THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

COLLEGE OF INFORMATION SCIENCES AND TECHNOLOGY

STUDENTS' USE OF SECURITY FEATURES ON PERSONAL DEVICES WITHIN WORK ENVIRONMENTS

ALEXANDER HUDOCK
FALL 2016

A thesis
submitted in partial fulfillment
of the requirements
for a baccalaureate degree
in Finance
with honors in Information Sciences and Technology

Reviewed and approved* by the following:

Jens Grossklags
Professor of Information Sciences and Technology
Thesis Supervisor

Marc Friedenberg
Lecturer of Information Sciences and Technology
Honors Adviser

* Signatures are on file in the Schreyer Honors College.

ABSTRACT

In the past decade, mobile phones have grown from being a simple convenience to an absolute necessity. Beyond simply being able to call or text whoever you like wherever you are, phones have become a resource unlike any other. Smartphones provide us the power of a mobile computer anywhere, anytime, and for almost anything. With the rise of the smartphone, the risk of cyber-attacks and data breaches is also on the growing—something most people never think about. Driving the raping adoption of smartphones are millennials, a group currently flooding the workplace. This population has a very different view on what the use of smartphones in a workplace should look like, and many of them would prefer (in most cases) to use their own devices at work. From a company standpoint, this is called Bring Your Own Device (BYOD), and is an ever-increasing trend in the modern workplace. Although this trend is popular in companies, it has received very little focus from the research community at large. Based on the previously mentioned rising security concerns, as well as the increased use of smartphones in a newer generation of workers, the purpose of this thesis is to explore the current state of smartphone security and to understand the typical level of knowledge college students have about smartphone security. Additionally, it will look at risks associated with identity, personal information, and BYOD for both individuals as well as the companies where they will inevitably work.

After my data collection, I hope to be able to understand what the typical college student understands about smartphone security and how it affects their own security as well as that of the business world. I will be performing a qualitative analysis of students through 1-on-1 interviews about personal habits both in and outside of the workplace. At the conclusion of the study, I will

be able to better understand the issues surrounding the future of smartphone security and what steps are necessary in preparing for it.

TABLE OF CONTENTS

LIST OF TABLES

ACKNOWLEDGEMENTS

I would like to thank my thesis supervisor Jens Grossklags for his support in shaping my research and providing excellent guidance throughout the process.

I would like to thank Jake Weidman for being excellent support throughout my research by providing suggestions based on his own research here at the university.

I would like to thank Marc Friedenberg for helping me explore a thesis in Information Sciences and Technology although my major is within the Smeal College of Business.

I would like to thank the Schreyer Honors College for generously providing me a research grant so that I could effectively recruit participants for this study.

Lastly, I would like to thank my mom, dad, sister, and friends for all their support throughout my life to push me to where I am today.

Chapter 1

Introduction

Over the past century, technology has evolved at an exponential rate. Back in 1876, Alexander Graham Bell invented the first telephone. Since then, phones evolved to become a household staple, then a mobile means of communication, and, now, an inseparable part of our beings. Smartphones allow us to do a great deal of things, such as organize our daily lives, quickly look up information, take pictures or video, and share experiences with friends. It has become so integral to our lives that our phones rarely leave our side and potentially hold more information about us than anything else. However, with the rise of technology, the issue of cyber security has become a heavily discussed topic.

Each year, the number of cybercrimes increases and has been doing so at an alarming rate [4,12]. Considering that our mobile devices hold our most personal information (i.e. social security number, bank account information, contacts, email and social networking account information), the threat of that information being compromised is frightening. Malware has begun to target mobile devices specifically and can exist in various forms, such as apps that request specific permissions or as seemingly harmless links [3]. Although this threat increases by the day, there seems to be a lack of a concerned response from the public. If we continue down the path of this technological revolution, cyber security is going to become the biggest issue we face. Not only is our own safety at risk, but so are our governments, banks, and businesses.

This thesis focuses on individuals at Penn State University who had just completed an internship during the summer of 2016 and will soon enter the workforce upon graduation. The

intent is to analyze these individuals' understanding of cyber security, their personal and professional habits toward security, the security protocols practiced by companies across industries, and finally any changes in behavior toward smartphone security. It delves into how serious this issue is currently, how much worse it could become in the future, and what steps need to be taken to avoid the potential implications of ignoring it.

Organization of Thesis

The thesis is structured as follows.

- Chapter 2 provides background information on smartphone security, the security practices of businesses, past data breaches and the subsequent impacts, and discusses related studies in the realm of security.
- Chapter 3 outlines the research methodology used, the purpose of performing a qualitative study on students' smartphone use, and students' experiences at their internships during the summer of 2016.
- Chapter 4 summarizes the results of the survey, as well as a comprehensive analysis of the interviews.
- Chapter 5 further discusses the findings of the study, identifies trends, and explores any limitations of the research.
- Chapter 6 summarizes the overall conclusion of the study as well as any opportunities for future research.

Chapter 2

Literature Review

In our fast-paced technologically evolving world, smartphone security has become an alarming issue. Many people opt to use the same few passwords for multiple social media, email, and bank accounts [5]. This is especially dangerous since once a password is stolen, hackers can have access to an individual's entire life. Even if individuals use different passwords, hackers are becoming better and more efficient at breaching devices, or finding other waysto retrieve information such as through social engineering [10]. Due to this increased threat, assessing current smartphone security and steps towards increasing it have become a heavily discussed topic from both the perspective of users and security developers.

Past Studies

Before beginning any study, exploring past studies is important. This provides a broader view of information to the researcher and helps shape their own questions. For my study, I wanted to see what past researchers explored in relation to smartphone security as it relates to students and businesses.

Kaspersky Labs, a security firm known for their desktop software, counted only eight new malicious mobile malware programs in January 2011 and then saw the number grow to 6,800 new programs monthly at the end of 2012 [11]. With the increase in the number of adults that use a smartphone, this stark increase in malware programs is alarming. Jones, Chin, and Aiken (2014) looked specifically into students' use of smartphone security practices. The study, which surveyed five hundred students, found that three hundred forty-seven, or 69% of respondents, had

smartphones [6]. This result stands in contrast to a 2012 Pew Study that found only 45% of adults had smartphones, clearly indicating that smartphone use is huge among the younger crowd.

In their study, Jones et al. asked those that responded to having a smartphone multiple other questions, including questions on smartphone use, use of passwords, logging out activity, and use of Wi-Fi, Bluetooth, and GPS on their devices. 28% of respondents always logged out of their email and social networking accounts, such as Gmail and Facebook. Although many students find this unnecessary, a hacked phone can access contact lists and personal information if these applications are left open. In regards to Bluetooth and GPS, 73% always disabled Bluetooth when not in use and 62% always disabled GPS. When Bluetooth is enabled, hackers can download contact information, texts, messages, and other pertinent information in certain scenarios [7]. Concerning GPS, if a phone is ever compromised, having GPS enabled could allow constant tracking of the phone's location.

Beyond this, the survey showed that more than half of students are practicing "safe" smartphone usage. 49% do not open attachments received via text or email if it came from an unknown source, 64% do not click on links received via text or email from unknown sources, 56% do not download applications from unknown sources, and 48% do not download apps that request access to contacts and other personal information [6]. This shows that while at least half of the students are being mindful of their security, there is still a large amount of students who are not considering the implications of their actions. To make matters worse, only 44% of students though using a password on their device was important.

When considering various smartphone applications, one of the largest security concerns involves the use of smartphones for financial services. Of the respondents, 65% stated that they used their phones for financial services. Within that group, only 54% thought it was important to

password protect their phones. Perhaps more concerning, within the subpopulation that does use financial services on their phone:: 24% click on links from someone unknown, 41% open email attachments from those unknown, 28% do not disable Bluetooth, 21% download apps from unknown sources, and 40% do not necessarily connect to encrypted networks [6]. These users are at much more risk than others, with their extremely personal banking information being readily available to hackers.

There are many issues with the survey performed by Jones, Chin, and Aiken (2014). First, the sample size is far from optimal. While 500 respondents is a decent size, it still has a margin of error of 4.5%. Second, questions regarding Bluetooth and GPS do not specify why the services are being disabled. While it is assumed that this is due to security concerns, disabling these services has long been tied to reducing battery consumption. The survey does not specify which of these two reasons the services are being disabled, which raises concerns. Third, the question regarding the use of encrypted networks does not specify when/why students connected them. For example, students may only connect to encrypted networks for business transactions but for nothing else. Finally, the survey only looks at students and not the general adult population. Even if the study was open to teachers and locals, the results would be much closer to real life than just looking at students.

Regardless of its faults, the Jones, Chin, and Aiken (2014) study has shed light on current issues with smartphone security. While users of smartphones understand that there are security risks, many of them choose not to take proactive actions against them. This could be due to a lack of understanding of what threat level personal information can be compromised, lack of understanding of the simple steps that can be taken to prevent hacking, or a misunderstanding of

how to use security features. The study concludes by calling for "increased education, training, and awareness" towards smartphones.

Industry Trends

Examining industry trends is important to identifying the risk level associated with security. With smartphone use increasing exponentially, the threat level may be greater than expected.

In an article from Information Management Journal (2015), smartphone security from the perspective of the business world is examined. A Symantec Threat Report from 2012 showed that 44% of adults did not know about mobile device security solutions. By 2013, that number grew to 57%, which is alarming considering smartphone users have grown exceptionally each year [15]. In addition to this, *Consumer Reports* stated that 1.2 million devices were lost without return in 2012, and this figure grew to 1.4 million in 2013[16]. With the sudden growth in smartphone use, the issues regarding security and loss of information have grown with it. The article pushes much of the same information found in the Jones, Chin, and Aiken (2014) report, calling for better user training towards smartphones. The article calls for employees to continuously be "made aware of the dangers of bypassing corporate settings on their devices, of falling prey to phishing, of losing their devices and not promptly reporting the loss." [6]If employees have improper security protocols in place or they lose their device, it could cost the company greatly.

In regards to Bring Your Own Device (BYOD), more employees are bringing their own devices to work than ever, connecting to the company's network, and at times routing their work email through the device. An article by Miller, Voas, and Hurlburt (2012) explores the dangers of

BYOD, stating, “as soon as external (personal) devices are attached [to a network], malware could migrate from the personal device into the company’s machines and over the company’s network.” [9] The threat personal devices present is extremely alarming, especially since many companies offer Wi-Fi access to their employees. If a company allows such behavior without ensuring employees’ devices are secure, they run the risk of massive security breaches. Conversely, employers run the risk of their private information becoming available to the employer. As Miller, Voas, and Hurlburt (2012) put it, “mobile devices contain a wealth of data that a user might deem private, and if personal data is co-mingled with the employer data on the same device, how are the barriers implemented between personal and employer data?” [9] With the advent of BYOD, there are a wealth of concerns that have yet to be fully explored. As BYOD becomes more common, companies are running out of time to prepare against the practice’s potential implications.

Morrow (2012) explores the growth of BYOD further. In a survey by Harris Interactive and ESET, over “80% of employed adults use some kind of personally owned electronic device for work-related functions.” [1] Of this, 24% are performing that work with smartphones, which are becoming the most used device for BYOD. Morrow (2012) goes on to address devices that had been or lost or stolen, stating that “64% of enterprise respondents reported that users’ devices containing sensitive or proprietary data had been lost or stolen.”[14] Businesses are clearly not taking a proactive approach to the BYOD shift and the implications may be staggering. The shift to BYOD is not slowing down either, as more individuals are adopting smartphones and taking them to work every day.

Security Breaches

Exploring the implications of security breaches is especially important to understanding how costly it can be for individuals and businesses should their information be stolen.

An article by Eddy (2013) reports on a flaw discovered in Samsung's Knox mobile security platform, which has been highly praised and publicized. The findings came out of security researchers at Ben-Gurion University's Cyber Security Labs in Israel. While the security platform had been thought to be highly secure, a Ph.D. student named Mordechai Guri found that all Knox security measures could be bypassed by any regular app. The flaw causes all phone communications to be capable of being captured, recorded, and exposed. Given that there is so much faith in our smartphone's own basic security, it is alarming how easily hackers can access our information. In fact, 79% of businesses reported a mobile security incident in 2012 with some huge costs [2]. 42% of these incidents cost businesses six figures, and 16% costing over $500,000. Of these businesses, 52% of large businesses saw incidents of over $500,000 while 45% of small businesses (less than 1,000 employees) saw incidents of over $100,000 [2]. In conjunction with the Information Management Journal (2015), clearly businesses need to educate their employees more on these mobile security threats, as it can become a very costly mistake.

In "BYOD: Enabling the Chaos", Thompson (2012) examines the shift to BYOD and what it means for businesses and employees. In regards to security breaches, Gordon states that "the cost of just one data breach can be staggering for an enterprise – Ponemon Institute estimates the range to be anywhere from $1m to $58m." [13] Considering that some smaller firms do not earn nearly that much in profit, single security breaches can be crippling. Even for larger companies, security breaches can wreak havoc on financial statements. Gordon (2012) explores other potential

side effects, including “damage to corporate reputation and loss of customers and market share.” [13] Given the overall impact of security breaches, BYOD presents a multitude of threats to small and large businesses alike.

Chapter 3

Research Methodology

The following chapter will describe the purpose of choosing a qualitative research approach, the data collection procedure, and data analysis methods used. Lastly, the validity of the data is explained.

Qualitative Approach to Research

In deciding how to find the data I was looking for, I decided a qualitative approach would be best. By performing qualitative interviews, I could get more personalized data and expansive information than through a survey or other means. In an interview setting, participants are more likely to share personal anecdotes and I can ask follow-up questions. This leads to a much more in-depth discussion and reveals more about the individuals and the issues being discussed.

Another option I explored was a quantitative survey, but the number of participants necessary for meaningful and valid data was too difficult to attain. In addition, there is a risk of participants filling out the survey quickly and not providing relevant information. By actively talking with participants, I could receive full explanations about their experiences.

Data Collection Procedure

The method for data collection included a preliminary survey followed by an in-depth interview. The preliminary survey included basic demographic information, as well as questions regarding current security practices, experience at the company of their last internship, and

behavior in regards to lost and/or stolen devices. The purpose of this data collection was to gain initial insight into the individuals and look for potential trends across participants.

After the survey, participants would then be interviewed by me to answer the more in-depth questions. These questions were more broad and were focused on their experience at their last internship, security protocols they were required to follow, and any changes in their security practices from before, during, and after their internship. This was also the time where I explored any additional experiences participants had in regards to having their data breached. This proved very interesting, as many participants had different experiences in regards to their internship as well as personal security breaches.

Data Analysis Method

Upon completing the study, there were two parts to analyzing the data. First, the survey results were gathered together and statistical analysis was performed. Graphs and tables were created to visualize results and identify trends. This information was then recorded so that it could be compared to participants' responses during the interview.

Next, the interviews were transcribed. Although notes were taken during the interviews, the transcription process was performed to have hard copies of the information. This made identifying trends and key points much simpler as well as providing the opportunity to include personal anecdotes to analysis.

Chapter 4

Findings

The following section will go into detail about the statistical results of the survey as well as unique findings from the interviews.

Survey Results

Below are the results for each survey question. The first question asked name, which was removed for participants' anonymity. The second and third questions asked age and year, respectively, to confirm the target demographic. The average age of our participants was 21.2 years old, and each of our participants was a graduating senior. Figure 1 details the major program and target industry from the participants' internships.

Figure 1: Q4 - What is your major? & Q5- What industry was your internship in this past summer?

What is your major?	What industry was your internship in this past summer?
Finance	Commercial Insurance
Finance	Corporate Finance
Economics	Business
Economics	Construction
Energy Business and Finance	Energy
IST	Aerospace Engineering
Economics	Financial Health Care
Economics	Business Services/Consulting
Chemical Engineering	Consumer Packaged Goods
Economics	Computer Software
Cyber Security	Technology
Supply Chain & Information Systems	Operations
Electrical Engineering	Private Defense Contracting
Finance	Telecom
Mechanical Engineering	Automotive

Figure 2 details the various positions and types of work the particiapnts completed at their internships over the course of the summer.

Figure 2: Q6 - What was your role (title) during your internship?

Distribution Intern
Finance Analyst Development Program
Summer Intern
Shadowed CFO
Energy Management Intern
Program Management
Finance Intern
Summer Business Development Associate
Manufacturing Engineering Intern
Sales
Business Operations
Operations Intern
Electrical Engineering Intern
Transfer Pricing Intern
Data Analyst Intern

In addition to determining positions held by students, we also sought to understand the types of phones they use regularly. Surprisingly, all students that participated in the study currently have an iPhone. However, during the interviews I learned that many had had another operating system in the past but had switched to iOS because they believe iPhone has the safest operating system.

Figure 3. Q8 - How secure do you believe your smartphone is? (1 is insecure, 10 is secure)

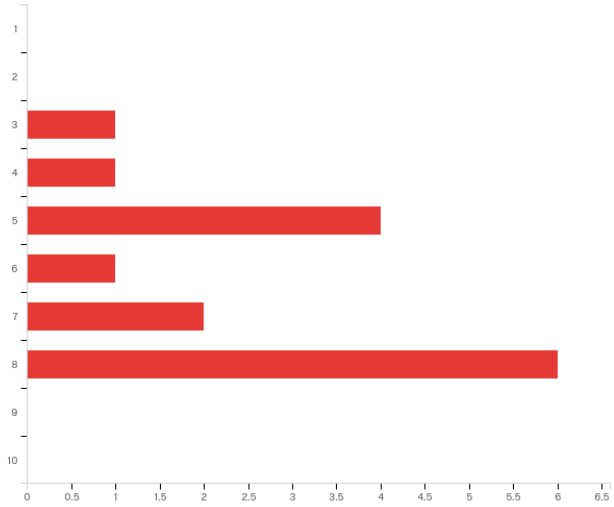


Figure 3 demonstrates students' general feelings towards their devices. While most believe their smartphones were secure (giving a score of 8, meaning very secure) it is interesting that a few participants gave scores of 5, 4, and even 3. These students still had sensitive information on their devices so it is interesting that they do not trust their phone to protect it.

Figure 4: Q9 - Do you password protect your phone?

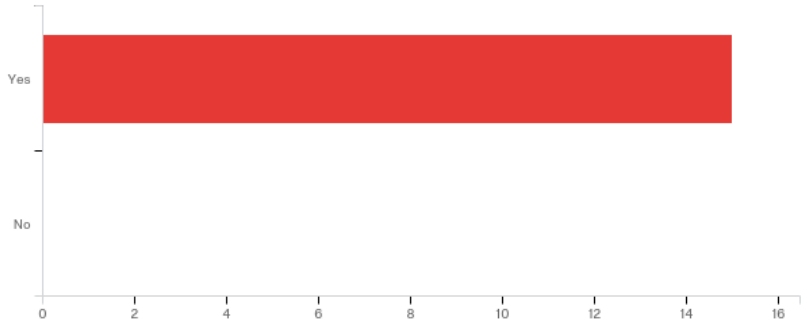


Figure 4 focuses on the use of mobile passwords by students. The result of this question is promising. Although some people do not password protect their devices, all these students take the necessary precaution to do so.

Figure 5: Q28 - What type(s) of protection do you use on your phone?

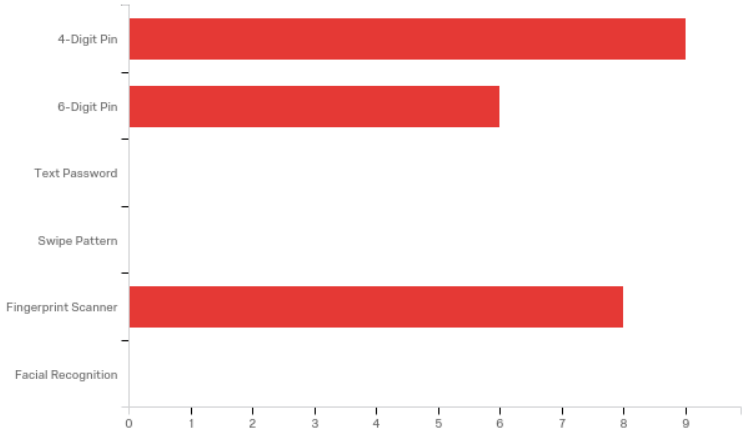


Figure 5 explored the type of security individuals used on their phones. It is interesting to find that more than half (53.33%) of participants use a fingerprint scanner, which is arguably the most secure method of the options.

Figure 6: Q12 - Do you always update your smartphone's software when a new patch/update is released?

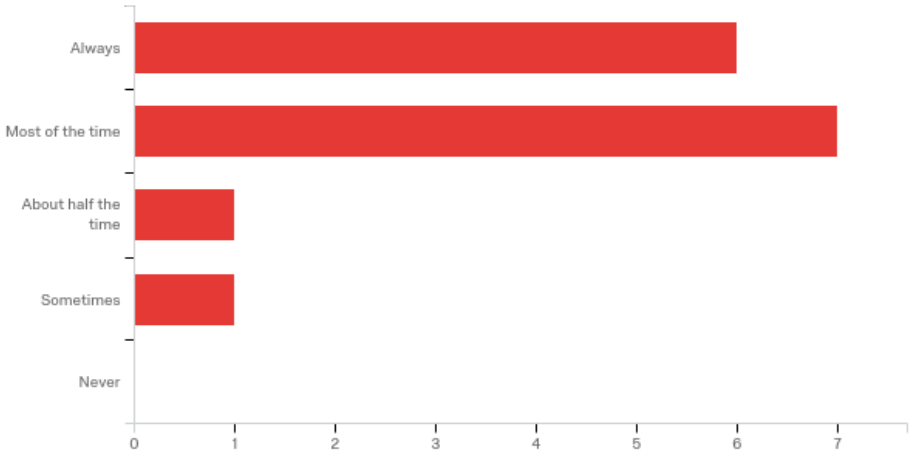


Figure 6 was focused on how frequently students installed updates or patches on their devices. It is noteworthy that 13 participants (86.67%) update their devices either always or most of the time. Also, it's alarming that one participant only updates sometimes and another only half of the time.

These updates sometimes fix huge security holes in the software and without updating, the devices can remain incredibly unprotected.

Figure 7: Q30 - How quickly do you update your smartphone's software when a new patch/update is released?

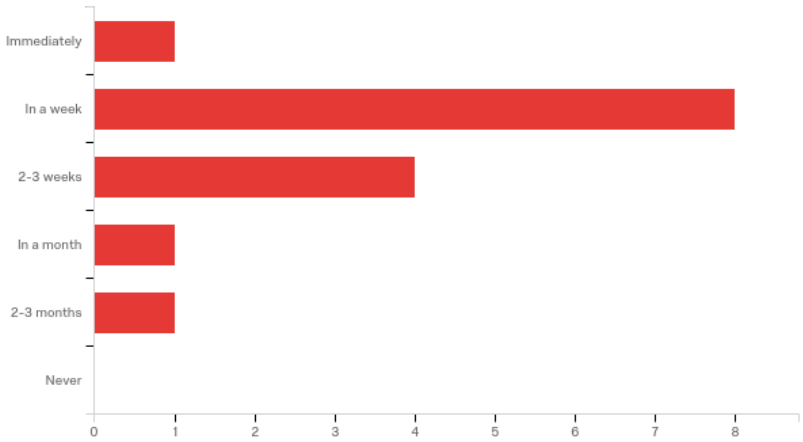


Figure 7 is an extension of Figure 6, but instead looks at how quickly updates are applied. Most respondents update within the first few weeks, meaning any security holes they had are fixed relatively quickly.

Figure 8: Q13 - Do you read the developer's notes to understand what was being fixed or changed?

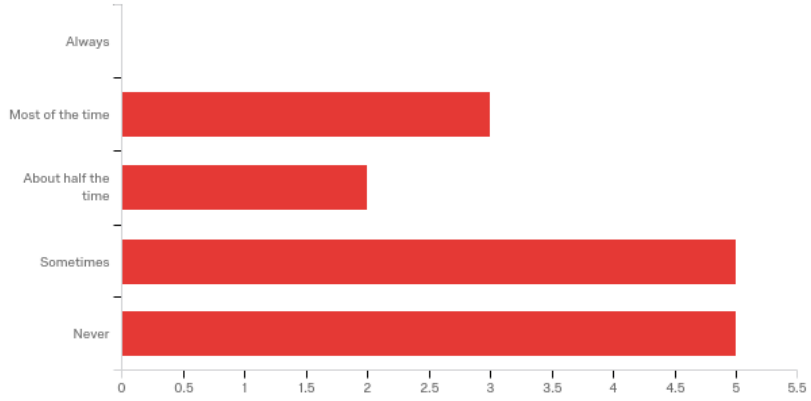
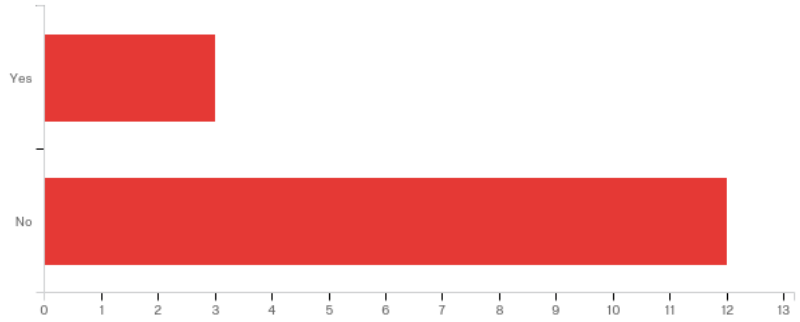


Figure 8 is aimed at the participants' understanding of updates. It's surprising that the majority of participants (66.66%) read developer's notes either sometimes or never. That means that these users have no idea if a security hole existed on their device or what threats may have occurred.

Figure 9: Q14 - Have you ever installed an alternative operating system on your phone? An alternative operating system is created by someone other than your phone's maker, examples being Jailbreak, CyanogenMod, etc.



While alternative operating systems allow vast customization, they are not supported by the manufacturer of the device and can have some dangerous security holes. It's interesting that 3 participants (20%), found in Figure 9, have installed one even though manufacturers advise against it.

Figure 10: Q15 - Do you always update your smartphone's apps when a new patch/update is released?

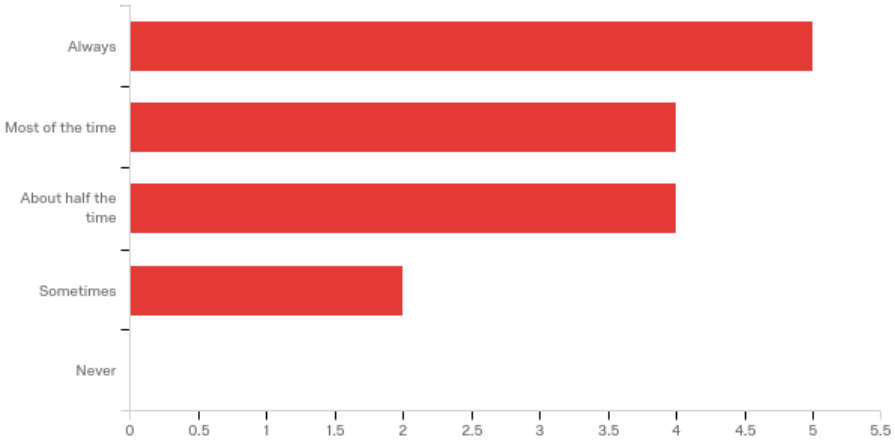


Figure 10 is an extension of habits related to updating a phone's software. Many applications have access to most of, if not all aspects of a device. That means these apps can read contacts, text messages, access the camera, etc. Sometimes, these apps can have security holes where hackers can access all parts of the device.

Figure 11: Q31 - How quickly do you update your smartphone's apps as soon when a new patch/update is released?

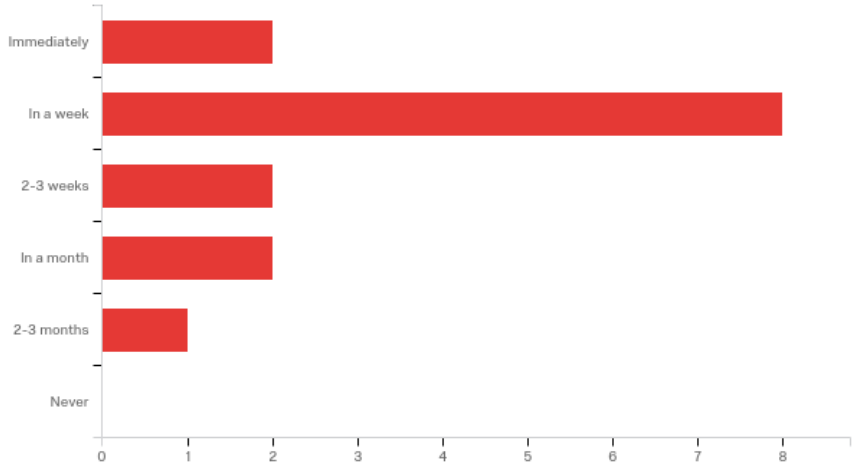


Figure 11 demonstrates similar results to Figure 10. This indicates that participants tend to have the same behavior towards updating their device and updating their apps.

Figure 12: Q16 - Do you read the developer's notes of the apps to understand what was being fixed or change?

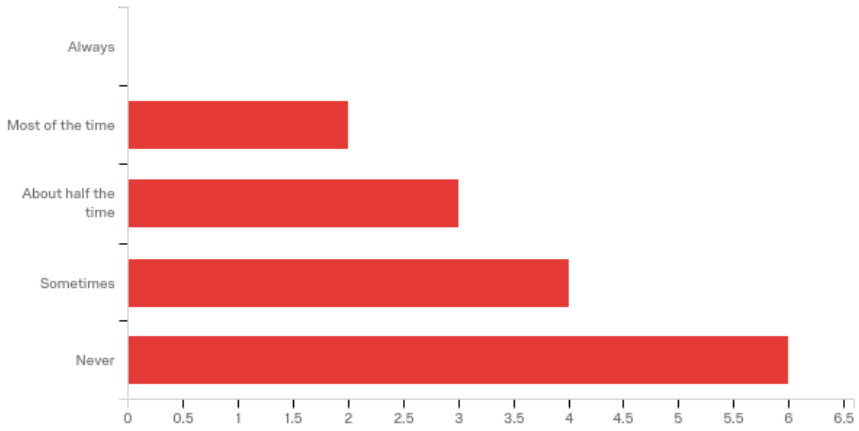
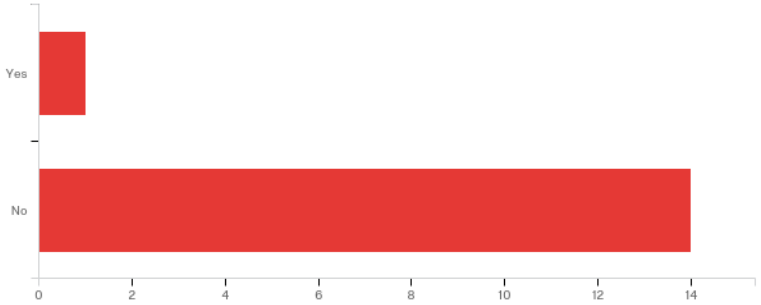


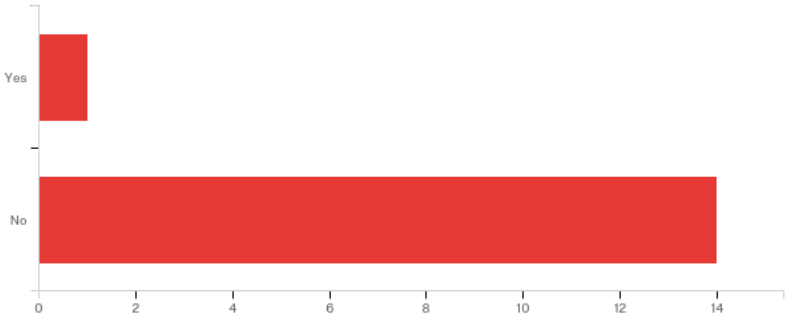
Figure 12 shows similar results to Figure 8. Generally, participants treat updating their devices and updating their apps in the same manner. Reading the developer's notes is important to understanding security concerns, so it is somewhat surprising most participants update without doing so.

Figure 13: Q29 - Have you ever installed apps not approved by the app store on your phone?



A smartphone's app store is monitored by the manufacturer to make sure only safe apps are installed on the device. However, not all apps are approved by the app store because of potential security concerns. These apps can still be downloaded, but they are done outside of the app store. It's interesting that although almost every participant has not done this, one of them has. This can lead to a ton of security issues with a device. These results are shown in Figure 13.

Figure 14: Q17 - Do you use anti-malware or anti-virus software on your smartphone?



In addition to a phone's developer having security measures in place, anti-malware and anti-virus applications can be downloaded for extra protection and monitoring. Although most people know to have these applications on their computer, it's surprising that almost every participant (93.33%), found in Figure 14, does not take that precaution with their smartphone. Smartphones are just smaller computers, so it is interesting that most participants do not treat them that way.

Figure 15: Q18 - Do you follow news surrounding security breaches of smartphones or smartphone apps?

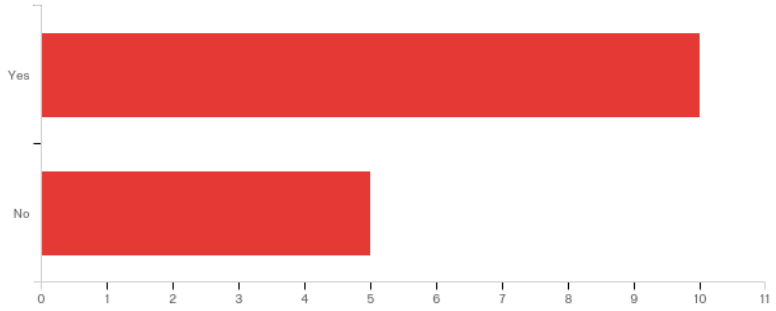
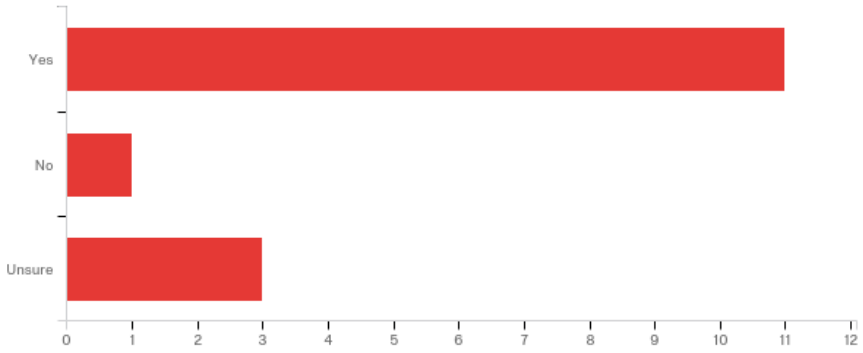


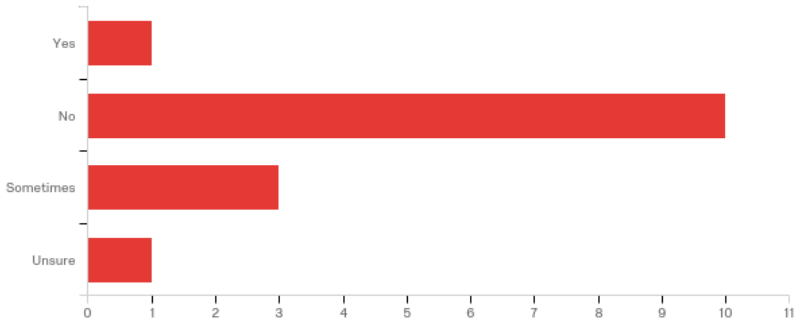
Figure 15 was aimed at understanding if participants remained informed about security breaches. If someone is informed about security breaches and threats, they are more likely to take proactive steps to securing their own device. While the majority (66.67%) followed the news about this, a third of the participants did not (33.33%) and are thus less likely to take these proactive steps.

Figure 16: Q19 - When you connect to wifi, are you sure that it is a secured network? A secured network uses a form of encryption, typically Wireless Access Protection (WAP), and all home, school, and business networks tend to have this type of security.



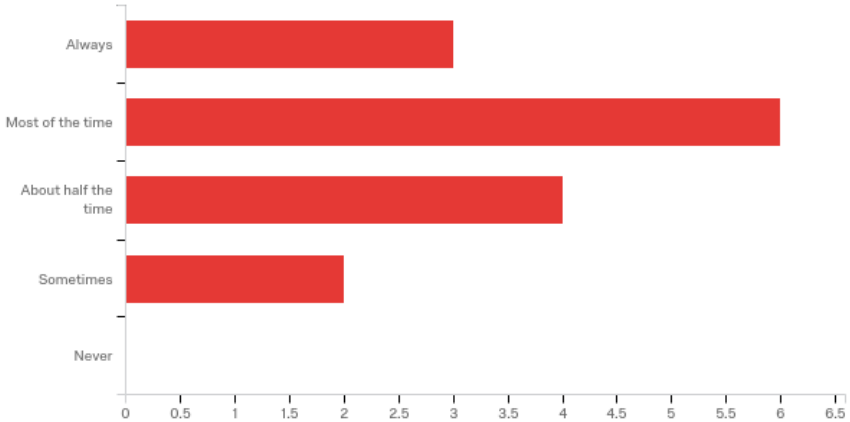
Typically, most people are aware if they are connecting to a secured network. The results of Figure 16 confirm that 11 participants (73.33%) ensure that they connect to secured networks.

Figure 17: Q20 - If you have connected to an unsecure network (those found in public places, like McDonald's or Starbucks), do you ever enter confidential information such as usernames, passwords, or credit card information?



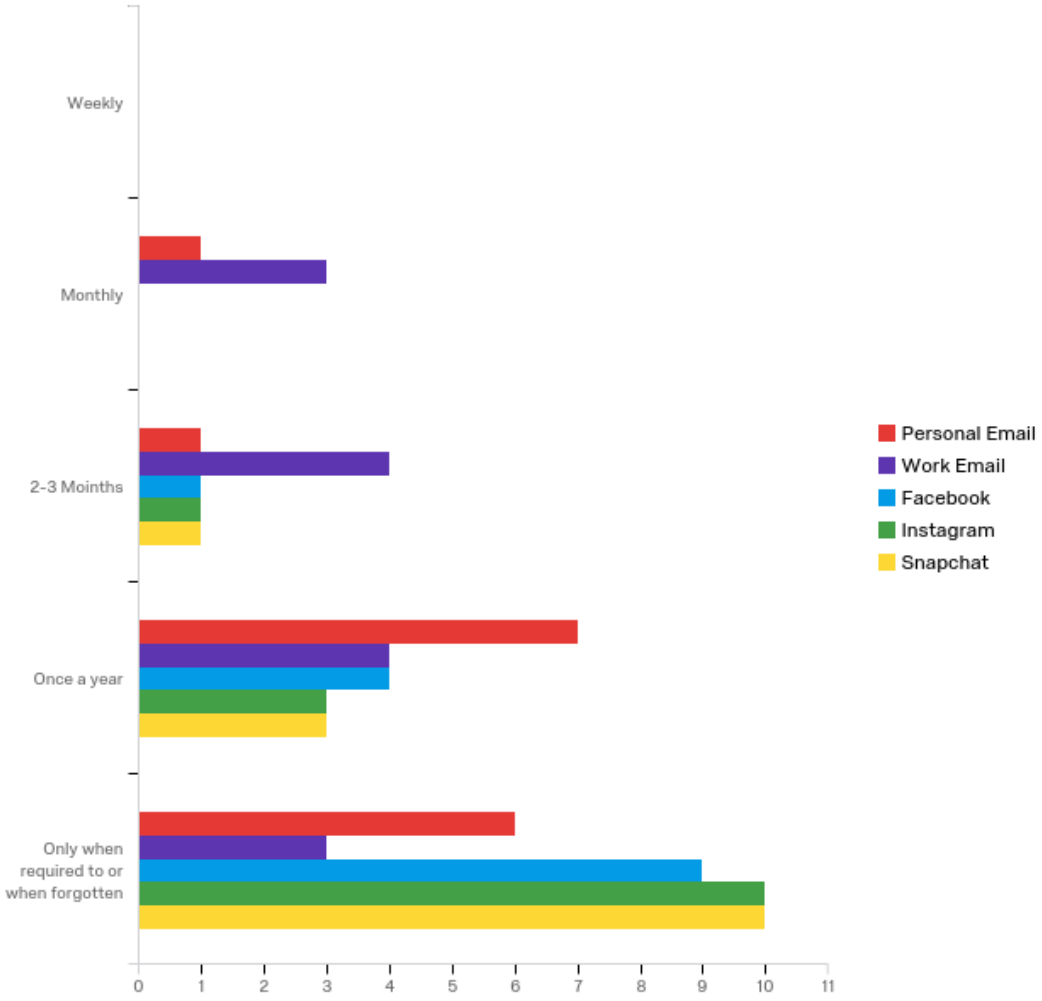
While most participants do not enter sensitive information when connected to unsecured networks, it is interesting to note that 1 participant does so freely and 3 participants do sometimes. This is shown in Figure 17. When connected to an insecure network, anyone on that network can see what you are doing. Hypothetically, someone could intercept your sensitive information and steal it.

Figure 18: Q21 - Do you use different passwords for each account accessed from your phone (Facebook, Instagram, Email, etc.)?



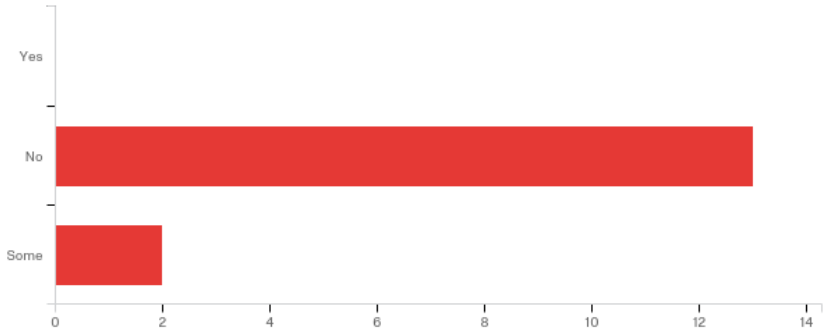
The purpose of this Figure 18 was to see how many different passwords participants use. 9 participants (60%) used different passwords most of the time or always, which is promising.

Figure 19: Q23 - How frequently do you change your passwords?



The purpose of Figure 19 was to determine how frequently participants changed their passwords and if their behaviors differed depending on the type of account. Unsurprisingly, participants changed their work password most frequently. However, it is interesting that most participants only changed their social media passwords when they were required to or when they forgot their password.

Figure 20: Q22 - Do you use the same password for personal accounts that you've used for accounts at your internship (i.e. email passwords were the same, laptop passwords were the same)?



The results of Figure 20 are promising, but still alarming. It is highly advised to have different passwords for different accounts since losing a password to one account can enable access to many accounts. If employees use the same password for personal accounts as they do for work accounts and those personal accounts get hacked, the hackers immediately gain access to the work accounts. This can be a major security hole for businesses if they do not proactively force employees to set different passwords.

Figure 21: Q24 - Have you ever lost a smartphone or had one stolen?

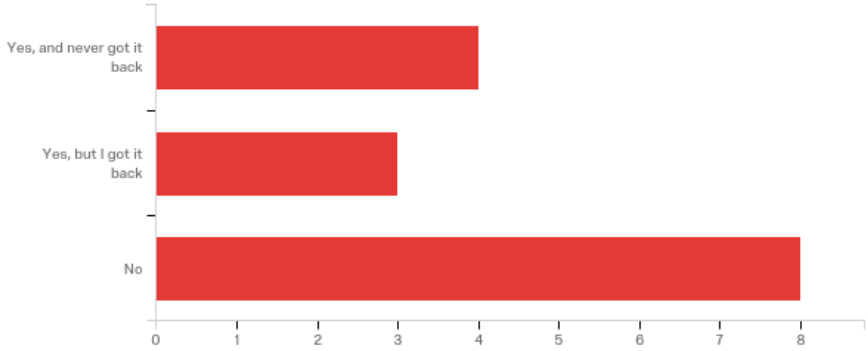


Figure 21 was meant to gain an understanding of how many devices people have lost in the past. Further, it is important to understand how many devices were never found because personal data still exists on it.

Figure 22: Q25 - When you lose your device, do you have a function to remote-locate it (i.e. Find-My-iPhone or other GPS-locating apps)?

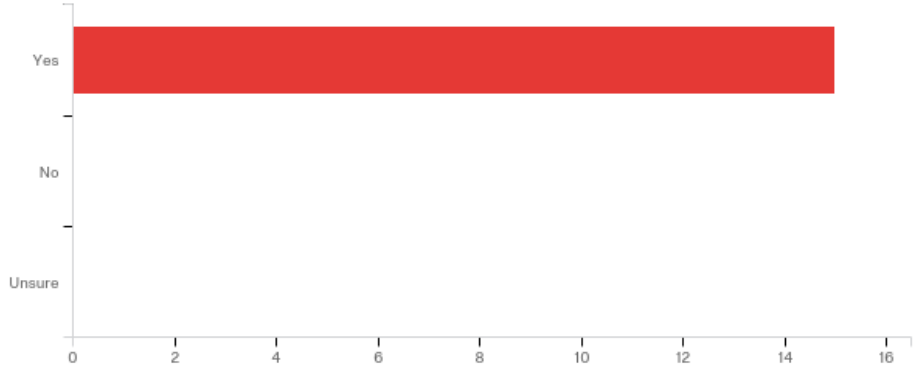


Figure 22 is an extension of the previous one to examine how easily lost devices can be recovered. Although all participants claimed that they can remote-locate their device, it is noteworthy that 4 participants (26.67%) still were not able to recover it.

Figure 23: Q26 - If you cannot locate your device, do you have a way to remotely wipe the data?

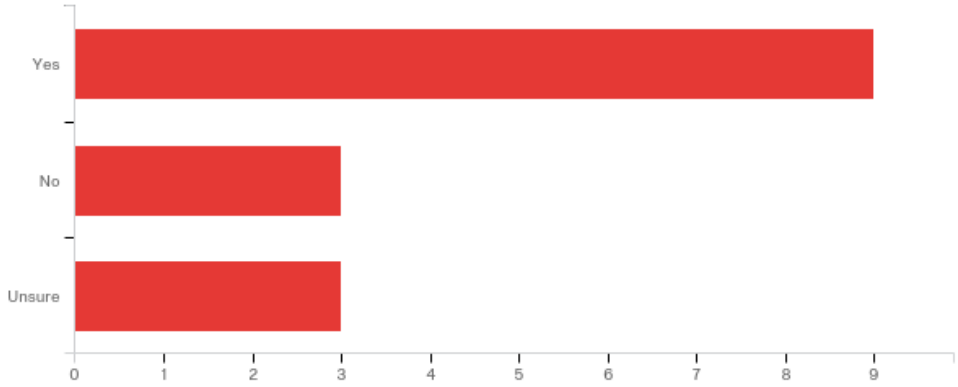


Figure 23 examines fail-safe procedures should a device be unrecoverable. The results are promising, with 9 participants (60%) having a method of remotely wiping their device.

Figure 24: Q27 - How many smartphones have you lost or had stolen that you did not recover or wipe?

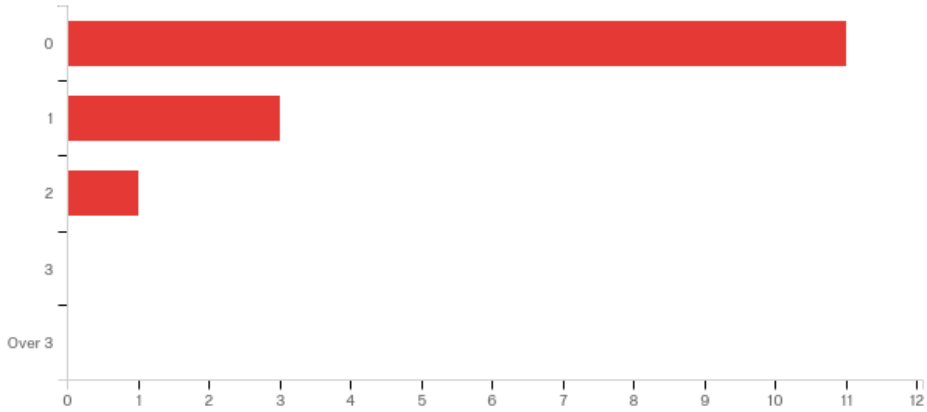


Figure 24 examines what participants have done in the past when they lost their devices. It's interesting that 3 participants (20%) had lost a device in the past and did not remotely wipe it, although they may have been able to. It's also alarming that a participant had lost not 1 but 2 devices and did not remotely wipe either.

Interview Results

The discussions during the interviews were much different than anticipated. With so many different cyber security threats that currently exist, one would assume that companies, no matter the size, would take exceptional precautions towards security by making their systems protected, their employees knowledgeable, and constantly updating their security practices. By talking to the fifteen participants, I found that companies had vastly different approaches to security. Some were as expected, like at a larger tech firm, while others were surprising, like at a large food manufacturer.

Throughout the study, I focused on specific areas that were of interest and would reveal most about the company. These areas including the onboarding experience of the participants, if the company allowed for BYOD, the general attitude of firms towards security, the behaviors of other employees, and finally the behaviors of the participants before, during, and after their experience. Also, four participants had direct experience dealing with security breaches so I explored that as well.

Onboarding Experience

Although the participants worked at various companies, many of them had similar onboarding experiences. These onboarding experiences typically included either a formal presentation, an online assessment, handwritten documents, or a combination of the three. As expected, larger companies tended to have a more structured onboarding process while smaller companies were more relaxed.

From the research, it was apparent that the largest companies had the strictest onboarding process. For example, Participant 2 worked at a business unit of a large government contractor and as such had a very formal onboarding process: "We had an orientation, we had a lot of web seminars going over basic security practices like making sure passwords were up to date. IT came in for a couple of days and told us everything needed to do (Participant 2 – ID 474)." Participant 10 worked for a government contractor as well and said they had "in-person lectures, a paper test, and online modules related to security (Participant 10 – ID 255)." Since both companies were large government contractors, it was no surprise that they had an intensive onboarding process since it is extremely important for their employees to protect the data they are working with.

In addition to larger companies having a structured onboarding process, some had more specific guidelines. Participant 13 worked at a large food manufacturer and had a series of online assessments as well as was told "never leave sensitive documents unintended at your desk. Don't leave things in the printer… And be aware of things that seem shady, like e-mails that are probably not from who they say they are (Participant 13 – ID 320)." These extra guidelines are important for companies to cover because there is only so much that can be included in an online assessment or document.

Some other guidelines were described by Participant 9, who worked at a large telecommunications company (Participant 9 – ID 932). He was required to sign several waivers and said a guideline put forth was "you weren't supposed to use your cell phone while at work (Participant 9 – ID 932)." This was interesting because every other company did not have that rule. However, Participant 9 said that despite there being a rule on cell phones, there was still widespread use and "no superior would ever challenge you if they saw you using your cell phone."

The fact that a company puts forth a rule and does not enforce it is dangerous behavior. If employees feel that some rules are simply optional, they may begin viewing all rules as optional.

While most of these large companies had structured onboarding procedures, it was interesting to find that not all of them maintained them. Participant 6 worked at a large investment firm and began his internship after the other interns (Participant 6 – ID 113). Because of this, he said that he had no onboarding process whatsoever and was never given security guidelines. While it is understandable that companies tend to onboard employees in groups, it was surprising to find that they ignored providing him any rules or guidelines. In fact, Participant 6 also used a personal laptop as his work device (Participant 6 – ID 113). BYOD presents a lot more security risks for a company, so for them to ignore that is dangerous.

Aside from large companies, some participants held internships at smaller firms and thus had less intensive onboarding. For example, Participant 3 worked at a hospital and was given an account to log into the hospital's internal system (Participant 3 – ID 887). During onboarding, he said, "they did require me to change my password but there was no original orientation (Participant 3 – ID 887)." This was interesting because from day one, Participant 3 had full access to the hospital's internal system without any guidelines about what he could or could not do on it.

Like Participant 3, Participant 14 also worked at a smaller company, specifically an automotive software company (Participant 14 – ID 198). When onboarding, Participant 14 said, "there was a real general computer usage guideline and the general do's and don'ts (Participant 14 – ID 198)." Interestingly, Participant 14 also did not have to sign anything or go through security protocols. He was required to change his password for his company account once a month but that was the only hard guideline provided.

As expected, larger firms had much stricter onboarding processes. However, it was interesting to see that one of them ignored the process altogether. Also, it was strange that the smaller firms generally disregarded security protocols as well. It is understandable that smaller firms have less capital to pay for strong IT departments, but they run the risk of uninformed employees making security mistakes, especially if they allow BYOD.

BYOD or Company Device?

Although most companies provided their employees with laptops, a small number of participants used their own personal laptops (20%). When companies allow BYOD for work-related activities, they are also allowing a whole range of security issues should they not properly assess the personal device for security holes.

Of all the participants, only Participants 1, 3, and 6 were not provided a laptop or desktop by their company. Participant 1 worked at a mid-size drug detox center where he worked with the CFO and CEO on payroll financials (Participant 1 – ID 361). When asked about being provided a computer, Participant 1 explained, "no, I brought in my own laptop from home and anything I'd do, any reports I'd write up, I would send through Gmail to the CEO (Participant 1 – ID 361)." Although Participant 1 was using private company information, it was surprising that the company was comfortable allowing a personal device and email to manage that information. Further, I asked Participant 1 if the company took any steps to make sure the computer was password protected and he said, "not so much in that sense. They didn't ask me if it was password protected or anything (Participant 1 – ID 361)."

Participant 3, who worked at a hospital, was not provided a computer either (Participant 3 – ID 887). Instead, he was given access to the hospital's internal system on day one and could do everything from his personal laptop. The hospital did not make sure the personal laptop was secure or had a password itself, they merely provided login credentials to their database. Also, when asked if he could access the hospital's internal system from outside the network, he said, "yeah, I had the option to work from home (Participant 3 – ID 887)." So not only did the hospital give Participant 3 full-range to access their database, they allowed that to occur anywhere. Practicing security in this manner is extremely risky for companies because they put full faith in their employees and have limited control of what those employees do.

As was stated in the previous section, Participant 6 worked at a large investment firm (Participant 6 – ID 113). Unlike the other interns, he was not provided a work computer nor had any structured onboarding experience. Instead, work was "emailed to me from whoever was working on it and just sent back and forth through my laptop (Participant 6 – ID 113)." Although Participant 6 claimed that none of the work he was doing was confidential, it is still surprising that a large investment firm would be so lax regarding BYOD. Especially considering Participant 6 said the company "managed pension plans and assets for different companies, both international and domestic," so there had to be a lot of sensitive information available regarding the company's clients (Participant 6 – ID 113).

Other than Participants 1, 3, and 6, all other participants were provided either a laptop or desktop during their internships. While this led to much greater security for those companies in regards to the main device being used for work, many of these companies allowed BYOD for smartphones and had almost no security protocols in place for that.

BYOD Security Protocols

Aside from BYOD for work-related activities, there was no clear difference in BYOD in regards to smartphones between large and small companies. However, there was a vast difference between how well each company managed BYOD. Some had restrictions on allowing personal devices to access Wi-Fi or email, some let employees do whatever they chose, and one even had specific software installed on employees' devices for extra protection. With many employees having their work email on their devices, it was surprising how little most companies did to ensure that was secure.

Participant 13, who worked at a large food manufacturer, had almost no guidelines in regards to BYOD (Participant 13 – ID 320). He said that he routed his email through his phone and although he was not asked to do it, he was provided instructions on how to do it. When asked if the company took any precautions towards making sure his phone was password protected, he said they did not. Additionally, he said all interns routed their work emails to their phone. This seemed incredibly risky, especially for a large company, to allow employees to freely add their work email to their phones without ensuring any level of protection. Hypothetically, if an employee lost their device and it was not password protected, any of the work information on the phone is then available. This was exceptionally intriguing as well because this was the same company who was extremely strict about leaving documents in the printer.

Other large companies had similarly lax rules in regards to BYOD. Participant 4 worked on a manufacturing floor like Participant 13, except Participant 4 was not allowed to route his work email to his phone (Participant 4 – 779). Participant 4 used his personal device for work-related activities including "taking pictures of the factory floor to highlight process improvement"

although he said the company "offered cameras if I wanted (Participant 4 – 779)." This seemed to be a conflicting security practice since Participant 4 was not allowed to have his work email on his phone, yet he could have other company information. With instances like this, it would make more sense to have blanket rules for BYOD, especially when the company has the tools available anyway, in this case being cameras.

While some large companies allowed BYOD for work-related activities, there were some who completely forbade it. Participant 7 worked at a large investment bank where no employees were allowed to route their work emails to their phones (Participant 7 – ID 735). The investment bank had strict guidelines between keeping work and personal separate, which Participant 7 explained: "You weren't allowed to send any emails to a personal email at all… Everything had to be within your work account. You weren't allowed to send anything home and they really stressed that if you do that then you're getting fired right away (Participant 7 – ID 735)." It was interesting to see the stark difference between companies that allowed or did not allow BYOD. Since BYOD can lead to a mess of security issues and costs companies millions, it is not surprising that some companies opt to disregard it completely.

Of all the companies that allowed BYOD, only one had stringent guidelines surrounding it. Participant 15 worked at a large consulting firm that worked with the majority of the Fortune 500 (Participant 15 – ID 220). He explained that "if we wanted to be on the corporate Wi-Fi or have email on our phones, we had to go to our I.T. desk and they would install this software called "MobileIron" which essentially encrypts your phone and emails and securely connects you to the Wi-Fi through VPN (Participant 15 – ID 220)." In addition, Participant 15 explained that the software required your phone to have a passcode. So, while other participants could access their work emails without having a passcode, this company made it a requirement. Also, Participant 15

explained that the software allowed the company to remote-wipe phones should they be lost or stolen, which no other companies could do. Overall, it seemed that Participant 15's company was the only one with best practices in regards to BYOD and sets an example for all other companies in managing BYOD.

Passwords

A large part of security is effectively setting and managing passwords. It has been proven in the past how dangerous it is to have one password for multiple accounts and most of the participants recognized this. For example, Participant 15, who worked for a large government contractor, explained, "I have passwords for [around] fifteen different accounts and maybe three of them are the same (Participant 15 – ID 220)." He went on to add that he has so many different passwords "because if one password is compromised then you're compromised on multiple accounts (Participant 15 – ID 220)." Having so many different passwords and variations of those passwords is extremely important in regards to best practices, both in terms of personal security and for that of the business.

Coming from a technology background and working at a large tech company, Participant 12 had similar practices to Participant 15 (Participant 12 – ID 476). Participant 12 explained that "the complexity of the security in my passwords changed. Not just making it something short I can remember but making it a lot longer, adding characters and whatnot (Participant 12 – ID 476)." Having complexity in passwords is just as important as having different ones and Participant 12 absolutely understands that. In addition, he changes his passwords every month or two, adding an extra layer of security.

On the other hand, even though most participants used a variety of passwords, some still used only a few or slight variations of past passwords. Participant 7, who worked at a large investment firm, said he "typically used three different ones. And I kind of do variations of them but they're all pretty much based off of the same three things (Participant 7 – ID 735)." This was surprising, especially since Participant 7 worked at such a large investment firm that was very strict during orientation on security. When asked why he uses only three passwords, Participant 7 explained, "it's all out of laziness (Participant 7 – ID 735)." While laziness is certainly not an excuse for lack of security, it is interesting that his own lack of security could have vast implications for the investment firm.

Like Participant 7, Participant 5, who worked at a small construction company, used the same password for a lot of his accounts (Participant 5 – ID 769). However, unlike Participant 7, Participant 5 used different passwords for different types of accounts. Participant 5 explained, "I try to change up my email. But my Facebook and Twitter and Instagram will be the same password… I guess the more secure or more sensitive information I change the password for (Participant 5 – ID 769." While it is still important to have a variety of passwords, the accounts with the most sensitive information should have the most secure passwords.

Overall, most participants were proactive towards password protection. Some of them had always used best practices while some had recently began using them due to hacking experiences.

Data Breach Experiences

Interestingly, a surprising number of participants had experience with cyber attackers. Two participants had their own devices breached, one had his company attacked the very first day he

arrived, another had his Yahoo account leaked, and another had his phone stolen, wiped clean, and made untraceable within the hour. Although these situations were all different, they show how frequent security breaches are becoming today and how necessary it is to prevent them.

In the past month, both Participants 3 and 4 had experiences with Chinese hackers. Participant 4 recounts the experience: "At approximately 4 AM I noticed a series of text messages being sent from my phone. And then I received a notification on my iMac that my iCloud was signed in on another iMac. So immediately I started reading these texts and they were all in Mandarin Chinese to local Chinese area codes. I proceeded to change all my passwords and lock them out. And then I received notifications about people trying to sign in my account unsuccessfully after that so I had to come up with a completely random password to keep these people out (Participant 4 – 779)." In many account breach experiences, it is often difficult to reclaim an account. One of the first things attackers do is change passwords, but Participant 4 was able to reclaim his account relatively easily. Participant 3, on the other hand, was much less successful: "Immediately after I got all these texts it said I was locked out of my Apple ID and I was freaking out. So what I did was I went to the Apple store and they had me completely change my password and actually ID myself to make sure it was actually me (Participant 3 – ID 887)." Fortunately for both participants, neither believes to have lost any data and were able to reclaim their accounts.

In a similar fashion to Participants 3 and 4, Participant 9 experienced a data breach experience with his Yahoo account (Participant 9 – ID 932). According to USA Today, Yahoo stated on September 22, 2016 that at least 500 million accounts were stolen from the company in 2014 (Hjelmgaard and Johnson). Participant 9 experienced this firsthand and now uses Two-Factor Authentication (2FA) for his account to ensure it cannot be accessed by anyone other than him. As

of now, Participant 9 does not believe any of his information has been stolen and he is confident in 2FA as a security practice.

Interestingly, Participant 5, who worked at a small construction company, learned on his first day that the company had been the victim of a cyber attack (Participant 5 – ID 769). He explained that the police were present at the company, everyone was very concerned, and all computer systems were down. While he was unable to find out what the final ramification of the breach was, the company did begin hiring more IT professionals to ramp up their security. Overall, the experience made Participant 5 realize that these breaches are a real threat and it is important "to change passwords and take precautions (Participant 5 – ID 769)."

The only participant to deal firsthand with having a device stolen was Participant 7 (Participant 7 – ID 735). Last spring, Participant 7 was studying abroad in Barcelona and at the time didn't have a passcode on his phone. He had it stolen and tried using Find My iPhone immediately but he said it was turned off already, the SIM card had been removed, and the phone was unreachable. Although stolen iPhones can be located as soon as they are turned back on, the criminals had wiped the device to make it untraceable. Participant 7 said "after that experience I have a lock on my phone because that would have been an opportunity for them to steal my entire life (Participant 7 – ID 735)."

While all these data breach experiences were different, they all changed the participants' perspectives on security. Many times, people act reactively instead of proactively to security, and fortunately the participants did not suffer from being reactive.

Behavior Changes

With more cyber threats occurring each day, it is unsurprising that people are taking steps to increase their security. From interviewing the participants, I found that the majority did not change their security practices due to their internships. Instead, changes occurred due to either personal experiences or news related to hacking.

While Participant 1 did not make any changes in regards to security practices due to his internship, he did make changes due to personal research (Participant 1 – ID 361). He explained different hacking methods that hackers use and that one of them is a software that runs hundreds of thousands of password combinations over time to gain access to accounts. He continued, "I actually found articles where it shows for every extra digit or character that you add to a password how long it would take a specific software to break into your account. And it shows that after something like thirteen or fourteen characters, computer software takes anywhere from forty to fifty years to break into that (Participant 1 – ID 361)." This information was interesting because it can be used by companies when setting password requirements for employees. By setting strict, complex standards, companies can limit the chances of employee accounts being hacked.

Similar to Participant 1, Participant 13 made security changes due to news he read online (Participant 13 – ID 320). During the interview, Participant 13 referenced "Celebgate", which was a collection of nude celebrity photos obtained from hacking celebrity's' iClouds [8]. Participant 13 explained that the hacker used "brute force" on Find My iPhone and then "daisy chained" passwords from there (Participant 13 – ID 320). In his own words, "that concept led me to think if Find My iPhone lets you do unlimited things, I need to be better about security (Participant 13 –

ID 320).” There is no doubt that hackers are getting better at accessing whatever accounts they choose and it is exceptionally important to have different passwords for every different device.

The only participant who improved his security practices due to his internship was Participant 11 (Participant 11 – ID 275). Since his internship, he has made passwords stronger for his email, laptop, and other accounts. In addition, he now changes them more frequently since he became used to that while working.

Overall, it was surprising that participants did not change their security behaviors due to their internships. This is most likely because their security behaviors were already up to par with the company they worked at.

Chapter 5

Discussion

The following chapter will explore the findings in detail, identify any trends in data, explore conclusions from the data, and lastly identify any limitations of the research.

Trends

Importance of Proper Onboarding

From the study, it became apparent that one of the biggest trends was the importance of proper onboarding. Not all companies performed proper onboarding for their employees, which is pivotal because it clearly defines all security protocols of the company that employees must follow. Without clear communication to the employees, questions may arise about security protocols. For example, Participant 8 was required to sign a confidentiality agreement for his work and was given clarification on rules about communication between his work and personal email. At one point during the internship, he sent a file to himself to work on at home and he was unsure if that would fall under their privacy rules. With clear and concise onboarding procedures, situations like this would be avoided and potential loss of sensitive information would be avoided.

In addition to providing complete guidelines during onboarding, companies must uphold them. Participant 9 explained how his company had a strict "no cell phone" policy during work, yet no one followed it and superiors did not address it (Participant 9 – ID 932). This causes confusion for employees, who may view the security guidelines as optional instead of there for a reason.

Even worse than improper onboarding is the lack of reviewing security protocols at all. Participant 6 did not receive any onboarding, was not required to review any security protocols, and even used his personal laptop as his work computer (Participant 6 – ID 113). Not reviewing security protocols can lead to a variety of security breaches, especially when employees are using personal devices.

Of all companies examined, the largest companies had the most extensive onboarding processes. Participant 15, who worked at a large consulting firm, not only had extensive training but also had IT put security software on his device (Participant 15 – ID 220). Participant 10, who worked for a large government contractor, had every security protocol reviewed, as well as a written test (Participant 10 – ID 255). Finally, Participant 7, who worked at a large investment bank, had an extensive review of security protocols as well as multiple presentations threatening termination if personal and work information intertwined (Participant 7 – ID 735).

Overall, it's clear that a proper onboarding process is important for the security of a company. It limits confusion of employees, avoids unnecessary security breaches, and prepares employees to follow all rules completely.

Lack of BYOD Security Procedures

Another major trend from the study was a lack of proper BYOD security procedures set forth by companies. When companies allow BYOD, they open a multitude of doors for security breaches. Most of the time, personal devices are not examined for proper security features although companies allow employees to use them for work-related activities. Most commonly, employees will route their email accounts to their smartphones.

Out of all the participants interviewed, most did not work at a company where BYOD was allowed. Most of the time this was due to it being unnecessary for interns, but it was available for full time employees. Examples included Participants 8 and 9, who were not allowed to route their emails during their internship, but could once they were fully employed.

The only company where BYOD was strictly regulated was Participant 15's, which was a large consulting firm (Participant 15 – ID 220). The company had all employees put specific software on the devices that required a passcode to unlock. Additionally, it granted the company the ability to remote-wipe devices. Overall, this is the best way to approach BYOD because it gives the employee freedom to use their device while also maintaining control at the same time.

All other companies that allowed BYOD did not monitor it. For example, Participant 13 worked at a large food manufacturer where almost every employee had their email account routed to their phone (Participant 13 – ID 320). However, there were no security protocols in place to make sure that personal devices were secure. Theoretically, employees could have unprotected devices, leaving their work accounts open for anyone to see should they lose their device. This practice held true with Participant 14, who intertwined his work and personal email (Participant 14 – ID 198). Other participants, such as 1, 3, and 6, used their personal emails for all work communication, leaving the largest security threats for their companies.

Overall, it seemed that companies have a lot to work on in the realm of BYOD. Those that do not allow it are avoiding the problem altogether, which is not a bad security practice. Those that do allow it tend to have it widely unregulated. This is incredibly dangerous since the cost of a security breach is far more than paying for each employee's device.

Behavior Changes – Only When Something Happens

A large focus of this study was to discover any behavior changes caused by entering the workforce. Surprisingly, almost every participant did not adjust their security practices due to their internship. Instead, changes occurred when an event happened to them or someone they know, such as a security breach.

Surprisingly, two participants had just experienced personal security breaches of their smartphones. Participant 3 and 4 both had their iClouds breached by what seemed to be Chinese hackers. Once the attackers gained access, they began firing off texts in Mandarin Chinese to random Chinese phone numbers. The individuals did not see any permanent damage, but had to go through a rigorous process reclaiming control of their accounts. Since the experience, they've both drastically increased the complexity of their passwords as well as diversifying them across accounts.

Similar to this experience, Participant 7 had his phone stolen and wiped (Participant 7 – ID 735). Fortunately, the theft was not for data purposes but was instead to wipe and resell the phone. This was a relief to Participant 7, who did not have a lock on the phone at the time. Should the thieves have had different intentions, his bank account, stock accounts, and any other sensitive information were wide open to be acquired. Since the experience, Participant 7 has added a lock to his phone as well as adding complexity to his passwords.

Finally, Participant 9 was involved in Yahoo losing the information of at least 500 million accounts (Participant 9 – ID 932). Yahoo was his main email account, so he was a victim of losing all of his information. Since the incident, he has opted for 2FA so that he is the only one able to access the account.

With all these experiences, the change in behavior was reactive to something that occurred instead of proactive in fear of something happening. This is interesting to note since after a serious security breach occurs, it's typically very difficult to recover. Fortunately, the individuals affected did not experience any significant personal or monetary damages, beyond the loss of the data. However, this draws a comparison to the behaviors of companies. If companies are not proactive in their security protocols, such as establishing strict BYOD guidelines, the reactive response may not be enough to fix the damages.

Limitations of Research

While the study delved comprehensively into each participant's experience, the sample size was relatively small. Because of this, the information gathered cannot effectively generalize a college senior or how specific industries handle security. In addition, the study allowed participants to discuss their work but kept the company they worked for anonymous. All specifics were withheld to protect participants' confidentially agreements they would otherwise break. If it were possible to perform research on specific companies, it may lead to a greater understanding of how different companies approach research. For instance, comparing two similar companies in the same industry where one is public and one is government-contracted may lead to interesting results.

The research also had human-limitation as it relied on participants recalling information from over the summer. For example, participants were asked about their orientation process and what online assessments, presentations, or documents they had. While the data collected from this was helpful, it may not have been recalled completely accurately as some participants may have

forgotten parts of their orientation. Further, the interviews were kept to approximately only twenty-minute time periods. In that time, there is only so much information that can be discussed and it is possible that participants forgot information and then remembered it afterwards. Finally, each participant had a different level of interest in the topic. Due to this, it is possible that some participants withheld personal anecdotes or information simply because they did not want to discuss them.

Like any research study, there are limitations to obtaining the desired data. This study had limitations due to size, anonymity, and human error. Regardless, the research was successful in acquiring the desired result.

Chapter 6

Conclusion

The following chapter will draw an overall conclusion from the data and identify opportunities for future research.

Conclusions

This research study has revealed a lot about a typical college senior and the current security practices of businesses. Both the survey and the interviews provided unique data on the topic and the responses proved similar conclusions. In the survey, it was clear that most participants password-protected their devices, used different passwords for different accounts, updated their devices quickly, and have security measures in place for retrieving or wiping lost devices. Looking to the future, these are security measures that businesses will want their employees to use in practice. While not all participants have perfect security practices, the participants were all aware of the importance of security.

The interviews strengthened these findings, but found some major security concerns for businesses. First, many businesses did not have adequate onboarding processes. The onboarding process is the first few weeks that employees start at a company where they should be briefed on security protocols, any guidelines they must follow, and any restrictions on their behavior in regards to both work and personal devices. While most participants had good security practices overall, that is not enough for companies to have peace of mind in regards to their own security. Without proper onboarding, employees can have confusion in regards to proper protocols, and may

make decisions that put companies at risk. If companies want to mitigate the risk of security breaches, they must adopt and refine excellent onboarding practices.

Second, the interviews revealed a lack of proper BYOD security procedures. BYOD involves employees using their personal devices at work as well as doing work-related tasks. Most often, BYOD allows employees to use their work email from their smartphone. This involves putting a lot of sensitive and confidential email on the device. After talking with the participants, it was apparent that most companies that allowed them to put their email on their smartphones did not ensure proper security. Without doing so, companies put a lot of faith in employees to properly protect their device, which can be dangerous. Of all participants, one described how his company forced all employees to put software on their devices that secured them, forced a passcode, and enabled the company to remote wipe them. In the new, rapidly-growing BYOD environment, this type of proactive behavior is best to protect against potential security breaches. If companies wish to protect themselves in the future, security practices like this must be adopted.

Third, most participants adopted better security practices only as a reaction to security breaches. A reactive approach is a poor security practice because it does nothing to undo damage that has already been done. Considering the general behavior of participants is reactive, companies need to be proactive. This means being at the forefront of security and preparing for breaches instead of waiting for one to happen. Without taking this approach, companies risk a load of security breaches and the subsequent cost that comes with them.

Overall, the security practices of individuals are promising. They may not be perfect, but they do protect against most threats. Conversely, the security practices of businesses have some catching up to do. They need to better manage employees, improve communication, and adapt to the growing trend of BYOD. In the future, it must be a joint effort between these individuals and

the companies they work for to prepare against security breaches. With more threats occurring each day, it is imperative that the improvement of practices begins immediately.

Future Research

The primary area for future research is in a larger scale study as well as more detailed analysis of each industry. By taking a comprehensive qualitative approach, I learned extensively about each participant's experiences, behavior, and opinion of security, but the sample size was relatively small and concentrated. Each participant was a college senior and attended Penn State. By attending the same university, the participants may have all shared views on security due to the curriculum at the university. In a larger study, students from various universities should be interviewed as that would be a better representation of the overall workforce. Also, the study was limited to fifteen participants and a future study should include more than that.

Since this was a qualitative study, it would be worthwhile to perform a large-scale quantitative study. The information acquired from the survey was interesting, but it does not hold tremendous weight on its own due to the small sample size. Having a much larger sample with similar questions as those in the survey would help gain a better general view of a typical college senior.

Furthermore, concentrating on specific industries could produce interesting results. This study showed that large businesses had better security than smaller businesses, but there were clear differences across those larger businesses. If a study was performed of equal or greater size for each industry, there would be more information available regarding the overall security practices of each industry.

Appendix A

Research Survey

Below is the survey as was provided to participants. The survey was generated using Qualtrics. Q1 was initially the participant's name, which was deemed unnecessary during research as participants were to remain anonymous.

[Q1 Redacted]

Q2 Age

Q3 Year (Junior, Senior, 5th Year Senior)

Q4 What is your major?

Q5 What industry was your internship in this past summer?

Q6 What was your role (title) during your internship?

Q7 What kind of phone do you have?

- ❍ iOS (1)
- ❍ Android (2)
- ❍ Windows Phone (3)
- ❍ Other (4)

Q8 How secure do you believe your smartphone is?

	1 (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 (7)	8 (8)	9 (9)	10 (10)
1 = insecure, 10 = secure (1)	❍	❍	❍	❍	❍	❍	❍	❍	❍	❍

Q9 Do you password protect your phone?

- ❍ Yes (1)
- ❍ No (2)

Answer If Do you password protect your phone? Yes Is Selected

Q28 What type(s) of protection do you use on your phone?

- ❑ 4-Digit Pin (1)
- ❑ 6-Digit Pin (2)
- ❑ Text Password (3)
- ❑ Swipe Pattern (4)
- ❑ Fingerprint Scanner (5)
- ❑ Facial Recognition (6)

Q12 Do you always update your smartphone's software when a new patch/update is released?

- ❍ Always (1)
- ❍ Most of the time (2)
- ❍ About half the time (3)
- ❍ Sometimes (4)
- ❍ Never (5)

Q30 How quickly do you update your smartphone's software when a new patch/update is released?

- ❍ Immediately (16)
- ❍ In a week (17)
- ❍ 2-3 weeks (18)
- ❍ In a month (19)
- ❍ 2-3 months (20)
- ❍ Never (21)

Q13 Do you read the developer's notes to understand what was being fixed or change?

- ❍ Always (1)
- ❍ Most of the time (2)
- ❍ About half the time (3)
- ❍ Sometimes (4)
- ❍ Never (5)

Q14 Have you ever installed an alternative operating system on your phone? An alternative operating system is created by someone other than your phone's maker, examples being Jailbreak, CyanogenMod, etc.

- ❍ Yes (1)
- ❍ No (2)

Q15 Do you always update your smartphone's apps when a new patch/update is released?

- ❍ Always (1)
- ❍ Most of the time (2)
- ❍ About half the time (3)
- ❍ Sometimes (4)
- ❍ Never (5)

Q31 How quickly do you update your smartphone's apps as soon when a new patch/update is released?

- ❍ Immediately (1)
- ❍ In a week (2)
- ❍ 2-3 weeks (3)
- ❍ In a month (4)
- ❍ 2-3 months (5)
- ❍ Never (6)

Q16 Do you read the developer's notes of the apps to understand what was being fixed or change?

- ❍ Always (1)
- ❍ Most of the time (2)
- ❍ About half the time (3)
- ❍ Sometimes (4)
- ❍ Never (5)

Q29 Have you ever installed apps not approved by the app store on your phone?

- ❍ Yes (1)
- ❍ No (2)

Q17 Do you use anti-malware or anti-virus software on your smartphone?

- ❍ Yes (1)
- ❍ No (2)

Q18 Do you follow news surrounding security breaches of smartphones or smartphone apps?

- ❍ Yes (1)
- ❍ No (2)

Q19 When you connect to wifi, are you sure that it is a secured network? A secured network uses a form of encryption, typically Wireless Access Protection (WAP), and all home, school, and business networks tend to have this type of security.

- ❍ Yes (1)
- ❍ No (2)
- ❍ Unsure (3)

Q20 If you have connected to an unsecure network (those found in public places, like McDonald's or Starbucks), do you ever enter confidential information such as usernames, passwords, or credit card information?

- ❍ Yes (1)
- ❍ No (2)
- ❍ Sometimes (3)
- ❍ Unsure (4)

Q21 Do you use different passwords for each account accessed from your phone (Facebook, Instagram, Email, etc.)?

- ❍ Always (1)
- ❍ Most of the time (2)
- ❍ About half the time (3)
- ❍ Sometimes (4)
- ❍ Never (5)

Q23 How frequently do you change your passwords?

	Weekly (1)	Monthly (2)	2-3 Moinths (3)	Once a year (4)	Only when required to or when forgotten (5)
Personal Email (1)	❍	❍	❍	❍	❍
Work Email (2)	❍	❍	❍	❍	❍
Facebook (3)	❍	❍	❍	❍	❍
Instagram (4)	❍	❍	❍	❍	❍
Snapchat (5)	❍	❍	❍	❍	❍

Q22 Do you use the same password for personal accounts that you've used for accounts at your internship (i.e. email passwords were the same, laptop passwords were the same)?

- ❍ Yes (1)
- ❍ No (2)
- ❍ Some (3)

Q24 Have you ever lost a smartphone or had one stolen?

- ❍ Yes, and never got it back (1)
- ❍ Yes, but I got it back (2)
- ❍ No (3)

Q25 When you lose your device, do you have a function to remote-locate it (i.e. Find-My-iPhone or other GPS-locating apps)?

- ❍ Yes (1)
- ❍ No (2)
- ❍ Unsure (3)

Q26 If you cannot locate your device, do you have a way to remotely wipe the data?

- ❍ Yes (1)
- ❍ No (2)
- ❍ Unsure (3)

Q27 How many smartphones have you lost or had stolen that you did not recover or wipe?

- ❍ 0 (5)
- ❍ 1 (1)
- ❍ 2 (2)
- ❍ 3 (3)
- ❍ Over 3 (4)

Appendix B

Interview Transcripts

Participant 1 – ID 361

Me: All right thank you Participant 1 for being here today and partaking in this interview study. So first and foremost, if you can tell me a little bit more about your internship this summer. What kind of work you did, types of projects you worked on, anything like that.

Participant 1: So this summer I worked at a drug detox center at their corporate office working side by side with the C.F.O. and C.E.O. mainly in finances. The main projects I was working on were gathering data on employees and payrolls and essentially creating reports to look at how much hours they worked total and how much of those hours are getting paid for overtime and regular hours and then I'd create reports based on that to try and figure out worker efficiency and see if we're over staffed in a department or understaffed. That was the main bulk of what I did while I was there.

Me: So how large was the company?

Participant 1: The company was I'd say between two hundred fifty to three hundred and fifty employees.

Me: So relatively small?

Participant 1: Yeah.

Me: So going back to the beginning of the internship. When you were onboarded, how did they prep you on different security protocols? Did they give you a presentation, did they have you sign forms, did you have do online assessments?

Participant 1: It was a little informal in the sense that there was not presentation or anything like that. But when I got there they gave me pretty much the rundown. Where their main corporate office was and how to get into the office. Then once I was there for about a day or two they gave me--There's a thumbprint clearance to get into the building so they put me on that system so I can use my fingerprint to get in. But besides that there wasn't any key cards or any things I needed to wear.

Me: Did they provide you a computer?

Participant 1: No. I brought in my own laptop from home and anything I'd do, any reports I'd write up on there I would send through gmail to the CEO.

Me: From your personal e-mail?

Participant 1: Yeah.

Me: Wow OK. So all the information and work you did was on your own device. Did they take any steps to make sure that your computer was password protected or anything like that?

Participant 1: Not so much in that sense. They didn't ask me if it was password protected or anything but everything had to be sent to secure e-mails that they were using.

Me: That's interesting. So how confidential was the information you were working with?

Participant 1: I guess it confidential enough where you have a report with every employee and termination dates and hire dates and pay rates. So it's not something that you really want going out to other employees but as far as to all the execs it wasn't a big issue.

Me: So you had that and all of their information on your personal device which is pretty interesting. How about your smart phone usage while at work?

Participant 1: We didn't do a lot of work on our smartphones but if needed to it was mainly a communication means.

Me: So there were no rules against anything you could do on your phone?

Participant 1: No.

Me: Would you connect to the wifi from your phone at work?

Participant 1: No, not really.

Me: Was it password protected?

Participant 1: Yes.

Me: Was it specific to different people's accounts or was it just a general wifi?

Participant 1: It was a general wifi for that corporate office.

Me: So how many other employees would have their own personal devices or personal laptops at the office?

Participant 1: There was just me, the C.F.O., and the C.E.O. would. I'm not sure if it was their personal devices but it was laptops where all the data was on that they would take to and from home but it almost seemed like it could be a personal or work device.

Me: So you weren't sure if it was provided by work or if it was their own laptop?

Participant 1: Exactly.

Me: So besides just you guys--I guess if it's a drug detox clinic a lot of the employees aren't doing a lot of stuff on their computers anyways.

Participant 1: I mean as far as actual clinics themselves. Yeah there wasn't like a lot of technology going on because that's where the drug detox goes on but at the corporate office no one really needed to bring their own things. Everyone already had a computer ready there in the office that was pretty much theirs and each employee had their own password and account to get in. And every employee was given, I guess, their own rights or clearance to get into certain aspects of the company. So if you really wanted to get into certain clients data only the C.F.O. and a couple other people were able to access that while other people were only allowed to access certain areas of quickbooks and whatnot.

Me: So did they have their own laptops?

Participant 1: So when every other employee except for the C.F.O., C.E.O., and myself were coming in to work they weren't coming with any laptops, they had a desktop computer and they would use that with a password.

Me: That's definitely very different. So think about your password usage. Do you generally use the same password for multiple different accounts?

Participant 1: Not really. I use a lot of different ones. It really depends on how much I feel I need to keep the accounts secure. For some of my accounts where I need a good password like my email I have a longer thirty character a password but then for some of my other accounts like Facebook where it's more of a social media I have a more standard password.

Me: OK. So I guess I'll just talk about other sort of personal experiences. Have you ever had an issue where somebody hacked into one of your accounts in the past?

Participant 1: Yeah, in middle school.

Me: What was that experience?

Participant 1: Well it was a person who was essentially my friend at the time and I don't know why, we were in middle school and not very smart and I gave him my password to my email and at the time I had my email password as a few other passwords. So he essentially got into my email and changed my password to multiple other accounts and then I was pretty much locked out. After a while of being locked out I finally changed my password and got my accounts back.

Me: How did you know it was him who did that?

Participant 1: Well because there was no one else I had told my passwords to. And so from that point on all my passwords have been pretty secure since.

Me: Yeah absolutely. That's definitely good and even though it's like a childish little thing that happened when you were younger, it taught you that right away, So some of the stuff that I've been learning about from these interviews are that some of these blatant security holes in companies can be bad, especially the fact that you're coming in and you're running all this information and connecting to the wifi at work on your personal device. What are your thoughts on that because if your computer got stolen or somebody got onto it because you may not have a secure encryption or password on it as a work computer, that information can just get out there. This is something I had actually just talked about, that if you can get into a company's network then you can go wherever, especially to payroll. What are your thoughts on that since you had payroll stuff on your computer?

Participant 1: Yeah I mean definitely. I think if you want to start any company of hundreds or even thousands of employees I think you definitely have that under a better lock and key. Like as you said, I think it is a possibility that if something were to happen that someone were to get access to my personal computer or get information. I mean luckily enough the information I was given that didn't give any incriminating information such as bank account numbers or anything too personal but the fact that maybe you're able to see the discrepancies between payrolls between employees that work the same type of position may cause issues within the company between employees and that's definitely not something you want when you're trying to run a company as efficiently as possible. So I definitely think once you get up there in the size of a company you definitely need to start having more discrepancies as far as who is getting what information where that information is being kept and how easily it is access.

Me: Absolutely. What do you think about BYOD? A lot of people are able to put their Outlook email right on to their phones and hook that up pretty easily. And then all of the sudden any communication that they have within the company, any confidential documents or anything like that is then floating around outside of the company grounds. What are your thoughts on that? Do you think Bring Your Own Device is something that companies should continue to push or do you think going back to either work phones or having a laptop that is completely secure with the company's own security measures on it as your means of communicating. What are your thoughts on either of those situations?

Participant 1: I definitely think that for any company you should provide laptops if you have a laptop system. You should be allowed to take the laptop home at your own discretion and maybe work from home but I believe there should be maybe an e-mail server or something along those lines that can only be accessed if you're on that working device. So you should only be able to access through a secure wifi. If you are at a public cafe or like a Starbucks you shouldn't be able to get on the wifi and access all of your personal work data because at that point you're at risk. So I think I think there should be some freedom with how you choose to

take your work home via laptop but there needs to be measures made such as server only e-mails. Anything along those lines.

Me: Absolutely. I think the exact example being at a Starbucks or something, anybody can see anything on that network so then the information is floating around and you can grab it. So this is kind of a follow up question here and I know that you've been pretty secure with having different passwords and everything like that. Have you found any changes before, during, or after your internship in the way you view security or the complexity of passwords or anything like that?

Participant 1: I guess have. I don't think my thought processes changed due to my internship, it's more just what's happening in the real world and how you see hackers and everything out there. Learning to break all these passwords and codes using different methods such as brute force and one-out, which are different hacking methods. So I mean to combat that, I essentially started doing--since all these hackers use these nefarious tools that run hundreds of thousands of combinations over time, I actually found articles where it shows for every extra digit or character that you add to a password how long it would take a specific software to break into your account. And it shows that after something like thirteen or fourteen characters, computer software takes anywhere from forty to fifty years to break into that. So if you have a password beyond twenty characters you're essentially--it's not saying that you're completely safe--but it's saying that at least you're safe against these hackers that have this software that can run thousands of combinations and hopefully fall on your combination.

Me: That's actually really interesting going to be cool to see of companies could implement something like that. Really making sure that everything is as crazy secure as possible. Alright well thank you Participant 1. If you have any further questions you can feel free to reach out to me. If not I'll be happy to share my findings at the end of this research and we'll be in touch.

Participant 1: Thank you for your time.

Me: You as well.

Participant 2 – ID 474

Me: Alright thank you for being here today Participant 2. I really appreciate your time. So we're going to get started. If you could just tell me a little bit more about your internship this summer, the type of work that you did, different projects you worked?

Participant 2: I worked at [redacted] which is a business unit of [redacted] this summer in Williamsport, Pennsylvania. I guess you'd call it aerospace engineering and I was a program management intern so I worked with the PMO office and my job was to integrate a master schedule on Microsoft Project, kind of looking across resource allocation, being physical resources and labor resources.

Me: For what type of project?

Participant 2: For all of the engine manufacturings. They are working on like twelve new engine builds that are all in the P.M.O. office They're building a lot more of those just on the floor so I was just focusing on around twelve projects for different aircraft engines and for different companies.

Me: And what does PMO stand for?

Participant 2: Program Management Office.

Me: OK so does this fall in line with what your major is?

Participant 2: Well I started with being a software developer and going that path in IST but then I started taking program management courses in IST and you learn about Microsoft Project and the whole class is focused around Microsoft Project and resource allocation, so at the Career Fair I said I wanted to do something in the program management office and they told me about that job and I had all the skills necessary. So it did align with some classes I've taken but mostly IST is focused more on software engineering but it definitely was in the realm of my education.

Me: Absolutely. So thinking back to the beginning your internship, during that orientation, how did they explain security protocols to you? Was it a presentation, did you have to sign some papers, or was it an online assessment?

Participant 2: Most of [redacted] works with the government so it's a lot more strictly regulated but Lycoming Engines is public and so they are more loose with that. We had an orientation, we had a lot of web seminars going over basic security practices like making sure passwords were up to date. IT came in for a couple of days and told us everything needed to do. I made sure that my passwords were something I've never used before. They gave us a default password the first day and made sure that we all changed it. I know that the protocol was to change it every six months but none of the interns were there long enough to do that. So I was due to change it in another three months if I were to stay working there. And there was no paperwork

to sign because... actually I don't know why there was paperwork to sign. But I didn't have to sign anything or security paperwork or anything.

Me: Nothing necessarily that said I went through this, I understand it, and I will follow it?

Participant 2: Oh OK. No I did sign paperwork saying that I completed all the requirements to say that I am up to date with all the I.T. security protocols.

Me: So then when it comes to bringing your personal device to work like your smartphone, were there are any rules or stipulations with doing that?

Participant 2: Yeah we were allowed to bring our cellphones. We didn't bring our laptops, I don't know if that was because of security protocol or we just didn't feel comfortable doing that. But they did give laptops to use there to certain people whose job needed it. So they made seem like they didn't want your personal laptop but you were able to use personal mobile devices.

Me: Were you able to put your e-mail or anything on that personal device?

Participant 2: The interns were not. You had the request to have your work e-mail put on to your phone and none of the interns did that. I think it was on a need basis for full time employees.

Me: OK so if you did that, do you know if there was special software that they added to your phone? Or was it just through Microsoft Exchange which is pretty easy to do.

Participant 2: I think that you had to get special permission from I.T. and they had inspect your phone to make sure that it wasn't jail broken and it was up to date with whatever software you were using. And I'm pretty sure they guide you through steps. I don't know if they used normal Outlook or they had something else they used.

Me: What was the email client or did you even have one?

Participant 2: Nah, I didn't use that.

Me: So did you get a computer?

Participant 2: I had a desktop.

Me: So then bringing your phone to work, would you connect to wifi there?

Participant 2: I wouldn't because I knew that they had a bunch of firewalls up so you couldn't stream music and this and that so I didn't even bother. I know that a bunch of people run different apps and half way through the summer they start kicking them off. So there's no reason for me to be on the wifi so I would just not be on wifi.

Me: OK so what were some of the things that you would do on your phone at work?

Participant 2: In free time I would use Snapchat and Instagram, things like that. So that's one of the reasons why I didn't use the wifi because one I didn't want them to see that and two there are security concerns if you're going on random internet pages and articles. So for both of those reasons I didn't really connect to wifi.

Me: Ok that's interesting I also talked to somebody else from Textron and they said Snapchat was blocked.

Participant 2: Yeah Snapchat was blocked.

Me: I mean that's kind of going around their security measures, was that I frowned upon?

Participant 2: It's not that we were told not to do it, they never said anything about it. They never once said we noticed people are on Snapchat or anything. I just was assuming that one I was at a very small business unit at Textron so I think it was more of just them trying to save bandwidth honestly more than anything else. I think that was the main reason why and I wasn't that bad about doing it so I didn't really have a concern about what would come of it if they did say anything because I was never connected to wifi.

Me: Did most people connect to wifi while there?

Participant 2: Yeah most people did but just me being in IST I knew that they had a clear list of every website you've been on so I didn't do that but other kids I saw were on Snap Chat at the beginning of the year and then halfway through got kicked off, and same with Pandora and Eight Tracks and everything like that. So I knew going in that they would be tracking that so I just didn't. And I was trying to get a full time job there after.

Me: Do you think that it's good for companies to be able to see what websites you are visiting and everything else? Or at least being able to track while you're at work?

Participant 2: Yeah I think being in IST I have a bias towards thinking that that is the right thing to do one just to track bandwidth and cost and two with productivity and whatnot. I feel like in some cases blocking things like music apps, I happen to work more efficiently with music. I think that it is OK to monitor everything and then pick and choose what is OK and what's not OK because I saw a ton of people obviously on like AOL and things that weren't directly work related that they let go by. So I'm sure they have a list of was acceptable is not acceptable. So I think it's OK to monitor everything.

Me: Absolutely. So then just playing off of that, do you think it's better to require everyone when you do BYOD to have everyone connected to the network?

Participant 2: Yeah if I were higher up in a company that would be beneficial. And just say that it's OK to check everything once and a while to make employees comfortable with that. But I definitely think that would be beneficial to track everything and make sure you all are connected to wifi at all times to monitor everything even more, making sure nothing in terms of security is a problem.

Me: OK that's definitely interesting as well. Somebody I was talking to said they were required for IT to put software on your phone to ensure that it was password protected and then would give you access to work email and things like that. Do you think that forcing employees to put certain security software on their phones is something that should be done or do you think that kind of steps boundaries.

Participant 2: I think that should be catered to on a need basis with once you reach a certain level. If you were to have a business phone where you're using your phone for any sort of business I think that's like a necessity but I think that people who are working down at the shop floor or like interns is obviously a different boundary. But I think that if you're using your phone for work purposes there's no reason to not have the company be able to install something on your phone whether it monitors things while you're in work or make sure something the company is paying for is actually being used properly.

Me: So what are your thoughts overall in the whole BYOD versus being provided something?

Participant 2: I like the idea of BYOD but I'm pretty sure the next company I'm working for you have to leave your device at the door. And so I definitely see where anything where government is involved I feel like that you shouldn't have any problem leaving your device at the door for obvious reasons I feel like at a public company it's a little harder to do that and so I think overall that you should be able to bring your own device being a mobile phone. I feel that they should have a strict law whether or not you can bring your own laptop and if you do bring your own laptop then there should be much harder regulations on a laptop opposed to a mobile device since there are so many more vulnerabilities with that and I feel that if there was a rule saying to not bring any mobile devices that that would be completely fine as long as it was spelt out in advance. And then employees should be OK with doing that.

Me: OK so obviously you are probably pretty secure with your passwords and everything else. Do you use a lot of blanket passwords or is everything kind of different for you?

Participant 2: There's a certain amount of passwords that I know have no--I guess I kind of use levels of passwords. There's like a password I made when I was like twelve or something that has no connection to anything besides Facebook and Instagram and Snapchat that I use so I don't even care if that was to be taken because there's nothing attached to me besides just that. Then for anything school related I make sure to change that every year as prompted for the school. And then for business, I make a new one that's not related to school or anything in

the slightest. That's changed I think every six months and not every year. So I definitely have levels but I do reuse a password for basic accounts that I know that no personal information is stored in.

Me: Thinking about your behaviors before, during, and now after your internship, have you had any changes in security? You know, increased security, decreased security?

Participant 2: I think now, I'm not sure if it's a choice, but just the way the apple does it now is two factor authentication. So that's just something that was done for me that I definitely don't dislike at all. In terms of old mobile device I'm definitely more secure than in the past. I know with my Android before my iPhone just because my screen was somewhat broken too, I turned off my pass codes because it was easier to get into it. So now that I'm using Apple, I think it's a little more safe in terms of that and just their encryption as a whole to begin with. For my laptop, because it's a personal laptop and does not have business things on it I've kept the same password for a while. So I guess that would be my most vulnerable because I haven't changed that and because it does have personal information on it.

Me: Definitely makes sense. I definitely agree with you that certain things need to be safer than others and certain things don't necessarily matter as much. Do you have any other thoughts on this, especially being an IST major?

Participant 2: One of the things I've been thinking about a lot is because I was working at Textron and the part I was working at was public that was not that secure and now me working at Northrop next year is going to be completely different. And right now I'm going through citizenship validation and all that, so I know for a fact I'm not going to be able to bring my phone or computer anything like that. So it's going to be weird being at home and having to make a conscious decision to use my personal laptop for personal matters and business laptop if I want to get any work done and not being able to interchange that at all. So nothing as of now but it's definitely started to pop in my head how all the choices I'm going to have to make it a little later to make sure that all my passwords are secure and whatnot. So that's interesting.

Me: It is. There's a lot going on when you're moving towards blending it when you do BYOD. Personal then becomes work and work is personal. So it's definitely very secure to keep them separated like that. So yeah it will be interesting to see what that experience is like. Well, Participant 2, thank you for being here today. I think I got a lot of really good information here. So if you have any further questions you can feel free to reach out to me. Otherwise I'll be happy to share the results of this research when I finish. I really appreciate your time today.

Participant 2: Thank you.

Participant 3 – ID 887

Me: All right thank you Participant 3 for being here today. So just to start off if you could tell me a little bit more about your internship this past summer, some of the work you were doing, projects you were working on?

Participant 3: So I started at [redacted] and I worked in their engineering department. More specifically I was in energy management because my major is Energy, Business, and Finance. Some of my responsibilities were tracking our energy consumption in each building in the [redacted] system and I would enter the data into the government database called Energy Star. Then from that I would do an analysis of which buildings were doing well and which buildings could use some work and then I would bring that to my manager because he was the head energy manager. And he would use that information to try to strategize on what they can do better in their health system to make it more energy efficient. Because they have three hospitals and hospitals are always running, they're always running AC, they got to keep it cool so that the germs aren't there. So basically we were just strategizing ways that we could cut our energy consumption because actually if you stay under a peak load, which is the amount of energy you can use in one day and if you stay under that, the utility companies will actually pay you to stay under that. That's because they don't have to start up another generator because that costs more money for them. So it cost more money for them to start up a new generator than to just pay you to stay under your consumption level. And then also I wrote reports to each building manager saying like, "hey you guys are doing good" or "you guys are doing badly, this is where we can improve". And it was only a short internship. It was about six weeks, unpaid. It was just a short amount of time so that was a general gist of what I was doing.

Me: Yeah that's still pretty cool. Definitely very unique. Cool, so I guess because it was shorter did they give you a laptop or anything like that?

Participant 3: Oh no they just gave me a log in to get in through their internal hospital system.

Me: Was that through a desktop computer?

Participant 3: I brought my own laptop and they created the account for me.

Me: OK. So going back to the beginning of your internship when they told you about security and everything else, obviously they provided you an account, password and everything. Did they have a formal orientation. did they have you do any online assessments, or did you have to sign any forms in relation to that?

Participant 3: Actually no I didn't because it was like a volunteer opportunity because it was unpaid so it was quite informal. They did require me to change my password but there was no original orientation. So they didn't really put me through any secure clearance or anything like that.

Me: So when you were logged on, was that just a web page?

Participant 3: Yeah well it was through own internal network on the UPMD website.

Me: Could you log in when you weren't at work?

Participant 3: Yeah, I had the option to work from home.

Me: OK, interesting. So theoretically, let's say you don't even have a password to unlock your laptop. Theoretically you could have been logged into that, left your laptop somewhere briefly, somebody could potentially open it up and have access to that information. And they didn't take any steps to make sure that something like that didn't happen?

Participant 3: No because the information that I was able to see wasn't really confidential and was just about the energy consumption data and stuff like that. So to them I guess it wasn't as important as actually securing their medical patients' information.

Me: Yeah absolutely I definitely get that. So on that web site, you said it was only energy stuff. So there wasn't--

Participant 3: I would have to have someone higher up to come in.

Me: I'm just thinking too on the sense that once you're in there, if someone was a skilled hacker maybe they could play around with some stuff to fake the system and make you think that you had higher security clearance. Actually back when I was in high school and I was a lifeguard, our Web site for that... me and my friend figured out a way to kind of hack through the system and make ourselves supervisors.

Participant 3: Really?

Me: Yeah and we could, theoretically we never did it, we used to just see the schedules and see the hours of employees, but we could theoretically change hours, give ourselves more hours, and kick people off of things. So that was kind of interesting and that was just us having a base account and getting to the website and figuring out different ways to manipulate it. OK so then when you would come in to work, obviously you're probably allowed to bring your smartphone, right?

Participant 3: Yeah.

Me: So would you ever do anything work related on that like login through there?

Participant 3: Generally not because a lot of my work was done in excel so I needed a laptop or desktop to do that. When I was using my phone for work, it was just making phone calls to the managers and stuff like that. So there was nothing really related to the hard information I was dealing with.

Me: Would you ever connect to wifi from your phone?

Participant 3: Yes and if I wanted to connect to wifi I would have to use that same hospital log in that they gave me in the beginning.

Me: So with that loggin, did it come with a unique email to use or was it a personal e-mail that you used to communicate with people?

Participant 3: I used my personal GMail account to send emails out to people.

Me: OK so then you would sending these files and everything through that personal email?

Participant 3: Yeah.

Me: OK. You know it's interesting as well, as you said it isn't super confidential information and what could someone even do with that but at the same time it wasn't secured and it could have been there intercepted or accessed. How many other people did you work with?

Participant 3: I was actually the only intern in my department. But I would say in the engineering department there's probably about fifteen people in there. And so everybody kind of had their jobs, like head mechanics that fixed the HVAC systems because that's probably the most important thing for the hospital. And general other administrators in the office with me.

Me: Did they have their own work laptops?

Participant 3: Yeah, they all had their own work laptop. I think everyone else had access to the confidential information of the hospital.

Me: OK cool. It would be interesting to find out what security measures they take with that. OK so when it comes to passwords, do you tend to use a lot of the same ones across different accounts?

Participant 3: I would say for my social media passwords I generally use the same one. But for things like my personal email, my school email, I use completely different ones for each and I actually change them a two times a year, every six months. I try not to use the same password because I just know once somebody gets one, you're done.

Me: So Participant 4 said you also got hacked by the Chinese people? Could you tell me a little about that?

Participant 3: So I just like woke up one night after a Friday night and I had like forty text messages from this random number. It was the same number but each new text message changed the last digit in the number. It was really weird and each text was--I don't know what language it was, it was definitely an Asian language--and then immediately after I got all these texts it said I was locked out of my apple ID and I was freaking out. So what I did was I went to

the Apple store and they had me completely change my password and actually ID myself to make sure it was actually me. And so once they were sure that it was me, they allowed me to change my password and unlock my account.

Me: Wow. So do you know if any harm came out of that?

Participant 3: Not that I know of yet, my bank accounts fine. I haven't seen anything on any of my other social media or my email or anything like that. There's hasn't been any suspicious activity. It was just a really, really weird situation.

Me: Yeah it's strange. So how long ago did that happen?

Participant 3: That happened like three weeks to four weeks ago.

Me: OK So relatively recently. I'm interested to see if this is something where they got your information and they're just waiting to do something. Because obviously you're going to react right away, but if they had access to some things and waited a little bit and then did something, at that point you may have the peace of mind and not be thinking about it. So thinking before your internship, during your internship, and then after this newest thing, have there been any changes with your security practices? Maybe frequency of changing passwords, how secure certain passwords are, and your overall awareness of everything?

Participant 3: Well getting my phone hacked definitely made me a little bit more aware and then immediately after that I basically changed all my passwords. Making sure I'm using special characters, upper case, lower case, and just being more secure. Just so it doesn't happen again.

Me: That whole hacking your iCloud... that's... that's scary.

Participant 3: And in those texts, it had all these Asian characters and then a link to a website. Obviously I didn't click the link but it would be interesting to see where that actually led.

Me: Participant 4's was sending these texts to different numbers. Was yours doing the same or was it all the same number?

Participant 3: It was a bunch of different numbers except the last couple digits would be changed. I would be all the same for first six digits and the last four would be changed. It was all the same identical text.

Me: That probably was some automated system. That's really interesting, I wonder what the heck it actually was. Well I think that's all the general information I need. If you want to follow up with any questions feel free, otherwise I will be happy to share with you my research findings at the end of it. And again just thank you for your time today.

Participant 3: No problem.

Participant 4 - 779

Me: All right well thank you Participant 4 for being here today and I really appreciate your time.

Participant 4: No problem I'm happy to help out.

Me: So you mentioned when you were doing the survey that you recently got hacked. Could you explain that a little more?

Participant 4: Yeah. It had occurred in the middle of the night when I was up all night studying for an exam. And at approximately 4 AM I noticed a series of text messages being sent from my phone. And then I received a notification on my mac that my iCloud was signed in on another iMac. So immediately I started reading these texts and they were all in Mandarin Chinese to local Chinese area codes. I proceeded to change all my passwords and lock them out. And then I received notifications about people trying to sign in my account unsuccessfully after that so I had to come up with a completely random password to keep these people out.

Me: Yeah that's pretty interesting. You always hear about this type of stuff and you always think that it's not going to happen to you and that did. Do you know if there's any other sensitive information that may have been acquired through somebody signing on that?

Participant 4: Well they had access to all my text messages and pictures and they could have downloaded them if they chose to. There's nothing really on it actually except for my bank account information. Interestingly though, the same thing happened to [name redacted] about a week before.

Me: Really? That's interesting because you are friends and typically that would occur randomly.

Participant 4: It seems interesting that it happened to someone I would know.

Me: Maybe it's the location too. I know that Penn State had got hacked. I think it was by Chinese hackers as well and that's why they're now doing a lot of 2FA especially out of the IST college and different engineering colleges.

Participant 4: I actually had the same password for my iCloud as well as my school so that's probably where it came from.

Me: Wow that's actually pretty interesting if they still have that information from before.

Participant 4: Yeah that's the only way I can think someone could have my passcode. I checked for key loggers on my computer and I couldn't find anything. So that's most likely where it came from.

Me: That's actually really interesting considering I'm doing this study here and having those things kind of connect. Alright so now we'll step into talking a little about your internship

experience this past summer. So if you could just tell me a little bit more about what type of work you did, different projects you worked on, anything like that.

Participant 4: Yeah I did operations for [redacted] this summer. Specifically I did operations planning as well as a series of process improvements. Throughout my time there I would come up with a production plan for the factory floor which would take me about two hours and after that I would update the MDI numbers for managing daily improvement. I would run a series of Excel calculations to come up with our efficiency, our on-time-deliver, our first pass service level and after that I would present that to our team.

Me: Cool, cool. Was any of the information you were working on considered top secret or requiring a higher security clearance than basic supply chain work?

Participant 4: Nothing would require an actual national security clearance but it would be information that would be damaging if it came out to our competitors.

Me: Absolutely. So then think back to the very start of the internship. What type of security procedures did they walk you through? Did they give you a presentation, did they make you do online assignments?

Participant 4: Yeah we did online assignments and I had to take an online class on how to prevent privacy breaches as well as sign confidentiality agreements.

Me: So what were some of the rules that they had with that?

Participant 4: You had to change your password fairly frequently.

Me: Do you know how frequently?

Participant 4: Three times over a twelve week period so if I had to guess, once a month.

Me: That's pretty good. What about any rules or stipulations for BYOD like bringing your smartphone to work?

Participant 4: They were very lenient on that. It was more that they had a good amount of trust with us on that.

Me: So they didn't specifically give you any rules about what you could do with your phone while at work?

Participant 4: No I was allowed to have it out at work. I was allowed to send text messages. And I know it would be unprofessional to be on fantasy football but if I so chose to I would be allowed.

Me: OK. So what about connecting to a network? Did you have a good guest wifi, did you have an account?

Participant 4: I had no wifi access on my phone. I had to use cellular data.

Me: OK so what about having your e-mail account on your phone, did you do that?

Participant 4: Oh no I wasn't allowed to do that. They said that when you're a full-time employee they give you a phone and make you use that phone. They keep work life and personal life separate.

Me: OK, what about any cross communication? Would you ever send something from your work e-mail to a personal email?

Participant 4: Yeah I would. I would send documents that I needed at work to my home email on days that I didn't feel like bringing my laptop home. And when I had my laptop at home I would have to sign in through a proxy.

Me: So those documents you would send, would that be a problem for competitors or things like that?

Participant 4: Not anything that would be an issue. It was mostly my own private work like for instance when I was applying for a full time job there I would send my resume to myself and send cover letters. And the presentation I was giving to my superiors to determine if I got the job but never anything damaging if it got out.

Me: So what about like password wise. Did you originally use passwords that you used for personal accounts?

Participant 4: No, when I started there they gave me a series of random letters, capital, lower case, and numbers. But after I had to change it the first time I switched it to one I could easily remember but it was not one I had used for anything else.

Me: So you said you would use your phone for texting and stuff like that. Were you ever asked to use your phone for work?

Participant 4: There were instances where it was a lot more convenient to have a phone. For instance I was taking pictures of the factory floor to highlight process improvement and I would use my phone for that but they offered cameras if I wanted.

Me: OK yeah. I know with my internship one of the interns used his phone for taking pictures during a cadaver lab. And that's good that when you become a full time they give you a phone for that and it's good that they offer the camera as well. But let's say for instance these Chinese competitors are direct competitors, they could go ahead and grab those photos and see how you guys proces things. But I know it is difficult to have higher levels of secure when you are just interns while you're there. So I know you said everything was lenient, did anyone ever get reprimanded for using their phones?

Participant 4: They were definitely very lenient. Nobody was really reprimanded. I was definitely seen texting during the internship and nothing ever came of it.

Me: Absolutely. So how did you observe other employees using their phones?

Participant 4: At their own discretion.

Me: So relatively the same?

Participant 4: Yeah. Especially with the full time employees they would use their phone all the time. Listening to music, or just sending a text.

Me: So I'm sure that that hacking experience changed how you manage your passwords and everything else. When did that occur?

Participant 4: I can check the date, it was probably about two weeks ago.

Me: Oh this is recent.

Participant 4: Yeah, I can actually show you some of the text messages. Yeah it was on the 21st of October, I sent a bunch of those texts to mainland China.

Me: That's weird... that's really weird. Are they a whole bunch in a line--oh my god!

Participant 4: I cut them off early. [Name redacted] probably had about 50 of these sent. I called them early as soon as these were sent.

Me: Were they all in a quick amount of time?

Participant 4: Yeah they were firing them off and interestingly this was the first text that was sent.

Me: What the heck...

Participant 4: "2787 ok?"

Me: I'm wondering--this may be something worthwhile to include actual photos in this study.

Participant 4: Yeah you're welcome to.

Me: Since that's absolutely a pin to something.

Participant 4: Yeah.

Me: Wow OK. So wipe that aside and everything--So before your internship and then during your internship and then after your internship, before that happened, did you have any changes in the way you treated your security on your devices?

Participant 4: No I didn't. I had to change my password for work but it didn't influence on how I changed my personal passwords.

Me: So with your personal passwords, do you change them relatively frequently?

Participant 4: Next to never.

Me: Makes sense, it would definitely be harder to remember if you're constantly changing it around.

Participant 4: Yeah unless I hear of an actual breach I'm not going to change it.

Me: Ok, so then after this hacking incident, have you changed how you've done things?

Participant 4: I have. I've changed my banking passwords and I have more randomized passwords.

Me: That's good. So are you worried about something like this happening again in the future?

Participant 4: Yeah, I'm going to be more on top of my passwords, specifically having different password for different things especially banking.

Me: Absolutely. Have you thought about making things longer or--have you heard of 2FA?

Participant 4: No, I haven't.

Me: OK so two factor authentication. When you log in to something, whenever there's a log in attempt, even if it's the correct password, it will send a notification to your phone and you press yes or no if it is you accessing it. That way you know if someone is trying to access something remotely or if it's you. That's something I've found interesting and I know it's something Penn State is doing now and the engineers have to do it every time they have to log on to their angel or something.

Participant 4: Wow, that sounds incredibly annoying.

Me: And I know there was a recent attack with Yahoo and now they give you the option of 2FA. So it's definitely a step forward into being more secure.

Participant 4: Actually, I use my yahoo email password as my password for my Apple ID. So that could have been the cause too. It's actually pretty likely.

Me: Well that just goes to show that these can be pretty sticky situations. So in the future, I know you're changing passwords, but are you going to take any extra steps?

Participant 4: Yeah, I don't really see myself doing that. I will probably do the same things I've always done.

Me: So last is more of an opinion. Do you think the security of your company was appropriate, or do you think they need to do anything more?

Participant 4: I don't see anyone there really taking advantage of that smartphone policy and stealing documents. Everything is pretty password protected, so you need actual access to documents that you wouldn't need. They do a pretty good job keeping documents individualized so I wouldn't be able to access anything I didn't need to.

Me: So do you have anything else that you want to add?

Participant 4: Nothing particular. I can send you those screenshots.

Me: Yeah that could be very interesting to dive in to a little bit. Well thank you very much for your time Participant 4. I really appreciate your time. If you have any questions, you can feel free to reach out to me. If not, I'll keep you in the loop if you want to see the study when it's done.

Participant 4: Awesome. Thanks!

Participant 5 – ID 769

Me: All right thank you Participant 5 for being here today and taking part in this study. I really appreciate your time. So to get started here, if you could tell me a little bit more about your internship this past summer? What type of work you were doing, any projects you worked on, really any information.

Participant 5: So I was basically the shadowing a C.F.O. of a relatively small construction company that was doing around one hundred fifty million dollars in revenue which is relatively small for the construction industry. So I would shadow him throughout the day, seeing how he does everything, how makes sure everyone's on the budget, and how all the other guys are doing. And then I worked with the budget department as well and saw how they created their minimum of ten million dollar projects. So the budgets were just so extensive and I got to learn how to make a budget and how much time actually goes into, and how much planning, and then the C.F.O. has double check with that to make sure that they have enough leeway to make sure that they make a profit on the project and that's big. And then he would meet up with the project managers for at least four hours a day to make sure that the projects were on time and the budgets were looking well. And then I got to see his checks and balances system and how he prepared his sheets and how he'd document everything to make sure that everything was in line. I got to actually be on a couple of projects they were working on and it was really cool. I got to see the day-to-day working of the construction, and what they have to do which is show around the investors of the project. He would be there as well talking about the budgets and how much all the stuff is costing. And so that was pretty much what I was doing.

Me: Cool. So with that, were you able to actually play around with the budgets at all? Was there ever an assignment where you had to run the numbers and provide a report?

Participant 5: He put me on a project to make a budget, it was a make-believe project, for a fifteen million dollar project and it took me two and a half weeks to make sure that I had all the specs down right because you had to read the floor plans that the architect gave you. That was tough. That was a tough task in itself and making sure that you have fifteen million dollars worth of materials in one budget sheet and then you had to make sure everything was correct. Then he checked it. So that was the most hands on I got, but I saw budgets being made at least once a week because he would always send me down to the budget department since that was his job to double check them. So that's how I was doing the projects, by watching these guys make these huge projects, fifteen million dollar projects budgets. It was really cool.

Me: OK so you weren't necessarily doing any work, it was more just shadowing and understanding?

Participant 5: No it was just straight shadowing because I don't think they would trust an intern with a fifteen million dollar project. But it was a good experience and I got to read floor plans and it was great.

Me: So considering that it was shadowing, I'm guessing they didn't give you a company computer?

Participant 5: They did give me a company computer because I was working on the budget and he would give me projects with the accounting side of it as well. So I was really just doing practice work the whole time but they gave me a company computer. They also gave me a flip phone on the side because they put me on the job site, like I said, a couple of times when walking with the C.F.O. and sometimes I had to stay there and look around and see if I saw anything. So that was pretty helpful to have that.

Me: So with the computer they gave you, were there any security measures on it? Like passwords or stuff?

Participant 5: They just gave you the password, and everyone knew your password so it really wasn't that secure.

Me: And so if you were doing some accounting work in the budgets, there were some documents that relate exactly to the type of work they were doing, it wasn't just practice documents on that computer?

Participant 5: Yeah.

Me: OK. With that, did they tell you at the start about any security practices you had to follow?

Participant 5: Not really because it was a relatively small company. It was like sixty five to seventy people so it really wasn't huge. So it really was kind of laid back but actually the first I was there they got hacked.

Me: Really?

Participant 5: Yeah. Their whole systems were down for two days. The cops were there and stuff it was crazy.

Me: Really? Did they figure out how that happened?

Participant 5: They didn't really talk to me about it because they were freaking out. So that was pretty crazy actually. But I mean I think they were trying to step up their security after that but it really didn't happen.

Me: Yeah absolutely, I know for smaller firms it's difficult to do that because it's very expensive. But that's interesting because I wonder... hacking a smaller company like that that does construction, I wonder what information is there. The biggest thing I think about is payroll. If

you dug deep enough into somebody's system you can get access to people's bank accounts because all of that information is saved.

Participant 5: Well I mean the clients they're working with are private investors, so it's probably big time people and there's a lot of money there.

Me: Wow OK that's interesting. So how much time did you spend and how much time did he spend on site versus doing stuff in the office?

Participant 5: On site, he was probably on site once a week. He would bounce around between different projects because he had to give showings to the clients. So he would always be there ensuring that they had their top superintendent and sometimes a V.P. and then the C.F.O. would normally be there for the walk throughs to make sure that everything was going according to plan. So probably once a week, maybe a little less, but he was normally doing that and I would go with him. It was actually really cool seeing all the jobs that they were doing because these places are just huge buildings and seeing the progress throughout my internship, and it was really cool seeing a finished product.

Me: Oh absolutely. That is really cool. It sounds like a really unique internship there. So, you probably brought your phone to work right?

Participant 5: Yeah.

Me; And even though you had a work phone, you used your smartphone at work right?

Participant 5: Yeah.

Me: What type of stuff did you use your phone at work for?

Participant 5: Texting probably, or Snapchatting sometimes.

Me: So the office that they had, was it their office or was it shared?

Participant 5: It was their office. Since they're a construction company they built it.

Me: So that location, did it have a secured wifi?

Participant 5: I think so. It definitely had its own thing.

Me: Could you tell me more about the office?

Participant 5: Their main office was smack dab in the middle of where all of their projects were. It was a big, concrete, three floor building. They're growing really fast and expanding so only two floors were used. They wanted a really big space so they can they fill it out. It was a pretty big space, I was surprised by it.

Me: Yeah OK. I was kind of imagining that as projects change and locations change that they would build up smaller offices.

Participant 5: Well it's the project managers that make twenty to twenty five people of the office technically, but they aren't really in the office because they need to be on site. It's a whole different atmosphere honestly with the construction industry honestly. The sales people stay in the office all the time, marketing people stay in the office all the time, but VPs are running around doing all types of stuff.

Me: It's certainly different than what I'm used to.

Participant 5: It's different every day.

Me: So this is a good question, did they have IT people?

Participant 5: Yeah they had four IT people, which I don't know why they had four IT people that really didn't do anything. I guess because they wanted to expand. I was talking to the CFO and he said they had just started a security program. I think they had two before and they had just hired two that summer. By the time I graduate they wanted to have around one hundred thirty to one hundred fifty people. During the summer there was like fifteen new hires to coming in for sales and project management because they wanted to expand their project areas as well. So it was growing, it was really cool.

Me: I'm just trying to understand how this company is built up, especially with the hack and everything.

Participant 5: Literally the first day there they got hacked and they were like, "Participant 5... listen... this isn't what it is normally like." And I said it's fine, we just couldn't get on the computers or whatever.

Me: Yeah that's absolutely insane. So they're hiring on IT people to develop a better company network?

Participant 5: Exactly. They're trying to go and he said they're just starting security because it just wasn't working. But they'll probably get it together, hopefully.

Me: Yeah absolutely. It's hard sometimes when a hack like that occurs. Whatever information they can get or things that they can do, you can cripple a company at that stage since they aren't large enough yet. This is really good to talk about because I don't want to get just large companies. So do you generally use the same password for a lot of your different accounts?

Participant 5: A lot of them. I try to change up my email one. But my Facebook and Twitter and Instagram will be the same password. But my school one is different too. So I guess the more secure or the more sensitive information I change the password for.

Me: Have you always done that?

Participant 5: When I got to college, yeah. In high school I used the same password for everything.

Me: What caused that change when you got to college?

Participant 5: I was getting so many different emails that I was like alright, I have to change it up. Also my uncle, who is a security tech guy, has like a hundred different passwords so he kind of hounded on me about it so I listened to him. He has this app that has hundreds of passwords and he has to copy and paste it. It's kind of crazy.

Me: That's something I thought of doing and I tried it once but I just didn't like it.

Participant 5: I mean he's a V.P. of a software company so he's really, really secure.

Me: No absolutely. So it's definitely interesting coming into a company and seeing them being hacked right away and all the other things that have gone on as of late. All that in mind, have you changed the way you look at this?

Participant 5: So I had never actually seen anyone get hacked or see a reaction to somebody hacked like that. So it's definitely real. There's a lot of sensitive information that could get you in trouble or get clients in trouble so it did change my perception just that it is a real threat and you need to be prepared for it and you need to change your passwords and take precautions. Especially in this day and age.

Me: Do you think that when you enter a company, it's up to the IT people or do you think it's more a joint effort when it comes to security?

Participant 5: I think it's a joint effort but I think the IT people need to take proactive measures to make sure they hound it in employees minds to do it. I worked at the software company two summers ago and the IT and the security team worked together. If you went to the bathroom you had to lock your computer. If you didn't, you'd have to bring in donuts or some little punishment like that. And they gave quizzes about different types of attacks to make sure you're aware of e-mail links that cause viruses. We had a seminar on that which was really interesting. But I do think it is a joint effort to work together.

Me: That's actually really cool that they had little punishments.

Participant 5: Yeah and it happened to me on the first day and I had to bring in donuts for the whole team.

Me: That's definitely an interesting approach. I know most companies tell you things on the first day and then you forget it. So I think that's all that I have. Thank you, Participant 5. If you have any more questions feel free to reach out. Thank you for coming today.

Participant 6 – ID 113

Me: All right well thank you Participant 6 for being here today. I really appreciate your. So to get started, could you tell me a little bit more about your internship this summer? You know, what work you were doing, any different projects you were working on?

Participant 6: Well I was part time so I would go in maybe three times a week and to be honest I didn't have a ton of responsibilities because I was on the ground floor of the company and it was mostly whatever excel, powerpoint, projects. I would get different presentations, different Excel pivot tables, really whatever they needed to do on a daily basis. It kind of switched and a lot of it was with pension plans so I would look through different companies and 10K's, what their foreign assets were, and if they were involved in the company. Things of that nature. That's pretty much what I would do on a daily basis.

Me: So what exactly does [redacted] do?

Participant 6: They manage pension plans and assets for different companies, both international and domestic. One example was Major League Baseball.

Me: So I'm sure there is a lot of information they have on different companies.

Participant 6: Yeah, a ton. I would use their servers and databases to find information about them abroad or whatever else.

Me: So the stuff you had to do, you would have to put together a report for X company and that would change from week to week?

Participant 6: Less about what company and more that I was in charge of research when they were trying to put an Excel sheet together for certain data on a specific company. It was vague on a day to day basis but it was usually about pension plans. But a lot of I did for like three or four weeks was just going through a massive list of companies that they represent. And I had to go through all of those and go through 10K's which is honestly kind of boring, just long annual reports. And I would find out if they had foreign assets and if they were with their company and if not, where they were and what they could do better to pretty much acquire them.

Me: For sure. That's pretty interesting. So did they give you a laptop or anything like that?

Participant 6: I usually just used my own laptop unless it was something that I needed to access that was on their servers that I couldn't get on my laptop. For the most part, the Excel stuff I could just get emailed to me from whoever was working on it and just sent it back and forth through my laptop.

Me: So some of this stuff that was being sent back and forth, was any of it confidential to these companies or was it more just the 10K's which you can find online?

Participant 6: Almost all of it was stuff you could find online and if there was anything that was their SEI software I would need to ask someone above me to get a password for their secure server that I couldn't do on my laptop. And that wasn't too often but they had a database that you could search through that you couldn't access on the internet. It was their own database.

Me: So you would never have those confidential--

Participant 6: No nothing on my computer.

Me: OK, but you would still have email communication for the other stuff?

Participant 6: Yeah like Outlook and whatever else.

Me: So let's go back to the beginning of the internship. Did they walk you through any security practices that they had or things you could and couldn't do?

Participant 6: Not really and I think it was because I was part time and I'm not going to lie that I had a huge role because I didn't. But most of the stuff was pretty straightforward and I came in a little later than most of the other interns. One of them was actually a cousin of mine so he was able to walk me through the processes and get me caught up. It was mostly just pretty simple stuff.

Me: Absolutely. It is just always important to make sure that companies walk you through those things. Did you have to sign anything or do any assessments when you first got there?

Participant 6: No. But as I said, I was more informal of an intern. They had a more formal internship program and I'm sure those kids had to go through and I'm sure those kids had to go through more of a vetting process than I did.

Me: No, no, for sure. Just thinking about that it was kind of loose. So thinking about that, you had your laptop and your smartphone obviously. Did you browse websites like Facebook or anything?

Participant 6: I guess a little bit, on occasion.

Me: Were there any restrictions on that?

Participant 6: I'm sure that if you were using their wifi they didn't want you going on your own personal stuff. So I would just use my own data if I was going on personal stuff.

Me: So other employees in the company, are they provided their own laptops?

Participant 6: Most of them had their own desktop station and it was interesting, their set up was kind of like a Google almost, I want to say, where it wasn't cubes it's like a big open floor. Everyone had their own desk and set up but there were no walled off segments from person to person. It's all pretty open which is cool because when you need to communicate with people

it's really easy. They were pretty informal to go over and talk to someone. It wasn't like you were reserved your own little cubicle and it was pretty open communication which I thought was cool. I thought that made everything flow better and made everybody more connected rather than everyone being boxed off in their own little segment.

Me: Yeah I hate the boxing off myself. So about passwords, do you tend to use the same password for a lot of different things?

Participant 6: I think I do, but all my important things like Penn State or Gmail I'll change often but then when it's like apps like Snapchat or Instagram that I don't really care about, I use more of a similar password.

Me: I'm thinking about something right now. When you log into something like Facebook, you're using your e-mail. And even if it's not your e-mail password, I wonder if someone got into Facebook that they could continue the process to your email.

Participant 6: Along with those passwords for those apps I don't really care about, I use an email I don't really care about. I have a couple emails and an old AOL email that I had got hacked. I ended up wiping that and my mom's computer-IT guy recommended GMX which is supposedly a super secure email server. And so I have that but I still use my Gmail for most things.

Me: So I guess playing off that, before internship, during your internship, and after your internship. Have you seen any changes in how you view security or how you handle your passwords?

Participant 6: I think definitely. I think when I was younger I didn't think twice about using the same password that was easily accessible. But now that we have so many more important things related to our email address, I feel like now everything you do you have to enter an email address and it's linked to a million things. Back in high school it was something I never really would have thought twice about using the same password for everything. Whatever doesn't really matter. But now with work and school and so many other things you need to have a more secure email.

Me: Yeah absolutely. This is something I never really thought about and I still use a lot of the same passwords.

Participant 6: I think as a whole, we're in an even more technological era than we were before and the hacking era is definitely a lot bigger than it was when we were younger.

Me: It's definitely an interesting age that we live in and it's going to be exciting to see what the future brings. So thank you, Participant 6, for your time today and if you have any questions feel free to reach out to me.

Participant 6: Thank you.

Participant 7 – ID 735

Me: Well Participant 7, thank you so much for being here today. I really appreciate your time for this interview study. So first and foremost, if you just tell me a little bit more about your internship this past summer, the type of work you were doing, and any projects you worked on?

Participant 7: OK. I worked at J.P. Morgan in financial control. I was in the finance analyst development program with about one hundred twenty other interns I think.

Me: Oh wow, that's a pretty big program. Is that in one location?

Participant 7: Yeah that was in Newark, Delaware but they have locations in New York, Columbus... I think there's like five other locations that had about the same number of interns. So pretty big program but each intern was placed in a team and that's like where your desk was located and you worked with them for the entirety of the internship. Most of the interns are placed in financial control. So mine personally was different expense accounts for the tech and ops business so we basically managed those expense accounts and made sure that everything was right between different financial statements. And then on top of that work that I did with my team there was a lot of networking and senior leader speakers. So I would say once or twice a week we would have events that were either a networking event. So you got to know each other interns or other senior managers and stuff like that. Or it would be a senior leader speaker series they were called and they would basically go throughout their career path and how they got to where they were.

Me: Cool. It sounds like a lot of really interesting work and definitely a lot of people and moving parts there. So thinking back to the very beginning of the internship, did they give you a laptop to use while there?

Participant 7: Yes, they did give us a laptop on our first day actually. The laptop was only allowed to be used at work. You were allowed to bring it home but you weren't supposed to use it at home or anything like that.

Me: What would be the purpose of that?

Participant 7: I think it was because if you did any work at home then they would have to pay you for it. I think it was more being reimbursed for your work. So you were allowed to, like the full time employees are allowed to, but they're obviously paid full time and we're paid by the hour. So yeah that was the main reason.

Me: That makes sense. So passwords for that, they gave you a password and then you had to create one?

Participant 7: Yes. At first it was a password that we kept for I think it was a week and then they made us make a new one but it was a very complicated password. It had to be like twelve characters, had to have a certain amount of numbers, and then another random symbol or something like that. So it was a complicated password.

Me: So during that first day in a orientation, how did they tell you about security protocols for the company? Did they give you a presentation or did you have to take online assessments?

Participant 7: Yeah the first week was the orientation. The first day was pretty much committed to security and making sure that you keep everything at work and everything's pretty much confidential. You weren't allowed to send any emails to a personal email at all. Especially if it had to deal with work. Everything has to be within your work account that you were working on. You weren't allowed to send anything home and they really stressed that if you do that then you're just getting fired right away. They stressed that very hard and if anyone did do that, the amount of times they stressed that you kind of deserved to be fired.

Me: So past that, did you bring your smartphone into work?

Participant 7: Yes.

Me: And did you use that at work?

Participant 7: Yes.

Me: Doing what?

Participant 7: Texting friends, all the basic stuff I would normally do. Instagram, Twitter.

Me: Did you put your work email on your phone?

Participant 7: No.

Me: Did they not want you to?

Participant 7: No.

Me: Did full time employees put their work email on their phone?

Participant 7: Not that I'm aware of. I don't think that they do.

Me: I know some companies do and some don't. So while you were there did you connect to wifi?

Participant 7: Yes, the visitor wifi.

Me: OK so it was just a general guest wifi?

Participant 7: Yes, a visitor wifi.

Me: That's interesting because it's basically just free internet and do whatever you want.

Participant 7: At first I didn't even use wifi because I wasn't aware of it. But then I found out about the visitor wifi so obviously I hopped on.

Me: Were there any rules about what you could do on your phone at work?

Participant 7: Not really. It was a pretty relaxed atmosphere. Obviously all the workers had families so they were allowed to text or do whatever they wanted but you obviously shouldn't just sit on your phone all day because then you're not doing work.

Me: Another question, were there any rules about what you could or couldn't do on your work computer?

Participant 7: They didn't. They basically said to keep it to work stuff but you could go on news sites and stuff. I tried to go on a few sites and they were blocked, for example I tried to go on Barstool Sports and it was blocked. So basically anything that could really get you in trouble was already blocked so you didn't really have to worry about it.

Me: So over all of your different accounts and everything, do you typically use the same password for everything or do you use a lot of different ones?

Participant 7: I typically use three different ones. And I kind of do variations of them but they're all pretty much based off of the same three things. So I'll change up the numbers and the caps but it's pretty much the same three.

Me: Are those for different levels of security? Say like email, bank account gets this one, this account gets that one, and accounts I don't care about get this one.

Participant 7: It's kind of just out of laziness. In the last six months I have a new password that I've started using. And then I haven't changed my old emails and stuff like that. So I still know those are the same but now I have a new password for any new accounts I create. It's all out of laziness.

Me: I actually just started using a new one in the past year and I set my passwords by level of security I need on my account. So have you experienced anything with hackers or knew someone who had something hacked?

Participant 7: I do have one story. When I was in Barcelona I got my phone stolen. And at the time I didn't have a passcode on it or anything like that. Obviously all my bank accounts, stock accounts, pretty much everything important to me was on it but nothing ended up happening. I just kept an eye on it and I think what they did was just shut down the phone right away, took out the SIM card, and then after that experience I have a lock on my phone because that would have been an opportunity for them to steal my entire life.

Me: That's insane. So after that experience, have you taken any other steps towards security? Because you had Find My iPhone, right?

Participant 7: I did use Find My iPhone right away, but it was turned off right away already. They were career criminals. They knew what they were doing. So after that I did get an app to write down all my passwords because before I had it all in my notes. So they could have literally taken my entire life, but they didn't.

Me: So this was relatively recently?

Participant 7: This was last spring.

Me: Wow. So that's definitely a traumatic life event. Did it change the way you approach this type of stuff?

Participant 7: Definitely.

Me: So big closing question I like asking people, have any of your security practices changed from before, during or after your internship? And I'm sure this event sparked something?

Participant 7: Yeah it is changing and I'm probably going to change more. I've been watching Vice and the stuff hackers can do is just so scary. And I just want to be as cautious as possible. So I'll probably change my passwords in the near future--maybe tonight after this conversation!

Me: Absolutely because most people are not that secure with their information. And hackers are getting better and better, so just accessing one account can open a whole lot of doors.

Participant 7: I think people don't change things unless they happen to them directly or someone they know closely.

Me: I agree. Everyone turns a blind eye and assume, "it will never happen to me." Well Participant 7, that wraps up the interview. Thank you so much for your time and if you have any further questions do not hesitate to reach out.

Participant 7: Great.

Participant 8 – ID 199

Me: Alright. Thank you so much for being here today Participant 8, I really appreciate it. So if you could just go ahead and tell me a little bit more about your internship this summer, what type of work you were doing, any projects you were working on?

Participant 8: Yeah definitely, no problem. So I was working for [redacted] in Boston, Massachusetts. I was specifically placed in their commercial insurance department and within that I was specifically placed in large businesses of over a thousand employees and the work I was doing entailed insurance lines that deal with what they call "casualties." So that was worker's compensation, auto liability, and general liability. So my manager was the head of distribution for that area of the business so basically how can we reach out to these big businesses and using our broker partners in bringing a new business and maintain our current book of business. So pretty much I was working alongside her all summer working on a new initiative that pretty much consumed a lot of the time that I was at my internship this summer. It was just how can we more effectively and efficiently bring in new business by leveraging existing relationships and just making a more collaborative environment when it goes after developing new business. So that's pretty much what it entailed and a lot of it was also meeting with other leaders throughout the company and getting to know them so I could really get a feel of if this is an industry that I want to work in, and if so, where specifically.

Me: Absolutely. So would you deal with documentation that were confidential about these companies that you worked with?

Participant 8: Yeah, so I had some information on some of the projects I was working on, but more so on another project I was working on that entailed two different business units. It was kind of cross selling their products so I had some confidential information about clients, how their account is, what lines we have, when they were renewed. So yeah, I had to deal with that.

Me: So did they give you a laptop when you begin your internship?

Participant 8: Yeah, they gave me a laptop for throughout the summer.

Me: So during the onboarding process, did they give a presentation about security practices, make you do online assessments, or have you sign anything?

Participant 8: Yes. So I believe I signed a confidentiality agreement on my first day there, just a privacy agreement because they knew I'd be dealing with some sensitive information. And then also once I got onboarded, part of that process was an online tutorial walkthrough that pretty much just walked me through the privacy codes of the company. I watched a video that showed how it's unethical to release some of this confidential information, how to handle it properly, whether someone's asking about it if they actually need it for their work or they're just asking about it.

Me: That's pretty good that they did that. How about as it relates to your laptop itself. Were there restrictions as to what you could or couldn't do? Were there types of passwords that you had to have on there?

Participant 8: Yeah definitely. So there are certain things that I couldn't access on my laptop, I guess you could say software that contains--I don't know if you've ever heard a sales force, I know it's used a lot throughout businesses but pretty much contains a lot of private information about clients. So I never had access to that and then a lot of the times when I needed access to some files that might have some information that could be sensitive I had to reach out to someone or get approved to get access. And also within the company network you were pretty much able to go on some sites but a lot of them were blocked like Facebook, E.S.P.N., and everything like that. So I know they look into that pretty well as far as what their employees are doing and what information they're accessing online.

Me: OK so when you had to create your password for that laptop, did you use of password that you used in other places or was it something completely brand new?

Participant 8: Yeah, so actually thinking about it I thought that it might be good to come up with a unique password specifically for work, so I did come up with a password that I never used before.

Me: That's definitely good. I've noticed a trend in a lot of people that once they begin work they end up using unique passwords. So how about across your other accounts? Do you tend to cycle through a lot of the same passwords?

Participant 8: So yeah I'd say that's a little different. I would say more important accounts, like banking or a broker account for trading stocks, I like to do more unique passwords that I've never done before and then I'd say below that, school accounts, e-mail, and stuff like that are a little less unique. And then when it comes to social media I think the passwords are almost the same on all accounts. And then for my personal laptop, the password is similar to that.

Me: Absolutely. I feel like I've seen a solid trend of people doing the same thing. So I'm assuming you brought your smartphone to work?

Participant 8: Yes sir.

Me: So what types of things that you would do on your phone at work?

Participant 8: So I wasn't allowed to access their network, or their wifi. I know that once you're a full time employee you are able to but I guess just being intern they didn't want us to have access to the wifi. But I still had the access to the cellular network so it was a lot of communicating with my boss and the other intern I was paired up with. I also went on a couple business trips to Dallas and Chicago so that involved communicated my boss to meet her at the

airport and all sorts of stuff like that. And then I guess during break hours I would use my phone as well.

Me: So that's telling me you didn't have your email on your phone?

Participant 8: So yeah, I'm not sure if I would be able to. I know that once you're a full time employee there, they give you work phone.

Me; I'm finding that with BYOD, your personal device is becoming your work phone as well.

Participant 8: Yeah, I saw some discrepancies. My mentor had a work phone but my manager used her personal phone so I don't know if it was preference there or not. I'm working there full time next year so I'll find out. But I think it was a mix of either or if you wanted personal and work to be completely separate.

Me; OK. So personally, did you ever send anything from your work e-mail to a personal email?

Participant 8: I have, yes, I was going to mention that. I had a presentation so I just sent a Powerpoint with no information that was private, just a presentation, so I could prepare outside of work. Unless you had clearance, you were not able as an intern to access any other network than the Liberty Mutual network. So I had a big presentation for some of the managers in my department, so I sent the presentation over so I could study and work on it at home.

Me: Is that something that you asked to do or did you just do it?

Participant 8: Looking back I probably didn't ask to do it. And that could be against their privacy rules, but again there was no confidential information in there.

Me: So do you think, in circumstances like that, do you think that it's good to have a clearance system where you need to ask to do that?

Participant 8: Definitely. I think that's definitely a big thing working in a business that has very private information about clients with financial specific information about individuals and worker's comp and medical records. I think it's definitely important to have someone overseeing that there is some sort of clearance when it comes to sending something outside the company. You know boundaries. So I definitely think that's a good idea.

Me: Absolutely. It's something to think about because yeah. there wasn't anything confidential in it but it definitely went underneath the radar. You went ahead and sent a document created at work to home when it's against the rules, and they're just relying on a confidentiality agreement. And say someone were able to gain access to your computer, they could theoretically get that information and it's not like you gave it away, it got stolen.

Participant 8: Yeah and there was no specific rule or anything that said that was not allowed during my onboarding process, but I think it needs to be a clearly defined line.

Me: I'm right there with you. So have you changed your thoughts or behaviors from before your internship, during your internship, or now afterds?

Participant 8: I haven't actually done it, but I definitely thought about revamping my passwords specifically on my computer just thinking about all these firms out there now that are mining data off of everything you do and tracking every movement you make online and then selling that information to marketing firms. So it is a little concerning to me that there is a file out there that has everything I've done online. Not that there's anything I should be scared about or anything, but it's just odd that that's a thing that they have the capability to do that. And then also with apps on my phone like Venmo, if I didn't have a password someone could open by phone and empty my bank account in 10 seconds. So I definitely thought of coming up with more unique passwords and making sure apps log you out with fifteen minutes of inactivity. And so I think going into the workforce, graduating this year, and working full time, I have a lot more to lose now. I mean I don't have that much money now but once I establish myself it'll be a really big deal.

Me: I absolutely agree with you. I'm interested to see where things go. If you have any further questions, feel free to reach out to me. Otherwise I'll be happy to share the results of the study in the end and thank you for your time today.

Participant 8: Thanks, looking forward to it.

Participant 9 – ID 932

Me: All right thanks for being here, Participant 9, I really appreciate your time. To start off if you could tell me a little bit more about your internship this summer. What type of work you were doing, the type of projects, and kind of the industry a little bit?

Participant 9: So I interned at [redacted] which is a telecommunications company. They produce electronics components for a variety of industries. Most notably telecommunications and even more specific for harsh weather environments. So planes, automobiles, underwater, that type of stuff. And so I worked in the tax side of things with the transfer pricing department. So the company is a multi-national company we have entities in over one hundred fifty countries. So you're dealing with the variety of taxing authorities and basically as a transfer pricing intern I was not issuing the transfer pricing adjustments but making sure they are offered in correct denominations, just validating the numbers through the system, and then eventually preparing reports for the taxing authority because we're dealing with not only the US taxing authorities but around the world. So there's a specific set of rules and guidelines that each one has to follow and then stuff like transferring from GAP to STAT in regards to the accounting.

Me: So is this like public stuff or was it for the government?

Participant 9: Customers of the company you mean?

Me: Yeah.

Participant 9: So it's both government and public.

Me: Were you doing both or were you mostly one side?

Participant 9: I guess mostly public but some government. I wasn't really, say, looking at where the income was coming from but I was dealing with the income in like nominal terms. So I could have been depending on what authority you're dealing with, either private or public.

Me: So they didn't separate the two, the work was all intermixed?

Participant 9: No, they didn't.

Me: Interesting. So going off that, if you could think back to the very beginning of the internship, during your orientation, did they go over their security protocols at all and could you explain that some more?

Participant 9: Well see I had access to nonpublic information regarding like accounting practices so I was required to sign several waivers. I was not able to trade the stock, obviously, and then just general workplace safety. The cell phone use was touched on. You weren't supposed to use

your cell phone while at work was a guideline put forth. And no information was to be taken out of the office.

Me: So no cell phone use at work, do people still use their cell phone?

Participant 9: Yes. Widespread use.

Me: So nobody listened to that?

Participant 9: Yeah, no superior would ever really challenge you for it if they saw you using your cell phone.

Me: Interesting. So do people ever put their emails or that type of stuff on their phones?

Participant 9: As interns we actually were not able to access our work e-mail (it was through Outlook) anywhere but specifically our assigned computer within the intern department at the company.

Me: Do you know if other people did that?

Participant 9: Yes, full time workers did have access to their work e-mails from their smartphones.

Me: Was it work phones?

Participant 9: They were personal devices actually.

Me: OK Interesting. Do you happen to know if there were extra security protocols that they put on for that?

Participant 9: Not sure.

Me: OK, because I know with my internship over the summer we were able to do so as well but somebody came into our intern room and was like, "You probably shouldn't do that because things can get hacked pretty easily." But yeah. So I guess kind of playing off of that did you ever have any communication between your work e-mail and personal e-mail such as like one of things I had to do was send directions to drive to the Apple store to fix my phone over lunch break. Did you ever do anything like that?

Participant 9: Other than one day that I was sick and communicated with my boss from my personal e-mail there was no overlapping of the two.

Me: That's interesting. So talking more about smartphones you said everybody kind of used them at work. How did you use it at work?

Participant 9: Kinda just sit by your desk, text people all day, go on whatever app you may want to access whether it be any social media source or news source or whatever you would want to

do on your phone. There was really no guidelines as to how you could use it. There was really no restriction of use even though it was supposed to be frowned upon.

Me: Great, so did you connect to wifi or did other people connect to wifi while at work?

Participant 9: Yes, so there was a wifi that people could use but I have unlimited data with AT&T so I had no use for wifi.

Me: So do you know if it was password protected or if there was a blanket password?

Participant 9: So you had a company login almost, it was that of your email. And that way they would know, I guess, who is doing what on wifi.

Me: I guess that's better than a blanket wifi then. So as you said nobody nobody kind of followed the rules of smartphone use. Do you know of anyone at all who got reprimanded for that?

Participant 9: No, it seemed pretty lax.

Me: Do you happen to know if there were any security breaches that happened in the past or when they updated their security protocols or any changes that they may have had?

Participant 9: I'm not aware of anything. I never really worked in close unison with that department.

Me: So I guess to round it out right now, the last kind of question I want to ask you is similar to something from the survey. Before your internship, how did you protect your phone?

Participant 9: Password protection and fingerprint, but it was structured so either or would work.

Me: And so then throughout your internship and then afterwards, have you changed the way you've done security?

Participant 9: No, I have not.

Me: Not on your other devices, like laptops?

Participant 9: Well, so I actually use Yahoo. And they recently had that breach so I have to look at an authentication key now. I know that if I want to log into email on a school computer I'll need to go on a Yahoo app on my phone and it will give me a four digit code and I have to put that in in addition to my password to log into my Yahoo account.

Me: Yeah, it's two factor authentication that's something that here at Penn State they're pushing out after that last security breach. So that's that's definitely a next step in security that some people find annoying especially if you don't have your phone on you. You need to get up

and go find it but it's definitely better and it's interesting. So you have that for your e-mail because that was the change in policy from them?

Participant 9: Actually just the Yahoo breach kind of stirred up the idea in my head because I also at the time had been using not one password for everything but like two or three passwords for everything. So I kind of changed all my passwords and then did an authentication thing with Yahoo.

Me: Did you choose to do that?

Participant 9: They offered it to me immediately following that breach because I think that was a big deal and they kind of did it to cover their own ass. It would look like they're paying more attention to security. Anyway so I just did it. I was offered it and I agreed to do it because I mean I just have so many e-mails through it. I use Yahoo as my primary email so everything gets funneled through that e-mail and in light of recent events I would prefer not to like have that hacked. Who knows what could happen?

Me: Absolutely. So is there anything else besides your e-mail that you have opted for two factor authentication or anything that you're aware of?

Participant 9: I've played around with Coinbase, which is almost like a BitCoin wallet and I've done it for that also because that's another thing that I like feel as if it would be important to protect. I don't possess any BitCoin or crypto currency in general but as a finance major I'm interested by it and kind of took the first steps if I ever were to want to acquire something like that. I never have actually used it but with my account yes it is set up that way.

Me: So I know they said no smartphones at work. Just out of curiosity, were you every required to use your phone for anything at work?

Participant 9: Not outright, but we did have several trips like to a factory to see how it worked and then we had an intern presentation. I was actually stationed in Berlin which is in Harrisburg and is actually a big center for the company so I had to drive up to Harrisburg. So it was more so just like Google Maps directions to that place and communicating with the other interns. But never was I explicitly told to use my phone to carry out tasks for work.

Me: I feel like that could just be specific to work. Like with my internship, one of the things was that we went to a cadaver lab and tested a new product. One of the interns was in charge of this as part of concept development. For the new product, the intern had to take pictures for his records and such, so I wasn't sure if you had a similar experience. And that's also something that's interesting to think about because with apps like Pokemon Go, you're constantly recording your surroundings inside a company when some of that stuff should be private. Just thinking about if any of those types of things could be major security breaches down the line.

But alright, wrapping up is there anything specifically want to share or anything that maybe popped up during our conversation?

Participant 9: I can't think of anything off of the top of my head.

Me: OK well thank you so much for your time today Participant 9. I really appreciate it and if you have any other questions, feel free to reach out.

Participant 10 – ID 255

Me: Thank you so much for being here today Participant 10. I really appreciate your time. So just to start off if you could tell me a little bit more about your internship this summer. What industry it was, the work you did, maybe the projects you worked on?

Participant 10: So this past summer I was working for [redacted]. They are a defense contractor out of the greater Boston area and I was working as an electrical engineering intern.

Me: So I know electrical engineering but I don't know a ton about it because it's not my field. Could you explain some of the stuff that you would do?

Participant 10: Most of my job focus was used to create wiring diagrams for distant testing interfaces that we would use to test different subsystems for the product we were working on. OK, so whether it was for troubleshooting problems or testing if a subsystem met the requirements that it was built to meet.

Me: So if I understand correctly it would be like, let's say you had a missile or something. It would be like the wiring attached to it that you would make sure all the sensors are collecting the right data?

Participant 10: Yes, so if we wanted to check the voltage level at some point on a missile we would create an interface to measure that subsystem. In particular, measure the voltage or currents or whatever we're looking at under different tests whether it's a vibration based test, an in-lab test, or like a grounded flight test for example.

Me: That's pretty cool. It's definitely out of my realm but definitely is pretty interesting. So the stuff that you were doing, was it a lot of government contracted or was there some public sectors as well?

Participant 10: It is government contracted. The product I was working on was something we got funded for but was not yet purchased by a buyer from the government although there was large interest in it.

Me: I ask because when I think of Textron, I know Bell Helicopter is a part of that and that can be public stuff as well. So let's think back to the very beginning of your internship. When you first got there, I'm sure they had a type of orientation. How exactly did they prepare you with their security protocols? Did they have a formal presentation? Did they have an online test? Did they have forms you had to sign?

Participant 10: Yes, there were multiple security measures that we had to go through. We went through the company's I.T. policy, we did training on how to uphold and maintain it. There were forms and signatures that we had to sign saying that we've gone through the training and gone through the training modules and they rated us on our performance.

Me: The training modules, was that an online assessment?

Participant 10: There were both. So they were both in-person lectures, a paper test, and online modules related to security.

Me: OK that's good that they did the whole realm of everything. I know there are some companies that are just like, "yeah when you get a chance do this online module" and they don't ensure you pay full attention as you go throught it. What specifically were the rules about a smartphone and bring your own device?

Participant 10: So we are allowed to bring our personal devices into work but we're not allowed to do anything work related on our phones at the time. So for example, if I was working on a matlab code for data acquisition, which is something that I would do in the workplace, I would be able to listen to music while I wrote that code. That's basically the extent of what I use my smartphone for was either listening to music or at lunchtime maybe searching the internet.

Me: OK so was that really the only rule, no work stuff and otherwise it's kind of free free reign of whatever you wanted to do?

Participant 10: I could not use personal email for anything work related and I could not do anything work related using my smartphone.

Me: So was that specific to interns or did people have company phones? Because when I first began my internship they showed us how to put outlook on our phones and then quickly like a week later told us to take it off. Did established employees do that or how was it handled?

Participant 10: So established employees if they need a work phone they can get a work phone through the company. I am not sure if established employees can set up their personal devices for work related material or not. For interns though we did not have to have any kind of personal device outside of work. To do work related stuff we were assigned laptops. If we wanted to, we could sign out and do work from home using the work issued laptops.

Me: When you say "sign out", you actually had to do a formal, "I'm taking my laptop home today?"

Participant 10: Yes.

Me: That's interesting. I haven't really heard of that. I feel like typically they give you the laptop and it's like whatever.

Participant 10: No, we had to mention when we're bringing the laptop out of work and sign it back into work then so they know which employees' personal computers are leaving and when it's coming back in.

Me: Do you know what the purpose is for that? Because I feel like yeah they know that it's away but that's not really preventative. It's not like when they bring it back in they do a scan to see if anything happened.

Participant 10: To tell you the truth I'm not sure.

Me: Huh, that's definitely interesting. I feel like it's a preventative measure that's only halfway there to preventing something. So when you were at work, did you or other people connect to the wifi network?

Participant 10: Yes.

Me: Was it a guest wifi or did you log in with your own credentials?

Participant 10: You would log in with your own credentials. Actually... OK, yes I remember correctly. Yes you log in with your own credentials.

Me: I know some are different, my first job was guest and my second one was log in with your own credentials. So were there rules set up as to what you could access or not?

Participant 10: Yes, they did block specific sites related to retail or Snapchat, for example, was blocked on smart phones.

Me: Really. That's interesting. What about Pokemon Go?

Participant 10: I don't recall, I was not using it at work.

Me: I know that blew up over the summer and a lot of people around my office used it. One of the interns worked in the warehouse and he would walk around all day playing it which was pretty silly, but it raises an interesting point. Especially with Snapchat because you're taking photos of things and technically if somebody was able to access your phone they can see everything that's going on inside of the company while you're using that. So very interesting that they took a step against Snapchat. Was there anything else, I know you said retail, but anything else specifically maybe app-related that was blocked?

Participant 10: Not that I recall off the top of my head. Nothing in particular other than Snapchat. Snapchat is just one I remember.

Me: So Snapchat being blocked. What if you weren't connected to the network?

Participant 10: You would be able to use Snapchat

Me: Interesting. OK.

Participant 10: So if you were connected through data, instead of wifi, you would be able to use it.

Me: Do you know what the purpose was behind that?

Participant 10: I assume to not be taking pictures in the workplace which is company policy.

Me: So outside of just like personal use and breaks and stuff like that, were you ever required to use your phone for work?

Participant 10: No, I was not.

Me: Not for anything, like even directions somewhere or things like that?

Participant 10: Nope, nothing work related on my phone.

Me: So then another question, did you ever have any cross communication between your work email and your personal email?

Participant 10: No, not in any way, shape, or form.

Me: And you weren't allowed to use your personal email at work, right?

Participant 10: The only thing that we could send from our work email into our personal e-mail is a travel itinerary. So if we were doing travel for business and we received an itinerary about flight times and our flight tickets we can send that flight itinerary to a personal account to access it outside of work but that is the only exception.

Me: Yeah, that's what I used it for a couple of times.

Participant 10: So I would be able to if I received an email from like Southwest Airlines to my work account, I could send that email to my personal account to have my flight information for when I would be traveling.

Me: Did you travel at all?

Participant 10: Yeah, I traveled twice actually.

Me: So where were you located for your job?

Participant 10: I was located in Greater Boston and I travelled down to Hunt Valley, Maryland twice to run some tests with our partner organization Textron Unmanned Systems using some of their equipment.

Me: During those trips, you brought your laptop with you?

Participant 10: Yes, I did bring my work laptop with me.

Me: And when you were down there were you able to be connected to a network that would connect you to the people back in Boston?

Participant 10: So it's the same network because it's greater Textron.

Me: OK cool stuff. So let's talk a little bit about how some of the other people used their devices. You said that you only used it for listening to music and then maybe briefly browsing the internet over lunch or something like that. How did you see either other interns or other employees use their devices?

Participant 10: In the same manner I did.

Me: I did not know of nor see anyone using their devices in a way that would be frowned upon by the company.

Participant 10: Did some people use their phone more than others? Like were some people on it a lot or did everybody kind of stick to the same policy?

Me: I mean I guess if we're on break some people would use their phone more on breaks compared to others. A few during lunch time but outside of that... No, not during hours that would be considered I'm actively working.

Participant 10: So I know probably you specifically didn't, but do you know anybody who did break any of the rules while at work?

Me: I mean I guess it could have occurred but I have no idea. I've never seen it.

Participant 10: Ok. So I want to ask this, I know I'm going to see it in the survey as well but I want to understand a little bit more about your password usage. Do you generally use the same password for multiple different accounts or like a personal versus work account?

Me: My work password is always different than my personal passwords. If I'm required to use a password for something work-related it is unique to that job. My personal passwords for anything like Facebook, Instagram, personal e-mail... There might be. I mean I have passwords for maybe fifteen different accounts just ballparking a number and maybe three of them are the same but for the most part they're all different.

Me: How do you keep track of all that? That's a lot.

Participant 10: Memory. That honestly basically it. I've gotten good at it.

Me: That's great that you do that because most people--

Participant 10: Just to stay secure because if one password is compromised then you're compromised on multiple accounts so I try to keep my bases covered and have a different password for mostly everything.

Me: Are you selective with that? Like if you had Facebook, e-mail, bank... Are you very selective where certain passwords are more unique?

Participant 10: Sure, I will use a heavier mode of encryption on my passwords for something that I would consider myself being more secure. So I'm more worried about my bank account password being compromised than my Facebook account password so there's a higher level of encryption on my bank account password. Whether it's more symbols, capital letters, more digits in general. And most of the things you sign up for it's required anyway to have a certain level of encryption.

Me: Absolutely. So based on how you treat security on your devices before your job, then during your job definitely having that higher level of security with them banning certain sites and things like that. Have you found that your level of protection has changed at all?

Participant 10: I mean from my internship no. I think I had the same level of encryption before my internship as after my internship. Coming into college, I would say I created stronger passwords for my accounts than I had in high school originally. And that's just because of exposure to real world scenarios where accounts are being hacked which has happened more so in the last three to four years than it has before.

Me: It's definitely interesting because you took a proactive approach while some people do more of a reactive one where they go to a job and realize when they come out of it that they should change their level of protection.

Participant 10: It's all about when you realize it.

Me: This is just a side question, but do you use two factor authentication for anything?

Participant 10: I do not, no. I know some people are required now to do it at Penn State.

Me: I am aware of that. I was intrigued that some people actually opt for it in some way for e-mail or different accounts. It is definitely the highest level of protection but it's not something that I personally have thought about too much. I don't know if you have either but it's the number one way to make sure you don't get hacked becaue you are the one who is in control of everything. So this wraps up everything that I had, is there anything else unique about your experiences or anything you are interested in that you would like to share?

Participant 10: No, I don't believe so other than using two factor authentication being a good idea depending on the account. So it's something I'll consider.

Me: Absolutely. Well thank you so much for your time today Participant 10. I'll definitely keep you in the loop if you are interested in finding out the results of the study and if you have any questions feel free to reach out to me.

Participant 10: Alright, thank you very much.

Participant 11 – ID 275

Me: Again, thank you Participant 11 for being here today and taking part in this study. I definitely appreciate your time. So just to start off if you could tell me a little bit more about your internship this summer, the work you did, and what industry it was?

Participant 11: Sure. I was working for the automotive industry and basically I was just some sort of statistician this summer where my job entailed going through trends in data that the company had and trying to analyze those trends and make some sort of decision based on if we saw a trend or if some of our other software saw a trend.

Me: So what exactly the type of trends and stats and such--like crashes or?

Participant 11: So the data that we record is... let's see... It's basically how the products are performing after we sell them. And so because it's automotive these are cars right. So any time that they're brought in to get repairs done, any time that recalls were done on those cars, and any complaints from the customers to our complaint hotline.

Me: So was that type of work more secretive or is that more like the type of stuff that is announced to the public?

Participant 11: So some of the data is available to the public and some it's not.

Me: Cool. And so let's just think back to at the very beginning of everything you did. Did they have kind of a meeting where they sat you down about different security protocols you were supposed to follow with your your computer or your phones or any of that type stuff?

Participant 11: Yeah. The first day there was a portion of the introduction to working there that was about an hour section on what we could and couldn't use our phone for, the option for a company phone if we wanted one, and then following the first day because some of the data that I handed was a little more sensitive, I guess, I had meetings that whole first week on what I can and couldn't, you know, talk about even to coworkers.

Me: Interesting. So you know they taught you all that kind of stuff, did they then test you on it or did you just sign off on it? How do they make sure that you know past telling you that it was something that you were going to abide by.

Participant 11: Basically there was one or two online courses that you had to take. And so in those you would do an electronic signature saying that you understood and would abide by everything that they put in front of you.

Me: Makes sense. And you were saying that because the stuff you did it was a little bit more than what a normal employee would go through?

Participant 11: Yeah, I'm trying to think if I had extra online classes or not. Not sure if the stuff they had online was any more than a typical employee but just within my group like my boss was much more direct with me and saying you know like you can't talk about this stuff to me.

Me: So just to clarify too--engineering, right?

Participant 11: Yes.

Me: What type of engineering?

Participant 11: I'm studying mechanical engineering.

Me: OK I just wanted to make sure to clarify for the type of work you're doing with stats and understanding how the car works. Cool. So then past that, how did you use your smartphone at work? Was it just kind of for like I know you said there's some things you couldn't couldn't do certain like well

Participant 11: So I chose not to get a company phone but I also did not put any of my company email on my phone. Basically all I used my phone for was a phone number for other people in the company to get contact with me. Like my profile or whatever within the company had that phone number to be used on it but work related just my phone number was the only thing that was used.

Me: Just out of curiosity, would you ever send an email from your company email to a personal email or have any kind of traffic like that?

Participant 11: Yeah there was from company to person.

Me: Like what type of stuff?

Participant 11: Never ever work related things but let's see what was one example... I think I bought tickets on StubHub. Sent them from work to my personal.

Me: Was that while at work?

Participant 11: Yes.

Me: While you were working was your phone connected to my wifi?

Participant 11: Yeah, yeah. I had my phone connected to whatever wireless network in the building.

Me: So I'm figuring that maybe over lunch and stuff like that you used your phone for other things besides just having it there. What types of stuff would you check, like the typical, Facebook?

Participant 11: Check my email, check Facebook, look at Snapchat, the usual things.

Me: That wifi you connected to--was there any username and password, was there any extra things you had to use to connect to it?

Participant 11: No, I think it was a company campus guest wifi that I was on.

Me: OK make sense. Now how did do you find other people used their devices? Did a lot of people opt for that work phone?

Participant 11: Let's see... probably twenty people I knew about their decision between choosing a work phone and not choosing were phone. I think maybe four of them out of twenty got work phones and then of that same twenty I would say probably another eight downloaded skype onto their phone and so the Skype was to use Skype instant messaging. So they could do the instant messaging on their phone but I do know that they had to sign another form in order for them to do that.

Me: And then how many of them used the company email on their phone?

Participant 11: Probably half. But these are interns.

Me: Yeah. So did you find that the more established employees or maybe the older crowd opted for the work phone more often?

Participant 11: That's a good question. I could definitely tell you that the group that I worked with was actually pretty young so I wouldn't be able to tell you about the older crowd. When you say older crowd, what exactly do you mean?

Me: Well I mean I'm thinking if you break it up, younger would be up to thirty and then older would be thirty or forty and then you know past that. Because I feel like it's more of an established type of thing to get a work phone.

Participant 11: Yeah and I would say that the majority of employees that work there had work phones. It was more of like an intern thing about "Well do I really need to get a work phone for 3 months?"

Me: Absolutely. So within those protocols that they kind of talked to you about, were there rules against accessing some of your social networks or any of that type of stuff?

Participant 11: I can't remember any restrictions that they put on us for accessing our phones or laptops. They didn't outline any specific sites or anything.

Me: Did you find that people would visit that type of stuff off of their work computers? Personally I kind of feel like accessing Facebook or any kind of personal stuff while you're at work is not what you should be doing at work. Did a lot of people just kind of act carefree or?

Participant 11: Yeah I would say it was kind of carefree. I think kind of informally it was like, "Yeah if you need to go on Facebook at lunch, go ahead. But you know, not while you're working."

Me: So within those rules or restrictions do you know anybody or hear of anything about somebody getting in trouble or any type of security breaches that may have occurred in the past?

Participant 11: Not while I was there. I don't think anybody had any issues with their phone, company phone, or anything like that.

Me: Do you know how well established their protocols are? Like if it's something that was new?

Participant 11: They didn't mention anything about being new. I couldn't tell you.

Me: You know with everything constantly changing in technology and--

Participant 11: Yeah, sometimes they'll say, you know, we have a new system out but I didn't see anything about it. So I don't know.

Me: So with your devices, do you use a passcode?

Participant 11: Yes, I use a four digit pass code and the fingerprint scanner.

Me: So before you started work, you've always had that?

Participant 11: Yeah that's what I've used.

Me: So then what you had back then versus what you had at work and then afterwards, did you make any changes in the kind of security that you have either password-related on devices or?

Participant 11: I'd say that since my internship the passwords I use for e-mail and unlocking my laptop--not so much on my phone--I feel like e-mail and accounts and stuff and unlocking my laptop, I'd say those passwords are stronger.

Me: Do you change them more frequently?

Participant 11: Yes.

Me: Is that because of what you went through?

Participant 11: Yeah. I'd say I'm just more aware of what kind of stuff could happen. So I think that now I'm just more strict for my personal stuff.

Me: Awesome. Well thanks Participant 11. I really appreciate your time here. Is there anything else, any questions you have about the things we discussed?

Participant 11: I'm curious to see what you find!

Me: Do you think that there is any difference across industry?

Participant 11: That is a great question.

Me: That's what I'm looking to find but I'm just curious what your thoughts are.

Participant 11: So I've worked in the automotive industry and I've worked in a research setting and I would say that in both cases they were fairly strict but outside of that, I'd be curious to see if there is a difference.

Me: As am I. Well again, thank you Participant 11. I appreciate your time.

Participant 12 – ID 476

Me: Alright well thank you Participant 12 for being here today. I really appreciate your time. We're going to get started here after the survey. So first question, could you tell me a little bit more information about your internship this summer? What industry it was, the type of work you didm different projects you may have worked on?

Participant 12: So this past summer and even right now I worked for [redacted] so I was working in the tech industry. My role was specifically business operations intern. And so kind of the role of that is to know each part of the business, so a bit of the business side, tech, H.R. So when we first began they eased us into some easy H.R. stuff like recruiting, setting up interviews, helping people book conference rooms, the client, all that stuff. Then they moved us on to the more business oriented work and so one cool thing that [redacted] did over the summer was they began rolling out these remotely driven shuttles. So they did a test in the beginning of summer before we started and so they got a lot of feedback back and so our role was to kind of input that data into a database and then also into excel and make spreadsheets from that so they can kind of see like what kind of feedback they got from like what demographic and kind of organize it that way. So after we worked on that, they had us do more technical related stuff because I mean I'm a cyber security major and the other guy I worked with was industrial engineering. And so they had us make a community website that the employees used to just kind of have a resource database for them to use for projects and also like connect if they ever needed help from a software engineer from, say, the West Coast because a lot of people work remotely and people that work together aren't necessarily the same office. So me and the other intern we're responsible for doing the front end of that website. So mostly the appearance of making it look sleek and user friendly. Whereas we don't really do the backend which is more actual functionality of the website. So we did that for a while and then after that project ended, they extended us till January seventh to work remotely. And all that work previously was in Kansas City. We moved there for a little bit and then we start working remotely. It's been kind of slow recently and they've had us doing more research specifically on ways they can improve their onboarding process and recruiting. Coming up next week they're going to give us our next big project that will take us till the end of our internship. They said it's going to be revolved around one of their statistical softwares that they use, V.M.S., T.S.S. They're making modifications to make it more accurate and they also want to get feedback from some of the new concepts in using it such as [redacted] was one of them and a couple other banks are starting to use it a lot more often. And so that will probably take us to the end of the internship in general.

Me: Well that sounds like a lot of different stuff.

Participant 12: Yeah.

Me: So you said automated shuttles. So what exactly is that, like a box that drives itself?

Participant 12: So yeah they have this thing called Ali. They teamed up with [redacted] and they basically have like a Siri sort of thing running the shuttle. And they can seat up to six to ten people and it's used more for like a conference style rather than actual transportation because it goes really slow. So the purpose of it is going to be primarily for to use it so they can have conferences in there and they might pick people up and take them to where they're going and that whole time they can be like talking about work and whatnot rather than, you know, just an individual traveling. So basically it works just like Siri. It will pick you up and you can be like "take me to the nearest Chinese restaurant" or you'll give the address and it has like a radius that it can travel to and it only goes I think top speed about fifteen miles per hour. And so they ran the test in D.C. and later this year they're running a test in I believe Vegas and a couple in Miami and couple of the big cities. And so they had people test it out, comment on what they liked, what they didn't like. One of the big questions was whether they would use this type of technology if it was commercially sold in like individual vehicles. The one thing that we found from our research was that people were more inclined to use this kind of transportation as a public service rather than buying a remotely driven car. That was one big thing because it is kind of I guess sketchy in a way for an individual in a car that has no driver in it but if it's like a public transportation, I think people are a lot more comfortable with that. So that was one thing that we found through reading all the feedback.

Me: Yeah absolutely I think it's something that's going to take a little bit before people are more comfortable with it.

Participant 12: Especially for security reasons it's a lot riskier when it's just you in a car by yourself.

Me: I mean also though, if somebody were to hack public transportation that's a lot of people than can get hurt at once.

Participant 12: That's very true. And on the flip side of that you have a lot more people working on the security if it's public transportation. Whereas I think it would be a little easier to breach an individual's vehicle but this technology is all still in the early stages but they're refining it and working on it to hopefully make it more commercially used in the next like five years.

Me: So you said it only goes fifteen miles an hour. Does it drive on the road?

Participant 12: Yeah it has coordinated routes. Kind of like the White Loop, it has the same route that it goes on. That's how it works. It has a certain route so you can wait near one of the stops for it. It'll pick you up. What they're doing right now if you have to reserve it. But when it becomes more of a public transportation service they're going to make it so it has pick up

points and whatnot that you can get in it. But right now it's more privately used because you have to book it so a lot of companies are using it and testing it out for their purposes.

Me: I'm sure that might be causing a little bit of issues in the roads because it moves so slow, especially in D.C. since it's so congested

Participant 12: Yeah that's why they're testing it out right now in old big cities obviously because that's where it's really going to be used because traffic there is ridiculous.

Me: OK. So then if you think back to very beginning of your internship, how did they walk you through security protocols? Did you have a presentation given to you? Did you have to take online assignments? Did you have to sign some things?

Participant 12: So within our first like two weeks of being there we had to take a mandatory cyber security course where it walked us through the security aspects of every device, like your cell phone, work computers, anything issued to you by your company. E-mails, like what to look out for, that kind of stuff. So yeah me and the other intern and all the other employees were required to do that as a part of the onboarding process.

Me: That sounds like it's... well I guess not necessarily intense, but comprehensive.

Participant 12: Yeah it wasn't like too challenging but you learn a good amount. The way they set up was online so you get watch a video first and then it asks you questions about the video afterwards. They were really basic questions but you have to watch the video so you at least hear what they have to say.

Me: So everybody did this individually?

Participant 12: Yes everyone had to do that in their first two weeks and if it was getting towards the two weeks the manager would start getting notifications about it. They were pretty on top of us about getting that done.

Me: So they definitely assessed you, but they didn't have to make sure you actually watched the videos as I know some of the stuff is just basic questions at the end.

Participant 12: Well also, when we first got hired they issued us laptops and we had to download a bunch of applications both for work and also security purposes and after we had our manager check that we had downloaded all those things. A lot of them were dealing with security and keeping our computers more private, I guess. And so from that aspect yeah, they checked on us.

Me: That's definitely really good to have all this stuff.

Participant 12: Yeah and then after you watched the videos they gave you all these certifications to let your manager know you completed the courses.

Me: So then what about your smartphone or bringing your own device to work? Is that something you were allowed to do?

Participant 12: Yeah we were allowed to do that. We mainly used our work computers because to use a lot of I.B.M.s applications and products you have to be signed onto an I.B.M. server. So now even when I work remotely I have to connect via V.P.N. to the I.B.M. server which could be anywhere--they have servers in China and all across the world--and so we have to sign onto that in order to use the Internet and office and also to like get our work done. So from that standpoint that's the security they had for their devices. In terms of me bring in my smartphone, I could go on the Internet or whatnot and I could sign onto I.B.M.s wifi and it would be just fine.

Me: Was that a guest wifi or your employee information?

Participant 12: I had to sign in with my employee information. They gave everyone their own own unique code and password.

Me: Did you have access to your work email off of your phone or anything like that?

Participant 12: I believe there is a way you could download stuff your phone but I didn't have it on my phone. I just did everything through my computer but I'm pretty sure there's a way that I can get that email on my phone.

Me: Do you know if anybody did or do they give company phones for that?

Participant 12: They probably issue company phones for that but for interns the most you can do is... actually have you heard of Slack?

Me: Yeah, I actually just used it recently.

Participant 12: Right it's being used a lot more for team projects. Everyone was encouraged to download just for communicating instantly. But for the emails I didn't know if anyone had it on their phones.

Me: So what type of stuff would you do on your phone at work?

Participant 12: I never really used my phone at work other than if I got a call from home or I was like texting somebody but yeah I never really used any apps at work or ever surfed the web on my phone either. And usually if I did, I wouldn't sign onto I.B.M.s wifi I would just use my data because I have a lot of data space. So I never connect my phone really to their wifi or any of their servers. But yeah I usually just use my work computer for everything.

Me: Did you notice anybody using their phones for things or use it frequently?

Participant 12: Not really. There were some people who had H.R. roles, so if they were on the phone it was work related. It was kind of an old school kind of office with cubicles so everyone was kind of glued to their computers.

Me: Yeah absolutely. This is actually an interesting thought I just had. With all of those work phone calls from a personal device, if that device was hacked somebody could get your call logs and any voicemails you may have that would be more secure on a work phone. Did you ever have any communication between your work e-mail to a personal e-mail?

Participant 12: No. My work email and personal email is completely separate and private. That's why when I'm thinking about it I'm actually not sure if you can get the I.B.M. email onto your phone because it's not synced with Gmail or Yahoo or any other e-mail accounts, it's like its own separate entity.

Me: Is it done out of Outlook?

Participant 12: It's not, it's called [redacted].

Me: Yeah, so it's definitely separate. That's actually very interesting. Because typically companies just go Outlook because it's very easy to do but that adds another level of security.

Participant 12: My internship before I worked at I.B.M. it was all through Outlook and Microsoft products. So yeah, something new.

Me: So then a final question here about your own security practices. Were there any differences in how you treated your passwords before your internship, during, and afterward the summer experience?

Participant 12: I think after my internship, in terms of changing my actual passwords and the frequency of that didn't change. But I guess from after my internship, the complexity of the security in my passwords changed. Not just making it something short I can remember but making it a lot longer, adding characters and whatnot. That's something I started doing more because a lot of the devices they gave us had these long passwords for security purposes. And so you kind of learned. So I started making passwords on my own stuff like my Facebook, e-mail, and personal stuff a lot more complex but I still change the password same amount of times, usually every month or two months.

Me: I mean that's pretty good. It sounds like you definitely have a handle on your own security. OK, well thank you very much Participant 12. If you have any questions, you can feel free to let me know and if you're interested I can share the thesis with you with you once all the research is completed.

Participant 12: Yeah definitely, I'd actually be really interested. It's right up my alley.

Participant 13 – ID 320

Me: Thank you Participant 13 for being here today and taking part in this interview and this study. So we'll start off now if you could tell me a little bit more about your internship over the summer. Whatever work you did, projects you worked on, things like that.

Participant 13: Sure. I worked as a manufacturing engineering intern at [redacted]. I worked in one of their manufacturing plants where they made a bunch of different snack foods and a bunch of other things. I worked with [redacted] specifically. They were implementing a new management system and I worked directly with a lot of the operators who work the equipment explaining the new system and convincing them it was a good idea and creating documents that were part of the system that they would have to use. So working with them and engineers to create new online documents that people would have to use.

Me: And what did you say your major was again?

Participant 13: Chemical Engineering.

Me: OK. So was that chemical engineering work?

Participant 13: No this was industrial engineer work.

Me: OK Interesting. So then thinking back to the very beginning of your internship. Did they walk you through the type of security protocols, either give you a presentation about things or maybe take online assignments or anything like that?

Participant 13: I had a series of online assignments and one was specifically about security things and others had little bits of security things in them.

Me: What were some of the rules that they had for personal devices?

Participant 13: Like never leave sensitive documents unintended at your desk. Don't leave things in the printer. So like if you print something out go pick it up. Don't leave it over there. Especially if it's something sensitive and be aware of things that seem shady, like e-mails that are probably not from who they say they are. These "corporate espionage" things I think was the term they used.

Me: Interesting. Was this because something had happened in the past?

Participant 13: Nothing they had said or that anybody talked about.

Me: That's interesting. So what was the whole idea behind not leaving something in the printer? I mean you all work for the same company right?

Participant 13: Well the facility I was in had like swipe access. You couldn't get in to the building without you having a reason to be there so I guess the idea behind that one was even within

the same company, not every bit of information is for everyone. So if you lose something in the printer and it's not for a certain level of employee presumably below you to see. Presumably there's no one lower than the interns for me, but that was the idea.

Me: Was the type of work you were doing more than just a base level? Was it more of a higher security level?

Participant 13: Probably. I worked with several sensitive documents that certainly shouldn't be for anyone outside the company and there were people inside the company that they wouldn't want to see it too. But the majority of my stuff would have just been OK for every anybody inside the company.

Me: Interesting. So they gave you a laptop, and I presume you obviously probably brought your smartphone to work, right?

Participant 13: Yes.

Me: Did you use your phone at work at all?

Participant 13: Yeah. More than I expected to, yeah. That was how people in the plant communicated. You used your own personal device to call other people because the plant was huge couldn't find people most of the time and nobody was ever in the office. So you'd use cell phones most of the time.

Me: OK, so did they did they provide work phones to people or did basically everyone use their personal?

Participant 13: I believe that there was a time when they provided people with work phones but I think right before I got there they stopped doing it. So only very high up people had work phones.

Me: So did you have access to your work e-mail on your phone at all?

Participant 13: Yes I routed my work email through my phone.

Me: Was that something they asked you to do or something that they knew about or said anything about?

Participant 13: They didn't ask me to do it but they did provide instructions on how to do it.

Me: OK and then did they have anything on top of that for protection to make sure that your phone was password protected?

Participant 13: No.

Me: So theoretically somebody could not have a password on their phone and someone else could, if they lost their phone, go on and see all of their work emails?

Participant 13: Correct.

Me: That's dangerous territory thinking about that and it's funny, almost, that they are so on top of not leaving something in printers and other protocols yet that's something they didn't even address.

Participant 13: Yeah.

Me: So was there other stuff that you would do on your phone at work? Like did you connect to company wifi?

Participant 13: No.

Me: What about during off times, would you surf the web or do things like that?

Participant 13: Occasionally, yeah.

Me: Like the basic things, maybe Facebook and stuff like that?

Participant 13: Honestly not frequently with this job. While I was there I was basically busy most of the time. I mostly used my phone for listening to podcasts.

Me: Makes sense. So I think you already answered this but other people within the company kind of used their phones for the same things. Was there anyone that had to use it more for work or was it relatively the same calling each other and things like that?

Participant 13: I think everybody was just calling each other and keeping their planner on there and everybody ran an Outlook schedule that was public to everyone. They just routed that to their phones. Everyone just did their work on their work computers.

Me: But everyone, or almost everyone, put their work email and Outlook calendars on their phones?

Participant 13: I actually have no idea. The interns definitely did.

Me: I know at my job, most of us did as well. It makes knowing your schedule really quick and easy. And they never told us anything preventative about it, just that we should take it off because as an intern you shouldn't be thinking about work while not at the office. Ok, so I guess I'll ask a little bit about your password usage. So how frequently did you have to change your password on your work computer?

Participant 13: I think it was roughly every two months.

Me: OK, when you chose a password for that, was it similar to past passwords?

Participant 13: It was completely unique.

Me: That's good. Did you find yourself making any changes in your behavior from right before your internship and then maybe during and after in terms of thinking about personal security?

Participant 13: Honestly, a little bit when I got my work computer. I don't know why I decided this but I decided I shouldn't keep any of the passwords the same as my own passwords. Mostly because I was concerned that maybe they could see the password and I didn't want them having my personal passwords. I've known for a long time that I should diversify my passwords, that they shouldn't be the same, and they really mostly were the same. So after I got in the habit of changing that work password I have started diversifying my own passwords.

Me: That's good. I know definitely down the line hacks may occur a lot more frequent. So overall, is this something you've ever really thought about?

Participant 13: Password protection?

Me: Password protection and just how accessible it may be for people to get to your data.

Participant 13: I never thought about password protection or whatever until--Do you remember that thing that happened like a year ago when all those like celebrities' nude photos got leaked?

Me: Yeah.

Participant 13: And then when they sourced it they found out it was the celebrity's e-mail, and then they brute forced Find My iPhone, and then just like daisy chain passwords from there. That concept led me to think if Find My iPhone lets you do unlimited things, I need to be better about security. I never thought of it before then but since then it is an actual concern of mine.

Me: Yeah absolutely. The whole thing was pretty crazy because they really did gain access to a ton of people and then just like boom. I don't know where that came out it was pretty wild. Well thank you Participant 13 for your time today. If you have any more questions you can feel free to reach out to me and if you want I can go ahead and share the results of everything in the end.

Participant 13: Awesome.

Participant 14 – ID 198

Me: All right thank you Participant 14 for being here today. I really appreciate your time. To begin, if you could tell me a little bit more about your internship this past summer? You know, what an industry it was, the type of work you did, any projects you may have worked on.

Participant 14: So the company, it's a software company in northeast Ohio, about three hundred employees, it's called [redacted] and they deal with software that helps car dealerships move their idle parts inventory because a lot of the dealerships will keep an onsite repair shop or something like that. So they keep a lot of the parts but then they'll have parts inventory just taking up space and it's tough to move them around. If they have them, tough to find, and if they need them. So we kind of established that network and basically I was just selling subscriptions to the different software programs that we offer.

Me: OK, is that related to your major?

Participant 14: My major is economics so it wasn't really related, it was more of a sales internship. But you know same lines.

Me: What was the size of the company?

Participant 14: It was relatively small, there's about three hundred employees. So there's a main site in Richfield, Ohio and there's two hundred there and they have about one hundred down in Columbus, so they deal mostly with Cleveland.

Me: So first question, did they provide you with a laptop or anything like that?

Participant 14: Yeah I had a desk, I didn't have like a laptop to take home or anything but we had a great computer, dual monitor set up and everything. I had my own phone, not a smartphone or anything just a landline.

Me: So thinking back to the very beginning of that internship, did they walk you through their security protocols for their devices or make you sign anything or take any on the courses?

Participant 14: There was a real general computer usage guideline and just kind of like the general do's and don'ts. What you can do on the Internet, that kind of thing. But as far as like security, the only measures that I can recall was we had to change our password for our billing to get that every other week and we had to change that every month. So pretty much password usage, that's about it.

Me: So smartphone usage. Were you about to bring your phone and kind of do whatever?

Participant 14: We were able to have our phones but in my role I was on the phone a lot so I would have my cell phone out quite a bit but there weren't any explicit rules about cell phone usage or anything like that.

Me: Did you have a work email?

Participant 14: Yeah.

Me: Were you about to put your work e-mail on your phone?

Participant 14: Yeah I did do that. I just routed my work e-mail through my personal e-mail so I just connected the two accounts.

Me: So if you would sign into your personal email you were able to see your work email as well?

Participant 14: Yeah different tabs but yeah so basically the emails would go to my work inbox and it would also go to my personal inbox because I checked that more frequently.

Me: So they were fine with that?

Participant 14: Yeah they didn't have any rules about that they just preferred if I was sending an outgoing message I would use the company email but you know I could read them on my personal email.

Me: That's interesting because if something happens with your personal, somebody can hack your phone and it's all out in the open.

Participant 14: That's true then yeah they would be exposed to that.

Me: When you were using your phone at work, did you connect to wifi?

Participant 14: Yeah they had wifi.

Me: Was the wifi general wifi or did you have to login in with your own credentials?

Participant 14: It was password protected. I don't remember if it was our own credentials or if it was one password everyone used but it was definitely password protected.

Me: So when you were on your phone at work, was it just general stuff?

Participant 14: Yeah just general stuff. You know, mess around on Twitter, honestly, Facebook, that kind of thing. I never really used my cell phone for business. Even though I had the email on it it was just to get the notification in my pocket.

Me: Yeah I know with my internship we did the same. They didn't want us to because as an intern, when you go home, go home. Don't think about work. But it was nice because there were times when 9 AM meetings were moved to 8 AM and I wouldn't know unless I had the email on my phone. So how did other employees use their devices at work? Like their smartphones? Like did a lot of people had their work email on their phone?

Participant 14: Yeah I would say to my knowledge people had the e-mail connected to their personal e-mail. I really don't think we did a whole lot mobily. We did use the whole Microsoft C.R.M. which I'm sure you've heard of. So that was what our system was and everything basically ran through that and I never really saw people using their phone for that.

Me: So about passwords, I know you did have to change your password. Did you choose passwords that were similar to other ones that you have?

Participant 14: Yeah I think I probably have six or seven passwords that I just kind of cycle through my different accounts and really the two--This is kind of off topic but the two accounts like my e-mail and my bank, those are the two that I really focus on changing and try to change those once every six months.

Me: That's pretty good.

Participant 14: That's a little off topic but--

Me: No, it's definitely important. I'm seeing a trend in a lot of people that those two are the most important and most unique. I guess email isn't the worst to get hacked, but at the same time both of those things are pretty sensitive.

Participant 14: And like you were saying, you're getting all that information on your phone like people sign up for email subscriptions for everything so there's a lot information you can be exposed to if you lost your email.

Me: So the last question here. It didn't seem like there was a ton of security measures in place. Did you find that before your job and during the internship and then after, were there any changes in the way you handle your security? Whether it be lockscreens, passwords, things of that nature?

Participant 14: I wouldn't say my internship sparked me to do that. I didn't ever feel like there was a lack of security because I never thought about it that way, so I didn't leave feeling insecure. Now that we're having this conversation it's kind of sparking me that maybe I should change a couple of those passwords but the internship definitely didn't spark that.

Me: I'm definitely seeing across different industries that a tech industry is really on top of everything and other industries that are exactly centered around that it's really really lax. It's one thing that they hack and they find out about work information but it could be so much more than that because once you're in, you're in.

Participant 14: And yeah I mean businesses keep so much information on their employees, like bank, bank account numbers, and all that stuff.

Me: Yeah because if you can find a way in through someone else's device into the actual company then you could get that bank account information because it's all there... for everybody.

Participant 14: It's somewhere. You can find it somewhere. Exactly.

Me: I actually never thought about that. If you can get into a company, all the information they have, you can just go straight to---

Participant 14: Straight for the cash. Right? I mean if I'm a hacker, yeah.

Me: That's pretty interesting.

Participant 14: But yeah, I don't know. I feel like in every professional setting I've been in, I feel like that whole section of the security, you kind of go through the motion check the box. You go through the protocol and then you don't really revisit it. It's what it kind of seems like. I think you know maybe if it was something that was monitored regularly and revisited every once and a while it would be a little more secure.

Me: That definitely happens. And I think that that might be changing a little bit as time goes on because you really need to have a firm hand on it.

Participant 14: Well this is definitely something interesting to look at it so it'll be cool to see where this goes.

Me: For sure. Do you have any other questions or anything else you'd like to share?

Participant 14: Nah, that's about it. Hopefully this helped.

Me: Well, thank you so much for your time. If you have any other questions you can feel free to reach out to me and if you want I will be sure to share the thesis with you once everythings completed.

Participant 15 – ID 220

Me: Thank you Participant 15 for being here today and taking part in this study. So if you could tell me a little bit about your internship this past summer? You know, what type of work you did, the projects you may have worked on.

Participant 15: Sure thing. So I worked at [redacted] which was previously known as the [redacted] as a summer business development associate working in the mid-market space helping heads of the marketing function transform their department, increase efficiencies, and gain access to [redacted] marketing leadership council for mid-sized companies. You want hear more about my day to day responsibilities?

Me: Yeah for sure.

Participant 15: So my job was to basically cold call and email heads of marking functions in midsize firms typically firms that produce around a billion dollars in revenue or less and try and get them to take a meeting with [redacted] to learn more about [redacted] marketing leadership council and our services. So that was my typical day to day stuff. I also had intern events where we would hear from executives of the company as well as an ongoing project where I researched and investigated the macro economic trends in our top five contributing industries for marketing sales which was computer software, health care, financial services, industrial manufacturing and one more industry I can't remember off the top of my head. Does that answer your question?

Me: Absolutely. So obviously when you're working with a lot of clients the data that you guys have is confidential and pertinent to them as well.

Participant 15: Yes.

Me: So let's go back to the beginning of your internship. What types of security protocols did they go over with you? Was there a presentation or online assessments or did you have to sign anything.

Participant 15: I definitely had to sign something. I definitely had a training about security protocol. Then I was given an eighty page packet about security of the firm and then I had to sign something about insider trading information. So yeah there's a lot of stuff about it.

Me: And so with this job did they give you a work computer?

Participant 15: Yes I had a work computer.

Me: Did they have anything about bringing a personal device like your smartphone to work?

Participant 15: Yes. So if we wanted to be on the corporate wifi or have email on my phone, we had to go to our I.T. desk and they would install this software called "Mobile Iron" or something

like that which is essentially encryptes your phone and emails and securely connects you to the wifi through VPN.

Me: How much do you know about that? Was that software capable of remote wiping your phone or anything like that?

Participant 15: I'm pretty sure they could remotely wipe my phone, yes.

Me: So with that software on it, did they also make sure you had a specific passcode on your phone? Let's say if your phone was unlocked all the time, could someone pick up your phone and access your email?

Participant 15: So the app made you set a passcode and you had to change it every sixty days. And then on top of that, to connect through this application for the first time to the wifi you had to download another app which every sixty seconds creates a six digit code and is only active for that sixty seconds. So when connecting to the wifi you need to go into that app, get the code that's currently active, then put it in and then you'll get access to the system.

Me: What about accessing your email?

Participant 15: Once that initial app, "Mobile Iron" was on my phone, I was fine to access my email whenever. But let's say I wanted to connect to the company wifi, I would have to enter that six digit code that changed every sixty seconds and the code is only valid for sixty seconds. But if you put it in within that sixty seconds then you're connected and your fine.

Me: So theoretically, this is what I'm getting at here, let's say you don't have to passcode for your phone. You just click the home button or whatever and it opens. Your out, away from work, and you lose your phone. Somebody would be able to pick it up and access your work e-mail from there?

Participant 15: Hypothetically speaking, yes, but the app makes you put a password on your phone. It's a requirement of the application. So technically my phone would be locked even if I didn't want it to be.

Me: OK that's good. I just wanted to make sure because some of the people I've talked to can put their e-mail on their phone and that's it. And so that's really good that they do those extra steps because I know when you have all those different clients with a ton of confidential information that would be very detrimental to get out.

Participant 15: Yeah I mean they work with like ninety percent of Fortune five hundred companies so they take security very seriously.

Me: So did everybody have that on their phone?

Participant 15: I'd say it was fifty fifty. Some had the application some did not.

Me: And when you say fifty fifty, was there a clear split? All the interns did it, half the interns did it, all the company half and half?

Participant 15: I mean I don't have like specific figures to give you. I would say it was pretty random. It was honestly like fifty fifty where some people would have it, some wouldn't. A lot of people didn't want to have work email on their phone so their personal lives aren't intertwined. Also you could get a work email at any point in the day or night. And then some people like to because if they are going to the bathroom and they just realize their meeting place change you can go there instead.

Me: Yeah absolutely. I definitely see the pros and cons of that. So with your smartphone, how did you use it at work?

Participant 15: In what regard, are you saying personal for personal reasons?

Me: Yeah maybe some personal stuff you would do or how frequently did you really use it for your work e-mail or did you typically send those off your laptop?

Participant 15: If I was going to send an email to someone in the firm, if I was on the move I would use my phone, especially if it was another intern it wasn't a big deal. If it was to a client, I would a hundred percent use a laptop. And then in terms of other things, I would use my phone to text my friends and check my Facebook but I would use my phone for reminders. I'd have Microsoft Outlook synced to my calendar, so if I had a meeting I would get a fifteen minute notification for it and I could go toit. I also used my phone just to check e-mail if I was not right in front of my computer. But besides that, going on Instagram and personal stuff in my off time.

Me: OK Interesting. Were there any limitations of what you were allowed to do on your phone at work?

Participant 15: Not that I recall.

Me: It was actually interesting one of the interviews talked about how they blocked Snapchat.

Participant 15: Yeah no that makes sense. One of my friends worked at an investment bank and he said they weren't allowed to have their phones out in certain rooms.

Me: Interesting. Cool. So how frequently did you have to change your password for your laptop?

Participant 15: They forced us to change it every sixty days. So throughout the internship I changed it once, essentially.

Me: OK so when you selected that initial password was it a password you had used before was this completely unique for work?

Participant 15: Completely different for work. And there were some specifications. I think it was one symbol, one upper case, like a few numbers. Try and do at least ten characters.

Me: And so thinking about that, have you seen any changes in your behavior there?

Participant 15: I've always used different passwords for all my different accounts and then I change them like once a year. So I'm pretty good about cyber security in that regard because you know if you keep everything the same, one person gets access to one password they get access to everything. So I guess my behavior just was reinforced seeing that a company that makes a billion dollars a year and works with ninety percent of the Fortune 500 is taking that many measures as I do with my information.

Me: Was there an event that occurred that sparked that behavior?

Participant 15: No, I've always been pretty secure about that. My family's always had an alarm system, always made sure we locked our doors and windows, and made sure our windows had sensors on them. So there's always been a level of security there,

Me: So do you have any other thoughts on this whole thing about security practices? What was really your opinion of the company? Did you think everything was as secure as it needed to be?

Participant 15: I mean everything was secure enough. I realistically couldn't see someone just waltz into the building get access to a company computer and take important and pertinent files especially since we are a research and advisory firm so we definitely knew things that could potentially ruin a company. Maybe not ruin a company, but maybe information that's their intellectual property. So I think they did a pretty good job in terms of security. That being said, I know friends of mine whose companies were pretty lax with their security measures. I know that many of them didn't have presentations they just got paperwork. But a lot of kids had told me that if you get a 100 sheet package on your desk you're not going to read the entire thing, they'll just sift through it or ask the person next to you.

Me: Absolutely. So overall how secure do you think companies should be? Do you think a company that lets you just put outlook on and doesn't make you install that security that you had. Do you think that's enough?

Participant 15: I think it ultimately depends on what kind of client information you are using. So for example, if I gave someone my credit card information I want that to be as secure as possible but at the same time I can see a different need of security if let's say holding my singular credit card info versus holding a corporations secret files, there should be no chances taken, let's say, for a Pepsi Co or a Fortune 50 company. They should be taking every measure possible to make sure everything is secure. Change your passwords frequently, probably not allowing phones out if it's an information sensitive area. But if it's a small mom and pop shop the need to be as secure isn't there. And you also wouldn't have the resources to do that.

Me: One thing I forgot to ask, did they provide work phones?

Participant 15: They did not provide work phones. I think they used to but since the introduction of that app, I think it was "RSA Secure ID" and "Mobile Iron" are the two they switched over to just using applications. And one of my friends who worked at Jeffries investment bank said the same thing. They used to give out Blackberries and now they use that application.

Me: Do you know when that shift occurred?

Participant 15: Before my time and I really do not have an exact date.

Me: Well I think I got some good information. It's definitely pretty interesting that they use that application. So if you have any follow up questions you can feel free to reach out to me. Thank you for being here today Participant 15.

BIBLIOGRAPHY

1. Cameron Camp. 2012. The BYOD security challenge: How scary is the iPad, tablet, smartphone surge? *welivesecurity*. Retrieved from http://www.consumerreports.org/media-room/press-releases/2014/04/my-entry-1/
2. Nathan Eddy. 2013. Samsung Knox Mobile Security Platform Flaw Discovered. *eWeek*. Retrieved from http://www.eweek.com/mobile/samsung-knox-mobile-security-platform-flaw-discovered.html
3. Adrienne Porter Felt, Matthew Finifter, Erika Chin, Steve Hanna, and David Wagner. 2011. A survey of mobile malware in the wild. *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices - SPSM '11*: 3–14. http://doi.org/10.1145/2046614.2046618
4. Jim Finkle. 2016. US cyber official warns of more attacks on industrial control systems. *Business Insider*. Retrieved from http://www.businessinsider.com/r-us-official-sees-more-cyber-attacks-on-industrial-control-systems-2016-1
5. Shirley Gaw and Edward W Felten. 2006. Password management strategies for online accounts. *Proceedings of the second symposium on Usable privacy and security - SOUPS '06*: 44. http://doi.org/10.1145/1143120.1143127
6. Beth H Jones, Amita Goyal Chin, and Peter Aiken. 2014. Risky Business: Students and Smartphones. *TechTrends: Linking Research and Practice to Improve Learning* 58, December: 73–83. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=eric&AN=EJ1042919&site=ehost-live\nhttp://dx.doi.org/10.1007/s11528-014-0806-x
7. Gary Legg. 2005. The bluejacking, bluesnarfing, bluebugging blues: Bluetooth faces perception of vulnerability. *TechOnline http://www. wirelessnetdesignline. com/showArticle. jhtml*.
8. Dave Lewis. 2014. iCloud Data Breach: Hacking And Celebrity Photos - Forbes. *Forbes*, 5–10. Retrieved from http://www.forbes.com/sites/davelewis/2014/09/02/icloud-data-breach-hacking-and-nude-celebrity-photos/
9. Keith W. Miller, Jeffrey M. Voas, and George F. Hurlburt. 2012. BYOD: Security and Privacy Considerations. *It Professional* 14, 5: 53–55.
10. Gregory L Orgill, Gordon W Romney, Michael G Bailey, and Paul M Orgill. 2004. The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. In *Proceedings of the 5th conference on Information technology education*, 177–181.
11. Bob Sullivan. 2013. Smartphone hacking comes of age, hitting US victims. *NBC News*. Retrieved from http://www.nbcnews.com/business/consumer/smartphone-hacking-comes-age-hitting-us-victims-f1C8989252
12. The Federal Bureau of Investigation. 2016. Incidents of Ransomware on the Rise. *FBI.gov*. Retrieved from https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise
13. Gordon Thomson. 2012. BYOD: Enabling the chaos. *Network Security* 2012, 2: 5–8. http://doi.org/10.1016/S1353-4858(12)70013-2
14. Jeff Wilson. 2012. Enterprises rate mobile device security vendors, reveal BYOD

concerns. *Infonetics*. Retrieved from www.infonetics.com/pr/2012/Enterprise-Mobile-Security-Strategies-Survey-Highlights.asp

15. 2013. *2013 Norton Report*. Symantec.
16. 2014. 3.1 Million Smart Phones Were Stolen In 2013, Nearly Double the Year Before. *Consumer Reports*. Retrieved from http://www.consumerreports.org/media-room/press-releases/2014/04/my-entry-1/

Academic Vita of Alexander Hudock

alexhudock93@gmail.com

Education:
The Pennsylvania State University
Schreyer Honors College

Major: B.S. Finance
Minor: Supply Chain and Information Sciences and Technology
Certificate: Enterprise Resource Planning with SAP
Honors: Information Sciences and Technology

Thesis Title: Students' Use of Security Features on Personal Devices Within Work Environments
Thesis Supervisor: Jens Grossklags

Work Experience:
Summer 2016
Strategic Sourcing Intern
Stryker
Allendale, NJ

June 2015-January 2016
Finance Co-Op
Johnson & Johnson, Inc.
Somerville, NJ

Summer 2014
Sales Team Leader
The Around Campus Group
Philadelphia, PA

Grants:
Schreyer Honors College Research Grant