Security Onboarding: An Interview Study on Security Training for Temporary Employees

Alex Hudock
The Pennsylvania State University
University Park, Pennsylvania
alexhudock93@gmail.com

Jake Weidman[*]
The Pennsylvania State University
University Park, Pennsylvania
jakeweidman@google.com

Jens Grossklags
Technical University of Munich
Munich, Germany
jens.grossklags@in.tum.de

ABSTRACT

After being placed into a position, it is common for new employees to be acclimated to an organization's culture, rules, and procedures via a process called onboarding. These processes are critical to ensure that employees become valuable assets to an organization and abide by organizational rules and procedures.

In this research study, we interviewed senior undergraduate students who had recently completed internships to determine what, if any, onboarding process they completed for their placement. Applying qualitative analysis, we find that the onboarding processes for these interns varied widely, from no onboarding at all to several extensive training sessions. Similarly, some interns reported high-level technical security training, while others reported almost no restrictions while on organizational networks. We build on our findings by providing recommendations for organizational improvements for interns, and by extension, full-time employees.

CCS CONCEPTS

• **Security and privacy** → **Human and societal aspects of security and privacy**.

KEYWORDS

Security in Organizations; Interview Study; Employee Onboarding

ACM Reference Format:
Alex Hudock, Jake Weidman, and Jens Grossklags. 2020. Security Onboarding: An Interview Study on Security Training for Temporary Employees. In *Mensch und Computer 2020 (MuC'20), September 6–9, 2020, Magdeburg, Germany.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3404983.3405525

1 INTRODUCTION

In early February 2018, core components of Apple's iOS were uploaded to a public repository on GitHub, making it one of the larger operating system source code leaks in history [22]. As this incident was investigated further, it was reported that the leak occurred via an intern; this individual was encouraged by friends in the jailbreaking community to take the code during an internship at Apple in 2016 for the purpose of security research, and to potentially develop novel jailbreaking techniques [21]. Upon taking the iOS source code from Apple, the intern then distributed the code privately among a small group of friends, but this code eventually was shared to wider circles, and ultimately was published on GitHub. This incident serves to introduce the topic of our paper: how organizations attempt to control security threats related to temporary employees, specifically interns.

Direct cyber-threats to organizations have continued to rise on an annual basis, prompting these organizations to continually consider and identify means to protect their organizations [15, 52]. These threats can take the form of direct, malicious attacks from external parties, such as the PlayStation or Yahoo data breaches [3, 62], or via accidental data leaking, such as a Boeing employee who accidentally emailed a non-employee of Boeing a spreadsheet containing sensitive information of 36,000 Boeing employees [51]. Unfortunately, a number of the more prominent data breaches are often at least partially attributable towards the action (or inaction) of an employee, whether this action is intentional or not [43, 58]. A key factor in ensuring that employees do not become potential weak links in an organizational security chain is an effective and comprehensive set of information security policies and procedures [32]. However, these policies and procedures are not enough, if employees are not correctly acclimated into a given organization's practices. Thus, the process of *employee onboarding*, or the training that a new employee receives upon starting a new position within an organization, becomes increasingly important [7].

Upon being hired by an organization, these new employees are exposed to varying lengths of onboarding, with 25% indicating that onboarding takes one day or less, and 47% indicating that this process takes approximately one month [14]. During this time, new employees are introduced into the organization's culture, provided with means of resources and support, and are generally provided with any equipment and training necessary to complete their work. After the onboarding process, employees are more informed about the expectations placed upon them and have a higher level of knowledge about what is permitted and explicitly prohibited. While this onboarding process for employees has become moderately standardized over time, full-time permanent employees are not the only individuals that organizations regularly employ; interns are another integral part of many organizations.

These interns tend to carry out similar tasks to permanent employees, and are often given access to the same resources. However, their time of employment within a given organization is generally pre-determined and limited, compared to their full-time counterparts. In situations in which organizations might have onboarding that takes one month or more, the concept of onboarding short-term interns might seem illogical, as by the time these new individuals

[*] Jake Weidman is now with Google.

MuC'20, September 6–9, 2020, Magdeburg, Germany

would be successfully onboarded, they would already be departing the organization. Thus, a situation could arise in which new employees, in this case interns, are welcomed into an organization and asked to complete standard job-related tasks using standard organizational resources, but may never be exposed to sufficient training on organizational policies and procedures.

In this study, we report the results from a qualitative interview study with 15 senior undergraduate students who completed internships at companies in various fields. Through these interviews, we attempt to describe current organizational practices as they relate to employee onboarding, as well as what security measures these organizations require. We find that, at a high level, many organizations observed different security practices and maintained very different onboarding procedures. Using interview data, as well as existing literature, we make arguments supporting positive organizational practices, and suggest improvements organizations can apply when working with limited time employees.

2 RELATED WORK

Organizational Security A major issue with unintentional or incidental cyber-threats is that many employees are not even aware that what they are doing could be potentially damaging to an organization. Utilizing an example from the literature, a now-common attack vector for hackers and other miscreants is to use popular objects, like USB drives, that they infect with advanced malware to infiltrate organizational networks [17, 64]. Without knowing it, an employee could attempt to use an infected USB drive in the process of their regular job, and ultimately infect their organization's systems with malware. Similar threats continue to persist with the growth of the Bring-Your-Own-Device (BYOD) paradigm, in which employees use their personal devices on an organizational network to complete work-related, but also personal tasks [4, 48].

Most, if not all, organizations recognize this continual threat by outside actors, and often work to construct means to combat these threats. A first means for many organizations to protect themselves is the formation and enforcement of an information security policy [32, 68]; a high-level document which indicates which technical practices and procedures are to be followed by all individuals within a given organization [5]. While a true 'universal model' of what should be included in an effective information security policy is missing [56], textbook examples and recent empirical research [66, 68] detail a number of features that should be included. At a high level, this includes an overview of organizational philosophies (providing a motivation for the policy), an acceptable use policy [67], an information security structure (definitions of organizational security roles), responsibilities of all network users (actual technical procedures to be followed), responsibilities for specific roles, and any supplemental materials (definitions, references, etc.) [34, 69]. By having an information security policy document, employees should become aware of appropriate security behaviors, begin to implement them, and in time internalize them into unconscious behavior, strengthening an organization's security [63].

While written policies themselves are important organizational documents, employee interactions with these documents, and the organizational structure by extension, are also critical. A number of previous studies have demonstrated that employee compliance (or deviance) effectively supports (or hinders) organizational security goals, with many works describing employees as 'weak links' in the organizational security chain [18, 24, 41, 70]. As noted in a 2013 interview study with CISOs, many security awareness messages are perceived as vacuous or repetitive, leading to a belief by employees that they are a waste of time [2]. For example, a 2015 study of a retail business found that "security policies were routinely ignored, and suggested bad practice became the behavioural norm", especially if it concerned time savings [26].

Other research suggests, however, that employees can become essential assets in securing and maintaining an organizational network, if properly motivated [10]. In the case of this work, the authors found that the concept of 'perceived inclusion' was a significant factor in determining employees' willingness to protect a given organizational network [10]. Alternative suggestions include making a determination of employees' trustworthiness, and then assigning them job tasks based on how much they can be trusted [40], or requiring a policy compliance evaluation for employees before placement [8]. Even these alternatives have problems, however; other research has found that if employees believe they are being too intensively monitored, or taken advantage of, by their organization, then they will not actively seek to protect organizational assets [37, 55]. Instances of this have been observed in the past with organizations that implement Bring-Your-Own-Device (BYOD) practices (to for example save money on IT purchases), and implement policies that employees believe infringe on their personal devices, and as a byproduct, their personal freedoms [50, 55, 65].

Employee Onboarding: From the perspective of individuals, internships provide valuable work experience, as well as connections to members of the workforce, and create the potential for full-time employment at a later time [30]. From the organizational perspective, internships allow work groups to evaluate potential future employees with minimal risk; general job performance can be assessed over the course of the internship, with no required commitment if an organization is not satisfied with a given intern's performance. A number of organizations treat internships like an extended interview, or cheaper labor [16]. When most students complete their internships, they have generally reached a heightened sense of maturity on par with that of standard full-time employees, though with less experience [47]. Interns, therefore, create an interesting opportunity to study organizational workplace behaviors.

Previous literature has showcased methods for improving employee compliance and training techniques [11, 36, 54], but these works tend to overlook the initiation of individuals to an organizational culture, and rather focus on enhancing security behaviors for pre-existing employees. Taking a step back, in order for employees to support an organization's security efforts, they must first be made aware of them. When many employees are hired, this happens via a process called *onboarding*, which is the act of acquiring and assimilating new hires; bringing them up-to-speed with organizational practices and beliefs [9]. Within traditional onboarding, there are four levels carried out by many organizations. The first level is *compliance*, which includes educating employees about organizational legal requirements, policies, and any other basic information required for employment. The second level, *classification*, focuses on employee comprehension of their new position, and all related responsibilities. Moving deeper within the process, the third level is *culture*, a phase which incorporates new employees into the social, as well as formal and informal organizational norms. The final level is *connection*, or the establishment of interpersonal relationships between new employees and their colleagues they will work with on a regular basis [6]. In practice, the topics covered in a standard onboarding process vary and lack standardization [9].

Some research suggests that the most commonly carried out levels of onboarding are the first two, compliance and classification, though they often take place over different amounts of time and vary in their presentation and level of detail. As previously mentioned, these times vary widely with some onboarding programs taking one to two weeks (or even just days), to upwards of one to six months [14, 25]. Regarding the coverage of these various levels, previous work has shown that while 100% of organizations discussed job expectations and organizational rules during onboarding, only 29% discussed organizational culture, and even less (24%) provided any type of connection, or a mentoring program [25]. Research in this space finds that onboarding should focus on the respective personal identities of new hires, rather than forcing these employees into a set cultural identity, as well as encouraging collaborative practices between new employees and tenured ones [12, 33, 38].

The literature in this space becomes more sparse when considering the role of interns within these organizations. While social integration into an organization is very important, we are far more interested in understanding the lesser-studied, foundational levels of the onboarding process including how and when new employees, in this case interns, are introduced to organizational security restrictions they must adhere to.

3 METHODOLOGY

This study consisted of two major components. The first component consisted of a pre-survey to solicit basic information about the participants. The second phase was a semi-structured interview to understand participants' varied experiences regarding onboarding at their internships, as well as the actual technology practices they were asked to follow.

Pre-Survey, Interview Items, and Analysis Steps: The pre-survey distributed to participants consisted of mostly demographic items including age, level of education, field of study, industry in which they completed their internship, and what their official position was. We also inquired as to these participants' personal technology security beliefs, and general technology habits to determine how these behaviors may translate or be different than actions taken in an organizational position.

We began the semi-structured interview by asking participants to generally describe their internship, including what work they did on a daily basis, what the themes of their project(s) were, and more. This was done to determine how impactful these interns' positions were within the organization, and whether they may have had to sign any non-disclosure agreements or work on any confidential projects. We continued by asking participants to describe their orientation or onboarding experience to determine what protocols were reviewed, or provided to them. As part of this interview, we asked the participants to express their opinions on the security restrictions (if any) imposed on them within their new position.

We were also interested in understanding the actual technology practices of these interns during their internship experience. The first of these topics focused on intern-owned BYOD devices used for work purposes (if applicable). We specifically inquired if they were allowed to use their personal device(s) in the work place, and if so, what tasks were they able to carry out on them. This included questions about personal/organizational email use on their personal devices, Wi-Fi access, and more. Participants were also asked if they noted any device behaviors of other interns, or full-time employees, as well as if there were any consequences for using personal devices if such rules were in place across groups. Lastly, we were interested in understanding if participants had changed any of their smartphone or computer security habits after having taken part in their internship; that is, did working in a professional environment change their own perspectives about the security of their personal devices.

After data collection, the first and second author independently analyzed the interview responses and identified key themes and topic categories. Subsequently, the researchers discussed their individual findings to identify common observations, to resolve disagreements, and to converge on a unified set of themes and categories. The researchers then revisited the interview data to match the interviewees' statements with the agreed-upon themes and categories.

Participants: We recruited 15 participants for this study, which is in line with established practices in the human-computer interaction community [13]. Current thinking in the qualitative research space dictates that coding saturation can typically be found between 6-9 interviews [71], and that the emphasis of any qualitative research should be more focused on the contribution of new knowledge from research subjects. In the case of this research, our participants provided us with a significant amount of diverse information, thus requiring a lower number of participants to reach topic saturation [46]. Participants were publicly recruited (e.g., via classroom announcements) at the Pennsylvania State University. Students who had completed 3 to 4 years of undergraduate education and had completed an internship during the previous summer break were eligible to participate in the study. Participants were all 21 or 22 years of age, and were all 4th-year, senior undergraduate students from different majors. Participants had completed their internships in various industries. The interviews were conducted in September 2016. See Table 1 for metadata about our participants.

Procedure and Research Ethics: The study protocol was reviewed and approved by the Pennsylvania State University's Internal Review Board (IRB). All participants were first given an informed consent document, which they were asked to read and sign. If the participants agreed to take part in the study, we then directed them to a provided computer to answer the brief pre-survey. The results of this survey were connected to the final interview data by a numerical identifier. The participants' names were not included with the data beyond consenting to take part in the study.

After concluding the pre-survey, participants completed the interview process. This was given by one of the members of our research team, and was recorded via audio for later transcription. Each of the interviews lasted approximately 20 minutes. Combined with the pre-survey, the entire study took about 30 minutes. Upon successfully completing the study, interviewees were thanked for their time and compensated with $10 for their participation.

Participant Designation	Age	Major	Industry Sector	Internship Title, Description
Participant 1	21	Finance	Commercial Insurance	Distribution Intern
Participant 2	21	Finance	Corporate Finance	Finance Analyst Development Program Intern
Participant 3	21	Economics	Business	Summer Intern (Generic)
Participant 4	22	Economics	Construction	CFO Shadow
Participant 5	21	Energy and Business Finance	Energy	Energy Management Intern
Participant 6	21	Information Science and Technology	Aerospace Engineering	Program Management Intern
Participant 7	21	Economics	Financial Healthcare	Finance Intern
Participant 8	21	Economics	Business Services/Counseling	Summer Business Development Associate
Participant 9	21	Chemical Engineering	Consumer Packaged Goods	Manufacturing Engineering Intern
Participant 10	22	Economics	Computer Software	Sales Intern
Participant 11	21	Cyber Security	Technology	Business Operations Intern
Participant 12	21	Supply Chain & Information Systems	Operations	Operations Intern
Participant 13	21	Electrical Engineering	Private Defense Contracting	Electrical Engineering Intern
Participant 14	22	Finance	Telecommunications	Transfer Pricing Intern
Participant 15	21	Mechanical Engineering	Automotive	Data Analyst Intern

Table 1: Participant metadata.

4 RESULTS

Throughout the analysis process, several themes began to emerge as it related to the experience of these interns at their respective positions. These were primarily reflected in the areas of onboarding, use of personal versus organizational devices, and the actual technical security requirements of organizations (with consequences for violating these requirements).

4.1 Onboarding Experience

The onboarding experiences of the interviewed participants tended to vary in terms of content covered and length of the onboarding process. Of the 15 participants, three of them reported that they did not undergo any form of security onboarding during their internships (i.e., Participants #1, #5, and #6). As Participant #1 noted:

> Actually, no, I didn't [have any onboarding] 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.

Although this particular intern was taking part in an unpaid internship, normal employee tasks were carried out throughout the duration of the placement. Participant 5 also expressed a similar experience with an unexpected twist:

> [I did not have an onboarding] 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 day I was there they got hacked [...] Their whole systems were down for two days. The cops were there and stuff. It was crazy.

While this particular breach should not imply that the lack of an onboarding process was to blame for this instance, it does showcase the point that even companies that are deemed to be 'relatively small' are still susceptible to these threats.

Continuing with smaller to medium-size organizations, we found that these interns generally completed modest levels of onboarding. For example, Participant 1 worked at a hospital and was given an account to log into the hospital's internal system. They noted that the hospital required them to change their password, but that there was no formal orientation given; simply sparse security practices to follow.

Participant 14 worked at a smaller, automotive software organization. They noted the following about their process:

> There was a real general computer usage guideline and the general *dos 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.

Throughout our analysis, it became apparent that the larger organizations had the strictest onboarding processes. For example, Participant 10 worked at a business unit of a large government contractor, and noted having a very formal onboarding process:

> There were multiple security measures that we had to go through. We went through the company's IT 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. [They gave us] in-person lectures, a paper test, and online modules related to security.

These larger companies seemed to not only have longer and more intensive onboarding processes, but they also, as noted above, tested the interns' knowledge on the policies, which they were now required to follow, through formal examinations. These types of examinations have been used in the past to evaluate the performance of full-time employees [59].

In addition to larger companies having a more structured onboarding process, some had much more specific guidelines and discussed concerns beyond cyber attacks. Participant 13 who worked at a large food manufacturer also had a series of online assessments, some related to security, and some not. They were also told:

> [...] Never leave sensitive documents unattended 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.

Such more specific guidelines seemed to be more present in organizations which dealt with highly confidential or financial data. These organizations with higher security needs also generally had requirements to sign additional non-disclosure documents, technology agreements, and more, that may otherwise have been included in a terms of employment document.

As the interviews progressed, we noticed that many participants described undergoing their onboarding process online, in part, or entirely. This onboarding procedure generally consisted of interns watching several brief videos detailing organizational policies and technology practices, and answering after each video a small exam or quiz. Participant 12 described their experience as follows:

> 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. The way they set it up was online so you get to 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.

Other participants noted a form of mixed-methods approach to the onboarding such as Participant 2, who stated:

> 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 we needed to do.

In each of the aforementioned instances, interns were exposed to multiple methods of onboarding; both online-only, and via a type of hybrid system where some lessons were carried out online, and others in-person. We found that 3 of our participants completed their onboarding entirely online, while 9 completed some type of mixed-method approach.

Although many of the organizations had structured onboarding procedures (whether in-person or not), it became apparent that not all organizations seemed to consistently onboard new hires, and in some instances, did not seem to enforce newly taught practices. While it is understandable that companies may onboard interns in groups, it was still surprising to find that one intern received neither onboarding nor basic instructions even though the intern worked at a large company. More specifically, Participant 6 worked at a large investment firm, but began his internship after the other interns. Because of this, he said that he had no onboarding process whatsoever and was never given security guidelines, though he believed the other interns received such training:

> [I didn't receive any onboarding and] I think it was because I was part time and I'm not going to [say] that I had a huge role [there] 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. I was more informal of an intern. They had a more formal internship program and I'm sure those kids had to go through more of a vetting process than I did.

Other participants noted that while their onboarding processes were extensive, many aspects of their training were not reflected in the actions of other employees, or themselves. A common occurrence of this related to the use of cellphones for both work and non-work-related tasks. Participant 9 noted this when talking about their onboarding process and subsequent employment:

> The cell phone use was touched on. You weren't supposed to use your cell phone while at work was a guideline put forth. [But] no superior would ever really challenge you for it, if they saw you using your cell phone. [There was] widespread use.

To summarize the onboarding experience of our participants, we first found that many organizations tend to have at least some form of onboarding process for interns. This onboarding was generally brief, lasting for one week or less, and was often carried out across multiple mediums including the reading of formal documents, in-person meetings/training sessions, and online instructional videos. In many instances, the interns were tested on their knowledge of these organizational procedures. Although many of our participants underwent some form of onboarding, others did not, either as the result of a lack of standard organizational practice, or being hired at a time after general onboarding may occur. However, smaller organizations are just as susceptible to cyber attacks as larger ones, and thus all organizations should be concerned with onboarding and educating their employees in order to best defend their resources.

Lastly, we found that while many organizations engage in extensive onboarding practices, a number of trained measures are not enforced in practice, thus questioning either their importance as procedures, or the lack of proper enforcement from management.

4.2 Devices

Beyond the onboarding process, we were interested to understand the device usage behaviors of our participants during the time of their internship. Specifically, we wanted to understand how many interns were issued devices by the organization they worked for, or how many were required to use their personal devices, or some mix of both.

Beginning with more traditional computers, we found that a majority of our participants (80%) were issued some type of organizational device, which was generally a desktop computer, or more often, a laptop. For those interns, who were issued a laptop, these devices usually came with tighter restrictions on how and where they were permitted to use these devices. When asked about their issued laptop, Participant 7 stated:

> 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.

Beyond physically limiting the use of organizational devices outside of the workplace, other participants noted restrictions placed on these devices, which is a fairly standard practice in the industry [44]. Many of our participants noted that their organization-issued devices contained internet firewalls, blocking sites such as Facebook, ESPN, and others.

A difference in a few rare cases was that some interns reported not being able to access standard organizational tools because they had not been given access, though full-time employees used these tools regularly. Participant 8's example is one of the few cases we discovered in which the organization seemed to dictate different levels of security for more temporary employees, such as interns, and full-time employees. The participant mentioned the following:

> They gave me a laptop for throughout the summer. [But] there are certain things that I couldn't access on my laptop, I guess you could say software that contains–I know [a lot of the software we used] 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.

While we found that it was common for most interns to receive some type of computer to perform their work during their employment, several of the interns we interviewed were required to use their personal devices for all work-related tasks. For these few participants, they noted that they believed that a majority of full-time employees were issued their own devices by the organization; that they were only using their personal laptops because they were interns. Participant 1 recalled:

> 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. 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. Everyone [all of the full-time employees] 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.

These previous two examples, in which one organization provided a computer and one did not, demonstrate the concept that organizations may not actually give interns the same level of access or organizational tools and data. This point contradicts one of the original concepts that postulated that interns are given the same tools as full-time employees but for a shorter period of time. The latter example highlighted this issue further based on the use of a personal Gmail account to complete all work-related tasks. This participant seemed to indicate that although full-time employees would be given their own organizational email address, they were still being asked to use an external email to complete their tasks. This external software use, while most likely secure enough, is the opposite of what some of our other participants were told about the use of their personal email for organizational tasks. Participant 7 offered about their experience:

> 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.

While laptops and desktops are critical components of the modern workplace, smartphones are now also used to regularly complete a number of work-related tasks, including email, groups chats (Slack, etc.), mobile work, and more. We sought to understand how these interns' mobile devices, and mobile device use, were controlled by the organizations they worked for. The most common response we received from our participants was very simple: the organizations did not manage mobile device usage at all. Reflecting experiences made by many of the participants, Participant 4 noted:

> They were very lenient on that [personal cellphone use]. It was more that they had a good amount of trust with us on that. 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.

Although all of our participants noted that they were allowed to use their personal mobile devices for common tasks such as texting, using Snapchat, etc., a number of them commented that there were certain things they were not allowed to do with their smartphones. These non-permitted items generally included completing work-related tasks on their phones, including emails, Slack, etc., and connecting to the organization's Wi-Fi. Similar to the use of personal laptops to complete work-related tasks, several participants also commented on the fact that while they were unable to connect their devices to WiFi or put their organizational email on their personal device, that this was something that standard, full-time employees were able to do.

For those employees who were permitted to use their personal mobile devices to complete work-related tasks or put their work email on their phone, this came at a 'cost'. Those interns were often required by their organization to install special security software on their devices; specifically, the software suite MobileIron, which is a mobile device management (MDM) solution that allows organizations to manage and secure the mobile applications, content, and devices of their employees [45]. Participant 15 described their experience with this as follows:

> So if we wanted to be on the corporate WiFi or have email on my phone, we had to go to our IT desk and they would install this software called "MobileIron" or something like that which is essentially encrypts your phone and emails and securely connects you to the WiFi through VPN. I'm pretty sure they could remotely wipe my phone. 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.

Though a vast majority of the interns we interviewed used their own devices on the job, we did find that two participants were offered or issued a mobile device by the organization they were employed by. Participant 5 was issued a flip-phone to directly communicate with their team while they were on projects, while another participant was given the option to take a mobile device provided by their organization. Participant 11, who was offered the mobile device, opted not to accept it, however, noting that they felt it would be too much of a hassle to configure and then return a device that they would own for a short period of time:

> So I chose not to get a company phone but I also did not put any of my company emails 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. 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?"

Reflecting on all of the participants' experiences regarding what devices they used to complete their work-related tasks, we were able to determine several key takeaways. First, as it relates to personal device use to complete personal tasks, many organizations have a fairly liberal attitude towards letting their employees use their devices how they see fit. However, these organizations were more reserved when it came to allowing these devices on their network. In most instances, the interns we interviewed did not ever connect their devices to the organizational Wi-Fi, nor did they put any sort of work-related email on their devices. For those who did, they were required to install additional software from the IT department to be able to do this. Lastly, we find that interns often did not receive organization-owned devices in instances where traditional, full-time employees would. The reasons for this are unclear from the perspective of this research, but show a separation in how organizations consider temporary employees, such as interns, from full-time, permanent employees.

4.3 Security Protocols and Enforcement

We were also interested in understanding what security practices each organization required of its interns, as well as what types of enforcement they would use in the event that someone violated one of these practices. In this section, we specifically address account and password creation/management, the transfer of information across personal and organizational accounts, physical security measures, and consequences for violating any of these procedures. While there were most certainly other aspects related to organizational security that these interns may have been exposed to, these points reflected what they remembered most about their time during their internship. As Participant 15 reflected:

> 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 [organizational security practices]. A lot of [people] had told me that if you get a 100 sheet package on your desk you're not going to read the entire thing, just sift through it or ask the person next to you.

Beginning with account creation and password management, we found that most of the participants had some requirements when forming passwords for their account, though 5 participants noted that they did not recall any type of requirements for their passwords on either their personal devices (if used for work), or their organizational accounts. For others, the most commonly found rule regarding password management was the need to frequently change passwords; often, at the rate of once per month. Several participants also noted that their passwords had high complexity requirements.

This type of password creation and management is presumably standard across many organizations. However, such a heightened concern (similar to password security) seemed to be less reflected in situations where interns were using their own equipment to complete work-related tasks. Participant 1, for example, used their own laptop during their internship, and noted that:

> They didn't ask me if it [my computer] was password protected or anything.

Beyond password creation and management, many participants also spoke about data confidentiality and integrity, and how they managed to work with sensitive data. Like many other measured factors, this topic was something that varied greatly among the participants we interviewed. One of the principle ways we asked participants about their organization's data management practices was to determine how they used their work-related email accounts. At one end of the spectrum, three participants recalled using their personal Gmail account to send work-related emails. One of these interns, Participant 14, recalled that they forwarded their work email through their personal email, and sent and received all messages that way:

> I just routed my work e-mail through my personal e-mail so I just connected the two accounts. Basically the emails would go to my work inbox and it would also go to my personal inbox because I checked that more frequently. 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.

In contrast, other participants were given strict instructions about maintaining strict control over their emails, and were instructed to never pass data out of the organization to any other source. Participant 7, quoted previously, stated that they were not permitted to send any emails or data to a personal email account at all, especially when dealing with work-related data, and that the punishment for this would be termination.

Most other participants did not recall any distinctive instructions about what they could or could not do with work-related data, and how it should be transmitted. Many of these participants reported using their work-based emails to send personal information to themselves at various times, but tended to not send work-related things to non-work emails. Participant 11 remembered the following:

> I never ever [emailed] work related things [to my personal email] but let's see what was one example... I think I bought tickets on StubHub [and] sent them from work email to my personal email.

None of the participants stated anything regarding alternative means of transmitting work-related data such as via USB drives or cloud storage. However, some of them remembered additional physical security measures that their respective organizations put in place for both the physical security of facilities and the security of information. Of the participants, only two noted any form of key card or biometric access to their work facilities. One was required to use a key card to access all of the facilities in which they worked, while the other (Participant 1) needed to use a fingerprint scanning system to enter a building.

Beyond physical building security, one participant also recalled an equipment procurement procedure for anyone wishing to take their work laptop home for an evening. In this organization, removing equipment from the office was a controlled process to ensure the physical security of the computer equipment. Participant 10 described it as follows:

> For interns, 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. We had to mention when we were 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.

This organization clearly took extensive inventory on their equipment, and ensured they would be able to track where their computers were at all times.

Other organizations defined strict physical security rules for their interns, as reported by Participant 5 about an earlier internship. During that previous internship (at a software company), the organization's IT department took active efforts to ensure that employees (and interns) followed certain steps of physical security, including locking workstations when using the restroom, or not leaving documents in the printer tray for extended periods of time. This organization even created clever enforcement strategies to encourage these physical security behaviors:

> 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.

Education and enforcement of security policies is a very important pillar of organizational security. A great deal of literature focuses on encouraging employee compliance with said security policies through a variety of techniques [29, 53, 60], with proper education being a foundational aspect of the process. Based on the information we learned from our participants, we find that most of the interns did not receive very comprehensive technical security training or policy coaching, with a few exceptions. Work-related data was frequently transferred by interns to their personal devices and emails, creating potential data leak scenarios or the chance for easy data theft. Additionally, in many instances, established rules, such as limited cell phone use in the office, were consistently ignored by not only the interns, but full-time employees as well. Such inconsistent enforcement over time can reinforce negative behaviors that may eventually adversely effect the organization. In contrast, we did find that some organizations took this training and enforcement quite seriously, not only requiring a strict security regiment, but also providing support and continuous education on security subjects, sometimes in an entertaining fashion, such as providing donuts for coworkers.

5 DISCUSSION

In this work, we interviewed 15 participants to understand their experiences as interns working across various industries in the contexts of onboarding procedures, device usage (personal vs. organizational), and enforced security policies and procedures. At a high level, we demonstrated that a majority of our participants did undergo some form of onboarding, though this varied significantly between interns. We also found that many organizations were hesitant to allow interns' personal devices on to their secured networks, and generally did not allow interns to complete any work-related tasks on their personal devices, with some notable exceptions. Lastly, we found that the interns we interviewed were not exposed to a large number of technology policies or procedures and would often ignore the limited number of policies in place, though this could be attributed to these interns witnessing full-time employees to ignore these rules as well.

As with many organizational studies, a major difficulty in constructing a series of impactful results from the data is the number of individual differences between each participant's experiences [20, 39, 61]. In this particular study, no two interns shared highly similar experiences, which demonstrates the diversity of organizational practices in this space; however, drawing conclusions about what is a 'good' or 'bad' practice can be challenging. For the remainder of this section, we posit what we perceive to be 'good' organizational practices as it relates to interns in the workplace by combining our results with existing literature.

Clear, Concise, and Consistent Onboarding: As has been discussed at numerous points in this paper, the process of onboarding employees is critical to the ultimate success of those employees within an organization; the same is true for interns as well. The principal difference between these two employee types is that of time. For traditional full-time employee onboarding, research suggests that the most critical portion of onboarding processes occurs within the first 30 days [31]. While this is not necessarily a substantial amount of time for a permanent employee, it is for an intern. Interns often only work for a limited period of 6 weeks to 3 months, and only 19% of these temporary positions ultimately turn into full-time offers [16]. Since a majority of the onboarding process is focused on creating workplace cohesion and instilling organizational values, this short-term employment reality places many organizations in a difficult position: how much time and effort should be invested in onboarding temporary employees (interns) when most of them will leave within 30-60 days of this extensive process being completed?

While it is clear via this study that some organizations simply chose to forgo this process (primarily in smaller organizations), others chose to implement extensive onboarding procedures by utilizing online tools such as pre-recorded video lessons and lectures, access to text-based training resources, and comprehensive examinations to ensure knowledge of the materials on the part of new hires. Although this method lacks personal interaction, it is likely time-efficient and warrants further attention by many organizations as an alternative to traditional, in-person onboarding.

There is not a great deal of literature which currently evaluates the effectiveness of onboarding via online resources, but we argue this method is viable based on literature surrounding MOOCs (Massive Open Online Courses) and other online forms of education. The similarities between the two (online courses and onboarding) are numerous. For example, both seek to provide education to a target audience, and contain similar information across multiple iterations with little to no modifications needed to educational materials (semester-to-semester/multiple hired employees).

In a 2015 study, it was found that 71% of educators deemed online education to be just as efficient as traditional education [1]. Similar research seems to suggest that online education can be, at times, more effective than in-person education given proper conditions and appropriately designed feedback from educators [19]. More specifically, two previous studies examining a MOOC-based college orientation, and general online course orientation, found video-based college onboarding to be highly effective in both scenarios in terms of learner comprehension, as well as increased retention of the course or program materials [35, 57]. Online education, and MOOCs specifically, are not without their downsides, however. These generally include motivational concerns (of the individuals taking part in the MOOCs), enrollment size issues, retention, diversity/disparity, interaction with the instructor, plagiarism/cheating, and success rate [49]. Although these are issues for MOOCs, we argue that many of these downsides are less applicable to employee onboarding as the educational process is not optional; it is required for given individuals to maintain their position.

By creating online educational videos, resources, and knowledge checks for the purpose of employee onboarding, organizations may be capable of reducing the amount of effort required to onboard new employees. This concept would be especially critical for short-term interns, who would have access to the same resources, at no additional cost to the organization in terms of time. Interns could simply be required to review these onboarding materials prior to the beginning of their internship to ensure that they are already fully up-to-speed on organizational expectations before they arrive, or alternatively, whenever the organization would prefer. This is also one potential solution to the issue raised by Participant 6, who started their internship after the other interns and was not onboarded as a result. The flexible nature of online onboarding would permit a new hire (intern, or not) to complete an onboarding process at any time without the need to schedule lengthy meetings or training sessions.

Interns and BYOD: The process of securing organizational systems can be challenging enough without the inclusion of employee-owned devices, such as laptops and smartphones, being connected to an organizational network. While installing custom software packages on employee or intern devices is one solution to the BYOD problem, there is another more simple solution: just don't allow personal devices on the network (or access to work-related assets, such as email), especially for shorter-term employees, like interns.

The concept of blocking personal devices from organizational network resources may seem extreme at first glance, but based on the participant data we collected, it is partly already being done in practice by the interns themselves, and indirectly by data protection policies around them. Of the 15 participants we interviewed, 13 of them described using their mobile devices in their respective workplaces. Of these 13, only 6 of them connected to their organization's WiFi network, and only 4 of those individuals did so with individual credentials. The other two participants noted that they only connected to the WiFi at their office because it was a public guest network, and their employer would be unable to track their web history. The remaining 7 participants never connected their phones to their organization's WiFi, whether they were given the ability to or not. Many of them cited the fact that dealing with their organization's firewall was cumbersome (Snapchat was blocked by many firewalls), and they preferred to be able to use their devices without their employer tracking their web history.

The practice of interns self-policing their device use while at work extended beyond WiFi access to other services such as email. Only 3 interns chose, or were permitted, to access their organization's email on their personal phone, and one intern was only permitted to do this if they installed MobileIron on their device. This is consistent with current literature that states only 25% of organizations currently allow employee's personal devices to access network resources [23]. Of the 12 interns who did not put their work email on their phones, 3 of them noted that this was based on an organizational policy stating that interns were not permitted to do this (full-time employees were). The remaining 9 interns gave very straightforward responses as to why they did not place their organizational email on their phone: they did not want to.

This may indicate that interns on a wider scale are choosing to self-enforce a greater degree of separation between themselves and their work, or are being barred from pairing their own personal devices to organizational resources. In either scenario, none of the participants expressed any form of resentment towards their respective organizations for mandating this requirement. As such, it seems feasible to suggest that organizations should simply enforce a policy that does not permit intern-owned devices to access organizational resources, except in the event that the intern allows the installation of a designated security product. By doing this, organizations could avoid potential threats caused by outsider devices and interns could continue to feel comfortable using their devices in the workplace (free from network activity monitoring). As such, these findings potentially point towards a simple and effective solution to further solidify organizational networks.

Interns and Access: A reasonable concern from a security-oriented perspective is the concept that interns may receive similar access to resources traditionally reserved for full-time employees, and thus could be potential liabilities as it relates to organizational security. However, after talking with our participants, we found that this concern was addressed by several organizations. Several of the individuals we interviewed noted that there were many things they were not given access to as part of their internship which would be normally given to full-time employees. This ranged from organization-issued cellphones and laptops, to remote email access, to access to restricted data required to complete work.

Some literature suggests that restricting the access of information to certain individuals can bolster security, but may ultimately result in those individuals circumventing these information blocks in order to accomplish their work more efficiently [27, 28]. While this may be true, the participants that we interviewed did not express any frustration with recalling this part of their work. Rather, they seemed to accept this as an organizational requirement and did not question it. While we are not willing to make any formal recommendations on the subject of allowing, or not allowing, interns to access sensitive or confidential organizational data, we do acknowledge that some organizations choose to restrict such information on a need-for-task basis. Our findings show that the interns did not seem to flag this practice as odd, and seemed to comply with it without hesitation. This data restriction practice could be useful in organizations that require a larger amount of discretion, or simply in the event that an organization wishes to keep tighter control over their information resources.

Limitations and Future Work: Regarding potential limitations and future work, we first want to reiterate that this was an *exploratory* qualitative study, and due to the nature of qualitative research more generally, the work cannot necessarily be generalized to a national, or international population unless taken as a part of a larger meta-analysis (and even then, this is still somewhat up for debate) [42]. Second, although this was outside of the scope of this initial study, a good next step for further evaluation of this topic space would be to explore the concept of security onboarding from the perspective of various companies themselves. This could be accomplished by interviewing individuals such as Chief Information Security Officers (CISOs), or others within companies who are responsible for constructing and implementing security policies. Further, this conceptual qualitative work could be accompanied by a more detailed look at these organizations' actual security policies to add more depth to the analysis (see, for example, [66, 68]).

6 CONCLUSION

In this work, we interviewed 15 senior undergraduate students who had recently completed a summer internship to understand what their experience was like from the perspective of organizational security onboarding, as well as personal device use and information security practices. The participants represented multiple industries and organizations that varied in size from small construction firms to large government contractors. At a high level, we found that each of these interns' experiences at their internships varied greatly.

We found that while some individuals received no onboarding, many did, though the sophistication of this practice varied greatly across participants. In the more simplistic forms, interns were required to meet with supervisors, IT staff, or others to go over organizational requirements over the course of one day to one week. In more complex scenarios, interns were required to complete onboarding via online-based systems where they would watch instructional videos, review text-based materials, and complete evaluations to prove their knowledge of the material. Based on issues with disparate onboarding processes across organizations, and literature involving online education, we recommend that more organizations consider utilizing resources such as pre-recorded videos or documentation to assist in the process of onboarding not only interns, but also full-time staff.

In the devices space, many participants noted that they were not issued any type of organization-owned device to complete their internship, aside from an office-based desktop computer or laptop. Regarding mobile phone use in the workplace, most interns never connected their personal device(s) to their organization's network, and were hesitant to do so, even if given the option. Additionally, most interns opted to not place their organizational email on their personal device, either by choice, or as per policy of their organization. As interns may be predisposed to not connect their personal devices to organizational networks, this could be an opportunity for organizations to formally disallow the use of personal devices for work-related tasks, unless additional security efforts are made, such as the installation of a mobile security suite.

While many interns rarely used their personal devices on their respective organizational networks, they often reported transferring information to and from personal and work-centric sources, usually via email. Although some interns reported that their organization had a policy against such an act, many interns did this regularly, and even forwarded their work emails to their personal email accounts in certain instances. This represents a high-risk security behavior, and one that should be addressed by more organizations. The lack of general governance over email policies is surprising, given that we also found several organizations which aimed to restrict the flow of confidential data to interns.

To the best of our knowledge, very little to no research has been conducted on the experience of interns within organizations with a focus on organizational security. We hope that this work takes first steps in exploring not only the potential threat that short-term employees, such as interns, can pose to an organization, but also actions an organization can do to better protect itself against these threats. Even well-designed security policies are rendered useless, if employees do not know how to follow them. Thus, it is up to organizations to ensure that proper care and focus is given to the onboarding and training of all employees, including interns, to ensure that critical resources continue to be secure.

Acknowledgements: We thank the anonymous reviewers for their constructive feedback. Alex Hudock was partially supported by the Schreyer Honors College, Pennsylvania State University.

REFERENCES

[1] Elaine Allen and Jeff Seaman. 2016. Online Report Card: Tracking Online Education in the United States. *Babson Survey Research Group* (2016).

[2] Debi Ashenden and Angela Sasse. 2013. CISOs and organisational culture: Their own worst enemy? *Computers & Security* 39 (2013), 396–405.

[3] Liana Baker and Jim Finkle. 2011. Sony PlayStation suffers massive data breach. *Reuters* (April 2011).

[4] Rafael Ballagas, Michael Rohs, Jennifer Sheridan, and Jan Borchers. 2004. BYOD: Bring your own device. In *Proceedings of the Workshop on Ubiquitous Display Environments, Ubicomp.*

[5] Richard Baskerville and Mikko Siponen. 2002. An information security meta-policy for emergent organizations. *Logistics Information Management* 15, 5/6 (2002), 337–346.

[6] Talya Bauer. 2010. Onboarding new employees: Maximizing success. *SHRM Foundation's Effective Practice Guideline Series* (2010).

[7] Talya Bauer and Berrin Erdogan. 2011. Organizational socialization: The effective onboarding of new employees. *APA Handbook of Industrial and Organizational Psychology* 3 (2011), 51–64.

[8] Scott Boss, Laurie Kirsch, Ingo Angermeier, Raymond Shingler, and Wayne Boss. 2009. If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems* 18, 2 (2009), 151–164.

[9] George Bradt and Mary Vonnegut. 2009. *Onboarding: How to get your new employees up to speed in half the time.* John Wiley & Sons.

[10] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. 2010. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly* 34, 3 (2010), 523–548.

[11] AJ Burns, Tom Roberts, Clay Posey, Rebecca Bennett, and James Courtney. 2015. Assessing the role of security education, training, and awareness on insiders' security-related behavior: An expectancy theory approach. In *48th Hawaii International Conference on System Sciences (HICSS).* IEEE, 3930–3940.

[12] Daniel Cable, Francesca Gino, and Bradley Staats. 2013. Breaking them in or eliciting their best? Reframing socialization around newcomers' authentic self-expression. *Administrative Science Quarterly* 58, 1 (2013), 1–36.

[13] Kelly Caine. 2016. Local standards for sample size at CHI. In *Proceedings of the CHI Conference on Human Factors in Computing Systems.* 981–992.

[14] Career Builder. 2017. Thirty-Six Percent of Employers Lack a Structured Onboarding Process for New Employees, According to New CareerBuilder Survey. http://press.careerbuilder.com/2017-05-11-Thirty-Six-Percent-of-Employers-Lack-a-Structured-Onboarding-Process-for-New-Employees-According-to-New-CareerBuilder-Survey.

[15] Brian Cashell, William Jackson, Mark Jickling, and Baird Webel. 2004. The economic impact of cyber-attacks. *Congressional Research Service Documents, CRS RL32331 (Washington DC)* (2004).

[16] Malcolm Coco. 2000. Internships: A try before you buy arrangement. *SAM Advanced Management Journal* 65, 2 (2000), 41.

[17] Goran Delac, Marin Silic, and Jakov Krolo. 2011. Emerging security threats for mobile platforms. In *Proceedings of the 34th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).* IEEE, 1468–1473.

[18] Mike Durgin. 2007. Understanding the importance of and implementing internal security measures. *SANS Institute Reading Room (https://www2. sans. org/reading_room/whitepapers/policyissues/1901. php)* (2007).

[19] Sean Eom, Joseph Wen, and Nicholas Ashill. 2006. The determinants of students' perceived learning outcomes and satisfaction in university online education: An empirical investigation. *Decision Sciences Journal of Innovative Education* 4, 2 (2006), 215–235.

[20] Shuchih Ernest Chang and Chienta Bruce Ho. 2006. Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems* 106, 3 (2006), 345–361.

[21] Lorenzo Franceschi-Bicchierai. 2018. How a Low-Level Apple Employee Leaked Some of the iPhone's Most Sensitive Code. *Motherboard* (Feb 2018). https://motherboard.vice.com/en_us/article/xw5yd7/how-iphone-iboot-source-code-leaked-on-github

[22] Lorenzo Franceschi-Bicchierai. 2018. Key iPhone Source Code Gets Posted Online in 'Biggest Leak in History'. *Motherboard* (Feb 2018). https://motherboard.vice.com/en_us/article/a34g9j/iphone-source-code-iboot-ios-leak

[23] Arnab Ghosh, Prashant Kumar Gajar, and Shashikant Rai. 2013. Bring your own device (BYOD): Security risks and mitigating strategies. *International Journal of Global Research in Computer Science* 4, 4 (2013), 62–70.

[24] Lawrence Gordon, Martin Loeb, William Lucyshyn, and Robert Richardson. 2006. 2006 CSI/FBI computer crime and security survey. *Computer Security Journal* 22, 3 (2006).

[25] Jolie Graybill, Maria Hudson Carpenter, Jerome Offord Jr, Mary Piorun, and Gary Shaffer. 2013. Employee onboarding: Identification of best practices in ACRL libraries. *Library Management* 34, 3 (2013), 200–218.

[26] Andrews Greig, Karen Renaud, and Stephen Flowerday. 2015. An ethnographic study to assess the enactment of information security culture in a retail store. In *2015 World Congress on Internet Security (WorldCIS).* IEEE, 61–66.

[27] Ken Guo. 2013. Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security* 32 (2013), 242–251.

[28] David Hannah. 2006. Keeping trade secrets secret. *MIT Sloan Management Review* 47, 3 (2006), 17–20.

[29] Tejaswini Herath and Raghav Rao. 2009. Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems* 18, 2 (2009), 106–125.

[30] Michael Hergert. 2009. Student perceptions of the value of internships in business education. *American Journal of Business Education* 2, 8 (2009), 9–14.

[31] Jo Hillman. 2010. Planning for employee onboarding: Finding ways to increase new employee success and long-term retention. *Noel-Levitz White Paper* (2010).

[32] Karin Höne and Jan Eloff. 2002. Information security policy - What do international information security standards say? *Computers & Security* 21, 5 (2002), 402–409.

[33] Maggie Johnson and Max Senges. 2010. Learning to be a programmer in a complex organization: A case study on practice-based learning during the onboarding process at Google. *Journal of Workplace Learning* 22, 3 (2010), 180–194.

[34] Andrew Jones and Debi Ashenden. 2005. *Risk management for computer security.* Butterworth-Heinemann.

[35] Kona Renee Jones. 2013. Developing and implementing a mandatory online student orientation. *Journal of Asynchronous Learning Networks* 17, 1 (2013), 43–45.

[36] Mari Karjalainen and Mikko Siponen. 2011. Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems* 12, 8 (2011), 518.

[37] Iacovos Kirlappos. 2016. *Learning from "shadow security": Understanding non-compliant behaviours to improve information security management.* Ph.D. Dissertation. University College London.

[38] Howard Klein, Beth Polin, and Kyra Leigh Sutton. 2015. Specific onboarding practices for the socialization of new employees. *International Journal of Selection and Assessment* 23, 3 (2015), 263–283.

[39] Sara Kraemer, Pascale Carayon, and John Clem. 2009. Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security* 28, 7 (2009), 509–520.

[40] Aron Laszka, Benjamin Johnson, Pascal Schöttle, Jens Grossklags, and Rainer Böhme. 2014. Secure team composition to thwart insider threats and cyberespionage. *ACM Transactions on Internet Technology* 14, 2-3 (2014).

[41] Jintae Lee and Younghwa Lee. 2002. A holistic model of computer abuse within organizations. *Information Management & Computer Security* 10, 2 (2002), 57–63.

[42] Lawrence Leung. 2015. Validity, reliability, and generalizability in qualitative research. *Journal of family medicine and primary care* 4, 3 (2015), 324.

[43] Divakaran Liginlal, Inkook Sim, and Lara Khansa. 2009. How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers and Security* 28, 3-4 (2009), 215–228.

[44] Vivien Lim and Don Chen. 2012. Cyberloafing at the workplace: Gain or drain on work? *Behaviour & Information Technology* 31, 4 (2012), 343–353.

[45] Jesse Wagner Lindeman and Thomas Edward Wagner. 2013. Management of mobile applications. US Patent 8,359,016.

[46] Kirsti Malterud, Volkert Dirk Siersma, and Ann Dorrit Guassora. 2016. Sample size in qualitative interview studies: Guided by information power. *Qualitative Health Research* 26, 13 (2016), 1753–1760.

[47] Sue McCaffrey, Theodore Miller, and Roger Winston. 1984. Comparison of career maturity among graduate students and undergraduates. *Journal of College Student Personnel* (1984).

[48] Bill Morrow. 2012. BYOD security challenges: Control and protect your most sensitive data. *Network Security* 2012, 12 (2012), 5–8.

[49] Sarah North, Ronny Richardson, and Max North. 2014. To Adapt MOOCs, or Not? That Is No Longer the Question. *Universal Journal of Educational Research* 2, 1 (2014), 69–72.

[50] Kevin Ortbach, Nicolai Walter, and Ayten Öksüz. 2015. Are you ready to lose control? A theory on the role of trust and risk perception on bring-your-own-device policy and information system service quality. In *Proceedings of the European Conference on Information Systems (ECIS).*

[51] Pierluigi Paganini. 2017. Boeing notified 36,000 employees following an accidental data leak. *Security Affairs* (Feb 2017). http://securityaffairs.co/wordpress/56736/data-breach/boeing-data-leak.html

[52] Joanna Page, Madison Kaur, and Emma Waters. 2017. Directors' liability survey: Cyber attacks and data loss - A growing concern. *Journal of Data Protection & Privacy* 1, 2 (Spring 2017), 173–182.

[53] Seppo Pahnila, Mikko Siponen, and Adam Mahmood. 2007. Employees' behavior towards IS security policy compliance. In *40th Annual Hawaii International Conference on System Sciences (HICSS).* IEEE.

[54] Petri Puhakainen and Mikko Siponen. 2010. Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly* 34, 4 (2010), 757–778.

[55] Frida Putri and Anat Hovav. 2014. Employees' compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory. In *Proceedings of the European Conference on Information Systems (ECIS)*.

[56] Jackie Rees, Subhajyoti Bandyopadhyay, and Eugene Spafford. 2003. PFIRES: A policy framework for information security. *Communications of the ACM* 46, 7 (2003), 101–106.

[57] Jan Renz, Thomas Staubitz, Jaqueline Pollack, and Christoph Meinel. 2014. Improving the onboarding user experience in MOOCs. *Proceedings EduLearn* (2014).

[58] Robert Richardson. 2008. CSI computer crime and security survey. *Computer Security Institute* 1 (2008), 1–30. http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf

[59] Frank Schmidt and John Hunter. 1981. Employment testing: Old theories and new research findings. *American Psychologist* 36, 10 (1981), 1128.

[60] Mikko Siponen and Anthony Vance. 2010. Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly* 34, 3 (2010), 487–502.

[61] Andrew Taylor. 1995. Organizational differences in ISO 9000 implementation practices. *International Journal of Quality & Reliability Management* 12, 7 (1995), 10–27.

[62] Sam Thielman. 2016. Yahoo hack: 1bn accounts compromised by biggest data breach in history. *The Guardian* (Dec. 2016).

[63] Kerry-Lynn Thomson, Rossouw Von Solms, and Lynette Louw. 2006. Cultivating an organizational information security culture. *Computer Fraud & Security* 2006, 10 (2006), 7–11.

[64] Matthew Tischer, Zakir Durumeric, Sam Foster, Sunny Duan, Alec Mori, Elie Bursztein, and Michael Bailey. 2016. Users really do plug in USB drives they find. In *2016 IEEE Symposium on Security and Privacy (S&P)*. IEEE, 306–319.

[65] Jake Weidman and Jens Grossklags. 2017. I like it, but I hate it: Employee perceptions towards an institutional transition to BYOD second-factor authentication. In *Proceedings of the 33rd Annual Computer Security Applications Conference*. ACM, 212–224.

[66] Jake Weidman and Jens Grossklags. 2018. What's in your policy? An analysis of the current state of information security policies in academic institutions. In *Proceedings of the European Conference on Information Systems (ECIS)*.

[67] Jake Weidman and Jens Grossklags. 2019. The acceptable state: An analysis of the current state of acceptable use policies in academic institutions. In *Proceedings of the European Conference on Information Systems (ECIS)*.

[68] Jake Weidman and Jens Grossklags. 2019. Assessing the current state of information security policies in academic organizations. *Information & Computer Security* (2019).

[69] Michael Whitman and Herbert Mattord. 2013. *Management of Information Security*. Nelson Education.

[70] Robert Willison. 2006. Understanding the perpetration of employee computer crime in the organisational context. *Information and Organization* 16, 4 (2006), 304–324.

[71] Diane Young and Erin Casey. 2019. An examination of the sufficiency of small qualitative samples. *Social Work Research* 43, 1 (2019), 53–58.