	Between Groups	3.062	1	3.062	8.005	.005
	Within Groups	206.555	540	.383		
	Total	209.617	541			
Perceived_Self_Efficacy	Between Groups	20.855	1	20.855	13.305	.000
	Within Groups	868.375	554	1.567		
	Total	889.230	555			
Locus_of_Control	Between Groups	17.029	1	17.029	16.655	.000
	Within Groups	565.406	553	1.022		
	Total	582.435	554			
SINTEX_SecSoftware	Between Groups	9.094	1	9.094	5.353	.021
	Within Groups	959.835	565	1.699		
	Total	968.929	566			
SINTEX_NetworkPro	Between Groups	105.434	1	105.434	16.725	.000
	Within Groups	3561.713	565	6.304		
	Total	3667.146	566			
SINTEX_IoTPro	Between Groups	125.071	1	125.071	47.606	.000
	Within Groups	1484.382	565	2.627		
	Total	1609.453	566			
SINTFUT_IoTChanges	Between Groups	81.910	1	81.910	14.013	.000
	Within Groups	3296.813	564	5.845		
	Total	3378.723	565			

Table 53 ANOVA of Effects of IoT Ownership on Variables

5.4 Survey Effects

Security Intentions (Existing) IoT Protection Measures were assessed early in the survey, while the assessment of Security Intentions (Future) IoT Changes was penultimate. Both questions had almost identical responses, with IoT Changes having an additional option to select "Find other alternatives for devices that don't need to connect to the Internet".

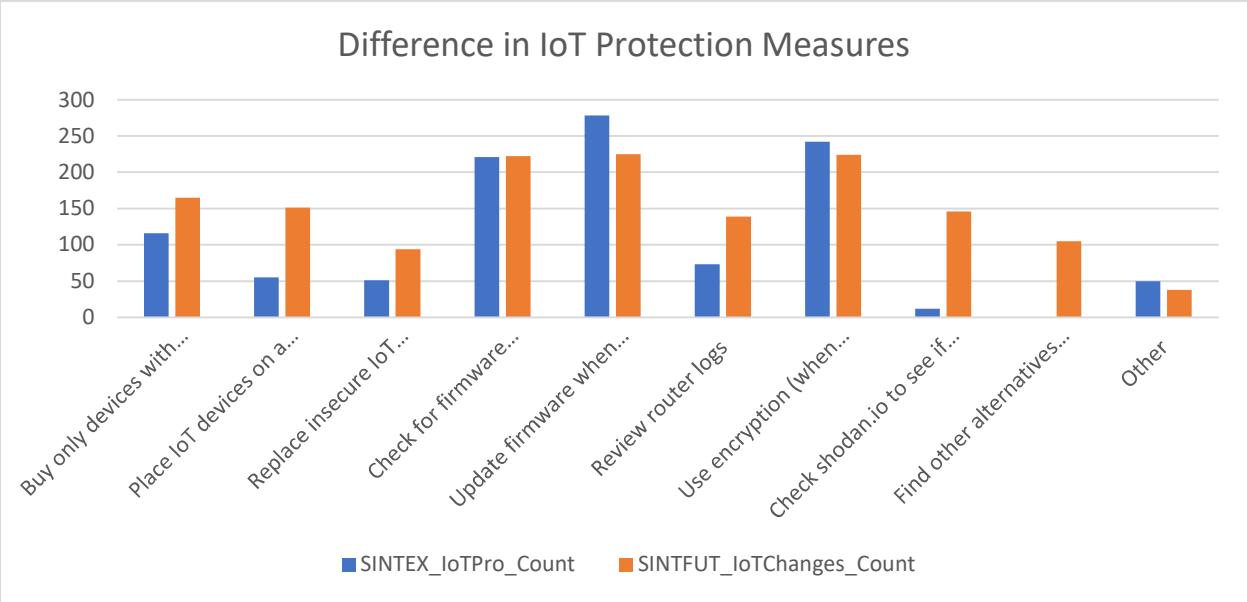

Figure 32 Difference in IoT Protection Measures

As seen in Figure 34, there is a decrease in the number of respondents with 4 or fewer IoT device protection measures compared to their answers to question 35, while the number of respondents planning to use 5 or more IoT device protection measures increased.

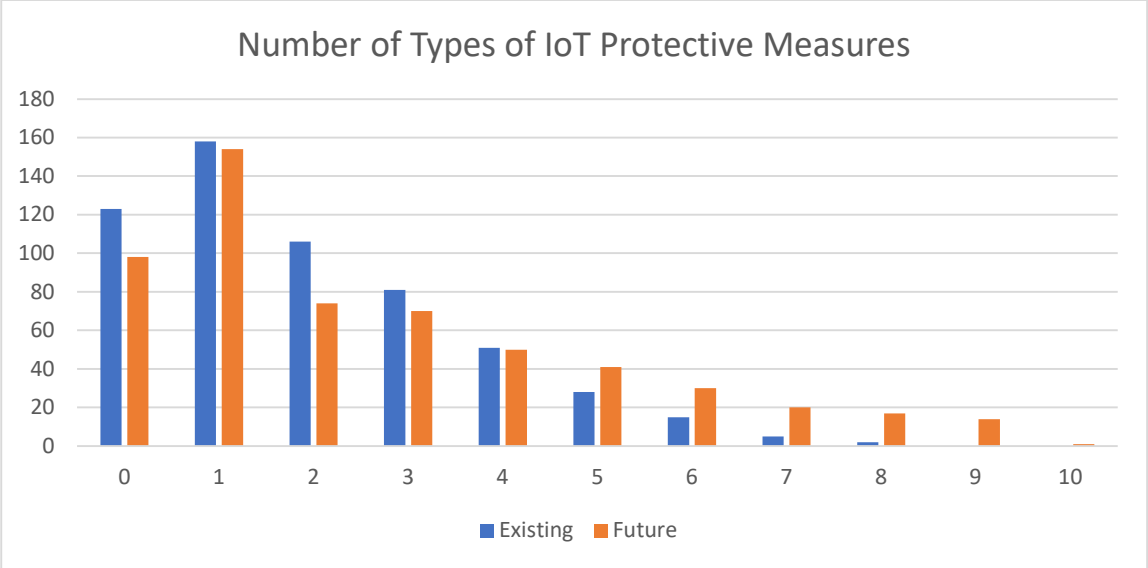

Figure 33 Comparison of the Number of IoT Protective Measures

To correctly compare the means of SINTEX_IoTPro and SINTFUT_IoTChanges, the count of using non-connected devices was removed to ensure that the available responses were the same. Then, a paired samples t-test was run to determine if the difference in means was statistically significant.

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	SINTEX_IoTPro	1.9330	567	1.68628	.07082
	Q51_PostHoc	2.6226	567	2.40407	.10096

Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference Lower	Upper			
Pair 1	SINTEX_IoTPro - Q51_PostHoc	-.68959	2.67542	.11236	-.91028	-.46891	-6.138	566	.000

Figure 34 Comparison of Means of IoT Protection Measures

The means of the same IoT protection measures increased by 35.68% over the course of the survey. However, because the question was focused on changes that the respondent intended to make, there is a chance that some users included all security measures they intend to use in the future, while other respondents only checked the boxes for additional security measures beyond what they reported using in Question 35.

5.5 Self-Reported Secure User Analysis

Question 50 asked why users were not going to make any changes to their network, to which 122 respondents answered that their network was already secure enough. To determine the accuracy of that statement, I compared means for all variables, excluding SINTFUT_Changes, based on whether the respondent selected that checkbox. SINTFUT_Changes was excluded because users who answered no to making changes in question 48 did not receive question 49, on which SINTFUT_Changes was based. PP_Likert was the smallest mean difference at 0.31, while SINTEX_NetworkPro was highest at 1.68. SINTFUT_IoTChanges was lower for the secure group because they planned to make fewer changes to their already secure home ecosystem.

Q50_1		PP_FormalEd	PP_InfEd	PP_Cert_Count	PP_ITCSJob	PP_Likert	Perceived_Self_Efficacy	Locus_of_Control	SINTEX_SecSoftware	SINTEX_NetworkPro	SINTEX_IoTPro	SINTFUT_IoTChanges
0	Mean	1.1345	2.2511	1.0022	2.0336	3.5109	4.2856	5.5229	1.6738	2.6794	1.7713	2.7011
	Std. Error of Mean	0.0655	0.0852	0.1438	0.0768	0.0303	0.0594	0.0484	0.0597	0.1099	0.0744	0.1162
	Std. Deviation	1.3836	1.7988	3.0357	1.6218	0.6237	1.2394	1.0117	1.2603	2.3210	1.5713	2.4510
	N	446	446	446	446	424	436	437	446	446	446	445
	Variance	1.914	3.236	9.216	2.63	0.389	1.536	1.024	1.588	5.387	2.469	6.007
1	Mean	2.0744	2.9835	3.2727	3.0744	3.8168	5.2139	5.8178	2.2727	4.3636	2.5289	2.1901
	Std. Error of Mean	0.1689	0.1668	0.4740	0.1652	0.0514	0.0990	0.0963	0.1253	0.2624	0.1772	0.2175
	Std. Deviation	1.8582	1.8348	5.2138	1.8174	0.5580	1.0843	1.0463	1.3784	2.8868	1.9497	2.3921
	N	121	121	121	121	118	120	118	121	121	121	121
	Variance	3.453	3.366	27.183	3.303	0.311	1.176	1.095	1.9	8.333	3.801	5.722
Total	Mean	1.3351	2.4074	1.4868	2.2557	3.5775	4.486	5.5856	1.8016	3.0388	1.933	2.5919
	Std. Error of Mean	0.0649	0.0768	0.1564	0.0721	0.0267	0.0537	0.0435	0.0550	0.1069	0.0708	0.1028
	Std. Deviation	1.5446	1.8297	3.7250	1.7177	0.6225	1.2658	1.0253	1.3084	2.5454	1.6863	2.4454
	N	567	567	567	567	542	556	555	567	567	567	566
	Variance	2.386	3.348	13.876	2.95	0.387	1.602	1.051	1.712	6.479	2.844	5.98

Figure 35 Comparison of Means of Self-Reported Secure Users and All Others

The results showed that the respondents who felt their network was secure enough (Q50_1 = 1) had statistically significant, far higher means in each of the independent variable categories, except for SINTFUT_IoTChanges, where the group who felt their network was secure enough had a lower mean. However, the question requested changes only, so those who don't feel a need to make changes due to their existing security configuration should have a lower mean.

Performing linear regressions for the post hoc more secure group, compared to the less secure group, resulted in an increased predictive power for the secure group for SINTEX_SecSoftware, SINTEX_NetworkPro, and SINTEX_IoTPro, but a lower predictive power for SINTFUT_IoTChanges. SINTFUT_Changes cannot be compared because those who selected that they would not be making any changes did not receive the SINTFUT_Changes questions.

The adjusted R^2 for SINTEX_SecSoftware for the insecure group was 0.198, while it was 0.222 for the secure group. For SINTEX_SecSoftware, the secure group equation was:

SINTEX_SecSoftware = 0.047*PP_FormalEd + 0.167*PP_InfEd - 0.25*PP_Cert_Count + 0.157*PP_ITCSJob + 0.416*PP_Likert + 0.006*Perceived_Self_Efficacy + 0.145*Locus_of_Control – 1.227.

Only PP_InfEd was statistically significant (p=.023). The insecure group equation was:

SINTEX_SecSoftware = 0.186*PP_FormalEd + 0.098*PP_InfEd + 0.032*PP_Cert_Count – 0.055*PP_ITCSJob + 0.238*PP_Likert + 0.121*Perceived_Self_Efficacy + 0.067*Locus_of_Control – 0.412.

PP_FormalEd (p=.002), PP_InfEd (p=.012), and PP_Likert (p=.022) were statistically significant.

The adjusted R^2 for SINTEX_NetworkPro for the insecure group was 0.332, but it was 0.452 for the secure group. The equations for the two groups were as follows:

SINTEX_NetworkPro (insecure) = 0.288*PP_FormalEd + 0.21*PP_InfEd + 0.059*PP_Cert_Count + 0.067*PP_ITCSJob + 0.884*PP_Likert + 0.272*Perceived_Self_Efficacy -0.004*Locus_of_Control – 2.582.

PP_FormalEd (p=.005), PP_InfEd (p=.002), PP_Likert (p=.000), and Perceived_Self_Efficacy (p=.014) were all statistically significant.

SINTEX_NetworkPro (secure) = 0.177*PP_FormalEd + 0.336*PP_InfEd + 0.149*PP_Cert_Count + 0.266*PP_ITCSJob + 0.684*PP_Likert – 0.278*Perceived_Self_Efficacy + 0.412*Locus_of_Control – 1.826.

PP_InfEd (p=.01) and PP_Cert_Count (p=.013) were statistically significant.

The adjusted R^2 for SINTEX_IoTPro for the insecure group was 0.268, while it was 0.345 for the secure group. The equations are as follows:

SINTEX_IoTPro (insecure) = 0.60*PP_FormalEd + 0.132*PP_InfEd + 0.021*PP_Cert_Count + 0.014*PP_ITCSJob + 0.813*PP_Likert + 0.104*Perceived_Self_Efficacy + 0.110*Locus_of_Control – 2.587.

PP_InfEd (p=.004), and PP_Likert (p=.000) were statistically significant.

SINTEX_IoTPro (secure) = 0.123*PP_FormalEd + 0.205*PP_InfEd + 0.029*PP_Cert_Count + 0.087*PP_ITCSJob + 0.725*PP_Likert + 0.123*Perceived_Self_Efficacy + 0.299*Locus_of_Control – 3.9.

PP_InfEd (p=.037) and PP_Likert (p=.031) were statistically significant.

The adjusted R^2 for SINTFUT_IoTChanges for the insecure group is 0.192 and the secure group is 0.047. An ANOVA determined the secure group regression was not statistically significant, nor were any of the independent variables for the secure equation statistically significant. The equations are as follows:

SINTFUT_IoTChanges (insecure) = -0.013*PP_FormalEd + 0.221*PP_InfEd – 0.075*PP_Cert_Count + 0.056*PP_ITCSJob + 0.112*PP_Likert – 0.159*Perceived_Self_Efficacy + 0.452*Locus_of_Control + 0.189*SINTEX_SecSoftware + 0.018*SINTEX_NetworkPro + 0.418*SINTEX_IoTPro– 1.091.

PP_InfEd (p=.005), Locus_of_Control (p=.001) and SINTEX_IoTPro (p=.000) are statistically significant.

SINTFUT_IoTChanges (secure) = -0.004*PP_FormalEd + 0.150*PP_InfEd – 0.046*PP_Cert_Count + 0.237*PP_ITCSJob – 0.311*PP_Likert – 0.459*Perceived_Self_Efficacy + 0.176*Locus_of_Control + 0.097*SINTEX_SecSoftware + 0.013*SINTEX_NetworkPro + 0.288*SINTEX_IoTPro + 2.78.

Neither the regression nor any of the variables were statistically significant.

This result was consistent with Torten, Raiche, and Boyle's (2018) extension of Hanus and Wu (2016), which found that information security professionals had a higher percentage of variance explained on the same questions.

5.6 Partial Least Squares – Path Modeling

Two PLS-PM analyses were conducted on the data, one to examine the relationship between latent variables and a second to determine the effect of demographic differences on the model.

The measurement or outer model was assessed by examining multicollinearity in the model and checking the weights of each indicator via bootstrapping. Multicollinearity was also examined with variance inflation factors (VIF) to assess the validity of the formative indicators. A VIF with a value greater than 10 indicates that there is extreme multicollinearity among the predictors (Henseler et al., 2009; Cenfetelli & Bassellier, 2009; Menard, 2009). No formative indicators exhibited multicollinearity, which suggests that the formative indicators are appropriate for the latent variables.

Indicator	VIF
PP	
Q38	1.74
Q39	1.39
Q40	1.27
Q41	1.59
SEFF	
PP_FormalEd	2.15
PP_InfEd	1.79
PP_Cert_Count	1.39
PP_ITCSJob	1.79
PP_Likert	1.27
LofC	
Q42	3.08
Q43	2.43
Q44	1.70
Q45_R	1.20
Q46	2.89
Q47	2.61
SINT_EX	
SINTEX_SecSoftware	2.58
SINTEX_NetworkPro	2.64
SINTEX_IoTPro	1.34
SINT_FUT	
Q49_1	1.79
Q49_2	3.06
Q49_3	3.44
Q49_4	3.45
Q49_5	4.87
Q49_6	3.28
Q49_7	1.91
Q49_8	1.70
Q49_9	2.43
Q49_10	1.86
Q49_11	2.22
Q49_12	2.92
Q49_15	2.66
Q49_16	4.49
Q49_17	3.57
Q49_13	2.94
SINTFUT_IoTChanges	1.25

Table 54 Variance Inflation Factors

Bootstrapping was performed with 500 resamples. The loadings were assessed for the reflective indicators, and the weights were examined for the formative indicators. Significance was determined using confidence intervals for the given parameter estimates, which were

calculated based on an alpha value of 0.05 (Henseler et al., 2009; Sanchez, 2013; Chinn, 2010). Since there were no reflective indicators, the bootstrapped loadings were not examined. The following formative indicators did not have a significant weight for its latent variable: PP_FormalEd, PP_InfEd, PP_Cert_Count, PP_ITCSJob, SEFF, SINTEX_SecSoftware, SINTEX_NetworkPro, SINTFUT, and SINTFUT_IoTChanges. Any indicator that does not have a significant loading or weight should be examined whether it belongs to the specified latent variable or if it should be kept in the model.

Construct-Indicator	*M*	*SE*	CI
PP-PP_FormalEd	0.11	0.24	[-0.37, 0.59]
PP-PP_InfEd	0.22	0.25	[-0.28, 0.71]
PP-PP_Cert_Count	0.17	0.23	[-0.29, 0.63]
PP-PP_ITCSJob	0.16	0.17	[-0.19, 0.51]
PP-PP_Likert	0.60	0.19	[0.22, 0.98]
SEFF-Q42	-0.14	0.36	[-0.87, 0.59]
SEFF-Q43	0.35	0.28	[-0.21, 0.92]
SEFF-Q44	0.17	0.29	[-0.40, 0.74]
SEFF-Q45_R	-0.21	0.23	[-0.68, 0.26]
SEFF-Q46	0.17	0.37	[-0.56, 0.91]
SEFF-Q47	0.51	0.33	[-0.14, 1.17]
LofC-Q38	0.74	0.42	[-0.11, 1.59]
LofC-Q39	0.15	0.57	[-0.98, 1.29]
LofC-Q40	-0.14	0.35	[-0.85, 0.56]
LofC-Q41	-0.06	0.53	[-1.12, 1.00]
SINT_EX-SINTEX_SecSoftware	0.33	0.38	[-0.42, 1.09]
SINT_EX-SINTEX_NetworkPro	0.33	0.35	[-0.38, 1.04]
SINT_EX-SINTEX_IoTPro	0.47	0.21	[0.06, 0.88]
SINT_FUT-Q49_1	0.03	0.18	[-0.34, 0.39]
SINT_FUT-Q49_2	0.16	0.33	[-0.51, 0.83]
SINT_FUT-Q49_3	-0.11	0.32	[-0.76, 0.54]
SINT_FUT-Q49_4	-0.19	0.30	[-0.79, 0.40]
SINT_FUT-Q49_5	0.60	0.38	[-0.17, 1.37]
SINT_FUT-Q49_6	-0.10	0.35	[-0.80, 0.61]
SINT_FUT-Q49_7	-0.04	0.26	[-0.56, 0.47]
SINT_FUT-Q49_8	-0.07	0.25	[-0.57, 0.43]
SINT_FUT-Q49_9	0.11	0.26	[-0.41, 0.63]
SINT_FUT-Q49_10	-0.28	0.24	[-0.77, 0.21]
SINT_FUT-Q49_11	0.59	0.22	[0.16, 1.03]
SINT_FUT-Q49_12	-0.14	0.29	[-0.72, 0.44]
SINT_FUT-Q49_15	-0.05	0.29	[-0.62, 0.53]
SINT_FUT-Q49_16	-0.16	0.34	[-0.84, 0.52]
SINT_FUT-Q49_17	0.08	0.27	[-0.46, 0.63]
SINT_FUT-Q49_13	0.21	0.27	[-0.32, 0.74]
SINT_FUT-SINTFUT_IoTChanges	0.24	0.19	[-0.15, 0.63]

Table 55 Bootstrap Results

The structural or inner model was assessed by examining the R^2-values for each endogenous variable and the goodness of fit (GoF) index for the model. Bootstrapping was also used to determine the reliability of the inner model.

Construct	Type	R^2	AVE
PP	Exogenous	--	--
SEFF	Exogenous	--	--
LofC	Exogenous	--	--
SINT_EX	Endogenous	0.61	--
SINT_FUT	Endogenous	0.68	--

Table 56 Structural Model Summary

A visual summary of the structural model with weights is below in Figure 38.

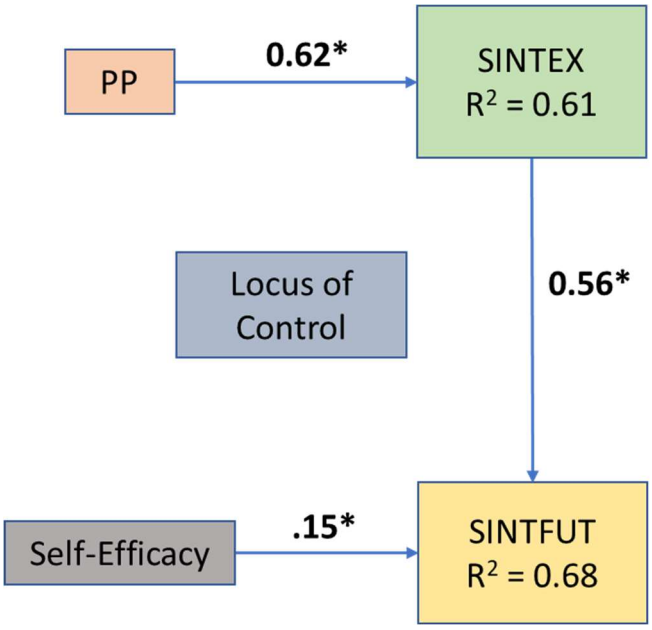

Figure 36 Structural Model

The hypotheses for this model were:

H_6: Locus of control, perceived self-efficacy, and past performance effect security intentions (existing).

H_7: Locus of control, perceived self-efficacy, and past performance effect security intentions (future).

H_6 was partially supported and partially rejected. Past performance effected security intentions (existing).

H_7 was partially supported and partially rejected. Self-efficacy effected security intentions (future).

To determine if the relationships among the latent variables are appropriate, R^2-values were calculated for each endogenous variable. Each endogonous variable should have an R^2-value ≥ .20 (Sanchez, 2013). There were no low R^2-values, indicating that each relationship is appropriate for the model.

The predictive power of the PLS-PM can be determined by the GoF index. The GoF index is calculated by computing the geometric mean of the average R^2-values and average communality for each latent variable. Values greater than .90 are considered a good model fit, while a GoF index less than .90 and greater than .70 is an acceptable model fit (Sanchez, 2013; Chinn, 2010). A model with poor predictive power is indicated by a GoF index less than or equal to .70. The GoF index, GoF = 0.47, indicates that the model had a poor model fit and poor ability to predict.

Bootstrapping was performed with 500 resamples. The regression coefficients were evaluated using confidence intervals to determine the significance of the regression paths using an alpha value of 0.05 (Henseler et al., 2009; Sanchez, 2013; Chinn, 2010). The following regression paths did not have a significant relationship: SEFF and LofC → SINT_EX, PP and LofC→ SINT_FUT. This suggests that the regression might not belong in the model, since the independent latent variable did not explain a significant portion of the variance in the dependent latent variable.

Path	Original B	*M*	*SE*	CI
PP → SINT_EX	0.62	0.60	0.12	[0.36, 0.85]
SEFF → SINT_EX	0.23	0.24	0.12	[-0.00, 0.48]
LofC → SINT_EX	0.06	0.07	0.13	[-0.20, 0.33]
PP → SINT_FUT	0.08	0.16	0.15	[-0.13, 0.46]
SEFF → SINT_FUT	0.15	0.27	0.13	[0.00, 0.53]
LofC → SINT_FUT	0.24	0.18	0.21	[-0.25, 0.60]
SINT_EX → SINT_FUT	0.56	0.38	0.15	[0.09, 0.68]

Table 57 Bootstrap Results for Inner Model

A partial least squares path modeling (PLS-PM) analysis was conducted to determine whether the latent variables, PP, SEFF, LocusofControl, SINT_EX, SINT_FUT, Gender, Ethnicity, and IoT_Ownership, adequately describe the data. The goal of PLS-PM is to accurately describe the network of variables and their relationships.

The PLS-PM model was assessed by evaluating the validity of the measurement model and the structural model. After model validation, the regressions of the PLS-PM were analyzed. The measurement or outer model was assessed by examining the unidimensionality of indicators, the loadings and communalities for each indicator, and the crossloadings. Bootstrapping was also implemented to check the significance of each loading in the model.

For reflective indicators, the latent construct must be positively correlated with one another, which is defined as the unidimensionality of indicators. To evaluate the unidimensionality of indicators, Cronbach's alpha (α) and Dillon-Goldstein's rho (ρ) were calculated. Unidimensionality of indicators can be assumed if the values of each Cronbach's alpha and Dillon-Goldstein's rho is high ($\alpha \geq .7$ and $\rho \geq .7$). All latent variables exhibited unidimensionality with its reflective indicators, suggesting the relationships between each latent variable and its manifest variables are appropriate for PLS-PM.

Construct	Indicator Type	Number of items	α	ρ
PP	reflective	5	0.77	0.85
SEFF	reflective	6	0.86	0.90
LocusofControl	reflective	4	0.77	0.85
SINT_EX	reflective	3	0.75	0.86
SINT_FUT	reflective	16	0.87	0.89
Gender	reflective	1	1	1
Ethnicity	reflective	1	1	1
IoT_Ownership	reflective	1	1	1

Table 58 Unidimensionality of Indicators

The factor loadings and communality were examined for the reflective indicators to identify any indicators with weak loadings for the latent variables. The variability in each indicator should explain at least 50% of its latent variable construct (|loading| ≥ .707; communality ≥ .50) (Henseler et al., 2009; Sanchez, 2013; Chinn, 2010). Otherwise, it is identified as a weak loading. The following reflective indicators did not explain a significant portion of its latent construct and was a weak loading: PP_InfEd, PP_Likert, Q44, Q45_R, Q40, Q41, Q49_1, Q49_2, Q49_3, Q49_4, Q49_5, Q49_6, Q49_7, Q49_8, Q49_9, Q49_10, Q49_11, Q49_12, Q49_15, Q49_17, and SINTFUT_IoTChanges. Typically, indicators with weak loadings would be removed, but in this case, all were retained due to reduced predictive power during analysis with them removed. The weak loadings of Q49 are particularly concerning, as those are all but one of the SINTFUT Changes questions.

Indicator	Construct	Weight	Loading	Communality	Redundancy
PP_FormalEd	PP	0.28	0.82	0.67	0.00
PP_InfEd	PP	0.28	0.69	0.47	0.00
PP_Cert_Count	PP	0.26	0.73	0.53	0.00
PP_ITCSJob	PP	0.24	0.76	0.57	0.00
PP_Likert	PP	0.34	0.62	0.39	0.00
Q42	SEFF	0.23	0.84	0.71	0.17
Q43	SEFF	0.26	0.89	0.79	0.19
Q44	SEFF	0.16	0.67	0.45	0.11
Q45_R	SEFF	0.08	0.42	0.18	0.04
Q46	SEFF	0.23	0.88	0.77	0.18
Q47	SEFF	0.27	0.88	0.77	0.18
Q38	LocusofControl	0.36	0.84	0.70	0.00
Q39	LocusofControl	0.38	0.83	0.68	0.00
Q40	LocusofControl	0.29	0.71	0.50	0.00
Q41	LocusofControl	0.25	0.70	0.49	0.00
SINTEX_SecSoftware	SINT_EX	0.37	0.82	0.67	0.32
SINTEX_NetworkPro	SINT_EX	0.46	0.88	0.78	0.37
SINTEX_IoTPro	SINT_EX	0.39	0.74	0.55	0.27
Q49_1	SINT_FUT	0.14	0.48	0.23	0.07
Q49_2	SINT_FUT	0.10	0.61	0.37	0.12
Q49_3	SINT_FUT	0.01	0.49	0.24	0.07
Q49_4	SINT_FUT	0.04	0.50	0.25	0.08
Q49_5	SINT_FUT	0.06	0.54	0.29	0.09
Q49_6	SINT_FUT	0.06	0.52	0.27	0.09
Q49_7	SINT_FUT	0.14	0.58	0.33	0.11
Q49_8	SINT_FUT	0.10	0.51	0.26	0.08
Q49_9	SINT_FUT	0.06	0.53	0.28	0.09
Q49_10	SINT_FUT	-0.05	0.15	0.02	0.01
Q49_11	SINT_FUT	0.28	0.66	0.44	0.14
Q49_12	SINT_FUT	0.07	0.64	0.41	0.13
Q49_15	SINT_FUT	0.08	0.56	0.31	0.10
Q49_16	SINT_FUT	0.18	0.71	0.50	0.16
Q49_17	SINT_FUT	0.17	0.70	0.50	0.16
SINTFUT_IoTChanges	SINT_FUT	0.19	0.54	0.29	0.09
Q6	Gender	1.00	1.00	1.00	0.00
Q4_PostHoc	Ethnicity	1.00	1.00	1.00	0.00
Q7	IoT_Ownership	1.00	1.00	1.00	0.00

Table 59 Outer Model Summary Table

Reflective indicator crossloadings were tested to assess the validity of the model. A crossloading occurs, when an indicator has a higher absolute loading on a different latent variable compared to the specified latent variable for that indicator (Henseler et al., 2015; Henseler et al., 2009; Sanchez, 2013). Q49_10 exhibited crossloadings and should be taken into

consideration for removal from the model, because it is not evident which factors or factor the variable is affecting. However, removal of Q49_10 decreased the predictive power of the model.

Indicator	PP	SEFF	LocusofControl	SINT_EX	SINT_FUT	Gender	Ethnicity	IoT_Ownership
PP_FormalEd	**0.82**	0.35	0.13	0.48	0.24	-0.26	0.12	-0.07
PP_InfEd	**0.69**	0.35	0.15	0.51	0.19	-0.26	0.05	-0.13
PP_Cert_Count	**0.73**	0.33	0.18	0.39	0.26	-0.21	0.12	0.00
PP_ITCSJob	**0.76**	0.31	0.16	0.39	0.21	-0.15	0.12	-0.07
PP_Likert	**0.62**	0.38	0.28	0.51	0.39	-0.16	0.11	-0.06
Q42	0.36	**0.84**	0.50	0.39	0.36	-0.26	0.26	-0.10
Q43	0.46	**0.89**	0.47	0.42	0.38	-0.32	0.22	-0.10
Q44	0.25	**0.67**	0.39	0.28	0.26	-0.07	0.19	-0.10
Q45_R	0.15	**0.42**	0.24	0.15	0.08	-0.25	0.17	-0.16
Q46	0.44	**0.88**	0.44	0.40	0.30	-0.28	0.21	-0.16
Q47	0.50	**0.88**	0.47	0.50	0.33	-0.29	0.15	-0.06
Q38	0.30	0.53	**0.84**	0.29	0.32	-0.06	0.08	-0.22
Q39	0.19	0.38	**0.83**	0.26	0.38	-0.02	0.15	-0.08
Q40	0.14	0.34	**0.71**	0.24	0.26	-0.08	0.12	-0.09
Q41	0.13	0.43	**0.70**	0.13	0.29	0.00	0.12	-0.06
SINTEX_SecSoftware	0.47	0.38	0.24	**0.82**	0.32	-0.30	0.11	-0.07
SINTEX_NetworkPro	0.63	0.46	0.29	**0.88**	0.42	-0.30	0.10	-0.13
SINTEX_IoTPro	0.45	0.34	0.22	**0.74**	0.41	-0.21	0.05	-0.26
Q49_1	0.21	0.26	0.27	0.18	**0.48**	-0.01	0.12	-0.05
Q49_2	0.14	0.15	0.22	0.15	**0.61**	0.06	0.16	-0.00
Q49_3	0.00	-0.05	0.12	0.07	**0.49**	0.14	0.02	-0.07
Q49_4	0.03	0.04	0.10	0.10	**0.50**	0.06	0.08	-0.05
Q49_5	0.07	0.09	0.14	0.13	**0.54**	0.08	0.02	-0.09
Q49_6	0.00	0.04	0.19	0.09	**0.52**	0.03	0.11	-0.00
Q49_7	0.16	0.20	0.18	0.29	**0.58**	-0.12	-0.03	-0.12
Q49_8	0.14	0.15	0.27	0.19	**0.51**	0.00	0.05	0.04
Q49_9	-0.10	0.09	0.13	0.10	**0.53**	-0.06	0.14	-0.01
Q49_10	-0.35	-0.02	0.05	-0.05	**0.15**	0.01	-0.04	-0.02
Q49_11	0.40	0.45	0.31	0.48	**0.66**	-0.25	0.19	-0.06
Q49_12	0.04	0.16	0.20	0.14	**0.64**	-0.03	0.05	0.07
Q49_15	0.06	0.11	0.14	0.17	**0.56**	0.03	0.17	0.02
Q49_16	0.24	0.27	0.34	0.30	**0.71**	-0.13	0.09	0.03
Q49_17	0.29	0.24	0.27	0.34	**0.70**	-0.05	0.06	-0.06
SINTFUT_IoTChanges	0.30	0.18	0.26	0.41	**0.54**	-0.14	0.06	-0.08
Q6	-0.29	-0.32	-0.05	-0.33	-0.13	**1.00**	-0.08	-0.08
Q4_PostHoc	0.14	0.25	0.15	0.11	0.16	-0.08	**1.00**	-0.05
Q7	-0.10	-0.13	-0.16	-0.19	-0.06	-0.08	-0.05	**1.00**

Table 60 Loadings and Crossloadings of the Outer Model

Bootstrapping was performed with 1000 resamples. The loadings were assessed for the reflective indicators, and the weights were examined for the formative indicators. Significance was determined using confidence intervals for the given parameter estimates, which were

calculated based on an alpha value of 0.05 (Henseler et al., 2009; Sanchez, 2013; Chinn, 2010). Q49_10 did not have a significant loading for its latent variable. Since there were no formative indicators, the bootstrapped weights were not examined. Any indicator that does not have a significant loading or weight should be examined whether it belongs to the specified latent variable or if it should be kept in the model.

Construct-Indicator	*M*	*SE*	CI
PP-PP_FormalEd	0.82	0.03	[0.77, 0.87]
PP-PP_InfEd	0.68	0.04	[0.60, 0.77]
PP-PP_Cert_Count	0.73	0.04	[0.66, 0.81]
PP-PP_ITCSJob	0.76	0.04	[0.68, 0.83]
PP-PP_Likert	0.63	0.04	[0.54, 0.71]
SEFF-Q42	0.84	0.03	[0.79, 0.90]
SEFF-Q43	0.89	0.02	[0.86, 0.92]
SEFF-Q44	0.67	0.05	[0.58, 0.76]
SEFF-Q45_R	0.42	0.08	[0.27, 0.58]
SEFF-Q46	0.88	0.02	[0.84, 0.91]
SEFF-Q47	0.88	0.02	[0.85, 0.91]
LocusofControl-Q38	0.83	0.03	[0.78, 0.89]
LocusofControl-Q39	0.83	0.04	[0.75, 0.90]
LocusofControl-Q40	0.70	0.05	[0.60, 0.80]
LocusofControl-Q41	0.70	0.06	[0.59, 0.81]
SINT_EX-SINTEX_SecSoftware	0.81	0.03	[0.75, 0.88]
SINT_EX-SINTEX_NetworkPro	0.88	0.02	[0.84, 0.92]
SINT_EX-SINTEX_IoTPro	0.75	0.04	[0.68, 0.82]
SINT_FUT-Q49_1	0.48	0.08	[0.31, 0.64]
SINT_FUT-Q49_2	0.61	0.07	[0.47, 0.74]
SINT_FUT-Q49_3	0.48	0.10	[0.27, 0.68]
SINT_FUT-Q49_4	0.50	0.09	[0.31, 0.68]
SINT_FUT-Q49_5	0.53	0.09	[0.35, 0.71]
SINT_FUT-Q49_6	0.51	0.09	[0.34, 0.69]
SINT_FUT-Q49_7	0.56	0.06	[0.44, 0.69]
SINT_FUT-Q49_8	0.50	0.08	[0.34, 0.67]
SINT_FUT-Q49_9	0.52	0.09	[0.34, 0.70]
SINT_FUT-Q49_10	0.15	0.11	[-0.07, 0.36]
SINT_FUT-Q49_11	0.65	0.05	[0.55, 0.76]
SINT_FUT-Q49_12	0.63	0.07	[0.49, 0.77]
SINT_FUT-Q49_15	0.55	0.07	[0.42, 0.69]
SINT_FUT-Q49_16	0.70	0.06	[0.59, 0.81]
SINT_FUT-Q49_17	0.70	0.05	[0.60, 0.80]
SINT_FUT-SINTFUT_IoTChanges	0.53	0.06	[0.41, 0.66]
Gender-Q6	1.00	0.00	[1.00, 1.00]
Ethnicity-Q4_PostHoc	1.00	0.00	[1.00, 1.00]
IoT_Ownership-Q7	1.00	0.00	[1.00, 1.00]

Table 61 Bootstrap Results for the Weights for Each Indicator

The structural or inner model was assessed by examining the R^2-values for each endogenous variable, the average variance extracted (AVE) for each latent variable with

reflective indicators, and the goodness of fit (GoF) index for the model. Bootstrapping was also used to determine the reliability of the inner model.

To determine if the relationships among the latent variables are appropriate, R^2-values were calculated for each endogenous variable. Each endogonous variable should have an R^2-value ≥ .20 (Sanchez, 2013). There were no low R^2-values, indicating that each relationship is appropriate for the model.

To verify that each latent variable has a strong relationship with its reflective indicators, the average variance extracted for each construct was calculated. Each latent variable should have an AVE ≥ .50, which suggests that 50% or more of the variance for the indicators is explained by its latent variable (Henseler et al., 2009; Sanchez, 2013; Chinn, 2010). AVE is only assessed for reflective variables. The following latent variables had an AVE < .50: SINT_FUT. However, it is one of two dependent variables and was retained.

Construct	Type	R^2	AVE
PP	Exogenous	--	0.53
SEFF	Endogenous	0.24	0.61
LocusofControl	Exogenous	--	0.59
SINT_EX	Endogenous	0.48	0.67
SINT_FUT	Endogenous	0.32	0.31
Gender	Exogenous	--	1.00
Ethnicity	Exogenous	--	1.00
IoT_Ownership	Exogenous	--	1.00

Table 62 Variance of Latent Variables

The predictive power of the PLS-PM can be determined by the GoF index. The GoF index is calculated by computing the geometric mean of the average R^2-values and average communality for each latent variable. Values greater than .90 are considered a good model fit, while a GoF index less than .90 and greater than .70 is an acceptable model fit (Sanchez, 2013; Chinn, 2010). The GoF index, GoF = 0.40, indicates that the model had a poor model fit and poor ability to predict.

Bootstrapping was performed with 1000 resamples. The following regression paths did not have a significant relationship: LocusofControl and Ethnicity → SINT_EX, PP, SEFF, Gender, Ethnicity, and IoT Ownership → SINT_FUT.

Path	Original B	*M*	*SE*	CI
PP → SEFF	0.49	0.49	0.05	[0.40, 0.58]
PP → SINT_EX	0.50	0.50	0.05	[0.40, 0.61]
SEFF → SINT_EX	0.14	0.14	0.07	[0.00, 0.28]
LocusofControl → SINT_EX	0.08	0.08	0.06	[-0.03, 0.19]
Gender → SINT_EX	-0.15	-0.15	0.05	[-0.25, -0.05]
Ethnicity → SINT_EX	-0.03	-0.03	0.05	[-0.13, 0.08]
IoT_Ownership → SINT_EX	-0.12	-0.12	0.04	[-0.21, -0.03]
PP → SINT_FUT	0.06	0.06	0.09	[-0.11, 0.23]
SEFF → SINT_FUT	0.04	0.05	0.09	[-0.13, 0.22]
LocusofControl → SINT_FUT	0.27	0.27	0.07	[0.14, 0.41]
SINT_EX → SINT_FUT	0.35	0.35	0.07	[0.21, 0.49]
Gender → SINT_FUT	0.04	0.04	0.06	[-0.08, 0.15]
Ethnicity → SINT_FUT	0.07	0.08	0.06	[-0.03, 0.19]
IoT_Ownership → SINT_FUT	0.07	0.07	0.06	[-0.06, 0.19]

Table 63 Bootstrap Results for PLS-PM with Demographic Variables

Figure 39 below shows the significant relationships between variables in this model. With the demographic variables included, self-efficacy has a statistically significant relationship with security intentions (existing) and locus of control has an effect on security intentions (future).

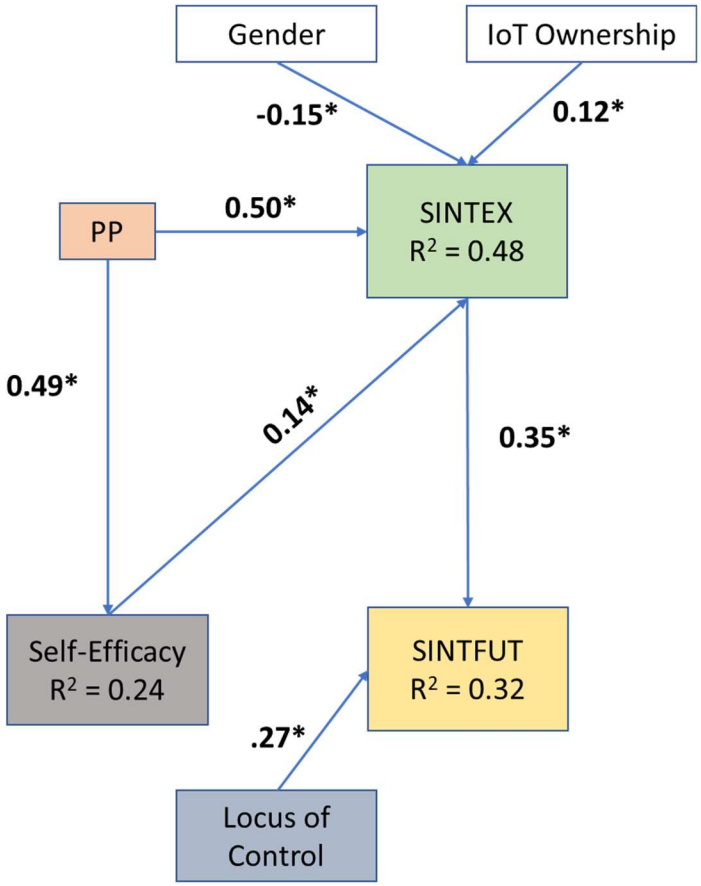

Figure 37 PLS-PM With Demographic Variables

The negative relationship between gender and security intentions (existing) demonstrates that female and transgender respondents have lower security intentions than males, as a group. IoT owners have higher security intentions. The percentage of variance explained by the model decreased for both existing and future security intentions. With the addition of demographics,

perceived self-efficacy effect security intentions (existing) and locus of control effects security intentions (future).

5.7 Structural Equation Modeling

The data was analyzed through structural equation modeling to determine the relationships between the latent variables. The squared Mahalanobis distances were calculated for the data and plotted against the quantiles of a Chi-square distribution (DeCarlo, 1997; Field, 2013). In the scatterplot, the solid line represents the theoretical quantiles of a normal distribution. Normality can be assumed if the points form a relatively straight line. The scatterplot for normality is presented in Figure 105.

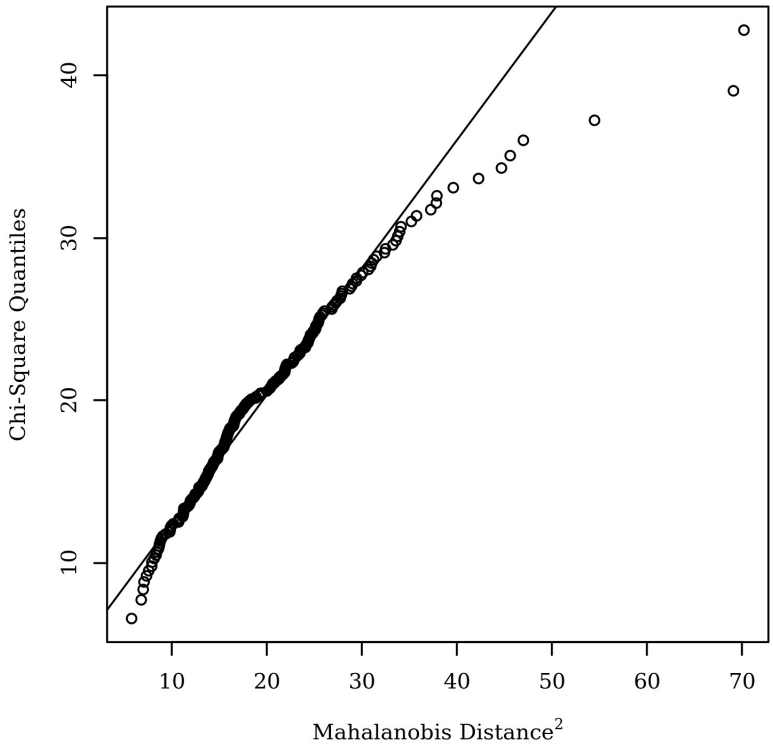

Figure 38 Mahalanobis Distance

Mahalanobis distances were calculated and compared to a χ^2 distribution (Newton & Rudestam, 2012). An outlier was defined as any Mahalanobis distance that exceeds 45.31, the

.999 quantile of a χ^2 distribution with 20 degrees of freedom (Kline, 2015). There were 5 observations detected as outliers.

Although variables should be correlated with one another to be considered suitable for factorization, variables that are too highly correlated can cause problems in SEM. To assess multicollinearity, the squared multiple correlations were inspected and the determinant of the correlation matrix was calculated. There were no variables that had an $R^2 > .90$. The value of the determinant for the correlation matrix was 0.00011, indicating that there was no multicollinearity in the data.

Reliability was tested based on the sample size used to construct the model and evaluated using the Chi-square goodness of fit test and fit indices. R^2 was calculated for each variable.

Parameter Estimate	Unstandardized	Standardized	*p*
SINT_EX ← PP	0.49(0.08)	0.60	< .001
SINT_EX ← SEFF	0.17(0.09)	0.19	.065
SEFF ← PP	0.48(0.07)	0.51	< .001
SINT_EX ← LofC	0.10(0.10)	0.10	.298
SINTFUT ← PP	-0.11(0.07)	-0.27	.122
SINTFUT ← SEFF	-0.09(0.07)	-0.20	.197
SINTFUT ← LofC	0.27(0.08)	0.48	.002
SINTFUT ← SINT_EX	0.39(0.10)	0.77	< .001
Indirect Effect of PP on SINT_EX by SEFF	0.08(0.04)	0.10	.065
Total Effect of PP on SINT_EX	0.57(0.07)	0.70	< .001
Indirect Effect of PP on SINTFUT by SEFF	-0.04(0.03)	-0.10	.201
Total Effect of PP on SINTFUT	-0.16(0.07)	-0.37	.036
Covariance for PP and LofC	0.26(0.08)	0.26	.002
Covariance for SEFF and LofC	0.47(0.08)	0.60	< .001
Error in PP	1.30(0.19)	1.00	< .001
Error in PP_FormalEd	0.63(0.09)	0.33	< .001
Error in PP_InfEd	1.95(0.21)	0.62	< .001
Error in PP_Cert_Count	4.60(0.51)	0.53	< .001
Error in PP_ITCSJob	1.41(0.16)	0.51	< .001
Error in PP_Likert	0.27(0.03)	0.81	< .001
Error in SEFF	0.83(0.12)	0.74	< .001
Error in Q42	0.65(0.07)	0.36	< .001
Error in Q43	0.59(0.07)	0.26	< .001
Error in Q44	1.11(0.11)	0.64	< .001
Error in Q45_R	2.01(0.19)	0.86	< .001
Error in Q46	0.58(0.07)	0.28	< .001
Error in Q47	0.71(0.09)	0.26	< .001
Error in LofC	0.75(0.11)	1.00	< .001
Error in Q38	0.42(0.06)	0.36	< .001
Error in Q39	0.48(0.06)	0.47	< .001
Error in Q40	1.33(0.14)	0.68	< .001
Error in Q41	0.72(0.08)	0.61	< .001
Error in SINT_EX	0.37(0.08)	0.43	< .001
Error in SINTEX_SecSoftware	0.84(0.10)	0.49	< .001
Error in SINTEX_NetworkPro	1.20(0.24)	0.25	< .001
Error in SINTEX_IoTPro	1.47(0.15)	0.67	< .001
Error in SINTFUT	0.09(0.05)	0.39	.051
Error in SINTFUT_Changes	0.53(0.07)	0.70	< .001
Error in SINTFUT_IoTChanges	4.29(0.59)	0.66	< .001

Table 64 Loadings and Significance for SEM

The correlation between locus of control and past performance is the lowest of all variable correlations, followed by the correlation between past performance and security

intentions (future). The correlation between past performance and security intentions (existing) is the highest.

Variable	PP	SEFF	LofC	SINT_EX	SINTFUT
PP	1.00	--	--	--	--
SEFF	0.51	1.00	--	--	--
LofC	0.26	0.65	1.00	--	--
SINT_EX	0.72	0.56	0.37	1.00	--
SINTFUT	0.31	0.40	0.57	0.64	1.00

Table 65 Latent Variable Correlations

While these analyses have included the Chi-square goodness of fit test, it is sensitive to sample size, causing the test to almost always reject the null hypothesis and indicate a poor model fit when the sample size is large (Hooper et al., 2008). The results of the Chi-square goodness of fit test were significant, $\chi^2(160) = 303.24$, $p < .001$, suggesting that the model did not adequately fit the data.

Conversely, the RMSEA index was less than .08, RMSEA = 0.06, 90% CI = [0.05, 0.07], which is indicative of a good model fit (Hooper et al., 2008). The CFI was between .90 and .95, CFI = 0.92, suggesting an acceptable fit. The TLI was less than .95, TLI = 0.91, which is indicative of a poor model fit. The SRMR was between .05 and .08, SRMR = 0.07, which implies that the model fits the data adequately (Hooper et al., 2008).

TLI	CFI	RMSEA	SRMR
0.91	0.92	0.06	0.07

Table 66 SEM Model Fit Indices

The regressions in the model can be assessed by examining the R^2 value of each endogenous variable. The R^2 value identifies how much the endogenous variable is explained by the regressions in the model. An R^2 value $\leq .20$ suggests the endogenous variable is not adequately explained by the regression(s) in the model and all regressions for that endogenous variable should be considered for removal from the model (Hooper et al., 2008). The following endogenous variables had R^2 values $\leq .20$: PP_Likert and Q45_R. However, removal of the items

reduced the predictive power of the model. Additionally, the importance of PP_Likert as a predictor was highlighted in hierarchical linear regression.

Endogenous Variable	Standard Error	R^2
PP_FormalEd	0.63	0.67
PP_InfEd	1.95	0.38
PP_Cert_Count	4.60	0.47
PP_ITCSJob	1.41	0.49
PP_Likert	0.27	0.19
SEFF	0.83	0.26
Q42	0.65	0.64
Q43	0.59	0.74
Q44	1.11	0.36
Q45_R	2.01	0.14
Q46	0.58	0.72
Q47	0.71	0.74
Q38	0.42	0.64
Q39	0.48	0.53
Q40	1.33	0.32
Q41	0.72	0.39
SINT_EX	0.37	0.57
SINTEX_SecSoftware	0.84	0.51
SINTEX_NetworkPro	1.20	0.75
SINTEX_IoTPro	1.47	0.33
SINTFUT	0.09	0.61
SINTFUT_Changes	0.53	0.30
SINTFUT_IoTChanges	4.29	0.34

Table 67 SEM Error and Variance Values

The regressions were examined based on an alpha value of 0.05, with PP significantly predicting SINT_EX and SEFF, LofC significantly predicting SINTFUT, and SINTEX significantly predicting SINTFUT.

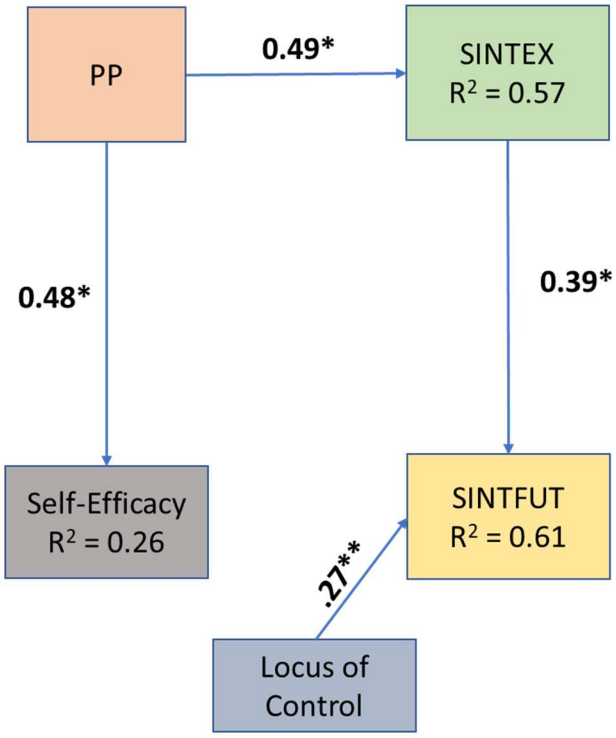

Figure 39 Structural Equation Model

The regressions were examined based on an alpha value of 0.05, with PP significantly predicting SINT_EX, LofC significantly predicting SINTFUT, and SINTEX significantly predicting SINTFUT. These results are consistent with the partial least squares path model that included gender and IoT ownership.

The hypotheses for this model were:

H_6: Locus of control, perceived self-efficacy, and past performance effect security intentions (existing).

H_7: Locus of control, perceived self-efficacy, and past performance effect security intentions (future).

H_6 was partially supported and partially rejected. Like PLS_PM, past performance had an effect on security intentions (existing).

H_7 was partially supported and partially rejected. Locus of control had an effect on security intentions (future).

5.8 Explanation of Findings

The null hypothesis that past performance, perceived self-efficacy, and locus of control had no effect on security intentions was partially supported. Therefore, the alternate hypothesis that locus of control, self-efficacy, and past performance have a statistically significant effect on existing and future security intentions was partially rejected. Across all of the models, different combinations of the variables and/or latent variables had different effects. The only variable completely excluded was past performance (IT/CS job), which had not statistically significant effect on any other variable. Locus of control only effected security intentions (future), while self-efficacy effected security intentions (existing) in some models and security intentions (future) in others.

One of the strengths of hierarchical linear regression is the ability to explore relationships amongst the variables directly and in-depth. Whereas in path modeling and structural equation modeling, the latent variable constructs are measured against the other latent variable constructs, in hierarchical linear regression, the effect of components of the construct are compared with components of other constructs. One example of this is the effect of PP_Likert, which has its strongest relationships with network protection measures and IoT protection measures at 0.90 and 0.85, respectively. However, in path modeling analysis, it had a weight of 0.34, which was only slightly higher than PP_CertCount at 0.24. PP_CertCount has a slight effect only on SINTEX_NetworkPro, but looking solely at the path modeling analysis would not provide that information. Additionally, the regression analysis determined there was a negative relationship

between self-efficacy and SINTFUT_IoTChanges and no relationship between self-efficacy and SINFUT_Changes.

However, one of the weaknesses of hierarchical linear regression is the complexity of the model and that it may be finding relationships that are not strong enough to be included in a parsimonious model. While HLR was able to exclude ITCS_Job as an influence, all other variables had at least one statistically significant relationship, even if it may have only had a small effect. For exploratory studies, this may not be a true weakness, in that it allows researchers to take the more detailed information and refine the survey instrument for continued research. Another weakness was the inability to analyze demographic variables to due to not having sufficient representation in the number of cases for each demographic. There were low-density categories within the respondents that would have been excluded from analysis in order to perform a regression exploring their effects on the main variables.

While the path modeling and structural equation modeling analyses are more parsimonious, due to analyzing the latent variable constructs, they contradict some of the findings from the linear regression. For example, in the path modeling analysis, when the five latent variables were explored, self-efficacy only effected SINTFUT and past performance only effected SINTEX, with locus of control not having a relationship with either variables. However, when demographics were added, self-efficacy had a statistically significant effect on SINTEX, past performance had a large effect on self-efficacy, and locus of control had a moderate effect on SINTFUT. The second model, including demographics, appears to be closer to the hierarchical linear regression model.

Structural equation modeling reported higher R^2 values for SINTEX, SINTFUT, and self-efficacy, as well as similar path coefficients to path modeling, but without including the

demographics in the analysis. One difference is that self-efficacy does not load on either of the dependent variables and is effected by past performance. While the relationship with past performance is not unexpected, it is unexpected that self-efficacy did not influence either SINTEX or SINTFUT.

The R^2 values for the dependent variables show promise in the amount of variance explained with a small number of variables. However, the inconsistency between the four different models, hierarchical linear regression, two partial least squares path modeling models, and structural equation model, deserves further investigation. While this study was based on three independent variables that are common in most information security theories, they usually do not appear together. In this case, it appears that adding additional variables may provide greater explanatory power, as opposed to removing variables. Each time, a question or variable was removed, the predictive power of the overall model decreased.

Additionally, standardizing the instrument would be beneficial in improving the consistency between the methods of analysis. One cannot directly compare the results of the hierarchical linear regression with those of the two partial least squares methods, which had similar, but not identical results.

Chapter 6 Summary and Conclusion

Studies of IoT tend to fall into the following groups: technology adoption and usability, IoT as an enabler, securing IoT around the user, human-computer interaction, privacy, and technical papers concerning specific technologies and protocols.

Studies of human factors in cybersecurity focus on users in an organizational context, cybersecurity professionals, and home PC users. One exception is Egelman and Peer's work, which is environment neutral and just focuses on users, even acknowledging that there is high variance in security-related behaviors based on the environmental context ("e.g. at home vs. at the workplace") (Egelman & Peer, 2015).

This study explored a research gap by focusing on home IoT users and cybersecurity in the context of the entire home interconnected ecosystem, including security software on a computer, network protection measures, and IoT device specific security measures. The study also offered a way to quantify cyber security knowledge without requiring skills tests or relying on self-reported comfort or time spent with technology.

6.1 Analysis of Survey Results

Previous studies have included past performance as a category of perceived self-efficacy or labeled it as knowledge. This study expanded past performance and explored the role of formal and informal education, as well as certifications, a job requiring IT/CS, and self-reported internet and email security questions. When separated from perceived self-efficacy, past performance accounted for 8-40% of the variance in the dependent variables. In the models themselves, past performance accounted for 50-97.5% of the total variance that the model could explain.

The survey results offered greater insight into home users, updating the information collected in a previous study (Cain, Edwards, & Still, 2018). While this study used a theoretical background and also evaluated and measured variables and constructs, the Cain, Edwards, and Still (2018) study was exploratory. Their focus was on home computing, social media, past cyber attacks, expertise and training, and demographic comparisons.

Unfortunately, their methodology may have degraded the quality of the information that they were attempting to analyze. During their three knowledge segments (concepts, threats, and behaviors), answers were collected on a Likert scale ranging from disagree to agree, which were then converted to binary scores of correct or incorrect. Neutral and disagree were converted to either correct or incorrect depending on the answer and agree answers were converted to correct or incorrect (Cain, Edwards, & Still, 2018).

The survey also differed from other studies in that it explored IoT security intentions along with traditional computing security intentions. Other studies have focused on IoT adoption, home user security behaviors or intentions, and organizational user information security compliance or security behaviors. In this study, the goal was to evaluate past performance, locus of control, perceived self-efficacy, and security intentions, but also to explore home IoT users, their devices, and their security posture. There are twenty-four (4.23%) respondents with no reported security software, network protection measures, or IoT device protections.

Some respondents who do not own IoT devices, but even among those who considered them and did not install them (17.71%) and those who did not consider them (25.64%), security was not a heavily selected reason for not installing IoT devices. Based on this survey, it is not clear how well home users understand the threat posed by IoT devices. The study was not

designed to measure the threat appraisal or coping appraisal, but should be incorporated into future studies of home IoT users.

Analysis of demographics on the survey determined that there are some significant differences in the means of some dependent and independent variables, based on age, gender, race, and household income. General education level had no significant effect on any of the dependent or independent variables, thus lending credence to Bandura's assertion that perceived self-efficacy is domain-specific (Bandura, Guide for Constructing Self-Efficacy Scales, 2006).

Differing variable scales made it difficult to create a parsimonious model. The advantage to keeping the elements of each latent variable separate is discerning the effects of each component of past performance on each component of security intentions, rather than treating them like monoliths. Adding all existing security intention scores together into a single variable would have obfuscated the effect of perceived self-efficacy on security intentions. Due to the security intentions (future) changes question only being presented to those who answered yes to making changes in the future, combining the future security intentions into a single variable would reduce the number of cases to 267, eliminating over half of the respondents.

Internet and email security questions (PP_Likert) was the strongest predictor of four of the five dependent variables, despite its low communality. Security Intentions (Future) IoT Device Protection Changes was the only variable where there were stronger predictors in some iterations of the model. Locus of Control and Security Intentions (Existing) IoT Protection Measures were both higher than Internet and Email Security, with the addition of existing security intentions in the fourth model not only reducing the strength of the variable, but also rendering it statistically insignificant.

Based on communality, PP_Likert should have been removed from the scale. However, that issue likely stems from the different scales that the counts of past performance items are on compared to the Likert scale that the internet and email security items are on. When PP_Likert was removed, the predictive power of the model was reduced.

Both security intentions (future) variables had mixed directional effects. Perceived self-efficacy had a significant negative effect on security intentions (future) IoT changes and past performance formal education had an insignificant negative effect. However, this may be due to the already strong respondents not feeling the need to make any changes to their network to improve security. A previous analysis of the 122 people who answered that they felt their system was already secure enough, showed that they did have higher means in the positive security categories and lower means the security intentions (future) responses. Past performance formal education, informal education, and having an IT/CS job had small negative effects on security intentions (future) IoT device protection measures. The security intentions (future) questions were framed as changes to their existing configurations, so for those who had a strong configuration, they were less likely to make changes, while those who had few, if any, security measures in place were likely to self-report an intention to add security measures.

An IT/CS related job had no statistically significant effect on the models for any of the five dependent variables. This deserves further exploration to determine whether the respondents are working in places that do not require cyber security awareness training, whether that training is effective, and whether the respondents perceive that some organizational cybersecurity measures can be used on home networks and devices. This study did not ask any follow-up questions regarding on the job training for those who work in IT/CS related jobs, so it is impossible to draw conclusions from the data available. However, there are a lot of studies

concerning user security in an organizational environment and results from those may not have a correlation to security in the home environment, as briefly mentioned in the literature review.

Formal education had a statistically significant effect on security software and network protection measures, but not on IoT protection measures. IT and CS programs teach computers and networking, but not IoT security configurations. It is possible that without learning the specific task of securing IoT, even those with an IT/CS background, are not comfortable with securing it.

Informal education scores had a statistically significant score on IoT protection measures. Perhaps those who are more comfortable seeking their own answers through the Internet or friends are more likely to pursue the information needed to secure their IoT devices. There is little formal training available in IoT security to home users, thus requiring them to seek their own answers through informal means. Seeking answers through informal means shows that the user is proactive, which, if measured as a variable, may provide further insight in future studies.

Certifications only had a statistically significant effect on network protection measures. Certifications tend to focus on organizational IT and security, which may not directly correlate to home security measures, and especially not to IoT security. While there are certifications in IoT, they are new, not focused on security, and designed for professionals, not home users (Wouk, 2020). Based on certifications and IT/CS jobs having little to no effect on home user security intentions, studying how respondents perceive the link between the two environments may provide insight into why those relationships are insignificant.

"Trying to change unsafe behaviors is difficult because there are no immediate obvious negative consequences (Pelgrin, 2014)." For IoT, this statement is even more prescient in that

there is no security feedback mechanism for the user unless an attacker chooses to make their presence known.

The difference in IoT protection measures between question 35 and question 51 highlight a missed opportunity to directly incorporate the fear appeals model into the survey instrument. It appears that there was a strong effect just from the questions asked in the survey, causing those who were less secure to want to improve their security posture. However, no questions were asked to measure the survey effect, such as a Likert item re-measuring anxiety (Q45). In post hoc analysis, I removed the additional answer that was available on question 51 to directly compare answers to question 35. Additionally, the question could be reworded asking users to include their existing IoT protection measures and check any additional protection measures they intend to implement as a result of the survey.

6.2 Implications

Based on the models, past performance, perceived self-efficacy, and locus of control explain between 16 to 41% of individual variables' variance amongst the security intentions variables. When grouped into latent constructs, the two security intentions constructs saw 32 to 68% of their variance explained by the models. Due to the

This study also highlights the interaction effect of more complex models. While there are some that explain 60% or more of variance in security intentions, there are many that explain closer to 25-46%, with far more than three latent variables. For example, Herath and Rao (2009) studied intention to comply with security policy with an R^2 value of 0.47, which had ten latent variables, comprised of an undetermined number of items, supporting four constructs.

From an academic perspective, insight into users' IoT security intentions as compared to their computer and network security intentions allows for future experimentation into

manipulating independent variables to determine the effect on the dependent variable. For example, determining how to approximate the confidence of past performance in an experiment could greatly improve home user security. From a practitioner perspective, the results of those experiments can help determine hardware, software, subscription services, and/or configurations users would feel comfortable configuring securely. Prior to an initial experimental run, a focus group to determine users' perspectives on security in IoT and what they need would make it easier to determine which independent variables to focus on first and how best to manipulate them.

Another actionable insight is the value in adding IoT specific curriculum to existing programs, such as K-12 education, college courses, and existing security certifications. Given the high loadings, weight, correlations, and path coefficients of past performance, it is a great place to start to improve security. However, in recent research, a study examined student interest and self-efficacy in secure design for IoT, where taking the course increased student interest in four of seven categories, while decreasing student confidence in all categories (Sharevski, Treebridge, & Westbrook, 2019). While one usually does not want to reduce confidence, the interest in continuing increased. Additionally, in the HLR model, a decrease in self-efficacy corresponded to an increase in future IoT changes. Paradoxically, lower confidence in IoT abilities may lead to better security.

In the instrument itself, adding a fear appeals measurement would likely greatly increase the percentage of variance explained. There was a noticeable difference between IoT security measurements approximately halfway through the survey and a similar question at the end. Thinking about security had a noticeable effect, but the phrasing of the question made it difficult to draw definitive conclusions.

6.3 Limitations

The following limitations shape the research, participants must have: opted-in, been over 18, sighted and hearing, had Internet access, and the initial sampling frame consists primarily of individuals with college degrees. This is likely due to the snowball sampling method, where the initial population is encouraged to share the information with their social networks. The overall participant population may have been more demographically balanced for a random sampling, particularly in educational background.

For the survey results to be generalizable independent of the experiment required 384 participants to achieve 95% confidence +/- 5% (Custom Insight, 2017), based on an estimated total population of 201,726,417 IoT device owners. That number is based on the United States population of 325,365,189 on July 4, 2017 (United States Census Bureau, 2017) and the estimate that 62% of Americans have at least one IoT device (Interactive Advertising Bureau; Maru Matchbox, 2016). For past performance, self-efficacy, locus of control, and security intentions (existing), there were 569 respondents. However, security intentions (future) was an optional question, which only 227 respondents answered.

The survey used an unweighted convenience sample, rather than a weighted population sample. While this is not as generalizable as a population sample, it can be completed more quickly and at no additional cost. Convenience samples cannot fully replace population samples, but exhibit the same trends and statistical significance as population samples at a lower cost (Mullinix, Leeper, Druckman, & Freese, 2015). The results of this research are generalizable to a higher income and more educated segment of the population, who have more technical education than the average American.

The study did not test a full theory, such as theory of reasoned action, theory of planned behavior, protection motivation theory, or health belief model. By focusing solely on past performance, locus of control, and self-efficacy, some of the explanatory power that comes with threat and coping variables, fear appeals, and response efficacy were lost.

6.4 Contributions

This study explored the relationships between locus of control, self-efficacy, past performance and user security intentions in depth. While various studies have explored these factors, they were either in the context of several other variables or excluded one or more of the variables. This was intended as a preliminary exploration to determine the interrelationships of these variables, what aspects of past performance have the most influence on security intentions, and how locus of control, self-efficacy, and past performance may contribute to the confidence construct. The main contribution of this study will be the role of past performance in security intentions, as well as the past performance factors that most influence user security behaviors.

Past performance has a single question derived from a prior study, where it was included as an aspect of perceived self-efficacy. The remaining questions are expansions upon various elements of past performance, such as informal education, formal education, and Internet security habits.

This study provided an initial set of measurements for past performance and security intentions, verification of the locus of control instrument, and verification of the perceived self-efficacy questions. While there is room for improvement, the instrument is adequately reliable and valid.

This instrument divides security intentions into security software, network protection, and IoT device protection, providing a modular instrument for testing various aspects of home users'

computing environment. Past performance also diversifies the information collected from the user, requesting information concerning certifications, classes taken in high school and college, working in IT/CS-related employment, and internet and email security questions. By collecting more detailed data from the user concerning their level of experience, the model can account for a solid portion of the variance in security behaviors with minimal variables.

There were significant race and gender discrepancies in the measured variables, which deserve further attention to determine the cause.

6.5 Future Work

The survey questions concerning locus of control and self-efficacy are derived from existing literature, modified for the IoT home user audience, but the other items were developed for this research. While they were sufficiently valid and reliable, there is room for improvement. Standardizing questions and scales will vastly improve the statistical analysis of the data. Attempting to eliminate elements with low loadings or communality reduced the predictive power of the model. This indicates that additional elements need to be added, rather than removed. Testing additional survey questions and variables could improve the predictive power of the models, especially those that account for barriers to adopting security measures such as response cost.

Testing user interfaces to improve security feasibility could improve security by having IoT devices boot directly into a secure setup menu. In an experiment, a control group would get a regular device without the secure menu, while the experimental group would get the special menu. A pre-survey would measure the human factors variables, while a post-test survey would determine whether the user was more confident in their ability to secure their device.

Experiments operationalizing the elements of behavior to determine their effects on security intentions could provide greater insight into improving the home security without waiting for manufacturers to incorporate security features and interfaces for users into their applications. One example would be an experiment where users are divided into two groups, a control group who receives an unopened IoT device and a group that receives the IoT device, along with complete step by step instructions to install it securely. Neither group would receive a prompt directing a secure installation, but would receive a prompt to install it as they would in their own home. Another experiment could measure the effects of being told to install an IoT device, one group with directions and one without.

Additionally, future work could explore the relationship between security intentions and security behaviors. A future study could obtain the participant's home security configuration, administer the survey, then check their security configuration 30 days later to determine if the participants made the changes to their security configurations after their experience. User's self-reported security intentions can be misconfigured, resulting in their reported configuration not matching their actual configuration. While a user may have the intention to secure their network, it may not happen in practice and future research should determine how intentions and behavior interrelate.

Future work will focus on continuing to evaluate and refine the full NOAH for IoT framework, as well as evaluating the role of each component of the framework to develop a predictive model to improve home network security for individuals. Having quantitative data regarding the effect of confidence may improve the focus placed on the role of the home user in securing their devices, as the goal is to improve home user security.

Experimentally validating the NOAH for IoT framework will allow for a predictive model that can be used by a home user to determine their current security posture, as well as to provide recommendations for how to improve it. Participants could complete the questions from the survey instruments concerning their home network and then receive an estimated security posture and recommendations for improving it. The survey, coupled with network scanning tools, could provide home users with actionable information similar to that organizations receive from their IT security personnel.

Additionally, after validating the NOAH for IoT framework, future work will focus on validating the larger, organizationally focused NOAH framework. A similar system would be created, allowing employees to complete surveys that would then be aggregated to determine the organization's security posture. While organizations have various tools to test the technical configuration of the network, they do not have complete oversight into the behavior of users on the network. Incorporating anonymous feedback concerning user behavior will allow an organization to determine when more education or enforcement may be needed.

6.6 Conclusion

According to the survey, 15.11% of respondents had no obvious security training, such as formal or informal education, certifications, or on the job training. That is a sizeable portion of the population with no obvious method to defend themselves, which puts them, and the rest of us at risk. By virtue of being connected, we are invested in each other's success with security.

Despite research into human factors of security compliance dating back to 1995 (Compeau & Higgins, 1995), there is still a sizeable percentage of user behavior that cannot be explained by predictive models. As IoT devices continue to be installed, the cyber attack surface is growing and vulnerability is increasing. While this survey provided information regarding IoT

home users, it has highlighted the need for more in-depth study into how to educate and motivate users to protect their devices and network from malicious actors.

The technical IoT research that is being conducted will move home users forward once it is commercially available, but in the interim, focusing on educating and empowering the user can improve security using existing, available methods and best practices.

Appendix A – Survey Instrument

Dissertation Survey

Start of Block: Introduction

Q1
Syracuse University School of Information Studies
Hinds Hall, 315-443-6887

Home User Internet of Things (IoT) Security

My name is Erica Mitchell and I am a PhD Candidate at Syracuse University. Dr. Joon Park of the Syracuse University School of Information Studies is the principal investigator for this study and my faculty advisor. We are inviting you to participate in a research study. Involvement in the study is voluntary, so you may choose to participate or not. This sheet will explain the study to you and please feel free to ask questions about the research if you have any. I will be happy to explain anything in detail if you wish.

We are interested in learning more about home user Internet of Things (IoT) security. You will be asked to answer survey questions. This will take approximately 15-30 minutes of your time. All information will be kept anonymous. This means that your name will not appear anywhere and your specific answers will not be linked to your name in any way.

The benefit of this research is that you will be helping us to understand home user IoT security. This information should help us to better understand how home users make IoT security decisions and evaluate security measures. By taking part in the research you may experience the following benefits: increased security awareness and methods for improving security.

The risks to you of participating in this study are an increased awareness of personal digital security concerns. These risks will be minimized by providing information that you can use to reduce your vulnerability to Internet attacks.

If you do not want to take part, you have the right to refuse to take part, without penalty. If you decide to take part and later no longer wish to continue, you have the right to withdraw from the study at any time, without penalty.

Whenever one works with e-mail or the internet there is always the risk of compromising privacy, confidentiality and/or anonymity. Your confidentiality will be maintained to the degree permitted by the technology being used. It is important for you to understand that no guarantees can be made regarding the interception of data sent via the internet by third parties.

Contact Information:
If you have any questions, concerns, complaints about the research, contact Dr. Joon S. Park or Erica Mitchell at 315-443-6887, jspark@syr.edu, or emmitc01@syr.edu. If you have any questions about your rights as a research participant, you have questions, concerns, or complaints that you wish to address to someone other than the investigator, if you cannot reach the investigator, contact the Syracuse University Institutional Review Board at 315-443-3013.

All of my questions have been answered, I am 18 years of age or older, and I wish to participate in this research study.

By selecting yes and clicking next I agree to participate in this research study. Please print a copy of this consent form for your records.

- ○ Yes (1)
- ○ No (2)

Skip To: End of Survey If Syracuse University School of Information Studies Hinds Hall, 315-443-6887 Home User Internet of T... = No

End of Block: Introduction

Start of Block: Demographics questions

Q2 What is your age range?

- ○ Under 18 (1)
- ○ 18 - 24 (2)
- ○ 25 - 34 (3)
- ○ 35 - 44 (4)
- ○ 45 - 54 (5)
- ○ 55 - 64 (6)
- ○ 65 - 74 (7)
- ○ 75 - 84 (8)
- ○ 85 or older (9)

Skip To: End of Survey If What is your age range? = Under 18

Q3 What is your education level?

- ○ Less than high school (1)
- ○ High school graduate (2)
- ○ Some college (3)
- ○ 2 year degree (Associate's or equivalent) (4)
- ○ 4 year degree (Bachelor's or equivalent) (5)
- ○ Professional degree (Juris Doctor/Master's/Graduate Certificate or equivalent) (6)
- ○ Doctorate (7)

Q4 What is your ethnicity?

- ☐ White (1)
- ☐ Black or African American (2)
- ☐ American Indian or Alaska Native (3)
- ☐ Asian (4)
- ☐ Native Hawaiian or Pacific Islander (5)
- ☐ Other (6) _____

Q5 What is your annual household income?

- Less than $10,000 (1)
- $10,000 - $19,999 (2)
- $20,000 - $29,999 (3)
- $30,000 - $39,999 (4)
- $40,000 - $49,999 (5)
- $50,000 - $59,999 (6)
- $60,000 - $69,999 (7)
- $70,000 - $79,999 (8)
- $80,000 - $89,999 (9)
- $90,000 - $99,999 (10)
- $100,000 - $149,999 (11)
- More than $150,000 (12)

Q6 What is your gender?

- Male (1)
- Female (2)
- Nonbinary (Please specify how you identify) (3) _____

Q7 Do you currently have any internet of things (IoT) devices (i.e. Internet-connected DVD/Blu-ray players, cameras, security systems, thermostats, outlets, light bulbs, etc.) installed in your home? *For the purposes of this survey, IoT devices do not include laptops or smartphones.*

- ○ Yes (1)
- ○ No (2)

End of Block: Demographics questions

Start of Block: No devices questions

Display This Question:
If Do you currently have any internet of things (IoT) devices (i.e. Internet-connected DVD/Blu-ray p... = No

Q8 Have you considered installing IoT devices (ie. thermostats, lightbulbs, outlets, etc.)?

- ○ Yes (1)
- ○ No (2)

Display This Question:
If Have you considered installing IoT devices (ie. thermostats, lightbulbs, outlets, etc.)? = No

Q9 Why have you not considered them?

- ☐ Don't know enough about them (1)
- ☐ Too costly (2)
- ☐ Too much effort (3)
- ☐ Too new (4)
- ☐ Security risk (5)
- ☐ My current setup works fine (6)
- ☐ Other (7) _____

Display This Question:
If Have you considered installing IoT devices (ie. thermostats, lightbulbs, outlets, etc.)? = Yes

Q10 After considering them, why have you not installed them?

- ☐ Haven't had the time (1)
- ☐ Still deciding (2)
- ☐ Too costly (3)
- ☐ Too much effort (4)
- ☐ Too new (5)
- ☐ Security risk (6)
- ☐ My current setup works fine (7)
- ☐ I found other workarounds (8)
- ☐ Other (9) _____

End of Block: No devices questions

Start of Block: Education

Q11 Do you have any formal information technology or computer science (IT/CS) education (technology classes in secondary school, certification courses, online classes, college courses, etc.)?

- ○ Yes (1)
- ○ No (2)

Q12 Do you have any informal technology or computer science (IT/CS) education? (hands-on playing with technology, Googling how to configure something, programming, being taught in an informal environment, etc.)

- ○ Yes (1)
- ○ No (2)

Display This Question:
If Do you have any formal information technology or computer science (IT/CS) education (technology c... = Yes

Q13 What formal education in IT/CS have you completed?

- ☐ Classes (high school and below) (1)
- ☐ Certification courses (A+, Security+, Network+, Cisco Certified Network Associate, Certified Ethical Hacker, etc.) (2)
- ☐ College courses (3)
- ☐ Minor in an IT/CS field (4)
- ☐ Bachelor's degree in an IT/CS field (5)
- ☐ Master's degree in an IT/CS field (6)
- ☐ Graduate certificate in an IT/CS field (7)
- ☐ PhD in an IT/CS field (8)
- ☐ Other (9) _____

Display This Question:
If What formal education in IT/CS have you completed? = Classes (high school and below)

Q14 How many IT-related classes did you take in school (high school and below)?

_____

Display This Question:
If What formal education in IT/CS have you completed? = Certification courses (A+, Security+, Network+, Cisco Certified Network Associate, Certified Ethical Hacker, etc.)

Q15 What certification courses have you completed?

- Entry-level IT certification (s) (CompTIA A+, Network+, Microsoft Technology Associate, ITIL Foundation and Practitioner Level, etc.) (1)
- Entry-level security certification (s) (CompTIA Security+, Systems Security Certified Practitioner, etc.) (2)
- Intermediate IT certification(s) (Cisco Certified Network Associate, ITIL Intermediate Level, Microsoft Certified Solutions Associate, etc.) (3)
- Intermediate security certification(s) (Global Information Assurance Certification Security Essentials (GSEC), Cisco Certified Network Associate Security, Certified Ethical Hacker, etc.) (4)
- Advanced IT certification(s) (Cisco Certified Internetwork Expert, ITIL Expert and Master Levels, Microsoft Certified Solutions Expert, etc.) (5)
- Advanced security certification(s) (Certified Information Systems Security Professional, CompTIA Advanced Security Practitioner, Offensive Security Certified Professional, etc.) (6)

Display This Question:
If What formal education in IT/CS have you completed? = College courses

*

Q16 How many IT/CS-related college classes have you taken?

_____

Q17 Do you currently work in an IT/CS-related field?

- ○ Yes, IT/CS is the majority (51%+) of my job (1)
- ○ Yes, IT/CS is 30-50% of my job (2)
- ○ Yes, IT/CS is less than 30% of my job (3)
- ○ No, but I have in the last 3 years (4)
- ○ No (5)

Display This Question:
If Do you have any informal technology or computer science (IT/CS) education? (hands-on playing with... = Yes

Q18 What informal IT/CS education have you had?

- ☐ Learning from friends/relatives (1)
- ☐ Looking up solutions to IT/CS problems on the Internet (2)
- ☐ Reading books on IT/CS-related topics (3)
- ☐ Hands-on tinkering with computers or other devices (4)
- ☐ Self-taught/Internet-learned programming (5)
- ☐ Other (6) _____

Display This Question:
If What formal education in IT/CS have you completed? = Minor in an IT/CS field
Or What formal education in IT/CS have you completed? = Bachelor's degree in an IT/CS field
Or What formal education in IT/CS have you completed? = Master's degree in an IT/CS field
Or What formal education in IT/CS have you completed? = Graduate certificate in an IT/CS field
Or What formal education in IT/CS have you completed? = PhD in an IT/CS field

Q19 What year did you earn with your most recent IT/CS-related degree or certificate?

_____

End of Block: Education

Start of Block: Technological Past Performance

Q20 What kinds of devices are connected to the Internet in your home?

- Computer (laptop, desktop, etc.) (1)
- Smartphone (2)
- Tablet (ie. iPad, Kindle Fire, etc.) (3)
- E-reader (ie. Kindle (not Fire), Nook, etc.) (4)
- Smartwatch (ie. Apple Watch, Galaxy Gear) (5)
- Fitness tracker (ie. Fitbit, Vivofit) (6)
- Video game system (ie. Playstation, X Box, Wii, etc.) (7)
- Home automation devices (ie. outlets, thermostats, lightbulbs, etc.) (8)
- Smart Appliances (refrigerator, CrockPot, coffeemaker, etc.) (9)
- Media device (Smart TV, Chromecast, Fire Stick, Roku player, DVD/Blu-Ray player, etc.) (10)
- Security system devices (cameras, sensors, etc.) (11)
- Monitoring devices (ie. baby monitors, nanny cameras) (12)
- Medical devices (ie. pacemaker, glucose monitor, etc.) (13)
- Do-it-yourself (DIY) lightweight computing (ie. Raspberry Pi, Arduino, etc.) (14)
- Other (15) _____

Q21 Approximately how many IoT devices do you have connected to your home network total? *(Do not include computers or smartphones in this count.)*

_____

Q22 Do you own your router or is it provided by your Internet provider? (*A router is the black box that supplies the wireless Internet to your house. Personally-owned routers normally have external antennae on them, while those supplied by your Internet provider (Verizon, Spectrum, etc.) are usually all-in-one devices that resemble a rectangle with no external antennae.)*

- Personally owned (1)
- Internet provider-owned (2)
- ⊗Other (4) _____

Q23 Did you set up your router yourself?

- Yes (1)
- No (2)

Display This Question:
If Do you own your router or is it provided by your Internet provider? (A router is the black box th... = Internet provider-owned

Q24 Have you logged in to the router provided by your Internet provider?

- Yes (1)
- No (2)

Display This Question:
If Did you set up your router yourself? = No

Q25 Who set up your router?

- Someone else who resides in the home (1)
- Commercial third party (ie. Geek Squad) (2)
- No one, it worked out of the box (3)
- Other (4) _____

Display This Question:
If Have you logged in to the router provided by your Internet provider? = No

Q26 Do you know how to log in to the Internet provider-owned router?

- Yes (1)
- No (2)

End of Block: Technological Past Performance

Start of Block: Security Past Performance

Q27 What do you do on the Internet?

- Check email (1)
- Online shopping (2)
- Play games (3)
- Social media (ie. Facebook, Twitter, Instagram, Snapchat, etc.) (4)
- Chat (5)
- Research (6)
- Read news (7)
- Search (ie. Google, Bing, Yahoo!, etc.) (8)
- Comment on news, blog posts, etc. (9)
- Online banking (10)
- Watch videos (ie. YouTube, Vevo, Netflix, etc.) (11)
- Communicate anonymously (ie. Whisper, Jodel, YikYak, etc.) (12)
- Communicate secretly (ie. Whisper, Signal, WhatsApp, etc.) (13)
- Other (14) _____

Q28 Approximately how many online accounts do you have?
An online account is any site or service for which you need a validation method. The validation method could be a username and password, a one time password texted to your phone, or a PIN number. Anything where you identify

who you are and prove that you are you to use it (Facebook, banking, apps on your phone, etc) would count as an online account.

- ○ 1-5 (1)
- ○ 6-10 (2)
- ○ 11-20 (3)
- ○ 21-30 (4)
- ○ More than 30 (5)

Q29
Approximately how many unique passwords do you have?
A password can describe a combination of letters and numbers, as well as just numbers, such as a PIN.

- ○ 1-5 (1)
- ○ 6-10 (2)
- ○ 11-15 (3)
- ○ 16-20 (4)
- ○ More than 20 (5)

Q30 When using the Internet, do you:

	Always (1)	Most of the time (2)	About half the time (3)	Sometimes (4)	Never (5)
Check for encryption when performing secure transactions? (Checking for encryption includes checking to see if the website begins with https instead of http or looking for a lock icon or looking for the browser to display a different color for secure websites) (1)	○	○	○	○	○
Use strong passwords? (At least 2 upper case, 2 lower case, 2 numbers, 2 special characters, total of at least 14 characters) (2)	○	○	○	○	○
Use the same password on multiple sites? (3)	○	○	○	○	○
Use a password vault? (software/app that stores all of your passwords with one master password for you to access it) (4)	○	○	○	○	○
Check the reputation of shopping sites? (Check to see if they have been compromised) (5)	○	○	○	○	○

Log out of secure sites when finished? (A secure site is any site that requires you to log-in) (6)	○	○	○	○	○
Close the browser when finished with a secure site. (7)	○	○	○	○	○

Display This Question:
If What do you do on the Internet? = Check email

Q31 When checking email, do you:

	Always (1)	Most of the time (2)	About half the time (3)	Sometimes (4)	Never (5)
Open emails from people you don't know? (1)	○	○	○	○	○
Open attachments from people you don't know? (2)	○	○	○	○	○
Click on links in emails? (3)	○	○	○	○	○
Use digital signatures/encryption? (4)	○	○	○	○	○
Log out when finished? (5)	○	○	○	○	○
Close the browser when finished? (6)	○	○	○	○	○

Q32 Are you responsible for securing and maintaining the Internet in your home? *(Do you interact with the Internet provider and/or fix your Internet when it isn't working properly?)*

- ○ Yes (1)
- ○ No (2)

Display This Question:
If Are you responsible for securing and maintaining the Internet in your home? (Do you interact with... = Yes

Q33 Which of the following security software do you use?

- ☐ Antivirus (Example: Bitdefender, Kaspersky, etc) (1)
- ☐ Malware Protection (Example: Malwarebytes Anti-Malware, AVG, etc.) (2)
- ☐ Application Whitelisting (Example: Microsoft AppLocker) (3)
- ☐ Personal Firewall (Example: Comodo Internet Security, Microsoft Windows Defender) (4)
- ☐ Monitoring Software (Example: GFI LanGuard, Nagios) (5)
- ☐ Other (6) _____
- ☐ ⊗None (7)
- ☐ ⊗I am unsure (8)

Display This Question:
If Are you responsible for securing and maintaining the Internet in your home? (Do you interact with... = Yes

Q34 Which of the following network protection measures do you use?

- Connect with Ethernet cable (instead of using wireless) (1)
- Don't broadcast SSID (network name on your wireless router) (2)
- Limit number of connections (only allow the number of devices that you have on the network at the same time) (3)
- Limit connections by MAC address (input the hardware address of your devices in the router and only allow those devices on your network) (4)
- Use encryption (WEP/WPA/PSK) (must have a code to log into the wireless network from your device) (5)
- Change default administrator username and password on router (personally owned routers come configured with the same administrator username and password) (6)
- Operate a guest network for visitors to the home and/or lower security devices (7)
- Change the WiFi password to a mix of letters, numbers, and characters (the WiFi password is what is used to connect wireless devices to the router) (8)
- Review router logs for unusual traffic (9)
- Change the IP addresses from the default ranges to random numbers (usually routers are configured to use 192.168.1.1 as the default gateway and assign IP address to devices starting with 192.168.1.100) (10)
- Turn off remote router management (11)
- Other (12) _____
- ⊗None of the above (13)

Q35 Which of the following IoT device protection measures do you use?

- [ ] Buy only devices with upgradeable firmware (1)
- [ ] Place IoT devices on a separate guest network (2)
- [ ] Replace IoT devices if they are insecure, even if they still work (3)
- [ ] Check for firmware updates regularly (4)
- [ ] Update firmware when available (5)
- [ ] Review router logs (6)
- [ ] Use encryption (when available) (7)
- [ ] Check shodan.io to see if any of your devices are vulnerable (8)
- [ ] Other (9) _____

Q36 How concerned are you with protecting your information on the Internet?

- ○ Very unconcerned (8)
- ○ Unconcerned (9)
- ○ Somewhat unconcerned (10)
- ○ Neither unconcerned nor concerned (11)
- ○ Somewhat concerned (12)
- ○ Concerned (13)
- ○ Very concerned (14)

Q37 Have you ever:

- ☐ been infected with malware? (1)
- ☐ had your identity stolen? (2)
- ☐ had one or more of your accounts hacked? (3)
- ☐ had someone pose as you on social media? (4)
- ☐ had any other negative consequence of Internet surfing? (Please list below) (5)

_____

End of Block: Security Past Performance

Start of Block: Locus of Control

Q38 Keeping my home network and devices safe is:

- ○ Beyond my control (8)
- ○ Mostly beyond my control (9)
- ○ Somewhat beyond my control (10)
- ○ Neither beyond my control nor within in control (11)
- ○ Somewhat within in my control (12)
- ○ Mostly within my control (13)
- ○ Within my control (14)

Q39 I believe that it is within my control to protect myself from information security violations at home:

- Strongly disagree (15)
- Disagree (16)
- Somewhat disagree (17)
- Neither agree nor disagree (18)
- Somewhat agree (19)
- Agree (20)
- Strongly agree (21)

Q40 The primary responsibility for protecting my home network belongs to:

- My Internet Service Provider (1)
- Mostly my Internet Service Provider (2)
- Somewhat my Internet Service Provider (3)
- Neither my Internet Service Provider or myself (4)
- Somewhat myself (5)
- Mostly myself (6)
- Myself (7)

Q41 Taking necessary security measures is entirely under my control:

- Strongly disagree (15)
- Disagree (16)
- Somewhat disagree (17)
- Neither agree nor disagree (18)
- Somewhat agree (19)
- Agree (20)
- Strongly agree (21)

End of Block: Locus of Control

Start of Block: Self-efficacy

Q42 I feel comfortable taking measures to protect my home network:

- Strongly disagree (20)
- Disagree (21)
- Somewhat disagree (22)
- Neither agree nor disagree (23)
- Somewhat agree (24)
- Agree (25)
- Strongly agree (26)

Q43 I have the resources and the knowledge to protect my home network:

- Strongly disagree (18)
- Disagree (19)
- Somewhat disagree (20)
- Neither agree nor disagree (21)
- Somewhat agree (22)
- Agree (23)
- Strongly agree (24)

Q44 Protecting my home network is:

- Hard (1)
- Mostly hard (2)
- Somewhat hard (3)
- Neither hard nor easy (4)
- Somewhat easy (5)
- Mostly easy (11)
- Easy (12)

Q45 I feel nervous when I think about online security issues:

- Strongly disagree (15)
- Disagree (16)
- Somewhat disagree (17)
- Neither agree nor disagree (18)
- Somewhat agree (19)
- Agree (20)
- Strongly agree (21)

Q46 I have the skills to implement preventative measures to stop people from damaging my home network:

- Strongly disagree (18)
- Disagree (19)
- Somewhat disagree (20)
- Neither agree nor disagree (21)
- Somewhat agree (22)
- Agree (23)
- Strongly agree (24)

Q47 My skills to stop information security violations on my home network are:

- Extremely inadequate (22)
- Moderately inadequate (23)
- Slightly inadequate (24)
- Neither adequate nor inadequate (25)
- Slightly adequate (26)
- Moderately adequate (27)
- Extremely adequate (28)

End of Block: Self-efficacy

Start of Block: Security Intentions

Q48 Will you make any changes to your home network or IoT devices after completing this survey?

- Yes (1)
- No (2)

Display This Question:
If Will you make any changes to your home network or IoT devices after completing this survey? = Yes

Q49 Thinking of your future actions, indicate the degree to which you agree or disagree with the following statements regarding your likelihood of implementing security measures to protect your home network

	Strongly disagree (15)	Disagree (16)	Somewhat disagree (17)	Neither agree nor disagree (18)	Somewhat agree (19)	Agree (20)	Strongly agree (21)
I am likely to take security measures to protect the Internet. (1)	○	○	○	○	○	○	○
I will upgrade my security measures to protect myself better online. (2)	○	○	○	○	○	○	○
I will change my passwords more often. (3)	○	○	○	○	○	○	○
I will use passwords that are harder to guess. (4)	○	○	○	○	○	○	○
I will change my browser security settings to a higher level. (5)	○	○	○	○	○	○	○
I will learn how to be more secure online. (6)	○	○	○	○	○	○	○
I will keep guests and IoT devices on a guest network. (7)	○	○	○	○	○	○	○
I will not use default passwords. (8)	○	○	○	○	○	○	○
I will limit connections to my router by MAC address. (9)	○	○	○	○	○	○	○
I will use WEP encryption. (10)	○	○	○	○	○	○	○
I will use WPA2 encryption. (11)	○	○	○	○	○	○	○
I will limit the number of connections to my router. (12)	○	○	○	○	○	○	○

I will change the WiFi password to a mix of letters, numbers, and special characters. (15)	○	○	○	○	○	○	○
I will change the IP address range and default gateway to random numbers (avoiding .1, .100, and .254) (16)	○	○	○	○	○	○	○
I will turn off remote router management. (17)	○	○	○	○	○	○	○
Other (13)	○	○	○	○	○	○	○

Display This Question:
If Will you make any changes to your home network or IoT devices after completing this survey? = No

Q50 Why are you not making any changes?

- ☐ My network is already secure enough. (1)
- ☐ No one wants to get into my network. (2)
- ☐ I don't know how. (3)
- ☐ It's too hard. (4)
- ☐ It works just fine as it is. (5)
- ☐ Nothing has happened to me yet. (6)
- ☐ Someone else manages my home network. (7)
- ☐ Other (8) _____

Q51 In the future, I plan to make the following IoT device changes:

- Buy only devices with upgradeable firmware (1)
- Place IoT devices on a separate guest network (2)
- Replace insecure IoT devices, even if they are still functional (3)
- Check for firmware updates regularly (4)
- Update firmware when available (5)
- Review router logs (6)
- Use encryption (when available) (7)
- Check shodan.io to see if any of my devices are vulnerable (8)
- Find other alternatives for devices that don't need to connect to the Internet (9)
- Other (10) _____

End of Block: Security Intentions

Start of Block: Additional Information

Q112 Is there anything else you would like to share about home user IoT security?

_____
_____
_____
_____
_____

End of Block: Additional Information

End of Survey message: Thank you for completing this survey! Your responses will be recorded and used to study home user security. Please visit https://www.us-cert.gov/Home-Network-Security to learn more about how you can protect your home network.

Appendix B – Research Appeals

B.1 – Facebook Friends Appeal

Hi everyone, as you all know, I am a PhD student at the iSchool in Syracuse University working on my PhD. My dissertation research is focused on the Internet of Things (IoT) and I would be forever indebted to you if you would click this link and complete a survey for me.

I am looking for people over the age of 18. Even if you do not own any IoT devices, I would appreciate your answers to a few short questions about them. For those that do own IoT devices, I would appreciate more information about your use of them.

The entire survey can be completed online in 15-30 minutes, depending on your answers to questions. I would also appreciate if you would share this with your friends list, in order to increase the number of participants. I would like as many participants as possible from all backgrounds.

The survey can be accessed here: (survey link)

If you have any questions about the research, please feel free to contact me on Facebook or at emmitc01@syr.edu.

B.2 – Facebook Military-Affiliated Groups Appeal

Hi everyone, my name is MAJ (P) Erica Mitchell and I am a fully-funded doctoral student at the iSchool in Syracuse University working on my PhD. My dissertation research is focused on the Internet of Things (IoT) and I would greatly appreciate it if you would click this link and complete a survey for me.

I am looking for people over the age of 18. Even if you do not own any IoT devices, I would appreciate your answers to a few short questions about them. For those that do own IoT devices, I would appreciate more information about your use of them.

The entire survey can be completed online in 15-30 minutes, depending on your answers to questions. I would also appreciate if you would share this with your friends list, in order to increase the number of participants. I would like as many participants as possible from all backgrounds.

The survey can be accessed here: (survey link)

If you have any questions about the research, please feel free to contact me on Facebook or at emmitc01@syr.edu.

B.3 – LinkedIn Appeal

Hi everyone, my name is Erica Mitchell and I am a doctoral student at the iSchool in Syracuse University working on my PhD. My dissertation research is focused on the Internet of Things (IoT) and I would greatly appreciate it if you would click this link and complete a survey for me.

I am looking for people over the age of 18. Even if you do not own any IoT devices, I would appreciate your answers to a few short questions about them. For those that do own IoT devices, I would appreciate more information about your use of them.

The entire survey can be completed online in 15-30 minutes, depending on your answers to questions. I would also appreciate if you would share this with your networks, in order to increase the number of participants. I would like as many participants as possible from all backgrounds.

The survey can be accessed here: (survey link)

If you have any questions about the research, please feel free to contact me on LinkedIn or at emmitc01@syr.edu.

B.4 – 53listserv Appeal

Hi everyone, my name is MAJ (P) Erica Mitchell and I am a fully-funded doctoral student at the iSchool in Syracuse University working on my PhD. My dissertation research is focused on the Internet of Things (IoT) and I would greatly appreciate it if you would click this link and complete a survey for me.

I am looking for people over the age of 18. Even if you do not own any IoT devices, I would appreciate your answers to a few short questions about them. For those that do own IoT devices, I would appreciate more information about your use of them.

The entire survey can be completed online in 15-30 minutes, depending on your answers to questions. I would also appreciate if you would share this with your friends list, in order to increase the number of participants. I would like as many participants as possible from all backgrounds.

The survey can be accessed here: (survey link)

If you have any questions about the research, please feel free to reply to this email, Erica.m.mitchell3.mil@mail.mil, or at emmitc01@syr.edu.

Appendix C – IRB Approval

SYRACUSE UNIVERSITY

INSTITUTIONAL REVIEW BOARD
MEMORANDUM

TO: Joon Park
DATE: February 21, 2018
SUBJECT: **Determination of Exemption from Regulations**
IRB #: 18-031
TITLE: *Home User Internet of Things (IoT) Security*

The above referenced application, submitted for consideration as exempt from federal regulations as defined in 45 C.F.R. 46, has been evaluated by the Institutional Review Board (IRB) for the following:

1. determination that it falls within the one or more of the five exempt categories allowed by the organization;
2. determination that the research meets the organization's ethical standards.

It has been determined by the IRB this protocol qualifies for exemption and has been assigned to category **2**. This authorization will remain active for a period of five years from **February 20, 2018** until **February 19, 2023**.

CHANGES TO PROTOCOL: Proposed changes to this protocol during the period for which IRB authorization has already been given, cannot be initiated without additional IRB review. If there is a change in your research, you should notify the IRB immediately to determine whether your research protocol continues to qualify for exemption or if submission of an expedited or full board IRB protocol is required. Information about the University's human participants protection program can be found at: http://orip.syr.edu/human-research/human-research-irb.html Protocol changes are requested on an amendment application available on the IRB web site; please reference your IRB number and attach any documents that are being amended.

STUDY COMPLETION: Study completion is when all research activities are complete or when a study is closed to enrollment and only data analysis remains on data that have been de-identified. A Study Closure Form should be completed and submitted to the IRB for review (Study Closure Form).

Thank you for your cooperation in our shared efforts to assure that the rights and welfare of people participating in research are protected.

Tracy J. Cromp

Tracy Cromp, M.S.W.
Director

DEPT: Information Studies, 334 Hinds Hall **STUDENT:** Erica Mitchell

Bibliography

(2017). Retrieved from Merriam-Webster: https://www.merriam-webster.com/dictionary/confidence?src=search-dict-hed

Ajzen, I. (1991). The Theory of Planned Behavior. *Organization Behavior and Human Decision Processes*, 179-211.

Amazon. (2018, 10 15). *IoT Devices sorted by Price Low to High*. Retrieved from Amazon.com: https://www.amazon.com/gp/search/ref=sr_1_1_hso_sc_smartcategory_2?rh=n%3A172282%2Ck%3Aiot&sort=price-asc-rank&keywords=iot&ie=UTF8&qid=1539626386&sr=8-1-acs&pf_rd_p=9bb01397-0efc-4293-b0d7-ec476f7f3045&pf_rd_r=DJF30WG39PZPFDAXBJN5&pd_rd_r=d9b25ba9-5d98-4

Amazon. (2020, 02 06). *Amazon*. Retrieved from Results for "smart outlet": https://www.amazon.com/s?k=smart+outlet&i=tools&ref=nb_sb_noss_2

Amazon. (2020, 02 06). *Amazon*. Retrieved from Results for "smart lightbulbs": https://www.amazon.com/s?k=smart+lightbulbs&i=tools&ref=nb_sb_noss_2

Amazon. (2020, 04 29). *smart socket with app control Smart plug*. Retrieved from Amazon Smile: https://smile.amazon.com/smart-socket/dp/B079KC9MTM/ref=sr_1_26?dchild=1&keywords=smart+plug&qid=1588173442&sr=8-26

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, 613-643.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior 69*, 437-443.

App My Home. (n.d.). *App My Home*. Retrieved 11 15, 2016, from http://appmyhome.com/smart-home-device-comparison/

Ascione, L. (2018, 04 17). *eSchool News*. Retrieved from K-12 computer science education makes strides: https://www.eschoolnews.com/2018/04/17/k-12-computer-science-education-makes-strides/

Ashford, W. (2019, 01 24). *Computer Weekly*. Retrieved from IoT application vulnerabilities leave devices open to attack: https://www.computerweekly.com/news/252456406/IoT-application-vulnerabilities-leave-devices-open-to-attack

Atkinson, J. W. (1957). Motivational Determinants of Risk-Taking Behavior. *Psychological Review*, 359-372.

Balaban, D. (2019, 10 21). *Ransomware and the Internet of Things*. Retrieved from Cyber Defense Magazine: https://www.cyberdefensemagazine.com/ransomware-and-the-internet-of-things/

Bandura, A. (1977). Self-Efficacy: Toward a Unifying Theory of Behavior Change. *Psychological Review (84)*, 191-215.

Bandura, A. (2006). Guide for Constructing Self-Efficacy Scales. In *Self-Efficacy Beliefs of Adolescents* (pp. 307-337). Information Age Publishing.

Barrett, B. (2017, 04 28). *Amazon's 'Echo Look' Could Snoop a Lot More Than Just Your Clothes.* Retrieved from https://www.wired.com/2017/04/amazon-echo-look-privacy/

Bates, D., Machler, M., Bolker, B. M., & Walker, S. C. (2015). Fitting Linear Mixed-Effects Models Using lme4. *Journal of Statistical Software*, 1-48.

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, 51-61.

Bernard, S. A. (2020). *An Introduction to Holistic Enterprise Architecture (4th Edition).* Bloomington, IL: Authorhouse.

Biddle, B., & Thomas, E. (1966). *Role Theory: Concepts and Research.* New York, NY: John Wiley & Sons.

Bishara, A. J., & Hittner, J. B. (2014). Reducing Bias and Error in the Correlation Coefficient Due to Nonnormality. *Educational and Psychological Measurement*, 785-804.

Blue, V. (2016, 10 28). *Engadget.* Retrieved from That time your smart toaster broke the Internet: https://www.engadget.com/2016/10/28/that-time-your-smart-toaster-broke-the-internet/

Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K. N., Nadeau, E., . . . Scarfone, K. (2019, 06). *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks.* Retrieved from NISTIR 8228: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

Bradley, T. (2019, 12 13). *What is a Firewall and How Does a Firewall Work?* Retrieved from Lifewire: https://www.lifewire.com/what-is-a-firewall-2487290

Brooks, T. T., & McKnight, L. (2017). A Steady-State Framework for Assessing Security Mechanisms in a Cloud-of-Things Architecture. In T. Brooks, *Cyber-Assurance for the Internet of Things* (pp. 227-247). John Wiley & Sons.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly Vol. 34, No. 3*, 523-548.

Butun, I., Osterberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. *IEE Communications Surveys & Tutorials*.

Cable, J. (2019, 08 19). *Every Computer Science Degree Should Require a Course in Cybersecurity*. Retrieved from Harvard Business Review: https://hbr.org/2019/08/every-computer-science-degree-should-require-a-course-in-cybersecurity

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, 36-45.

California Assembly. (2018, 09 28). *Assembly Bill No. 1906, Chapter 860.* Retrieved from California Legislative Information: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB1906

Carver, C., & Scheier, M. (1982). Control Theory: A Useful Conceptual Framework for Personality-Social, Clinical, and Health Psychology. *Psychological Bulletin*, 111-135.

Cert Nexus. (2020, 04 02). *Certified IoT Security Practitioner*. Retrieved from Certnexus.com: https://certnexus.com/certification/ciotsp/

Chen, D. Q., & Liang, H. (2019). Wishful Thinking and IT Threat Avoidance. *IEEE Transactions on Engineering Management, Vol. 6, No. 4*, 552-567.

Cimpanu, C. (2019, 06 25). *ZDNet*. Retrieved from New Silex malware is bricking IoT devices, has scary plans: https://www.zdnet.com/article/new-silex-malware-is-bricking-iot-devices-has-scary-plans/

Cisco. (2015, 05 27). *Cisco Introduces New Cloud and IoT Certifications to Address Key IoE Skills*. Retrieved from Cisco: https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1644181

Cisco. (2018, 02 15). *Chapter: Understanding and Configuring VLANs*. Retrieved from Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(25)EW: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/vlans.html

Cisco. (n.d.). *Cisco*. Retrieved from CCIE Security Certification and Training: https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/expert/ccie-security-v2.html

Claar, C., & Johnson, J. (2012). Analyzing Home PC Security Adoption Behavior. *Journal of Computer Information Systems*, 20-29.

Columbus, L. (2016, 11 27). *Forbes.* Retrieved from Roundup Of Internet Of Things Forecasts And Market Estimates, 2016: https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#3c785263292d

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

Confidence. (2017, 08 23). Retrieved from Merriam-Webster: https://www.merriam-webster.com/dictionary/confidence?src=search-dict-hed

Cortina, J. M. (1993). What is coefficient alpha? An examination of theory and applications. *Journal of Applied Psychology, 78*, 98-104.

Cox, J. (2012). Information systems user security: Astructured model of the knowing-doing gap. *Computers in Human Behavior 28*, 1849-1858.

Creswell, J. W. (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* Thousand Oaks, CA: SAGE Publications, Inc.

Critical Start. (2019, 08 29). *The Impact of Security Alert Overload*. Retrieved from Critical Start: https://www.criticalstart.com/wp-content/uploads/CS_MDR_Survey_Report.pdf

Custom Insight. (2017, 10 15). *Survey Random Sample Calculator*. Retrieved from Survey Tools: https://www.custominsight.com/articles/random-sample-calculator.asp

DeCarlo, L. T. (1997). On the Meaning and Use of Kurtosis. *Psychological Methods*, 292-307.

Department of Homeland Security. (2016, 10 14). *US-CERT*. Retrieved from Alert (TA16-288A): https://www.us-cert.gov/ncas/alerts/TA16-288A

Department of Homeland Security. (2017, 11 20). *Glossary.* Retrieved from National Intiative for Cybersecurity Careers and Studies: https://niccs.us-cert.gov/glossary

Dhillon, G., Oliveira, T., Sasrapu, S., & Caldeira, M. (2016). Deciding between information security and usability: Developing value based objectives. *Computers in Human Behavior*, 656-666.

DHS CISA. (2019, 11 14). *What is Cybersecurity?* Retrieved from Security Tip (ST04-001): https://www.us-cert.gov/ncas/tips/ST04-001

Dodd, C. D., Burris, S., Fraze, S., Doerfert, D., & McCulloch, A. (2013). Evaluating the Effectiveness of Traditional Training Methods in Non-Traditional Training Programs for Adult Learners through a Pre-test/Post-test Comparison of Food Safety Knowledge. *Journal of Agricultural Education, 54*, 18-30.

Drolet, M. (2016, 06 20). *CSO Online.* Retrieved from 8 tips to secure those IoT devices: https://www.csoonline.com/article/3085607/internet-of-things/8-tips-to-secure-those-iot-devices.html

Dunlap, T. (2019, 08 27). *Unsecured IoT; 8 Ways Hackers Exploit Firmware Vulnerabilities*. Retrieved from Dark Reading: https://www.darkreading.com/risk/unsecured-iot-8-ways-hackers-exploit-firmware-vulnerabilities/a/d-id/1335564

Dunn, J. (2017, 01 17). *Business Insider.* Retrieved from PC sales in 2016 were the lowest they've been in a decade: http://www.businessinsider.com/pc-sales-decline-year-chart-2017-1

Egelman, S., & Peer, E. (2015). Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). *CHI '15: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems.* New York, NY: Association for Computing Machinery.

Egelman, S., & Peer, E. (2015). The Myth of the Average User. *Proceedings of the New Security Paradigms Workshop.* New York, NY: Association for Computing Machinery.

Egelman, S., Harbach, M., & Peer, E. (2016). Behavior Ever Follows Intention? *CHI '16: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 5257-5261). Association for Computing Machinery.

Fabrigar, L. R., & Wegener, D. T. (2012). *Exploratory Factor Analysis.* New York, NY: Oxford University Press.

Fagan, M., Megas, K., Scarfone, K., & Smith, M. (2020, 01). *Recommendations for IoT Device Manufacturers.* Retrieved from Draft (2nd) NISTIR 8259 : https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259-draft2.pdf

Faklaris, C., Dabbish, L., & Hong, J. I. (2019). A Self-Report Measure of End-User Security Attitudes (SA-6). *Proceedings of the Fifteenth Symposium on Usable Security and Privacy* (pp. 61-77). USENIX.

Federal Trade Commission. (2015). *Internet of Things: Privacy and Security in a Connected World.* Retrieved from FTC.gov: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

Field, A. (2013). *Discovering Statistics Using SPSS.* Sage.

Fishbein, M. a. (1975). *Belief, Attitude, Intention and Behavior.* Reading, MA: Addison-Wesley.

Flores, A., Herman, J., Gates, G., & Brown, T. (2016, June). *How Many Adults Identify as Transgender in the United States?* Retrieved from The Williams Institute: http://williamsinstitute.law.ucla.edu/wp-content/uploads/How-Many-Adults-Identify-as-Transgender-in-the-United-States.pdf

Floyd, D., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, 407-429.

Franklin, C. J. (2019, 11 30). *Access Control Lists: 6 Key Principles to Keep in Mind*. Retrieved from DARK Reading: https://www.darkreading.com/attacks-breaches/access-control-lists-6-key-principles-to-keep-in-mind/d/d-id/1333757?image_number=3

Fruhlinger, J. (2018, 03 09). *The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet*. Retrieved from CSO Online: https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

Fruhlinger, J. (2019, 04 01). *What is a honeypot? A trap for catching hackers in the act*. Retrieved from CSO Online: https://www.csoonline.com/article/3384702/what-is-a-honeypot-a-trap-for-catching-hackers-in-the-act.html

Fu, K., Kohno, T., Lopresti, D., Mynatt, E., Nahrstedt, K., Patel, S., . . . Zorn, B. (2017, 03). *Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things.* Retrieved from Computing Research News: https://cra.org/ccc/wp-content/uploads/sites/2/2017/02/Safety-Security-and-Privacy-Threats-in-IoT.pdf

Furnell, S. M., Bryant, P., & Phippen, A. (2007). Assessing the security perceptions of personal Internet users. *Computers and Security 26*, 410-417.

Gartner. (2017, 02 07). Retrieved from Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016: https://www.gartner.com/newsroom/id/3598917

Gartner. (2017, 10 02). *IT Glossary*. Retrieved from Internet of Things: http://www.gartner.com/it-glossary/internet-of-things/

Geil, A., Sagers, G., Spaulding, A. D., & Wolf, J. R. (2018). Cyber security on the farm: an assessment of cyber security practices in the United States agriculture industry. *International Food and Agribusiness Management Review 21(3)*, 317-334.

Gibbs, S. (2015, 07 17). *The Guardian*. Retrieved from Windows 10: updates will be mandatory for home users: https://www.theguardian.com/technology/2015/jul/17/windows-10-updates-mandatory-home-users

Goodin, D. (2019, 08 05). *Microsoft catches Russian state hackers using IoT devices to breach networks*. Retrieved from Ars Technica: https://arstechnica.com/information-technology/2019/08/microsoft-catches-russian-state-hackers-using-iot-devices-to-breach-networks/

Goodin, D. (2020, 04 09). *Meet dark_nexus, quite possibly the most potent IoT botnet ever*. Retrieved from Ars Technica: https://arstechnica.com/information-technology/2020/04/meet-dark_nexus-quite-possibly-the-most-potent-iot-botnet-ever/

Google. (2017, 11 15). *Google*. Retrieved from https://www.google.com/search?rlz=1C1CHBF_enUS706US708&ei=oZ0XWpe6HM-D_Qbv2JOQAQ&q=home+internet+security+best+practices&oq=home+internet+security+best+practices&gs_l=psy-ab.3...3964.5252.0.5582.9.9.0.0.0.0.164.753.3j4.7.0....0...1.1.64.psy-ab..2.3.305...

Google. (2018). *Google* . Retrieved from Pre-College Computer Science Education: A Survey of the Field: https://services.google.com/fh/files/misc/pre-college-computer-science-education-report.pdf

Goumopoulos, C., & Mavrommati, I. (2020). A framework for pervasive computing applications based on smart objects and end user development. *The Journal of Systems and Software (162)*.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security 73*, 345-358.

Guhr, N., Werth, O., Blacha, P. P., & Brietner, M. H. (2020). Privacy concerns in the smart home context. *SN Applied Sciences*.

Hadlington, L., Popovac, M., Janicke, H., Yevseyeva, I., & Jones, K. (2019). Exploring the role of work identity and work locus of control in information security awareness. *Computers & Security 81*, 41-48.

Hanus, B., & Wu, Y. ". (2016). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management 33:1*, 2-16.

Hayes, T. (2014, 12 10). *Comcast Was Sued For Quietly Turning Customers' Home WiFi Into "Public" Hotspots*. Retrieved from Fast Company: https://www.fastcompany.com/3039682/comcast-was-sued-for-quietly-making-your-homes-internet-part-of-the-sharing-economy

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems 18*, 106-125.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. *Information Systems Journaal 24*, 61-84.

Higgins, K. J. (2019, 08 07). *DARKReading*. Retrieved from Boeing 787 On-Board Network Vulnerable to Remote Hacking: https://www.darkreading.com/vulnerabilities---threats/boeing-787-on-board-network-vulnerable-to-remote-hacking-researcher-says/d/d-id/1335463

Hochleitner, C., Graf, C., Unger, D., & Tscheligi, M. (2012). Making devices trustworthy: Security and Trust Feedback in the internet of things. *Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use.* Newcastle, UK: IWSSI/SPMU.

Hoffman, C. (2015, 06 20). *How-To Geek.* Retrieved from Warning: "Guest Mode" on Many Wi-Fi Routers Isn't Secure: https://www.howtogeek.com/219808/warning-%E2%80%9Cguest-mode%E2%80%9D-on-many-wi-fi-routers-isn%E2%80%99t-secure/

Hoffman, C. (2016, 09 28). *How-To Geek*. Retrieved from Is UPnP a Security Risk?: https://www.howtogeek.com/122487/htg-explains-is-upnp-a-security-risk/

Home Depot. (n.d.). *Home Depot Search for "smart"*. Retrieved 10 28, 2016, from http://www.homedepot.com/b/Appliances/N-5yc1vZbv1w/Ntk-All/Ntt-smart?Ntx=mode+matchall&NCNI-5

Home Depot. (n.d.). *Philips 60W Equivalent Soft White A19 Connected Home LED Light*. Retrieved 10 28, 2016, from http://www.homedepot.com/p/Philips-60W-Equivalent-Soft-White-A19-Hue-Connected-Home-LED-Light-Bulb-455295/206633282

Hooper, D., Coughlan, J., & Mullen, M. (2008). Structural Equation Modeling: Guidelines for Determining Model Fit. *Electronic Journal of Business Research Methods*, 53-60.

Hsu, C.-L., & Lin, J. C.-C. (2016). An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy. *Computers in Human Behavior*, 516-527.

Hurlburt, G. (2018). Toward Applied Cyberethics. *Computer*, Institute of Electrical and Electronics Engineers.

IAPP. (2020, 04 02). *About the IAPP.* Retrieved from IAPP.org: https://iapp.org/about/what-is-privacy/

IEEE. (2015). *Towards a definition of the Internet of Things (IoT) - Revision 1.*

Infinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security 31*, 83-95.

Interactive Advertising Bureau; Maru Matchbox. (2016, 12). Retrieved from The Internet of Things: https://www.iab.com/wp-content/uploads/2016/12/IAB-Internet-of-Things.pdf

ISC2.org. (n.d.). *ISC2*. Retrieved from CISSP – The World's Premier Cybersecurity Certification: https://www.isc2.org/Certifications/CISSP

James, S. E., Herman, J. L., Rankin, S., Keisling, M., Mottet, L., & & Anafi, M. (2016). *The Report of the 2015 U.S. Transgender Survey.* Washington, DC: National Center for Transgender Equality.

Jang, J., Shin, H., Aum, H., Kim, M., & Kim, J. (2016). Application of experiential locus of control to understand users' judgement toward useful experience. *Computers in Human Behavior 54*, 326-340.

Jang, J., Shin, H., Aum, H., Kim, M., & Kim, J. (2016). Application of experiential locus of control to understand users' judgments toward useful experience. *Computers in Human Behavior*, 326-340.

Jansen, J., & van Schaik, P. (2018). Testing a model of precautionary online behavior: The case of online banking. *Computers in Human Behavior*, 371-383.

Jena, A. K., Bhattacharjee, S., & Langthasa, P. (2015). Effects of Multimedia on Knowledge, Understanding, Skills, Practice and Confidence in Environmental Sustainability: A Non-Equivalent Pre-Test-Post-Test, Quasi Experimental Design. *i-manager's Journal of Educational Technology*, 37-47.

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, 549-566.

Jurcut, A. D., Ranaweera, P., & Xu, L. (2020). Introduction to IoT Security. In *IoT Security: Advances in Authentication* (pp. 27-64).

Keeney, R. L. (1992). *Value-Focused Thinking.* Cambridge, MA: Harvard University Press.

Keeney, R. L. (1999). The value of internet commerce to the customer. *Management Science 45(4)*, 533-542.

Kim, Y., Park, Y., & Choi, J. (2017). A study on the adoption of IoT smart home service: using Value-based Adoption Model. *Total Quality Management & Business Excellence*, 1149-1165.

Kline, R. (2015). *Principles and Practive of Structural Equation Modeling.* New York, NY: Guilford Publications.

Kolias, C., Stavrou, A., Voas, J., Bojanova, I., & Kuhn, R. (2016, January/February). Learning Internet-of-Things Security "Hands-On". *IEEE Security & Privacy*, pp. 37-46.

Krebs, B. (2015, 09 21). *Krebs on Security*. Retrieved from Inside Target Corp., Days After 2013 Breach: https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/

Krebs, B. (2016, 10 3). *Who Makes the IoT Things Under Attack?* (Krebs on Security) Retrieved from https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/

Kritzinger, E., & von Solms, S. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security 29*, 840-847.

Kruger, H., & Kearney, W. (2006). A prototype for assessing information security awareness. *Computers & Security 26*, 289-296.

Laliberte, M. (2019, 10 15). *DARKReading*. Retrieved from Why Bricking Vulnerable IoT Devices Comes with Unintended Consequences: https://www.darkreading.com/iot/why-bricking-vulnerable-iot-devices-comes-with-unintended-consequences-/a/d-id/1336009

Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly (33)*, 71-90.

Liang, H., & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal for the Association for Information Systems 11(7)*, 394-413.

Liberg, O., Wang, Y.-P. E., Sachs, J., Sundberg, M., Bergman, J., & Wikstrom, G. (2019). *Cellular Internet of Things.* Elsevier.

List, J. (2019, 01 14). *UPNP, Vulnerability as a Feature Just Won't Die*. Retrieved from Hackaday: https://hackaday.com/2019/01/14/upnp-vulnerability-as-a-feature-that-just-wont-die/

Lloyd, C. (2017, 03 28). *How to Control Your Amazon Echo from Anywhere Using Your Phone*. (How-To Geek) Retrieved from https://www.howtogeek.com/253621/how-to-control-your-amazon-echo-from-anywhere/

Maayan, G. D. (2020, 01 13). *Security Today*. Retrieved from The IoT Rundown for 2020: Stats, Risks, and Solutions: https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?Page=2

Maher, J. (2019, 09 23). *Newsweek*. Retrieved from HACKER TAKES OVER COUPLE'S SMART HOME, PLAYS VULGAR MUSIC AND RAISES TEMPERATURE TO 90 DEGREES: https://www.newsweek.com/google-nest-hack-milwaukee-1460806

Mandiant. (2017, 10 10). *Cyber Attack Lifecycle*. Retrieved from Law Enforcement Cyber Center: http://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/

Mathews, L. (2017, 12 12). *Forbes*. Retrieved from Hacker Ends Malware Mission After Bricking 10 Million Connected Devices: https://www.forbes.com/sites/leemathews/2017/12/12/hacker-ends-malware-mission-after-bricking-10-million-connected-devices/#7b574f69376a

Meerwijk, E. L., & Sevelius, J. M. (2017). Transgender Population Size in the United States: a Meta-Regression of Population-Based Probability Samples. *American Journal of Public Health*, e1-e8.

Meinert, D. B., Festervand, T. A., & Lumpkin, J. R. (1991). Psychology of computer use: XXV. Locus of Control, Information-system Dialogues, and End-Users' Satisfaction. *Psychology Reports 69*, 747-752.

Menard, S. (2009). *Logistic Regression: From Introductory to Advanced Concepts and Applications.* SAGE Publications.

Mitchell, E., & Park, J. S. (2017). NOAH for IoT: Cybersecurity Strategy for Home Users. *Proceedings of the 2017 International Conference on Security & Management* (pp. 68-74). Las Vegas, NV: CSREA Press.

Molin, E., Meeuwisse, K., Pieters, W., & Chorus, C. (2018). Secure or usable computers? Revealing employees' perceptions and trade-offs by means of a discrete choice experiment. *Computers & Security 77*, 65-78.

Mullinix, K. J., Leeper, T. J., Druckman, J. N., & Freese, J. (2015). The Generalizability of Survey Experiments. *Journal of Experimental Political Science*, 109-138.

National Fire Protection Association. (2020). *National Electrical Code 70.* Quincy, MA: National Fire Protection Association.

National Security Agency. (2016, 11 01). *Assess the Mess: ICS Host & Network Analysis Methodology*. Retrieved from Information Assurance Division Archive: https://apps.nsa.gov/iaarchive/customcf/openAttachment.cfm?FilePath=/iad/library/ia-

guidance/security-configuration/industrial-control-systems/assets/public/upload/Assess-the-Mess.pdf&WpKes=aF6woL7fQp3dJiyAsE6rCBWKfftWutTv9aL5yV

National Security Agency. (2018, 09 18). *Best Practices for Keeping Your Home Network Secure*. Retrieved from National Security Agency: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-best-practices-for-keeping-home-network-secure.pdf?v=1

National Security Agency Information Assurance Division. (2015, December). Retrieved from IAD's Top 10 Information Assurance Mitigation Strategies: https://www.iad.gov/iad/customcf/openAttachment.cfm?FilePath=/iad/library/ia-guidance/assets/public/upload/Top-10-IAD-Mitigation-Strategies-2015.pdf&WpKes=aF6woL7fQp3dJiRXFLhUEw8yeut5xwjezNPHt4

National Security Agency Information Assurance Division. (2015, 10). *Information Assurance Top 9 Architectural Tenets.* Retrieved from https://www.iad.gov/iad/customcf/openAttachment.cfm?FilePath=/iad/library/ia-guidance/secure-architecture/Assets/Public/upload/Information-Assurance-Top-9-Architectural-Tenets.pdf&WpKes=aF6woL7fQp3dJi7Gh46a9FK8F3TdHeDBMLyjSV

Nest. (2017, 11 15). *Technical specifications for Nest cameras*. Retrieved from https://nest.com/support/article/Nest-Cam-technical-system-requirements-and-specifications

Nest. (n.d.). *Nest Support*. Retrieved 12 10, 2016, from https://nest.com/support/article/Download-Nest-Thermostat-documents-and-get-started-using-your-thermostat

Newman, L. H. (2018, 04 16). *Wired*. Retrieved from An Elaborate Hack Shows How Much Damage IoT Bugs Can Do: https://www.wired.com/story/elaborate-hack-shows-damage-iot-bugs-can-do/

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems 46*, 815-825.

Nigam, R. (2019, 03 18). *Palo Alto Networks*. Retrieved from New Mirai Variant Targets Enterprise Wireless Presentation & Display Systems: https://unit42.paloaltonetworks.com/new-mirai-variant-targets-enterprise-wireless-presentation-display-systems/

NIST. (2020, 04 01). *NIST Cybersecurity for IoT Program*. Retrieved from NIST: https://csrc.nist.gov/CSRC/media/Presentations/NIST-Cybersecurity-for-IoT-Program/images-media/NIST%20Cybersecurity%20for%20IoT%20Program.pdf

NSA. (2014, 05). *DoD CIO.* Retrieved from Best Practices for Keeping Your Home Network Secure: http://dodcio.defense.gov/Portals/0/Documents/Cyber/Slicksheet_BestPracticesForKeepingYourHomeNetworkSecure_Web_update.pdf

NSA. (2016, 10). *Director of National Intelligence.* Retrieved from https://www.dni.gov/files/NCSC/documents/campaign/NSA-guide-Keeping-Home-Network-Secure.pdf

Official Journal of the European Union. (2016, 04 27). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da.* Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Olmstead, K., & Smith, A. (2017, 01 26). *Pew Research Center Internet & Technology.* Retrieved from Americans and Cybersecurity: http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

Osborne, J., & Waters, E. (2002). Four Assumptions of Multiple Regression That Researcher Should Always Test. *Practical Assessment, Research, and Evaluation*.

Owens, C. (2016, 11 3). *Stranger hacks family's baby monitor and talks to child at night*. (The San Francisco Globe) Retrieved from http://sfglobe.com/2016/01/06/stranger-hacks-familys-baby-monitor-and-talks-to-child-at-night/

Palmer, D. (2018, 11 07). *IoT security: Why it will get worse before it gets better*. Retrieved from ZDNet: https://www.zdnet.com/article/iot-security-why-it-will-get-worse-before-it-gets-better/

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 165-176.

Pelgrin, W. (2014). A Model For Positive Change: Influencing Positive Change in Cyber Security Strategy, Human Factor, and Leadership. In *Best Pratices in Computer Network Defense: Incident Detection and Response* (pp. 107-117). IOS Press.

Perera, C., Barhamgi, M., Bandara, A. K., Ajmal, M., Price, B., & Nuseibeh, B. (2020). Designing Privacy-aware Internet of Things Applications. *Information Sciences*, 238-257.

Perlroth, N., & Krauss, C. (2018, 03 15). *The New York Times*. Retrieved from A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.: https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

Pew Research Center. (2017, 01 12). *Internet and Technology*. Retrieved from Internet/Broadband Fact Sheet: http://www.pewinternet.org/fact-sheet/internet-broadband/

Pew Research Center. (2019, 06 12). *Pew Research Center Internet & Technology*. Retrieved from Internet/Broadband Fact Sheet: https://www.pewresearch.org/internet/fact-sheet/internet-broadband/#home-broadband-use-over-time

Quick, V., Corda, K. W., Martin-Biggers, J., Chamberlin, B., & Schaffner, D. (2015). Short food safety videos promote peer networking and behavior change. *British Food Journal, 117*, 78-93.

Rader, E., & Slaker, J. (2017). The Importance of Visibility for Folk Theories of Sensor Data. *Thirteenth Symposium on Usable Privacy and Security* (pp. 257-270). Santa Clara, CA: USENIX.

Raghunarayan, R. (2018). *Antivirus is dead: How AI and machine learning will drive cybersecurity*. Retrieved from Tech Beacon: https://techbeacon.com/security/antivirus-dead-how-ai-machine-learning-will-drive-cybersecurity

Rizvi, S., Orr, R., Cox, A., Ashokkumar, P., & Rizvi, M. R. (2020). Identifying the attack surface for IoT network. *Internet Of Things (9)*.

Rogers, E. (1999). The diffusion of interactive communication innovations and the critical mass: the adoption of telecommunication services by German banks. *Telecommunications Policy, 23*, 719-740.

Rogers, R., & Deckner, C. (1975). Effects of fear appeals and physiological arousal upon emotion, attitudes, and cigarette smoking. *Journal of Personality and Social Psychology*, 222-230.

Rubens, P. (2018, 03 21). *Types of Firewalls: What IT Security Pros Need to Know*. Retrieved from eSecurity Planet: https://www.esecurityplanet.com/network-security/firewall-types.html

Ryan, C. (2018, August). *Computer and Internet Use in the United States.* Retrieved from American Community Survey Reports: https://www.census.gov/content/dam/Census/library/publications/2018/acs/ACS-39.pdf

Sample Size Calculator. (2017, 11 3). Retrieved from http://clincalc.com/stats/samplesize.aspx

Schneiderman, B. (1979). Human factors experiments in designing interactive systems. *Computer 12*, 9-19.

Schneier, B. (2014, 01 06). *Schneier on Security*. Retrieved from The Internet of Things is Wildly Insecure - And Often Unpatchable: https://www.schneier.com/essays/archives/2014/01/the_internet_of_thin.html

Securitybros. (2017, 11 20). Retrieved from Network IP Camera System Bandwidth Calculator: https://securitybros.com/network-ip-camera-system-bandwidth-calculator/

Sedgewick, A., Souppaya, M., & Scarfone, K. (2015). *Guide to Application Whitelisting.* Retrieved from NIST Special Publication: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf

Seymour, W., Kraemer, M. J., Bims, R., & van Kleek, M. (2020). Informing the Design of Privacy-Empowering Tools for the Connected Home. Honolulu, HI: CHI.

Sharevski, F., Treebridge, P., & Westbrook, J. (2019, November). Experiential User-Centered Security in a Classroom: Secure Design for IoT. *IEEE Communications Magazine*, pp. 48-53.

Shen, A. X., Lee, M. K., & Cheung, C. M. (2011). Harness the Wisdom of Crowds: The Importance of We-Intention in Social Computing Research. In P. Papadopoulou, P. Kenellis, & D. Martakos, *Social Computing Theory and Practice Interdisciplinary Approaches* (pp. 19-35). Hershey, Pa: Information Science Reference.

Sheppard, B. H., Hartwick, J., & Warshaw, P. R. (1988). The Theory of Reasoned Action: A Meta-Analysis of Past Research with Recommendations for Modifications and Future Research. *The Journal of Consumer Research, 15*, 325-343.

Sieniuc, K. (2016, 08 16). *Tech Co. Can Be Sued Over Spouse Spying, 6th Circ. Says*. (Law360) Retrieved from https://www.law360.com/articles/829058/tech-co-can-be-sued-over-spouse-spying-6th-circ-says

Silverman, R. (2013). Investigating video as a means to promote vocabulary for at-risk children. *Contemporary Educational Psychology, 38*, 170-179.

Simes, D., & Sirsky, P. (1985). Human factors: an exploration of the psychology of human-computer dialogues. In H. Hartson, *Advances in human-computer interaction* (pp. 48-102). Norwood, NJ: Ablex.

Sophos. (2016, 08 16). *Naked Security*. Retrieved from NIST's new password rules - what you should know: https://nakedsecurity.sophos.com/2016/08/18/nists-new-password-rules-what-you-need-to-know/

Stevens, J. P. (2009). *Applied Multivariate Statistics for the Social Sciences (5th Ed.).* Mahwah, NJ: Routledge/Taylor & Francis Group.

Taylor, S., & Todd, P. (1995). Assessing IT Usage: The Role of Prior Experience. *MIS Quarterly*, 561-570.

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awarness on information technology professionals' behavior. *Computers & Security 79*, 58-79.

Torton, R., Reaiche, C., & Boyle, S. (2018). The impact of security awarness on information technology professionals' behavior. *Computers & Security 79*, 58-79.

Tsai, H.-y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security 59*, 138-150.

United States Census Bureau. (2017, 07 04). *U.S. and World Population CLock*. Retrieved from https://www.census.gov/popclock/

United States Computer Emergency Readiness Team. (2016, 09 06). Retrieved from The Increasing Threat to Network Infrastructure Devices and Recommended Mitigations: https://www.us-cert.gov/ncas/alerts/TA16-250A

United States Government Accountability Office. (2017). *Technology Assessment The Internet of Things: Status and Implications of an Increasingly Connected World.* Washington, DC: GAO.

US Census Bureau. (2010). *Overview of Race and Hispanic Origin.* Washington, DC: US Census Bureau.

US Census Bureau. (2016). *Educational Attainment in the US.* Washington, DC: US Census Bureau.

US Census Bureau. (2018). *2014-2018 American Community Survey 5 Year Estimates.* Washington, DC: US Census Bureau.

van der Meij, H., & van der Meij, J. (2014). A comparison of paper-based and video tutorials for software learning. *Computers & Education 78*, 150-159.

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

Venkatesh, V., Speier, C., & Morris, M. G. (2002). User Acceptance Enablers in Individual Decision Making About Technology: Toward an Integrated Model. *Decision Sciences 33*, 297-316.

VisualPing. (2017, 08 20). Retrieved from https://visualping.io/

Warne, R. T. (2018). *Statistics for the Social Sciences.* New York, NY: Cambridge University Press.

Warner, M. (2017, 08 01). *Internet of Things (IoT) Cybersecurity Improvement Act of 2017*. Retrieved from 115th Congress: https://www.congress.gov/bill/115th-congress/senate-bill/1691

Wash, R. (2010). Folk Models of Home Computer Security. *Smposium on Usable Privacy and Security (SOUPS) 2010* (pp. 1-16). Redmond, WA: ACM.

Weber, R. H. (2010). Internet of Things - New security and privacy challenges. *Computer Law & Security Review 26*, 23-30.

Weiner, N. (1948). *Cybernetics: Control and COmmunication in the Animal and the Machine.* Cambridge, MA: MIT Press.

White, G. L. (2015). Education and Prevention Relationships on Security Incidents for Home Computers. *The Journal of Computer Information Systems (55)*, 29-37.

White, G., Ekin, T., & Visinescu, L. (2017). Analysis of Protective Behavior and Security Incidents for Home Computers. *Journal of Computer Information Systems (57)*, 353-363.

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. *Cyberpsychology, Behavior, and Social Networking*, 3-7.

Wigfield, A., & Eccles, J. (2000). Expectancy-Value Theory of Achievement Motivation. *Contemporary Educational Psychology*, 68-81.

Williams, C. K., Wynn, D., Madupalli, R., Karahanna, E., & Duncan, B. (2014). Explaining Users' Security Behaviors with the Security Belief Model. *Journal of Organizational and End User Computing 26(3)*, 23-46.

Williams, C. K., Wynn, D., Madupalli, R., Karahanna, E., & Duncan, B. K. (2014). Explaining Users' Security Behaviors with the Security Belief Model. *Journal of Organizational and End User Computing 26(3)*, 23-46.

Witte, K., Cameron, K. A., McKeon, J., & Berkowitz, J. M. (1996). Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale. *Journal of Health Communication*, 317-341.

Woolf, N. (2016, 10 26). *DDOS attack that interrupted the internet was largest of its kind in history, experts say*. (The Guardian) Retrieved from https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

Woon, I., Tan, G.-W., & Low, R. (2005). A Protection Motivation Theory Approach to Home Wireless Security. *ICIS 2005 Proceedings* (pp. 367-380). AISEL.

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

Wortman, P. M. (1983). Evaluation Research: A Methodological Perspective. *Annual Review of Psychology*, 223-260.

Wouk, K. (2019, 05 29). *5 of the Best IoT Security Courses You Should Check Out*. Retrieved from IoTtechtrends.com: https://www.iottechtrends.com/best-iot-security-courses/

Wouk, K. (2020, 01 14). *IoT Tech Trends*. Retrieved from 5 Highly Valid Certifications for IoT Learners: iottechtrends.com/highly-valid-certifications-for-iot-learners/

Yang, Y., Wu, L., Yin, G., & Zhao, H. (2017). A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal Vol 4, No 5*, 1250-1258.

Yao, Y., Basdeo, J. R., Kaushik, S., & Wang, Y. (2019). Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. *Proceedings of CHI Conference on Human Factors in Computing Systems.* Glasgow, Scotland, UK: CHI.

Yin, L., Fang, B., Gou, Y., Sun, Z., & Tian, Z. (2020). Hierarchically defining Internet of Things Security. *International Journal of Distributed Networks*.

Zakon, R. (n.d.). Retrieved from Hobbes' Internet Timeline 25: https://www.zakon.org/robert/internet/timeline/

Zeng, E., Mare, S., & Roesner, F. (2017). End User Security & Privacy Concerns with Smart Homes. *Thirteenth Symposium on Usable Privacy and Security* (pp. 65-80). Santa Clara, CA: USENIX Association.

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. *Proceedings of the ACM on Human-Computer Interaction, 2* (pp. 1-20). CSCW.

Zimmerman, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to "human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*, 169-187.

Zmud, R. W. (1979). Individual differences and MIS success: a review of the empirical literature. *Management Science 25*, 966-979.

Curriculum Vitae

Erica M Mitchell
erica.m.mitchell@outlook.com

Education:

Syracuse University, Syracuse, NY 2015-2020
PhD in Information Science and Technology

Command and General Staff College, Intermediate Level Education 2012
Honor Graduate

Syracuse University, Syracuse, NY 2010-2011
Master of Science in Information Management
Degree Awarded December 2011

Syracuse University, Syracuse, NY
Certificate of Advanced Studies in Information Security Management
Certificate Awarded December 2011

United States Military Academy, West Point, NY 1997-2001
Bachelor of Science, Major in American Legal Systems, Engineering Track: Environmental Engineering
Degree Awarded June 2001

Relevant Academic Experience:

Cyber Defense Review
Area Editor

Locked Shields Estonia 2019
Strategy White Cell Lead for the United States

CyCon US 2018
Reviewer

National Cyber Summit 2016
Program Committee Member

Publications:

2019

Mitchell, Erica; Bell, Patrick; Hall, Andrew; Kelley, Terence; Kavaney, Mary; Butler, Robert; Monken, Jonathan; Bennett, Daniel; Maymi, Fernando; Korn, Erik; Nussbaum, Brian; Pfiefer, Joseph; Kramer, Frank; Lawton-Belous, Joshua; Hernandez, Rhett; Nowatkowski, Michael; Gordon-Tennant, Courtney; and Esquibel, Judy, "Jack Voltaic Critical Infrastructure and Public-Private Partnerships" (2019). *ACI Technical Reports*. 42.
https://digitalcommons.usmalibrary.org/aci_rp/42

Crowston, K., Mitchell, E., & Østerlund, C. (2019). Coordinating Advanced Crowd Work: Extending Citizen Science. *Citizen Science: Theory and Practice*, *4*(1).
https://doi.org/10.5334/cstp.166

Esquibel, Judy and Mitchell, Erica, "Jack Voltaic 2.0: Threats to Critical Infrastructure" (2019). *ACI Technical Reports*. 36.
https://digitalcommons.usmalibrary.org/aci_rp/36

2018

Mitchell, E., Crowston, K. G., & Oesterlund, C. (2018). Coordinating advanced crowd work: Extending citizen science. In *Proceedings of the 51st Hawaii International Conference on System Sciences* https://doi.org/10.24251/HICSS.2018.212

2017

Mitchell, E., & Park, J. S. (2017). NOAH for IoT: Cybersecurity Strategy for Home Users. *Proceedings of the 2017 International Conference on Security & Management* (pp. 68-74). Las Vegas, NV: CSREA Press.

2016

Mitchell, Erica and Joon S. Park (2016), "NOAH's Ark, Bring on the Flood: An Argument for a Cyber Branch of the Department of Defense" National Cyber Summit, Huntsville, AL

Presentations:

2020

"Jack Voltaic 2.5: Critical Infrastructure Resilience Workshop" - University of South Carolina, March 2
Invited Speaker
Presented Topics: Mini Scenario-Based Table Top Exercise, Lessons Learned from Jack Voltaic
Audience: Governor McMaster, LTG (R) Caslen, President of University of South Carolina, Critical Infrastructure industry leaders, Columbia, SC CISO

"Jack Voltaic 3.0: Law and Policy Workshop and Table Top Exercise" - Savannah, GA, February 18-20
Workshop Planner and Developer, Master of Ceremonies, and Speaker
Presented Topics: Partnerships, Incident Response Plans, and Law and Policy Focused Table Top Exercise
Audience: Critical infrastructure leaders and general counsel, city leadership and general counsel, county and state emergency managers, state and local law enforcement, federal defense support to civil authorities planners

"Jack Voltaic 3.0: Planner Workshop #2" - Savannah, GA, January 13-15
Workshop Planner, Speaker
Presented Topics: Introduction to Jack Voltaic, Planning for the Law and Policy Table Top

2019
"Jack Voltaic" - Presentation to Department of Defense/Department of Homeland Security Steering Group
Invited Speaker

"Jack Voltaic 2.5: Critical Infrastructure Resilience Workshop Series" - Charleston, SC - May 21; San Francisco, CA - July 16; San Diego, CA - July 31; Norfolk, VA - August 6; Augusta, GA - August 22-23; Savannah, GA - August 27; Tacoma, WA – September 10
Workshop Planner and Developer, Master of Ceremonies, Speaker
Presented Topics: Local threat assessment (some locations), Jack Voltaic: Lessons Learned, Mini Table Top Exercise, Interactive brainstorming session concerning gaps in government and critical infrastructure support

"Birds of a Feather: Avoid Reinventing the "Wi" in WiCyS: How Common are Gender and Recruitment Challenges?", Women in Cybersecurity Conference, Pittsburgh, PA

"Jack Voltaic" - 2nd INDOPACOM International Cybersecurity Engagements Forum, Hawai'i
Invited Speaker
Presented Topics: Jack Voltaic: Lessons Learned and Future Opportunities

2017
"NOAH for IoT: Cybersecurity Strategy for Home Users" International Conference on Security & Management, Las Vegas, NV July

2016
"NOAH's Ark, Bring on the Flood: An Argument for a Cyber Branch of the Department of Defense" Poster Presentation at the National Cyber Summit, Huntsville, AL

2015
"Host Mitigations Package" Several in-person and webinar lectures within the DoD and at meetings with representatives from each of the Armed Services

2012
"Secure Internet Protocol Router Network (SIPRNet) Token Management System (TMS)" Identity Protection and Management Conference, Anaheim, CA

Funding:

2019
$2,500,000 – Funding secured from Department of the Army to fund Jack Voltaic Critical Infrastructure Resilience research

$50,000 – Funding secured from the Office of the Secretary of Defense to fund Jack Voltaic 2.5 Critical Infrastructure Resilience Workshops

Relevant Professional Experience:

Department of Defense, West Point, NY
Strategy and Policy Team Lead/Research Scientist

-Team Leader of four researchers
-Developed, planned and executed the Jack Voltaic 3.0 Legal and Policy Table Top Exercise
-Developed, planned and executed Jack Voltaic 2.5 critical infrastructure resilience workshops in key port city locations throughout the United States

Department of Defense, Fort Meade, MD
Host Integrity Team Leader

-Team Leader of four technical personnel
-Developed, tested, and implemented host mitigation strategies for the entire DoD
-Evaluated products for future host mitigation strategies
-Led a successful pilot test on a full suite of products on a live network

Department of Defense, Fort Meade, MD
Public Key Infrastructure Project Manager, SIPRNetToken Management System and NIPRNet Enterprise Alternate Token System

-Served as project manager for two projects, totaling several million dollars, that implemented two-factor authentication across the DoD
-Collaborated with representatives for DoD services and agencies to determine system requirements
-Integrated the system with the DoD Information Network (DoDIN)

Department of the Army, Fort Carson, CO, Taji, Iraq, and Jalabad, Afghanistan
Information Assurance Manager/Information Systems Manager

-Provided information systems services to approximately 3500 users in austere conditions
-Planned and executed cybersecurity protections to ensure confidentiality, integrity, and availability of information

Department of the Army, Fort Gordon, GA
Information Systems Planner

-Planned Homeland Security and Unit Exercises, as well as support for Hurricane Katrina
-Initiated an Information Assurance Program for the unit

Department of Defense, Guantanamo Bay, Cuba
Information Assurance Manager

-Team Lead of four contractors, responsible for network security
-Completed recertification and accreditation process for the Joint Task Force
-Recognized by Southern Command for improvements in network security and incident reporting

Department of the Army, Fort Gordon, GA
Training Coordinator

Department of the Army, Uijongbu, Korea, Tallil, Iraq, and Fort Gordon, GA
Small Unit Leader, Operations Officer

-Leader of 20 – 36 soldiers
-Designed and built commercial cable backbone at Tallil Airbase

Membership in Professional Organizations:
Computing Technology Industry Association (CompTIA) – Security+
International Information Systems Security Certification Consortium ((ISC)2) – CISSP

Awards:
Bronze Star
Defense Meritorious Service Medal
Meritorious Service Medal
Army Commendation Medal
Joint Service Achievement Medal (2 awards)
Army Achievement Medal (2 awards)