ABSTRACT

Title of Document: SECURING THE HUMAN – EXPLORING CURRENT SECURITY AWARENESS AMONG EMPLOYEES AND FINDINGS WAYS TO IMPROVE IT IN THE ORGANIZATIONAL SETTING

Nina Sebescen, Master of Information Management, 2015

Directed By: Professor Jessica Vitak, iSchool, MIM

As organizational security breaches increase, it becomes imperative to understand the factors that lead to these breaches and take the necessary steps to minimize threats. Since employees are considered the weakest link in ensuring the security of corporate data, this paper evaluates various employee characteristics (demographic, company-specific, and skills-based) to understand their relationship with security knowledge and likelihood of becoming a security breach victim. This paper accounts for four different, yet intertwined, security risk areas: phishing, passwords, BYOD and laptop usage in the organizational setting. Findings from a survey of 250 employees at a medium-sized US consulting firm identify higher-risk employees and evaluate the relationship between employee characteristics, understanding of security policies, and security risks. Based on these findings and separate interviews with security experts, the study concludes with a set of recommendations for companies to improve organizational security and reduce risks caused by human factors in securing organizations' endpoints.

SECURING THE HUMAN – EXPLORING CURRENT SECURITY AWARENESS AMONG EMPLOYEES AND FINDINGS WAYS TO IMPROVE IT IN THE ORGANIZATIONAL SETTING

By

Nina Sebescen

Thesis submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Master of Information Management
2015

Advisory Committee:

Professor Jessica Vitak, Chair
Professor Brian Butler
Professor Vedat Diker

Dedication

I dedicate this study to my family (mom, dad, Daniel, Ana, aunt Sonja, and my grandparents), who all stood by me throughout all this time of getting my degree. They taught me to work hard and never give up on my dreams, so this thesis, with the amount of work and dedication put in, will make them all really proud. And for my grandparents, who didn't get to see me graduate, I couldn't have done it without your love and support. My dearest, love you all!

Acknowledgements

This thesis has been a challenging yet very rewarding journey and I want to take this opportunity to thank all the people who stood by me and helped me make it happen.

First, I would like to thank my amazing mentor (chair) for her unmatched dedication, advice and support. Even when things didn't look quite right, one talk with my mentor was enough to lift my spirits and further motivate me to do better. Thank you so much Prof. Vitak for always believing in me.

I would like to thank my great committee members for always challenging me, and getting the best out of me, because they believed in my potential. I am so grateful for the learning opportunities and the growth I experienced thanks to them. Thank you so much Dr. Butler and Dr. Diker.

I would like to thank the company employees who helped me get the necessary approvals, all of the employees who helped me pre-test the survey, all of them who agreed to participate in the survey and all of them who were willing to further distribute the survey among their peers to increase response rates. Special thanks to all of the HR managers, security officer and the IT team who helped in the process. Thank you all. I couldn't have done it without you.

Also, I would like to thank all of the security experts who readily accepted to talk to me and share their insights. I truly appreciate you all spending the time to talk to me and discuss the important security matters. Also, thanks so much to Prof. Vitak, all of my colleagues (current and previous) and friends who helped me find the security experts I had a pleasure to interview. Thank you all!

Additionally, I would like to thank all of my friends, colleagues and managers for their understanding and support. I am so grateful for friends who stood by me when times

were tough, for colleagues always ready to cover work for me and managers for giving me the flexibility to find the balance between work and school. Thank you all so much!

Finally, I would like to thank my family (mom, dad, Daniel, Ana, my aunt Sonja, and my grandparents) for the unconditional love and support they gave me throughout this whole process. No matter how good or bad the times were, they always stood by me. I did it guys! Love you all!

Table of Contents

List of Tables

List of Figures

1. Introduction

Due to advancements in technology, companies nowadays store an increasingly large amount of personally identifiable information (PII) within their infrastructure, ranging from customers' date of birth, social security number, and credit card information to health records and financial statements. With the cost of security breaches skyrocketing in recent years ($3.5 million on average per company in 2014—a 15% increase compared to 2013) [1], these companies also have an increasing need to secure the client and employee data they store. To obtain people's PII or financial information, modern hackers try to find the easiest way to access companies' networks without being detected. Instead of actively attacking the network, many opt for passive attacks that target company employees—companies' "greatest asset and most vulnerable target" [5]—to access the network. That is, no matter how secure the computer system architecture is, it will only be as strong as its weakest link—the people accessing and interacting with the data [2]. It then comes to no surprise that three of the most prominent "human" vulnerabilities are also among the top ten security concerns for companies in 2015 [4, 5, 6, 7, 8], including:

1) Hackers' use of **advanced persistent threats (APT)** that use **social engineering techniques** (phishing, spear phishing, etc.) to access the company network [4, 10].
2) Employees' use of insecure **passwords** [6]
3) Employees' use of **personal devices** in an organizational setting (i.e., the "Bring Your Own Device" or BYOD problem) [4, 5, 7, 8].

Due to the existence of these threats and vulnerabilities, it is important to educate employees of their roles and responsibilities they have on keeping the organizations secure. Steve Durbin, a managing director of the Information Security Forum (ISF), points out that instead of mere security awareness programs on which companies spent millions of dollars in the past decade, "organizations need to make positive security behaviors part of the business process, transforming employees from risks into the first line of defense in the organization's security posture" [5].

With this in mind, this thesis evaluates employees' knowledge of and compliance with four areas of organizational security policies: (1) phishing, (2) password complexity, (3) the use of personal devices (BYOD), and (4) company-issued laptops in an organizational setting. The lack of knowledge in these areas on the employees' end poses significant risks to the organizations, as those areas require human activity that cannot be as easily secured or controlled as an IT infrastructure. This study moves beyond existing research on organizational security because:

1) It covers three[1] of the most important vulnerabilities within the top ten security concerns for organizations in 2015;
2) It provides a *more holistic* view of security threats organizations face by including perspectives from employees and security experts;
3) It investigates employee awareness around these concepts and identifies what they see as the biggest risks to data security; and
4) It makes recommendations for organizations to create a security-oriented culture among employees.

[1] Company-issued devices (i.e. laptops) are not among the top 10 threats but are included in this study

To accomplish these goals, the following paper evaluates how demographic (sex, age, education), company-specific (employment time, job role, security training, industry sector) and skills-based factors (perceived Internet knowledge, perceived technical knowledge, perceived awareness of security concepts and security policy) affect (1) employees' susceptibility of falling victim to a security threat, (2) actual knowledge of security terms and concepts and (3) actual knowledge of company's security policies.

To derive to findings, the paper reviews the extant literature on cybersecurity broadly, as well as the three specific results from a multi-methodological study including a survey of employees at a mid-sized US consulting firm and interviews with leading security professionals and researchers. Based on the results of these analyses, the thesis concludes with a set of "best practices" for enhancing organizational security and protecting data from attacks.

2. Literature Review

2.1 Cybersecurity Changes over Time

Technological advancements over the past 20 years have resulted in dramatic increases in the volume of data transmitted over the Internet [11]. Similarly, technological advancements have shifted companies' reliance on information technology from being a mean of system automation to become the crucial component of the companies' business [11]. However, the rapid technological advancement was not followed by the same rapid advancement in security implementation which led organizations to become vulnerable to attacks [11]. One common mistake organizations often make is that they do not realize (by judging how much they spend on security) how much of their business relies on the technology until it is too late [12].

Business-driven technological changes often impact security and drive security changes [7]. For example, in the 1990s, an increased demand for personal computing and storage led many IT organizations to standardize on a single platform, Windows, to reduce overhead [7]. Using a single platform, with its security vulnerabilities, had its drawbacks and eventually resulted in denial-of-service attacks in 2001-2003 timeframe [7]. Similarly, the demand to reduce costs and increase reach to a large customer base led to increases in companies using Internet-based technologies (e.g., email, company websites) for transmitting sensitive information [7]. Also, the demand for speed and quick retrieval of data led to hasty bug fixes without considering common vulnerabilities such as SQL injection and cross-site scripting [7]. This all has resulted in various security loopholes within organizational IT infrastructure that, in turn, makes phishing and similar attacks become common ways to attack the endpoints while staying undetected [7].

Today, globalization of offices, the use of virtualization and cloud computing technology, mobility, and bring your own device (BYOD) policies further complicate the security landscape of an organization [10]. In modern organizations, employees are often geographically dispersed around the world, storing and sharing information on mobile phones and in the cloud. Unlike traditional security models, which focus on tightly defined boundaries [11], new models (virtualization, cloud computing, BYOD, etc.), extend traditional boundaries and complicate the security landscape as they "… cause breakage in our ability to control or monitor the flow of sensitive information into and out of the organization" [7]. Consequently, these newer methods for sharing data have increased convenience at the cost of creating a "target-rich" environment for hackers to cause security breaches [10]. That is why user education in security and the understanding of the roles and responsibilities users play in keeping organizations secure are of utmost importance for years ahead. As Paul Ferrillo points out: "Network security takes a village, involving every employee of the company. A culture of security needs to be instilled in every person touching a keyboard or a keypad" [12].

With the amount of sensitive data that companies store and the evolution of the threat landscape from adolescent hackers to organized crime networks and state actor campaigns [17], security today has transformed to be "… a fundamental aspect that must be considered alongside all other core functions to ensure that the business can meet its strategic objectives" [11].

2.2 Recent Events and Looking Ahead

Based on a recent report from the Identity Theft Resource Center (ITRC), there were 783 reported data breaches in 2014—the highest number of data breaches reported ever [29]. This number marks a 27.5% increase compared to 2013 and an 18.3% increase compared to 2010, which previously held that record [29]. The report further shows that hacking has been a primary cause of data breach with the 8-year average of 21.7% [29].

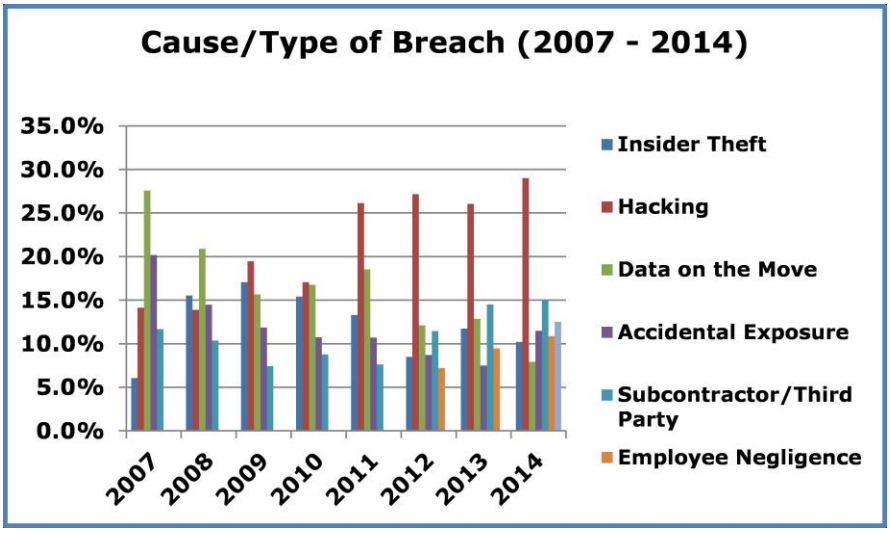

Figure 1: Data Breach Causes. Source: Identity Theft Resource Center [29]

In a global analysis on the cost of data breaches in 2014, the Ponemon Institute found that the cost of data breaches per organization was highest in the U.S. at $5.85 million per organization, costing organizations on average $201 per stolen record [32]. At the time of the study, the U.S. had the highest number of records breached with an average of 29,087 records per breach [32]. On the causes of data breaches in U.S. in 2014, research found that 44% were due malicious or criminal attacks, 31% due to the human factor and 25% due to the system glitch [32]. Three factors that can decrease the cost of the data breaches are strong security posture, well-defined incident response plan, and appointment of a Chief Information Security Officer (CISO) [32].

Twenty major data breaches in 2014 included famous retailers like Neiman Marcus, Michaels, UPS, PF Changs, Jimmy Johns', Home Depot, Staples, Kmart, Bebe, and Sony [30]. While customers' credit and debit card information was stolen for the majority of these breaches, Sony's data breach exposed over 47,000 social security numbers, 15,000 of which were of current or former employees [30]. Hence, security professionals believe that Sony's data breach should be an eye-opener for organizations to take cybersecurity seriously [12].

Among the top security concerns security professionals list for 2015 are four that will be discussed in this thesis. These include:

1) Social engineering, including advanced persistent threats (APTs), targeted attacks, and spear phishing [4, 10]
2) Insecure passwords [6]
3) Mobility and Bring Your Own Device (BYOD) [4,5,7,8][2]
4) User education and engagement as it relates to the above mentioned concerns [5, 9, 12]

Each of these concerns are described in more detail below.

2.2.1 Social Engineering

Advanced persistent threats (APT) are among the biggest concerns for organizations as they start with a hacker's use of social engineering techniques to gain access to the corporate network [10]. Social engineering attacks are:

> *"… security exploits that prey on the vulnerable attributes of humans rather than of technology. They stem from the fact that some criminals have found it easier to obtain the information needed to execute illegal activities from the people that operate the computers via some sort of social interaction than it is from the computers themselves"* [14].

[2] Company-issued devices (i.e. laptops) are not among the top threats but are included in this study

One example of social engineering is an exploit known as "Techie Talk" [15, 31]. This involves the "attacker" calling a low-level company employee and posing as a member of the technical support team, help desk, or a software maintenance company. The attacker alerts the employee to a "technical problem" that requires login credentials to fix. If successful, the attacker will be able to quickly access the company's network. Other common forms of social engineering are phishing and spear-phishing attacks [15], which are discussed below.

Jagatic and colleagues define phishing as:

> *"…a form of deception in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy entity… These attacks usually come in the form of an email that is transmitted to many different individuals that are unknown to the attacker under the guise of a notice from a large financial institution, online marketing firm, or a popular email site"* [14].

Unlike phishing, during which emails are sent to a wider population who may or may not be associated with the particular seemingly trustworthy entity, spear phishing (also known as context-based phishing) is an attack for which an attacker gains as much knowledge/context about the victim as possible prior to the attack by monitoring the victim's website and email use; the goal is for the attacker to credibly pose as one of the entities the victim is associated with [18]. Spear phishing attacks are powerful because they are harder to decipher than regular attacks, especially when playing on the emotional side of the victims in situations that deal with causes that victims support (charity, disaster, etc.) [18].

Parrish, Bailey, and Courtney describe the three components of every phishing attack [14]. These are also depicted in Figure 2 below.

a) **The hook** – email sent from a seemingly trustworthy entity with the goal to collect sensitive information

b) **The lure** - incentive (discounts, free offers, etc.) used to attract users to provide desired information to hackers

c) **The catch** - sensitive information that hackers wanted to obtain

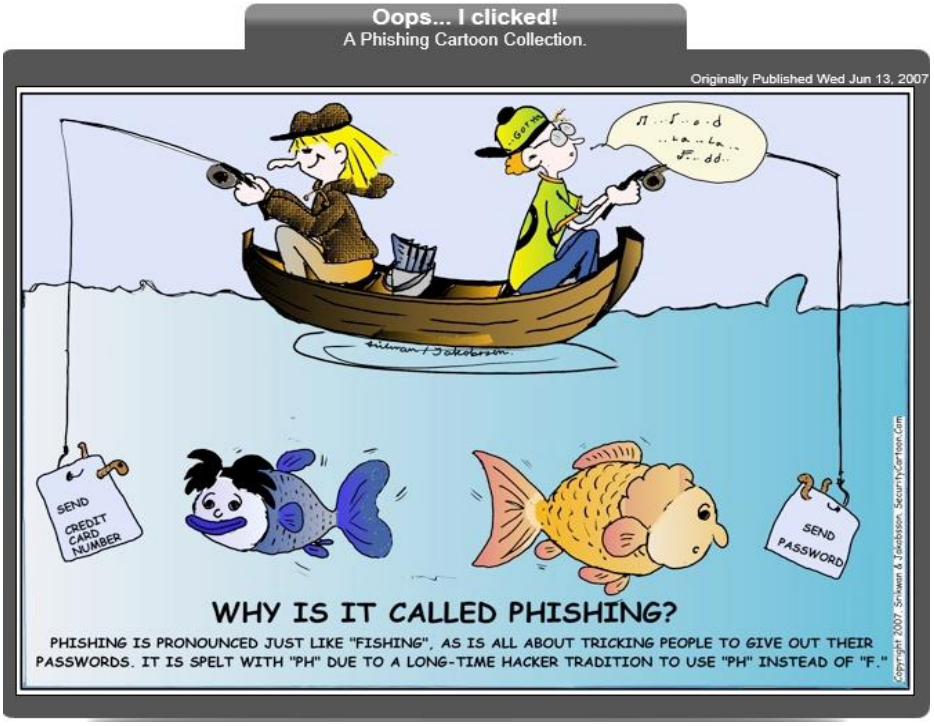

Figure 2: Phishing components analogy. Source: Security Cartoon [23]

Both phishing and spear phishing attacks are on the rise, and experts believe they will continue to be a significant organizational threat in 2015 [12]. Symantec research shows a 91% increase in spear phishing attacks from 2012 to 2013 [12] while Trend Micro found that 91% of cyber-attacks start with spear phishing [22]. As for the rising trend in phishing, the total number of phishing attacks in 2012 was 59% higher than in 2011 with over $1.5 billion spent globally in fraud damages [19]. Also, between Q4 2013 and Q1 2014, phishing increased by 10.7% [20]. Phishing emails were the most common form of

social engineering attacks organizations experienced in 2012, constituting 47% of all attacks [16].

Phishing targets vary by industry sectors. The highest percentage of phishing attacks, during the second quarter of 2014, were in the payment services industry at 39.8% followed by financial institutions at 20.2% [25]. The healthcare industry, rich with sensitive data, has seen a 100% increase in criminal attacks (not only phishing) between 2010 and 2014 [27]. However, since the beginning of 2014, with the increase of hacking and malware attacks, security professionals believe that phishing will be a major concern for healthcare in 2015 [26].

Phishing attacks often use one of the bigger financial institutions as the seemingly trustworthy entity to initiate an attack. A 2015 McAfee study shows that PayPal, Amazon, eBay, Bank of America, and HSBC are the most used "hooks" in phishing attacks [24]. In addition, phishing susceptibility varies across departments within an organization. McAfee survey of 60,000 business users found that employees in accounting, finance, and HR departments are more likely to fall for phishing attacks than employees in other departments [24]. This becomes a real issue for organizations given that these departments deal with most of the sensitive employee, client and financial data [24].

But why is phishing so popular among attackers? In their work, Parrish, Bailey, and Courtney note that phishing is popular because it provides a high return on investment (ROI) for attackers [14]. The cost of sending phishing emails continues to decrease - currently, an attacker can send tens of thousands of emails for less than $200, while a response rate as low as 1% can yield a 1000% return or higher [14]. Even though

viruses and spyware cause more overall damages than phishing, "the average amount of damage to the victim exceeds those damages eight times over (Singh, 2007)" [14]. In situations in which customer's credit card information is stolen, financial institutions often need to cover the cost associated with the damage [14]. "This makes phishing not only an individual problem, but an organizational problem as well with a ripple effect of higher costs to consumers as the institutions attempt to cover expenses caused by losses" [14].

2.2.2 People and Phishing

Why are people vulnerable to phishing? Sheng, Holbrook, Kumaraguru, Cranor, and Downs specify the four reasons that make people vulnerable to phishing [21]:

1) Focusing too much on the "look and feel" of the website to determine its legitimacy;
2) Not paying attention to the security indicators in the web browser;
3) Lack of knowledge or experience in identifying a phishing attack, even though awareness might exist; and
4) Perceived consequences of phishing attacks are not a good indicator of user's behavior.

Besides the four common reasons that make people vulnerable to phishing attacks, studies show that susceptibility to phishing attacks varies mainly with people's age and gender but those can be mediated using control variables such as education level, Internet activity, technological savviness, job roles and exposure to phishing training [21]. For example, Sheng et al. found that individuals 18-25 were most vulnerable to phishing attacks because younger people have less education and experience in navigating these

kinds of risks [21]. Similarly, Parrish et al. found that college students were "alarmingly susceptible to email phishing attacks" even though they are computer literate [14]. They also found that younger people are more susceptible to phishing due to having less prior negative experience (prior scams) compared to older people [14]. Darwish, Zarka, and Aloul explained that due to higher level of agreeableness, younger people are more likely to fall for phishing attacks, specifically, 62.3% from age 18-25 compared to 41.1% of 26 and older [28].

As previous research found, since younger people, merely due to their age, have less number of years of education, less number of years on the Internet and less exposure to security training [21], these three factors, combined with additional company-specific and perceived skills-based factors, will be used in this paper to determine the effect of age on phishing susceptibility, knowledge of security terms and concepts and knowledge of security policies. The effect of age will be examined both separately and in combination with other demographic, company-specific and skills-based factors.

When examining the relationship between gender and phishing susceptibility, Sheng et al. found that women are significantly more susceptible to phishing attacks than men due to their lower technical knowledge [21]. Technical knowledge, in this paper, can be defined as a combined effect of educational background and the current job role (technical vs. non-technical role). In regards to educational background, previous research found that while science and technology department students were invulnerable to phishing attacks compared to business, education and liberal arts students, all of them fell for spear phishing attacks (interestingly, highest percentage was among science

students) [28]. Sheng et al. further found that differences in income or education level did not affect gender differences on phishing susceptibility [21].

Darwish, Zarka, and Aloul explained that users who spend their time on the Internet doing online shopping and online banking are more likely to get phished than users who use Internet just to check their emails and do simple browsing [28]. They further explained that women's higher susceptibility to phishing attacks could be a result of their more agreeable personality and the fact that women do more online shopping than men ("… in 2010 women generated 58% of e-commerce dollars globally") [28].

This suggests that current technical knowledge (combined educational background and job role) and Internet activity can have an effect on the relationship between gender and phishing susceptibility. Additionally, since anti-phishing training is found to decrease overall phishing susceptibility by 40% [21], these three factors, combined with additional company-specific and skills-based factors, will be used in this paper to determine the effect of gender on phishing susceptibility, knowledge of security terms and concepts and knowledge of security policies. The effect of gender will be examined both separately and in combination with other demographic, company-specific and skills-based factors.

2.3 Passwords

Even though they are not the most secure way to protect organizational assets, passwords are still the most common form of user authentication [33]. To access organizational assets, it is imperative to establish and confirm user's identity [33]. Password authentication is a three step process: 1) the user enters a username (a commonly agreed upon code between the user and the company); 2) the user enters the

password (a code only known to him/her); and 3) the system verifies that the username/password pair matches with what is on file [33].

Zviran and Haga differentiate between the system-assigned passwords that are provided to users by administrators and user-selected passwords that are chosen by end-users [33]. System-assigned passwords, even though generally stronger than user-selected ones, are hard to remember for end-users and not as widely used in practice [33]. On the other hand, user-selected passwords are weaker but easily remembered by end-users [33]. Due to their simplicity, ease of administering and user-friendliness, user-selected passwords are the most popular mean of authentication [33]. All the below discussions about passwords are related to user-selected passwords.

On users' knowledge about password security, the literature highlights two different findings. On one side, Riley found that even though users know what it takes to create secure passwords, they do not apply those criteria in practice [34]. Likewise, users were able to identify the most common password recommendations, but the majority failed to identify the most secure combination of using numbers and special characters instead of letters [34]. On the other side, a CSID[3] study identified a disconnect between users' action and intention [35]. Despite the careless password practices (e.g., password reusability, sharing), 89% of users "feel secure with their current password management and use habits" [35]. This further strengthens the belief that even though weak passwords may cause data breaches, poor password habits are the result of user negligence rather than their malicious intent [36]. Company employees are unaware of security risks that come with creating weak passwords or using one password across multiple sites [36]. A

[3] CSID is "the leading provider of global enterprise level identity protection and fraud detection solutions and technologies." See www.csid.com

2014 Ponemon study found that 31% of data breaches in US have been caused by negligent employees or contractors [32].

So how do attackers exploit employee passwords? It is important to understand the attack methods that hackers use to be able to educate users on how to defend themselves (and the company) against the same. Besides phishing attacks during which employees give out their login credentials through phone or website, attackers can also use various password cracking methods to find user passwords [37]. The most common methods include guessing, dictionary attacks and brute-force attacks [37, 38].

Guessing works on creating lists of passwords that are most commonly used by users, including the list of "most commonly used passwords" by general public [39] and passwords created by meaningful items to the user such as name, family members' names, pet names, etc. [38]. Attackers check social networks and user online activity to learn about him/her and make an "educated guess" [37]. Similarly, dictionary attacks list the possible words that users can have as a password and often include few special characters at the beginning or at the end of the word to check for [38]. Important thing to note with dictionary attacks is that the password must exactly match the word in the list aka "dictionary" for the attack to succeed [38]. Brute-force attacks systematically check all the possible combinations for the password [38] by going through "all possible alpha-numeric combinations from aaa1 to zzz10" [37]. Due to their systematic check, they are pretty inefficient with long passwords so the best defense against them is password length [38].

To defend against the password cracking attacks, various password characteristics are considered, including length, composition, lifetime, and selection [33]. When it

comes to password length, even though technical specifications vary across operating systems, the recent versions of Windows (Windows Vista/7/ Windows Server 2008) allow passwords up to 127 characters[4] [40]. However, what is of more concern for organizations is minimum character length requirements [55], as brute force-style attacks are very efficient against shorter passwords [38]. Most organizations create security policies to enforce a minimum character length, generally 8 characters (although this varies by each company policy) [54, 55] and many require employees to change passwords regularly [56]. Shay et al. [41] found that NIST's (National Institute of Standards and Technology) assumptions about users creating passwords with minimum character length did not hold true, as the average password length for their users (students, faculty and staff of Carnegie Melon University) was 10 characters, which was 2 characters above the minimum length. Similarly, a CSID study found that American consumers choose passwords that are between 8 and 10 characters in length, with the average length 9.57 characters [35]. Additionally, Kelley et al. [42] found that password length is one of the most crucial aspects to consider in creating a strong password (16-character passwords without special characters were harder to guess than the 8-character password with mixed case and special characters); they suggest NIST should consider giving more value to password length.

Several factors play into password security, including composition, lifetime, and selection. First, the larger the character set (including uppercase and lowercase letters as well as special characters and symbols) from which the password is chosen, the harder it is to guess it [43]. That said, the majority of users (80%) in a 1999 study reported having

[4] Passwords this long are not practical for everyday use, but this threshold suggests we don't have to worry about the password's upper character limit in most modern operating systems.

alphabet-only-passwords [33]. Second, frequency of changing passwords may impact vulnerability. Zviran and Haga [33] found that 80% of Department of Defense (DoD) computer system users *never* changed their work passwords (mainframe computer system or its local area network). A more recent CSID study on American consumers found that 8% of users never change their passwords, 12% change it once a year, while 44% change it less than once a year [35]. It seems that users do not change passwords unless they are required to do so, hence to ensure that passwords are changed in a timely manner, organizations often reduce a given password's lifetime to 30, 60 or 90 days [56]. Finally, an individual's password selection method refers to how users choose their passwords (e.g., based on user's name, family member, or any meaningful detail or mix of meaningful details) [33]. Zviran and Haga [33] found that using passwords with meaningful details "limits the number of guesses a penetrator needs to make" and hence makes the password easier to guess. They further found that 78% of users had passwords based on meaningful details [33].

When choosing a password, there has to be a balance between its memorability and security [33]. If passwords are too complicated (depending on password selection method and composition), are not used very frequently or are frequently changed, they are more likely to be forgotten and hence written down [33]. Zviran and Haga found that if users write passwords down, they store them in insecure locations, which then changes the game of "guessing" to a game of "locating" for attackers [33]. Some of the most common places to store passwords include sticky notes posted on desks, keyboard or monitors, as well as on public white boards or notebooks, calendars and/or organizers left out on desks [33, 45]. The DoD's Password Management Guidelines strongly encourage

employees to take steps to protect written passwords so that they are "consistent with the damage that could be caused by their compromise" [33]. Research suggests that a large percentage of employees write down passwords at least occasionally [33, 41].

Demographic findings on password forgetting habits show that in the university setting with a new policy change, faculty and staff were three times more likely to forget their passwords than students while women were two times more likely to forget their passwords than men [41]. Shay et al. also found that age or IT experience did not show difference in password forgetting habits associated with the introduction of new policy [41]. However, CSID study found that 76% of individuals of age 18-24 are concerned with remembering passwords so they choose passwords to be secure but also easy to remember [35] which could explain why students forget passwords less than faculty.

Password sharing and reuse are big concerns for organizations nowadays [46]. A SailPoint survey found that 20% of employees share passwords with team members [46]. While people in IT related jobs and backgrounds are less likely to share their passwords with someone else, individuals age 22 and younger are most likely to share their passwords [41]. Office admins, managers, first level supervisors, and sales staff are also more likely to share their passwords than those in other job types [44].

Password reuse is a big risk for organizations [36]. A CSID study found that 61% of American consumers reuse their passwords across multiple sites [35] while a SailPoint survey found that 56% of company employees reuse passwords between corporate and personal apps [46]. "When a consumer reuses a password and login combination across multiple sites and one site is hacked, it opens the other sites to risk as well" [35]. This means that if employees use the same password for personal and work accounts, if their

personal account gets hacked (as it is generally less secure), the attackers will have an entry into the organization as well [36].[5] Hence, it is recommended that after major data breaches, company employees are notified about the breach and required to change their passwords [36].

Women and young individuals are more likely to reuse passwords across multiple sites [41, 35]. Women are significantly more likely to reuse passwords (considering slight modifications) than men (69% vs. 55%) [41]. Individuals in the age group 18-24 are more likely to reuse passwords than individuals from any other age group, with 76% of them admitting to reusing passwords across multiple sites [35].

As password length and composition are the most important factors in creating strong passwords [45], to determine overall password strength, password entropy or "guessability" are usually measured [42]. Entropy, or "the expected value (in bits) of the information contained in a string" [42] measures the password strength based on the password characteristics, including password length, character placement, number of each character type in the password, and the content of each character" [41]. Entropy can be used to measure the difficulty of guessing an individual password [41]. The study on guessability, i.e., "the time needed for an efficient password-cracking algorithm to discover a password," found that length is the most important factor when considering the password strength as a 16-character password without special characters and mixed case alphanumeric took longer to guess than the 8-character password with special characters and mixed case alphanumeric characters [42]. This suggests that "entropy might be useful

[5] This process, known as "daisy chaining," was described in detail by Wired's Mat Honan in 2012 after security flaws in Apple and Amazon's security policies, as well as his own poor password management, led to a number of his accounts being compromised. See www.wired.com/2012/08/apple-amazon-mat-honan-hacking

when considering an adversary who can make a large number of guesses, but not when considering a smaller number of guesses" [42].

In summary, the literature reviewed found a number of demographic and company-specific factors associated with employees' password habits. Employees in industry sectors such as financial institutions, military and telecommunications generally have better password management practices and longer job tenure positively affects the support for organizational security behaviors [44]. People in IT related fields (or IT background and education) have a lower tendency to share their passwords [41] while office admins, managers, first-line supervisors and sales staff are more likely to do so [44] as are individuals of age 22 and younger [41]. Individuals in the age group 18-24 are less likely to forget their passwords (they create passwords to remember them easily) [41] and are more likely to reuse the same password across multiple sites [35]. Women are more likely to forget passwords and reuse them across multiple sites compared to men [41].

Even though younger adults and women generally have less secure password habits, these factors combined with additional company-specific and skills-based factors, will be used in this paper to determine the effect of age and gender on password susceptibility, knowledge of security terms and concepts and knowledge of security policies. The effects of age and gender will be examined both separately and in combination with other demographic, company-specific and skills-based factors.

2.4 Bring Your Own Device (BYOD)

Bring Your Own Device (BYOD) or Choose Your Own IT (CYOIT) refers to the growing practice of using personal devices (smartphones, tablets and PCs) to connect to

the organizational network [7]. A PricewaterhouseCoopers study found that one third of small businesses and 75% of large businesses allow employees to connect to the organizational network with a personal device [47]. When it comes to the number of employees, 56% connected to the organizational network with a personal device in 2014, a 19% increase from 2013 [50]. BYOD has been identified as one of the increasing security concerns organizations will face in 2015 and beyond [4, 5, 7, 8]. Research by the Ponemon Institute found that while 9% of respondents in 2010 identified mobile devices as a risk to the IT environment, 73% expressed the same concern by the end of 2013 [48]. Additionally, 87% of IT managers believe that mobile devices, in the hands of negligent employees, presented the biggest security threat in 2014 [50].

Research by Gartner suggests that BOYD will become the "rule rather than the exception" in the near future [51]. Studies show that BYOD acceptance is a win-win situation for both employers and employees [49]. "BYOD strategies are the most radical change to the economics and the culture of client computing in business in decades. The benefits of BYOD include creating new mobile workforce opportunities, increasing employee satisfaction, and reducing or avoiding costs" [51]. Companies benefit in being able to achieve their goals without investing too much into software or hardware [49]. It also saves them money from buying corporate mobile devices or even desktops and laptops [49]. Employees also see a big benefit in BYOD. It increases employees' morale and job satisfaction as employees love the comfort of using their own devices [49]. Additionally, BYOD gives employees the flexibility to stay connected and get their work done anytime from anywhere which increases productivity [49]. BYOD also increases innovation, especially in the mobile app development area [51].

As seen in Figure 3 below, today's BYOD landscape consists of a multitude of connected devices. The most commonly used devices are Apple iPhones and iPads, Samsung Galaxy smartphones and Microsoft Windows tablets [51]. Security becomes increasingly difficult as the number and diversity of devices are incorporated into organizational network; for example, in 2012 more than 100 vulnerabilities have been found in iOS and Android devices [53]. This number is expected to increase as organizations allow more devices to connect to the corporate network, which in turn will attract more hackers to explore and find new vulnerabilities [53].

Figure 3: BYOD Landscape. Source: McAfee [51]

Despite its popularity, BYOD poses significant IT challenges when it comes to the complexity of securing the perimeter as well as the users [51]. With the introduction of BYOD, controlling the endpoints has become extremely hard (sometimes impossible) as the endpoint security became dependent on the users who own the device [7]. Moreover, users connecting to the corporate network with various different devices and different operating systems create challenges for IT administrators who need to

understand the security vulnerabilities for all the different devices [51]. Additionally, the myriad of apps that exist for each of the different operating systems (over one million for Apple Store and over 1.5 million for Google Play) makes it difficult to inspect, control and manage the apps that users install on their devices [51]. With users' tendency to share and store corporate data on the web (sending internal email to webmail), use cloud-based platforms (e.g., iCloud, Dropbox), and use their mobile devices over unprotected Wi-Fi networks, they are putting corporate data at risk [51].

Employees are often so focused on their productivity and getting their work done that they are unaware of the security risks that they pose to their organization [51]. Some of the most common mistakes that users make are [47, 51]:

1) They often do not implement screen-locking mechanisms on their devices (password, pin, pattern, biometrics, etc.). Studies show that users, especially under a lot of pressure to get the work done, find it annoying, or even intolerable, to constantly lock and unlock their devices. Hence, 40% of users do not have a password on their device.
2) They often do not apply updates to the mobile and laptop applications, even though it is widely known that mobile apps are not always very secure in their initial releases.
3) They keep both corporate and personal data on their devices and do not separate between the two. Without BYOD policies that will clearly delineate the two and make the corporate data secure (e.g. encryption), data loss or leakage with significant consequences is possible.

4) They may, unknowingly, store untrusted content on their devices (e.g. unsecure apps or phishing links in text messages).
5) They may share confidential information on social networking sites such as Facebook or Twitter.
6) They often use "free" unsecured Wi-Fi in cafes, airports and other public places which can open doors for hackers.

In addition to these common mistakes, security leaders cite data loss due to stolen or lost devices as their top concerns especially with devices that store unencrypted data and have no remote-wipe ability [52].

In this paper, company-supplied laptops will also be considered in a separate section as they pose significant security risks due to their dependence on end-users for the ultimate endpoint security. This is especially noticeable when it comes to employees' password and locking habits, corporate and personal data storage, desires for availability of particular software, connecting through unsecured Wi-Fi and leaving devices unattended [63].

Even though the literature reviewed did not evaluate how demographic, company-specific, or skills-based factors influence the knowledge of and adherence to companies' policies around BYOD and company-issued devices, this thesis will evaluate if any such differences exist.

3. Proposed Research Model and Hypotheses

In order to better understand how various factors influence employees' knowledge of security policies and ability to protect themselves from organizational security threats, this thesis evaluates organizational security using quantitative data collected from a survey distributed to employees of a mid-sized U.S. consulting firm and qualitative data from interviews with security experts. The primary focus of the data collections will be to understand the relationship between "human" factors (e.g., demographics, company-specific, skills-based) and an individual employee's security risk to the organization. More broadly, these data will be used to make recommendations for developing more inclusive strategies organizations can employ to increase knowledge of and compliance with organizational security policies.

Figure 4 below depicts the model being tested in this thesis. Independent variables (located in the leftmost column of the model) are grouped into three broad categories: demographic, company-specific and skills-based factors to determine how they, when examined both separately and combined, affect (if at all) the three dependent variables listed in the middle column: (1) likelihood of falling victim to a security threat, (2) knowledge of security related terms and concepts and (3) knowledge of current security policies.

Once analyzed, the findings from this model—combined with findings from interviews with security experts—will be used to create strategies that companies can implement to create/enhance their security awareness programs (right column).

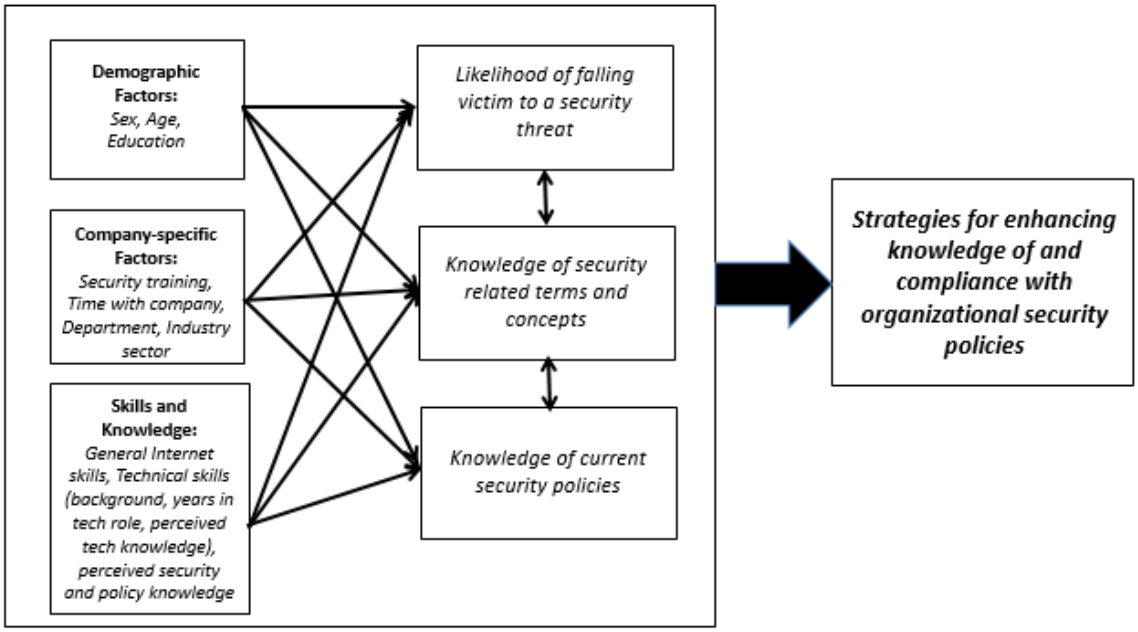

Figure 4: Proposed Model to be Tested

Hypotheses for the specified paths are as follows:

H1: Employees' demographic characteristics will significantly correlate with their (a) likelihood of falling victim to a security threat, (b) knowledge of security terms and concepts, and (c) knowledge of current security policies.

H1a: Female employees, in comparison to male employees, will have (a) a greater likelihood of falling victim to a security threat (b) less knowledge of security terms and concepts, and (c) more knowledge of current security policies.

H1b: Age will be (a) negatively correlated with likelihood of falling victim to a security threat, (b) positively correlated with the knowledge of security terms and concepts, and (c) positively correlated with the knowledge of current security policies.

H1c: Education will be (a) negatively correlated with likelihood of falling victim to a security threat, (b) positively correlated with the knowledge of security terms

and concepts, and (c) positively correlated with the knowledge of current security policies.

H2: Employees' company-specific factors will significantly correlate with their (a) likelihood of falling victim to a security threat, (b) knowledge of security terms and concepts, and (c) knowledge of current security policies.

H2a: Employees who have received security training on the job will have (a) a lower likelihood of falling victim to a security threat, (b) more knowledge of security terms and concepts, and (c) more knowledge of current security policies, compared to employees who have not received security training.

H2b: Employees' length of time with the company will be (a) negatively correlated with likelihood of falling victim to a security threat, (b) positively correlated with their knowledge of security terms and concepts, and (c) positively correlated with their knowledge of current security policies.

H2c: Employees in more tech-oriented departments (job roles) will have (a) a lower likelihood of falling victim to a security threat, (b) more knowledge of security terms and concepts, and (c) more knowledge of current security policies, compared to employees in less tech-oriented departments (job roles).

H2d: Employees in corporate sector[6] will have (a) a higher likelihood of falling victim to a security threat, (b) less knowledge of security terms and concepts, and (c) more knowledge of current security policies, compared to employees in all other sectors.

[6] That is, employees in corporate office management roles who don't visit client sites.

H3: Employees' perceived skills and knowledge will significantly correlate with their (a) likelihood of falling victim to a security threat, (b) knowledge of security terms and concepts, and (c) knowledge of current security policies.

H3a: Employees' perceived Internet skills will be (a) negatively correlated with likelihood of falling victim to a security threat, (b) positively correlated with their actual knowledge of security terms and concepts, and (c) positively correlated with their actual knowledge of current security policies.

H3b: Employees with a technical background will have (a) lower likelihood of falling victim to a security threat, (b) greater actual knowledge of security terms and concepts, and (c) greater actual knowledge of current security policies compared to employees without technical background, when compared to employees without a technical background.

H3c: Employees' length of time in technical role will be (a) negatively correlated with likelihood of falling victim to a security threat, (b) positively correlated with their actual knowledge of security terms and concepts, and (c) positively correlated with their actual knowledge of current security policies.

H3d: Employees' perceived technical knowledge will be (a) negatively correlated with likelihood of falling victim to a security threat, (b) positively correlated with their actual knowledge of security terms and concepts, and (c) positively correlated with their actual knowledge of current security policies.

H3e: Employees' perceived security awareness will be (a) negatively correlated with likelihood of falling victim to a security threat, (b) positively correlated with

their actual knowledge of security terms and concepts, and (c) positively correlated with their actual knowledge of current security policies.

H3f: Employees' perceived knowledge of company security policies will be (a) negatively correlated with likelihood of falling victim to a security threat, (b) positively correlated with their actual knowledge of security terms and concepts, and (c) positively correlated with their actual knowledge of current security policies.

4. Method

To address the research questions, the following data collection activities have been performed:

1) An invitation to participate in an online survey on employees' awareness on company's security policy and current security behaviors was distributed to 2000 employees from a mid-sized US IT consulting company.[7]
2) Interviews with the company's Security Officer, VP of Operations and two security team members (total of 4 interviews) were conducted in May 2015 to acquire information about the company's security policy, incidents caused by human behavior, and challenges in creating/enhancing user awareness programs.
3) Interviews were conducted with 15 security specialists from the private, educational, and government sectors to discuss security awareness best practices and initiatives they undertook when dealing with "Securing the Human" in organizational settings.

See Appendix A for the full survey instrument[8] and Appendix B for the interview protocol.

4.1 Data Collection Procedures

4.1.1 Surveys: Interested parties were directed to an online survey, hosted on SurveyGizmo, where they were presented with the consent form. If they agreed to participate, they were taken to the survey, which asked them general questions about current security policies and their thoughts about improving security awareness organization wide. Skip logic was used for follow-up questions; for example, people who

[7] The company being studied has requested its name be omitted from any write-ups of this study.

[8] Some of the knowledge questions were adapted from literature reviewed, namely [33] and [64].

received security training received additional questions compared to people who had not received training. The survey concluded with demographics. The full survey took 10-15 minutes to complete. By the end of the survey period of 9 days, a total of 266 responses were collected.

4.1.2 Interviews: Interview participants were contacted via email using known contacts in the security field. Interviews took place over the phone or through Skype. Interviews lasted, on average, 40 minutes (range: 22-76 minutes) and covered the most salient security topics organizations face. Participants were asked if they wished to use a pseudonym or if their real name could be used. The total of 19 interviews were conducted (including the company security team) and 18 were audio recorded. The interviews are currently being transcribed; therefore, in this paper, only high-level themes from the interviews will be presented as part of recommendations section. A future publication will include detailed results from the interviews.

4.2 Dependent Variables

There are three primary dependent variables included in this study: (1) employees' likelihood of falling victim to a security threat, (2) employees' knowledge of security related terms and concepts, and (3) employees' knowledge of company's current security policies. The outcomes of these three measures are then used to create strategies that companies can implement to create/enhance user awareness programs and create a security-oriented culture. All three dependent variables took into account the four components of the company's security policy: phishing, passwords, BYOD, and company-supplied laptop usage.

4.2.1 Likelihood of Falling Victim to a Security Threat

This set of variables measures employees' current security practices to determine what percentage of employees represents a significant security threat to an organization. Security practices measured include employees' ability to recognize malicious emails, understand employees' password habits and smartphone and laptop usage. Sample questions (which were multiple choice) include: "Have you ever clicked on a link in the email from your employer-supplied laptop or client PC that took you to a malicious site?"; "When creating a password in a work environment, what is your **top** priority?"; and "How often do you apply updates to your employer-supplied laptop, for applications which are NOT updated automatically by the employer?"

Variable recoding and averaging was used to create composite measures for each of the four threats. The below steps were performed:

1) To measure the likelihood of being a phishing victim, two items (clicking on phishing link and opening suspicious attachments) were combined into a single variable due to the low number of employees (i.e., 15) who either clicked on the link or opened a malicious attachment.
2) To measure the likelihood of being a password victim, a risk ranking system has been created for each password-related question to score individual answers based on the risk value from lowest (1) to highest risk (5) (see Table 1 below).

Table 1. Details on creating likelihood of being a password victim variable.[1]

	Risk Value				
Metric	**1**	**2**	**3**	**4**	**5**
Length	15+characters	11-15 characters	8-10 characters	5-7 characters	

Storage	Password manager	USB/External Drive In memory Only	Password protected document	Text file on computer In email received Hidden Sticky Notes Notebook	Sticky notes visible
Password Choice	Password Manager	Random combination of characters	Random meaningful combo	Not chosen by me (work) Pronounceable password	Meaningful detail Combination of meaningful details
Password Generator	Yes			No	
Priority	Strength & Security	Meeting corporations PWD requirements	Easy to remember	Easy to enter	
Usage	No			Yes	
Sharing	No			Yes	

[1] The risk value for each selected answer was determined based on security best practices, literature reviewed and in consultation with Raymond Gabler, founder and CEO of RGS Specialists.

For all the radio-button questions, values were recoded from the entered value to a risk value as given in Table 1 above. For all the checkbox questions (where multiple answers could be selected), the values were first recoded to a risk value, then summed up and averaged based on the number of choices an employee selected.

Once all the recalculated variables were created for different password parameters (length, storing, priority, etc.), the combined password victim variable was calculated as an average value of all seven password parameters. To minimize the number of missing values, the MEAN function of SPSS was used to calculate the average value as long as six of the seven password parameters were entered. For any case that had less than six password parameters, the average was not calculated; it was coded as missing and was dropped from analysis.

3) To measure the likelihood of being a BYOD victim, a risk ranking system has been created for each BYOD-related question to score individual answers based on the risk value from lowest (1) to highest risk (5) (see Table 2 below).

Table 2. Details for creating likelihood of being a BYOD victim variable.[1]

	Risk Value				
Metric	**1:**	**2:**	**3:**	**4:**	**5:**
Email Frequency	Less than a few days/week	Few days/week	Once a day	Few times a day	All the time
Phone Access		Outlook Webmail	Third-party app	Outlook App Default Mail App	
Phone OS	Blackberry	IOS	Android	Windows	
Lock	Biometrics	Biometrics/pin or password combo	Password only	PIN Only Pattern Only	No Lock
Lock Number of Characters	10+ character password	6-10 character password	0-5 character password	4+ digit numeric pin/pattern	4-digit numeric pin/pattern
Lock Contain	None of above	Family member's name (initials or full)	Family member's birthdate	Initials or full of your name	Your Birthdate
Updates	As soon as available	Once a week or longer interval	Only when automated updates	Once a month	Never
Anti-Virus	Yes			No	

[1] The risk value for each selected answer was determined based on security best practices, literature reviewed and in consultation with Raymond Gabler, founder and CEO of RGS Specialists.

For all the radio button questions, values were recoded from the entered value to a risk value as given in Table 2 above. For all the checkbox questions (where multiple answers could be selected), the values were first recoded to a risk

value, then summed up and averaged based on the number of choices an employee selected.

Once all the recalculated variables were created for different BYOD parameters (email frequency, lock, lock number of characters, etc.), the combined BYOD victim variable was calculated as an average value of all eight BYOD parameters. To minimize the number of missing values, the MEAN function of SPSS was used to calculate the average value as long as six of the eight BYOD parameters were entered. For any case that had less than six BYOD parameters, the average was not calculated; it was coded as missing and was dropped from analysis.

4) To measure the likelihood of being a laptop victim, a risk ranking system has been created for each laptop-related question to score individual answers based on the risk value from lowest (1) to highest risk (5) (see Table 3 below).

Table 3. Details for creating likelihood of being a laptop victim variable.[1]

	Risk Value				
Laptop	**1:**	**2:**	**3:**	**4:**	**5:**
Use Frequency	Every Day	Every work day	Few Times a week	Once a week	Once a month or less
Update Frequency	As soon as I see them	Once a week	Only when forced to	Once a month	Never

[1] The risk value for each selected answer was determined based on security best practices, literature reviewed and in consultation with Raymond Gabler, founder and CEO of RGS Specialists.

Since both of the laptop questions were radio-button questions, values were recoded from an entered value to a risk value as given in Table 3 above. Then the average value of the two variables was calculated to get the laptop victim variable. For every case, the average was calculated as long as both of the

laptop variables had valid values; otherwise, it was coded as missing and was dropped from analysis.

4.2.2 Knowledge of Security Terms and Concepts

The knowledge of security terms and concepts variable measures employees' comprehension of various security terms. For each survey item, a correct answer was given two points and an incorrect answer was given zero points (see Table 4 below).

Table 4. Computing knowledge of security variable.

Question	**Knowledge Value**	
Knowledge of security concepts	**Not Correct**	**Correct**
What is the goal of encrypted data transmission?	The data is protected against viruses | The data is not corrupted during transmission | Only the user herself can see the data	The data can't be eavesdropped
What is malware?	Software which is not working properly Software which is automatically updating itself A faulty technical device	Software which is unwanted and might be harmful
What is phishing?	The analysis of user's browsing behavior | The sending of unwanted ads | The uninstalling of software that needs too much resources	A form of deception using email or messaging in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy entity
What is social engineering?	Distribution of software-testing tasks to several engineers in order to find security leaks | The development of software for social networks | The development of charitable apps which are free of charge	Psychological manipulation of people into performing actions or divulging confidential information
How can you recognize malicious emails?	None of the above	By email sender | By email subject | By email content | By the seeming urgency

What helps you recognize a suspicious website?	None of the above	Checking the URL | Using toolbar tools like McAfee Site advisor or similar | Checking website safety ratings and reputation | Checking the site's digital certificate
What makes the password strong?	None of the above	Length Randomness Avoidance of dictionary words The use of alphanumeric and special characters
How can a device (laptop, smartphone) be protected from viruses?	None of the above	Always keep software and OS up-to-date | Avoid downloading unknown software (apps) from the Internet | Use antivirus to scan your device often | Avoid visiting unfamiliar or unknown websites | Avoid using unsecured wireless networks

For all the radio-button questions, values were recoded from the entered value to a point value as given in Table 4 above. For all the checkbox questions (where multiple answers could be selected), the values were first recoded to a point value, then summed up and averaged based on the number of choices an employee selected.

Once all the recalculated variables were created for individual knowledge questions, the combined security knowledge variable was calculated as an average value of the eight knowledge questions. To minimize the number of missing values, the MEAN function of SPSS was used to calculate the average value as long as six of the eight knowledge questions were answered. For any record that had less than six knowledge questions answered, the average was not calculated; it was coded as missing and was dropped from analysis.

Additionally, after the security knowledge questions were asked, another question was raised to ask employees how confident they were in their answers to these

knowledge questions. Their confidence levels were then tested against their knowledge score.

4.2.3 Knowledge of Current Security Policies

This variable measures employees' knowledge of the company's security policy, specifically, as it relates to general security policy (have employees read it, have they understood it) and password requirements based on the policy. For each security policy related question, the correct answer was given two points, partially correct answer one point, and incorrect answer zero points (see Table 5 below).

Table 5. Computing knowledge of general of organizational security policies.

Knowledge of current security policies	**Knowledge Value 0-2[1]**		
General security policies	**Not Correct**	**Partially Correct**	**Correct**
Does your employer have a security newsletter?	No		Yes
How often does the company security newsletter come out?	About once a quarter | About once a year | I am not sure	About once a week	About once a month
Does your company have a security policy?	No		Yes
How long has it been since your employer last updated its security policy?	About a year | I am not sure	About one month | About six months	About three months
Have you read the most current security policy?	No, but I plan to read it | No, and I hadn't planned to read it	I skimmed through it	Yes, thoroughly
Did you understand the security policy?	No, I need help to understand it	I could use some explanations to better understand it	Yes, it is all straight forward
Password policies	**Not Correct**	**Partially Correct**	**Correct**
What is the current password expiration timeframe based on your employer's password policy?	30- | 60- | 120 days | There is no expiration		90 days

What is the maximum number of password retries before your employer account gets locked?	10 | 20 | Unlimited		3[1] | 5
What is the current minimum password length for your organization?	There is no minimum | 5- | 10- | 15- characters		8 characters
When you change your password on your employer-supplied laptop, what is the minimum number of characters you need to change?	0 | 4 | 6 | 8 | I am not sure		1

[1] The maximum number of password retries for the surveyed company is 4, hence both 3 and 5 were accepted as correct answers.

Since all the policy-related questions had radio button response options, values were recoded from the entered value to a point value as given in Table 5 above. Then, all the general security policy questions (excluding passwords) were summed and averaged. To minimize the number of missing values, the MEAN function in SPSS was used to calculate the average value as long as four of the six general policy questions were answered. For any case that had less than four questions answered, the average was not calculated; it was coded as missing and was dropped from analysis.

Similarly, all the password policy related questions were summed up and averaged using the MEAN function in SPSS. The average value was calculated as long as three of the four password policy questions were answered. For any case that had less than three questions answered, the average was not calculated; it was coded as missing and was dropped from analysis.

Finally, the general security policy and password security policy variables were summed up and averaged to get the final variable that measures the knowledge of company's security policies. To minimize the number of missing values, the MEAN

function of SPSS was used to calculate the average value as long as one of the two final policy values (general or password) were calculated.

4.3 Independent Variables

All of the independent variables had to be recoded or slightly modified to be suitable for analysis.

4.3.1 Demographic Factors

Demographic factors, considered in analysis, include sex, age and education. For ANOVAs and t-tests, the *age* and *education* variables were converted into simple categorical variables. *Sex* (M=0.30, SD=0.46) was left unchanged. For regression analyses, the full (ratio or ordinal) variables were used.

Age (M=37.94, SD=11.18) was divided into four groups and was calculated using quartiles. Groups are as follows:

- Group 1: 18-28 years
- Group 2: 29-36 years of age
- Group 3: 37-47 years of age
- Group 4: 48+ years of age

Education (M=4.25, SD=0.59) was collapsed into three categories:

- Group1: Employees without Bachelor's degree
- Group2: Employees with Bachelor's degree
- Group3: Employees with higher degrees (Master's, PhD, professional, etc.)

4.3.2 Company-Specific Factors

Company-specific factors, considered in analysis, include security training, employment time with the company, job role (department), and the industry sector.

When it comes to *security training* (*M*=0.36, *SD*=0.48), only 35.6% of company employees received security training in 2015 (this number includes training received at the client sites as well). Of those, 66.3% received training in social engineering, 58.4% in password requirements, 33.7% in BYOD policies and 69.7% in proper company-supplied laptop usage.[9]

When analysis was performed for a particular security threat, two factors were considered: whether an employee received training or not, and the training topic (e.g., phishing topic for phishing security threat). For the knowledge of security terms and concepts and knowledge of policies DVs, the only factor considered was whether an employee received security training or not. No changes (variable recoding) were performed for either of the factors.

Employment time (*M*=3.91, *SD*=4.40) was calculated using data from the number of years and months the participant reported being employed by the company. Additionally, ranges of employment time were calculated based on quartiles:

- Group 1: Less than one year
- Group 2: 1-2.5 years
- Group 3: 2.51 -4.99 years
- Group 4: 5+ years

[9] Employees could select multiple responses for this question.

Job role initially started as department variable but due to too many variations, three broad categories were created and used in all analyses.

- Group 1: Employees in office management (including sales, HR, Admin work, etc.)
- Group 2: Employees working as Project Managers and Business Analysts
- Group 3: Employees working in IT (including programming, testing, product support, system analysis, etc.)

Industry sector variable has also been condensed due to too many variations. It was eventually divided into six categories based on the number of employees in each sector. This variable was used in all analyses.

- Group 1: Financial sector
- Group 2: Healthcare
- Group 3: Utilities
- Group 4: Retail
- Group 5: Corporate (within the company)
- Group 6: Other (includes transportation, manufacturing, government, legal, etc.)

4.3.3 Perceived Skills and Knowledge Factors

Employees' perceived skills and knowledge factors include: perceived Internet knowledge, technical skills, and perceived knowledge of security awareness and policies.

Perceived Internet knowledge (M=6.3, SD=1.07) variable was created as an average of two variables (perceived knowledge of (a) web skills and (b) Internet-specific concepts, with 1 being the lowest and 5 being the highest value). Since Internet-specific knowledge measures harder concepts (e.g., phishing, cookies) than the web skills variable

(e.g., online shopping), the value was multiplied by two (weighted higher) before the variables were averaged. This way the estimated average of two variables was a better representation of an employee's perceived Internet knowledge. For ANOVAs, ordinal variables were created based on the quartiles as given below. For regressions, continuous variables were used.

- Group 1: 0 - 5.5 points
- Group 2: 5.75 - 6.5 points
- Group 3: 6.75 - 7.0 points
- Group 4: >7 points

Technical skills were analyzed through three different variables: technical background (yes or no), number of years in a technical role, and perceived technical knowledge. For *technical background* (M=0.85, SD=0.36), there were no additional modifications.

Number of years in a technical role was divided into four groups based on quartiles:

- Group 1: 0 - 5.0 years
- Group 2: 5.01 -13.00 years
- Group 3: 13.01 - 20 years
- Group 4: 20.01+ years

Perceived technical knowledge (M=3.97, SD=0.87) was divided into three groups based on quartiles:

- Group 1: 1 - 3
- Group 2: 3.50 - 4
- Group 3: 4.50 - 5

Perceived awareness of security concepts and policies are two different variables. Those were mainly analyzed separately (although an aggregated variable was also created).

Perceived security awareness (M=4.11, SD=0.78) was divided into four groups based on quartiles:

- Group 1: 0 - 3.50
- Group 2: 3.51 - 4.00
- Group 3: 4.01 - 4.50
- Group 4: 4.51+

Perceived security policy knowledge (M=3.7, SD=0.95) was also divided into four categories based on the quartiles:

- Group 1: 0 - 3
- Group 2: 3.1 - 4
- Group 3: 4.1 - 4.5
- Group 4: >4.5

The combined variable, *perceived security policy and awareness knowledge* (M=3.91, SD=0.76), was calculated as the average value of the two variables above. The combined variable was divided into four groups based on the quartiles:

- Group 1: 1-3.25
- Group 2: 3.50-4
- Group 3: 4.25 -4.50
- Group 4: 4.75-5.00

4.4 Data Analysis

Before running analyses, a correlation matrix was evaluated with all the variables in the model (see Appendix C). The correlations were examined for potential multi-collinearity issues; if any variables appeared too similar, the weaker variable was dropped from analyses. This was the case with *age* and *number of years in a technical role* variables. Due to high collinearity (r=0.789, p<.001), *number of years in a technical role* variable was dropped from multivariate analyses.

Although the initial model posits relationships between the three dependent variables, there were no significant correlations between any of these factors, so no additional analyses were conducted.

Next, each of the independent variables from the three groups (demographic, company-specific and skills-based) were tested against the three dependent variables. T-tests and ANOVAs looked for differences between various groups for a specific dependent variable.

Finally, stepwise multiple regressions were run for each of the dependent variables. Each step contained a group of independent variables based on the proposed model (demographic variables, company-specific variables, and general skills and knowledge variables) to determine what the unique contribution is of each group of variables in explaining variance in the dependent variables.

5. Findings

Findings presented below are based on survey responses from 250 company employees (16 cases were deleted due to missing data). The study sample (which truthfully represents the company population[10]) includes employees from diverse age and employment duration groups but less diverse with other factors. The majority of employees are males, well-educated (Bachelor's and higher) with a technical background, facts to be considered when interpreting the study results. Sample demographic data is included in Table 6 below.

Table 6. Demographic Data (N=250).

Characteristics	Mean	SD	Specific Values	Percentages
Age	37.94	11.18	18-28 years	28.70%
			29-36 years	22.60%
			37-47 years	26.50%
			48+ years	22.20%
Sex	n/a		Male	70.40%
			Female	29.60%
Education	4.25	0.59	Without Bachelor's Degree	2.80%
			Bachelor's Degree	70%
			Higher Education	27.10%
Technical Background	n/a		Yes	84.60%
			No	15.40%
Employment Time	3.91	4.4	0-0.999 years	26.80%
			1-2.50 years	26%
			2.51 -4.99 years	20.80%
			5+ years	26.40%

ANOVAs were run for every independent variable to examine variance for a specific dependent variable. Findings below are organized by dependent variables.

[10] This was confirmed with the organization's HR manager.

5.1 Likelihood of Falling Victim to a Security Threat

ANOVAs show that various demographic, company-specific, and skills-based variables significantly affect the likelihood of employees becoming victims of security threats due to phishing, passwords, BYOD and the use of company-supplied laptops. All of these security threats were tested both separately and combined across all the demographic, company-specific, and skills-based variables.

5.1.1 Phishing Victims

Very few company employees reported ever clicking on a phishing link and/or opening a malicious attachment. Specifically:

1. 4% of employees (10 out of 250) said they have clicked on a link in email; 100% of those provided credentials on the site, and only one user reported a negative impact (i.e., a virus deleted all the .pst files and those backed up by the company).
2. 2% of employees (5 out of 250) said they have opened a malicious attachment sent via email; 100% of those reported a negative impact (e.g., deletion of .pst files, impact using IE, corrupted desktop/laptop).

The small number of "successful" phishing attacks could be due to the fact that the sample is male-dominated, well-educated, and technically savvy, which all affects phishing susceptibility [21]. Additionally, the small number of employees affected by phishing techniques created significantly imbalanced analysis categories. While none of the independent variables significantly affected the likelihood of an employee becoming a phishing victim (see Tables 7 and 8 below), this finding should be further evaluated with larger samples.

Table 7. ANOVA findings for the likelihood of being a phishing victim.

Variable Categories	Independent Variables	Mean Comparison
Demographic variables	Sex	$t(232)=-0.006$, *ns*
	Age	$F(3,223)=2.07$, *ns*
	Education	$F(2,240)=0.42$, *ns*
Company-specific variables	Security training (Yes/No)	$t(234)=1.365$, *ns*
	Phishing training	$t(56)=-1.427$, *ns*
	Employment time	$F(3,243)=0.651$, *ns*
	Job role	$F(2,238)=0.838$, *ns*
	Industry sector	$F(5, 221)=0.64$, *ns*
Skill-based variables	Internet skills	$F(3,241)=0.547$, *ns*
	Tech background	$t(44)=0.852$, *ns*
	Time in tech role	$F(3,197)=1.524$, *ns*
	Perceived tech knowledge	$F(2,238)=0.762$, *ns*
	Perceived security awareness	$F(3,242)=1.66$, *ns*
	Perceived security policy knowledge	$F(3,241)=0.199$, *ns*

Table 8. Regression findings for the likelihood of being a phishing victim.

Independent Variables	Model 1: Demographic Factors		Model 2: Company Factors		Model 3: Skills-based Factors	
	ß	**p-value**	**ß**	**p-value**	**ß**	**p-value**
Sex	.021	.774	.021	.787	.021	.803
Age	.120	.101	.117	.133	.105	.195
Education	-.003	.968	.005	.950	.015	.846
Security training			-.095	.195	-.100	.187
Employment time			.012	.873	.009	.913
Job role			.003	.966	.014	.870
Industry sector			-.014	.845	-.013	.858
Internet skills					-.089	.391
Tech background					-.020	.829
Perceived tech knowledge					.080	.482
Perceived security awareness					-.046	.625
Perceived security policy knowledge					.060	.487
F test	$F(3,199)=.91$, *ns*		$F(7,199)=.65$, *ns*		$F(12,199)=.50$, *ns*	
Adjusted R^2	**-.001**		**-.013**		**-.031**	

5.1.2 Password Victims

Demographic, company-specific, and skills-based variables were evaluated to determine which variables cause the highest likelihood for employees to be password victims. One-way ANOVA looked at differences between various groups for each independent variable. ANOVA findings are listed in Table 9 below (significant findings are bolded).

Table 9. ANOVA findings for the likelihood of being a password victim.

Variable Categories	Independent Variables	Mean Comparison
Demographic variables	**Sex**	**t(237)=-4.1, *p*<.001**
	Age	***F*(3,228)=5.86, *p*<.001**
	Education	*F*(2,245)=0.736, *ns*
Company-specific variables	**Security training (Yes/No)**	**t(247)=2.089, *p*<.05**
	Password training	t(87)=0.20, *ns*
	Employment time	*F*(3,248)=0.219, *ns*
	Job role	***F*(2,243)=7.2, *p*<.001**
	Industry sector	***F*(5,225)=2.359, *p*<.05**
Skill-based variables	**Internet skills**	***F*(3,246)=12.7, *p*<.001**
	Tech background	**t(244)=3.504, *p*<.001**
	Time in tech role	***F*(3,202)=6.408, *p*<.001**
	Perceived tech knowledge	***F*(2,243)=24.1, *p*<.001**
	Perceived security awareness	***F*(3,247)=7.12, *p*<.001**
	Perceived security policy knowledge	***F*(3,246)=4.42, *p*<.01**

ANOVA findings show that from demographic variables, sex and age significantly affect the likelihood of being a password victim. Females are at higher risk of being password victims than males, specifically when it comes to password storing ($p<.05$), password choice ($p<.01$), password priority ($p<.01$), password sharing ($p<.01$), and the use of random password generators ($p<.01$). Findings show that even though a

large number of females store passwords in their memory (head), they are more likely to store passwords in less secure places such as sticky notes, text files on the computer, in the emails and password-protected documents. They are also more likely to choose passwords based on meaningful details that are easy to remember, share passwords with others and reuse corporate passwords for personal matters (not significant). However, males are more likely to use random password generators for creating passwords than females.

Looking at age, young employees (ages 18-28) are at the highest risk of being password victims (significantly different from employees in age group 37-47, $p<.001$), specifically when it comes to password choice, password priority and password personal use. Employees ages 18-28 are most likely to choose passwords based on a combination of meaningful details (significantly different from age group 37-47 ($p<0.001$), and that are easy to remember and enter (significantly different from ages 26-36, $p<.05$). They are also most likely to reuse corporate passwords for personal matters (significantly different compared to employees in age groups 37-47 ($p<.05$) and 48+ ($p<.01$).

Employees with security training have better password habits than employees without training; hence they are less likely to be password victims. This is mainly visible with password priority as employees without training are more likely to choose passwords that are easy to enter and remember (which are then also easier to break) compared to employees who received training who are more likely to choose passwords based on strength and security ($p<.01$).

Employees who work in office management roles (HR, sales, finance, management, etc.) are at the highest risk of being password victims (significantly different from employees in IT roles, $p<.001$), specifically when it comes to password storing, password choice and password priority. Employees in office management roles are more likely to store passwords in riskier places (text files on the computer, email, hidden sticky notes, notebook, password protected doc) (significantly different from BA/PM ($p<.01$) and IT roles ($p<.001$)), choose passwords that are more predictable (significantly different from IT roles ($p<.05$)) and choose passwords that are easier to remember (significantly different from IT roles ($p<.05$)).

Employees working in various industry sectors also have a different likelihood of being password victims. In line with the findings from job role variable, employees working in corporate offices (including various geographical regions) are most likely to store password at insecure places and hence being password victims. Password storing habits of employees in corporate offices significantly differ from employees working in financial ($p=.01$), healthcare ($p<.001$), utilities ($p=.01$), retail ($p<.001$) and other sectors ($p<.001$). These findings could be due to the low number of people from corporate offices (5.7%).

Interestingly, employees working in financial sector are more likely to share passwords with others than people working in any other sector (this is significantly different compared to other sectors such as legal, government, transportation, manufacturing, etc. ($p=.013$).

Looking at skills-based factors, every independent variable examined is significantly associated with employees' likelihood of becoming a password victim. The more perceived knowledge and experience an employee has in using the Internet, dealing with technology and around general security awareness (including company's security policy), the less likelihood of an employee being a password victim.

Once all the individual factors were tested in ANOVA, an OLS regressions was run to observe the full model. Standardized betas for each model can be found in Table 10 below (significant findings are bolded).

Table 10. Regression findings for the likelihood of being a password victim.

Independent variables	**Model 1: Demographic Factors**		**Model 2: Company factors**		**Model 3: Skill based factors**	
	ß	**p-value**	**ß**	**p-value**	**ß**	**p-value**
Sex	**.248**	**.000**	**.202**	**.004**	.121	.097
Age	-.122	.080	**-.145**	**.043**	-.099	.160
Education	.020	.774	.010	.881	.018	.780
Security training			-.093	.167	-.056	.398
Employment time			.005	.943	.021	.753
Job role			**-.231**	**.001**	-.145	.051
Industry sector			-.087	.202	-.066	.310
Internet skills					-.135	.138
Tech background					.034	.666
Perceived tech knowledge					-.191	.058
Perceived security awareness					-.037	.658
Perceived security policy knowledge					-.107	.160
F test	$F(3,203)=6.21$, $p<.001$		$F(7,203)=5.11$, $p<.001$		$F(12,203)=5.30$, $p<.001$	
Adjusted R^2	**.071**		**.124**		**.203**	

In step one of the regression model (demographic variables), sex is the only significant predictor for an employee being a password victim. In step two, which adds company-specific variables, sex, age, and job role are significant predictors; however, job role (*ß*=-.23) has a stronger effect than sex or age. In step three, adding the skills-based variables mitigates the effects of other variables and no significant variables emerge as significant. However, job role and perceived technical knowledge show marginal significance in predicting an employee being a password victim. This suggests that one's job role (i.e., day-to-day work activities) and perceived technical knowledge (which goes hand in hand with job role) are most likely to determine employee's likelihood of being a password victim.

The adjusted R^2 value has been increasing with each step which further implies that besides making conclusions based on employee's demographic characteristics, company-specific and skills-based characteristics need to be checked as well to get the better estimate of employee's likelihood of being a password victim. However, since the adjusted R^2 predicts only 20.3% of the variable, future studies should examine additional factors that could predict employees' likelihood of being password victims.

5.1.3 BYOD Victims

Demographic, company-specific and skills-based factors were evaluated to determine which factors cause the highest likelihood for employees to be BYOD victims. First, one-way ANOVA was run to see the difference between various groups for each independent variable. ANOVA findings are listed in Table 11 below (significant findings are bolded).

Table 11. ANOVA findings for the likelihood of being a BYOD victim.

Variable Categories	Independent Variables	Mean Comparison
Demographic	Sex	*t*(190)=-0.7, *ns*

variables	**Age**	***F*(3,184)=2.84, *p*<.05**
	Education	*F*(2,196)=1.965, *ns*
Company-specific variables	Security training (Yes/No)	*t*(175)=1.539, *ns*
	BYOD training	*t*(70)=0.729, *ns*
	Employment time	*F*(3,198)=1.063, *ns*
	Job role	*F*(2,193)=1.213, *ns*
	Industry sector	*F*(5,176)=1.83, *ns*
Skill-based variables	Internet skills	*F*(3,197)=1.98, *ns*
	Tech background	*t*(195)=1.734, *ns*
	Time in tech role	*F*(3,160)=0.821, *ns*
	Perceived tech knowledge	***F*(2,194)=3.293, *p*<.05**
	Perceived security awareness	*F*(3,198)=1.586, *ns*
	Perceived security policy knowledge	*F*(3,197)=2.22; *ns*

ANOVA findings show that from demographic and skills-based variables, age and perceived technical knowledge significantly affect the likelihood of being a BYOD victim. Employees in age group 18-28 are at highest risk of being BYOD victims as they are least likely to use antivirus software on their smartphones compared to other age groups ($p<.05$; no significant difference between particular groups).

Employees with higher perceived technical knowledge are less likely to be BYOD victims compared to employees with lower perceived technical knowledge (significant difference between the lowest and highest knowledge groups, $p<.05$). This difference likely stems from the frequency of smartphone app updates. The more perceived technical knowledge employees have, the more frequently they update their apps (significant difference found between lowest and medium ($p<.01$) and lowest and highest knowledge groups ($p<.001$)).

Even though specific BYOD training didn't yield significant results, employees who received any security training are at less risk when it comes to phone locking than

employees without training ($p<.05$). This is best portrayed with the fact that 19.7% of employees without training don't lock their smartphones compared to 6.9% of employees who received training ($X^2=9.6$, *ns*). But the fact that security training is not significant for the aggregated BYOD victim variable is concerning. This could be due to the quality and relevance of the topic, and mode of training received which should be evaluated further in future studies.

Interestingly, employees in IT roles are at highest risk when it comes to phone locking compared to both BA/PM roles ($p<.05$) and office management roles ($p<.05$). This is due to the fact that 60% of IT employees use pins or sliding patterns to lock their smartphones, while employees in office management and BA/PM roles (~50% of both groups) use passwords and/or biometrics. This difference could stem from different OS usage (employees in IT roles use Androids and iPhone equally while BA/PM and office management roles mainly use iPhones) as well.

Employees in office management roles check their work emails on the phone significantly more than employees in IT roles ($p<.05$) and update their apps less frequently than employees in BA/PM roles ($p<.05$) and IT roles ($p<.05$).

Employees who have higher Internet skills ($p<.01$), technical background ($p<.001$) and perceived security awareness ($p<.01$) generally update apps more frequency than employees with less knowledge in these areas. Additionally, employees with higher Internet skills generally use longer passwords to lock their smartphones compared to employees with fewer reported skills ($p<.05$).

Once all the individual factors were tested in ANOVA, the full model was tested via OLS regression to determine the major predictors for becoming a BYOD victim. Regression findings can be found in Table 12 below (significant findings are bolded).

Table 12. Regression findings for the likelihood of being a BYOD victim.

Independent variables	**Model 1: Demographic Factors**		**Model 2: Company factors**		**Model 3: Skill based factors**	
	ß	**p-value**	**ß**	**p-value**	**ß**	**p-value**
Sex	.049	.544	.016	.846	-.066	.468
Age	.055	.493	.002	.985	.043	.623
Education	**-.181**	**.024**	**-.162**	**.046**	**-.164**	**.045**
Security training			-.073	.360	-.051	.541
Employment time			.118	.164	.142	.099
Job role			-.107	.182	-.018	.847
Industry sector			-.029	.724	-.017	.831
Internet skills					.085	.449
Tech background					-.035	.733
Perceived tech knowledge					**-.254**	**.045**
Perceived security awareness					-.021	.831
Perceived security policy knowledge					-.042	.644
F test	*F*(3,161)=1.99, *ns*		*F*(7,161)=1.71, *ns*		*F*(12,161)=1.51, *ns*	
Adjusted R^2	**.018**		**.03**		**.037**	

In step one of the regression model, education is the only significant predictor for an employee being a BYOD victim. Education remains significant with the addition of company-specific factors (step two) and skills-based factors (step three). In other words, the more education and more perceived technical knowledge an employee has, the less likely s/he will become a BYOD victim. In addition, perceived technical knowledge is also significant, with higher perceived technical knowledge negatively associated with becoming a BYOD victim. It is important to note though that the adjusted R^2 is quite low

(explaining just 4% of the variance in the full model), suggesting that additional factors are influencing the DV.

5.1.4 Laptop Victims

Demographic, company-specific and skills-based factors were evaluated to determine which factors cause the highest likelihood for employees to be laptop victims. One-way ANOVA was run to see the difference between various groups for each independent variable. ANOVA findings are listed in Table 13 below (significant findings are bolded).

Table 13. ANOVA findings for the likelihood of being a laptop victim.

Variable Categories	Independent Variables	Mean Comparison
Demographic variables	**Sex**	***t*(237)=-2.465, *p*<.05**
	Age	*F*(3,228)=1.74, *ns*
	Education	*F*(2,245)=1.059, *ns*
Company-specific variables	Security training (Yes/No)	*t*(247)=-0.53, *ns*
	Laptop training	***t*(87)=2.58, *p*<.05**
	Employment time	*F*(3,248)=0.505, *ns*
	Job role	*F*(2,243)=2.97, *ns*
	Industry sector	*F*(5,225)=1.280, *ns*
Skill-based variables	**Internet skills**	***F*(3,246)=3.214, *p*<.05**
	Tech background	*t*(195)=1.734, *ns*
	Time in tech role	*F*(3, 202)=0.971, *ns*
	Perceived tech knowledge	***F*(2,243)=5.234, *p*<.01**
	Perceived security awareness	***F*(3,247)=6.232; *p*<.001**
	Perceived security policy knowledge	***F*(3,246)=7.623, *p*<0.001**

From demographic variables, ANOVA findings show that only sex has a significant effect for employees' likelihood of being laptop victims. Females are at higher

risk of being laptop victims than males ($p<.05$) as they apply updates to their employer laptops less frequently ($p<.001$); that is 15.5% of females never apply updates compared to 10.1% of males. Also, 31% of females only run updates when forced to compared to 15.4% for males.

Even though there is no significance for the aggregate laptop variable, employees in age group 18-28 run updates significantly less than employees in age group 29-37 ($p<.05$); that is, 41% of employees in age group 18-28 never run updates or only run them when they are forced to compared to 23% of employees in age group 29-37.

From company-specific factors, security training on laptop-related topics is the only variable that shows significant difference. That significance mainly stems from a fact that employees with laptop training use their company laptops more frequently than employees without training ($p<.05$)[11]. 56% employees with training use their company laptops at least every work day compared to 30% of employees without training.

Employees with laptop training also update their apps on the laptop more frequently (as they use their laptops more) however that is not statistically significant ($p=0.123$). Additionally, employees in office management job roles use their laptops more frequently than employees in IT ($p<.001$) or BA/PM roles ($p<.001$) and hence are at less risk of being laptop victims.

Multiple skills-based variables affect the likelihood of being a laptop victim such as Internet skills, perceived technical knowledge, perceived security awareness and policy knowledge. The common theme for all of them is that the higher the perceived knowledge the less likelihood of employees being laptop victims, specifically related to

[11] Employees who use laptops more frequently get more frequent updates (considering automated updates) which decreases security risk.

the frequency of running updates on the company laptop. Significant differences between higher knowledge and lower knowledge groups are as follows: Internet skills ($p<.05$), perceived technical knowledge ($p<.01$), perceived security awareness ($p<.001$) and perceived policy knowledge ($p<.001$).

Once all the individual factors were tested in ANOVA, the whole model was tested via OLS regressions to see what the major predictors are for becoming a laptop victim when all variables are considered together. Regression findings can be found in Table 14 below (significant findings are bolded).

Table 14. Regression findings for the likelihood of being a laptop victim.

Independent variables	**Model 1: Demographic Factors**		**Model 2: Company factors**		**Model 3: Skill based factors**	
	ß	**p-value**	**ß**	**p-value**	**ß**	**p-value**
Sex	**.174**	**.015**	**.178**	**.015**	**.159**	**.035**
Age	-.100	.158	-.056	.446	.019	.796
Education	.120	.090	.110	.122	.110	.106
Security training			-.005	.944	.068	.318
Employment time			-.121	.100	-.099	.164
Job role			.120	.086	**.164**	**.033**
Industry sector			-.101	.153	-.082	.225
Internet skills					-.047	.617
Tech background					-.018	.823
Perceived tech knowledge					-.079	.446
Perceived security awareness					-.001	.991
Perceived security policy knowledge					**-.309**	**.000**
F test	$F(3,203)=3.52$, $p<.05$		$F(7,203)=2.71$, $p<.05$		$F(12,203)=3.90$, $p<.001$	
Adjusted R^2	**.036**		**.056**		**.146**	

In step one of the regression model, which only looks at demographic variables, sex is the only significant predictor for an employee being a laptop victim, with female

employees being significantly more likely than male. Sex remains significant with the addition of company variables (step two) and skills variables (step three), while one's position in the company and their perceived knowledge of company's security policies also emerge as significant. Given that perceived security policy knowledge is the most significant predictor, perceived knowledge of security policies, which list the proper laptop usage, should be considered first in determining employees' likelihood of being laptop victims.

The adjusted R^2 value has been increasing with each step, which further implies that besides making conclusions based on employee's demographic characteristics, company-specific and skills-based characteristics need to be checked as well to get the better estimate of employee's likelihood of being a laptop victim. However, since the adjusted R^2 predicts only 14.6% of the variable, future studies should examine additional factors that could predict employees' likelihood of being laptop victims. Those could include employee's laptop locking habits, frequency of leaving laptops unattended, frequency of using (un) secured Wi-Fi from these devices, family members accessing these devices and whether they have experienced stolen/lost company devices.

5.1.5 Security Victims

Finally, all the security threats (phishing, passwords, BYOD and laptop usage) were combined to test the likelihood of being a security victim. Demographic, company-specific and skills-based variables were evaluated to determine which factors cause the highest likelihood for employees to be security victims. One-way ANOVA was run to see the difference between various groups for each independent variable. ANOVA findings are listed in Table 15 below (significant findings are bolded).

Table 15. ANOVA findings for the likelihood of being a security victim.

Variable Categories	Independent Variables	Mean Comparison
Demographic variables	**Sex**	**t(237)=-3.27, *p*<.001**
	Age	***F*(3,228)=4.5, *p*<.01**
	Education	*F*(2,245)=0.249, *ns*
Company-specific variables	Security training (Yes/No)	t(247)=0.168, *ns*
	Employment time	*F*(3,248)=0.238, *ns*
	Job role	*F*(2,243)=2.05, *ns*
	Industry sector	*F*(5,225)=0.870, *ns*
Skill-based variables	**Internet skills**	***F*(3,246)=7.769, *p*<.001**
	Tech background	**t(73)=2.5, *p*<.01**
	Time in tech role	*F*(3,202)=2.058, *ns*
	Perceived tech knowledge	***F*(2,243)=11.1, *p*<.001**
	Perceived security awareness	***F*(3,247)=10.57; *p*<.001**
	Perceived security policy knowledge	***F*(3,246)=11.73, *p*<.001**

ANOVA findings show that sex and age from demographic factors significantly affect the likelihood of an employee being a security victim. Females are at significantly higher risk of being security victims than males ($p<.001$) as are employees in age group 18-28 who are at significantly higher risk from employees in age groups 29-36 ($p<.05$) and 37-47 ($p<.05$).

None of the company-specific variables significantly affect the likelihood of an employee being a security victim but all of the skills-based factors do. All of the factors show the same theme: the higher the perceived knowledge in Internet-based technologies ($p<.001$), technical background ($p=.015$) and skills ($p<.001$), perceived security

awareness ($p<.001$) and perceived policy knowledge ($p<.001$), the less likelihood of an employee being a security victim.

Surprisingly, security training didn't show any significant difference in determining employee's likelihood of being a security victim. This could be due to the relevance and quality of the topic, and mode of training that should be further checked in future studies.

Once all the individual factors were tested in ANOVA, the whole model was tested via regressions to examine the major predictors for becoming a security victim when all variables are considered together. Regression findings can be found in Table 16 below (significant findings are bolded).

Table 16. Regression findings for the likelihood of being a security victim.

Independent variables	**Model 1: Demographic Factors**		**Model 2: Company factors**		**Model 3: Skill based factors**	
	ß	**p-value**	**ß**	**p-value**	**ß**	**p-value**
Sex	**.207**	**.004**	**.182**	**.013**	**.149**	**.043**
Age	-.132	.060	-.140	.059	-.051	.470
Education	.108	.123	.097	.172	.099	.136
Security training			.002	.972	.084	.209
Employment time			-.011	.879	.017	.802
Job role			-.103	.141	-.054	.474
Industry sector			-.063	.374	-.037	.575
Internet skills					-.075	.412
Tech background					.032	.689
Perceived tech knowledge					-.121	.232
Perceived security awareness					-.037	.663
Perceived security policy knowledge					**-.324**	**.000**
F test	$F(3,203)=5.03$, $p<.01$		$F(7,203)=2.54$, $p<.05$		$F(12,203)=4.81$, $p<.001$	
Adjusted R^2	**.056**		**.051**		**.184**	

In step one of the regression, sex is the only significant predictor for an employee being a security victim. Then, when the company-specific variables are added, the R^2 drops, with none of these new variables significantly predicting the DV. Finally, in step three of the regression model, sex remains significant while one's perceived security policy knowledge emerges as a significant predictor of becoming a security threat victim. In light of this, perceived knowledge of security policies should be considered first in determining employees' likelihood of being a security victim.

The adjusted R^2 increased the most (from .05 to .18) with the addition of the skills-based variables, suggesting that these factors are most important (among those evaluated) in determining an employee's likelihood of becoming a victim of a security threat. However, since the adjusted R^2 predicts only 18.4% of the variable, future studies should examine additional factors that could predict employees' likelihood of being security victims.

5.2 Knowledge of Security Terms and Concepts

Knowledge of security terms and concepts variable measures the averaged employee knowledge of specific security terms and concepts as outlined in Table 4 above. Demographic, company-specific and skills-based factors were evaluated to determine which factors affect the employees' security knowledge the most. One-way ANOVA was run to see the difference between various groups for each independent variable. ANOVA findings are listed in Table 17 below (significant findings are bolded).

Table 17. ANOVA findings for the knowledge of security terms and concepts.

Variable Categories	Independent Variables	Mean Comparison
Demographic	**Sex**	***t*(107)=2.865, *p*<.01**

variables	Age	*F(*2, 229)=1.43, *ns*
	Education	*F(*2,246)=0.612, *ns*
Company-specific variables	Security training (Yes/No)	*t*(248)=-0.920, *ns*
	Employment time	*F(*3,249)=0.94; *ns*
	Job role	***F(*2,244)=5.49, *p*<.01**
	Industry sector	*F(*5,226)=0.83, *ns*
Skill-based variables	**Internet skills**	***F(*3,247)=4.093, *p*<.01**
	Tech background	*t*(45)=-2.42, *p*<.05
	Time in tech role	*F(*2,203)=1.74, *ns*
	Perceived tech knowledge	***F(*2,244)=5.72, *p*<.01**
	Perceived security awareness	*F(*3,248)=1.12, *ns*
	Perceived security policy knowledge	*F(*3,247)=0.749, *ns*

ANOVA findings show that from demographic variables, sex is the only variable that shows significance in relation to the knowledge of security terms and concepts. Males on average have a significantly higher knowledge of security terms and concepts than females ($p<.01$).

From the company-specific variables, job role is the only variable that shows significance in relation to the knowledge of security terms and concepts. People in office management roles have on average lower security knowledge than people in BA/PM ($p<.05$) and IT roles ($p<.01$).

When looking at the skills-based variables, perceived Internet skills, technical background and perceived technical knowledge affect employees' knowledge of security terms and concepts. For each of these variables, the higher the perceived knowledge in Internet-related technologies ($p<.01$), technical background ($p<.05$) and skills ($p<.01$), the higher the knowledge of security terms and concepts.

Surprisingly, security training was unrelated to employees' knowledge of security terms and concepts. This could be due to the relevance and quality of the topic, and mode of training that should be further checked in future studies.

After answering all the knowledge questions, employees were asked to rate their confidence level on their answers to the security knowledge questions. ANOVA was run to determine the effect of questions confidence on the averaged security knowledge. Findings show significant results ($F(3,232) = 12.04$, $p<0.05$, $p<.001$), that is, employees with higher confidence in their answers on average have higher knowledge of security terms and concepts.

Once all the individual factors were tested in ANOVA, the whole model was tested via OLS regressions to see what the major predictors are for determining employees' knowledge of security terms and concepts. Regression findings can be found in Table 18 below (significant findings are bolded).

Table 18. Regression findings for the knowledge of security terms and concepts.

Independent variables	**Model 1: Demographic Factors**		**Model 2: Company factors**		**Model 3: Skill based factors**	
	ß	**p-value**	***ß***	**p-value**	***ß***	**p-value**
Sex	**-.203**	**.005**	**-.173**	**.019**	-.086	.272
Age	-.072	.306	-.055	.463	-.055	.467
Education	.060	.398	.068	.341	.058	.413
Security training			.019	.782	.036	.611
Employment time			-.008	.909	-.009	.901
Job role			**.157**	**.026**	.066	.408
Industry sector			.046	.514	.041	.558
Internet skills					.072	.463
Tech background					.027	.747
Perceived tech knowledge					.187	.084
Perceived security awareness					-.019	.828

Perceived security policy knowledge					-.081	.322
F test	*F*(3,204)=3.38, *p*<.05		*F*(7,204)=2.26, *p*<.05		*F*(12,204)=2.17, *p*<.05	
Adjusted R^2	**.034**		**.042**		**.065**	

In step one of the regression, sex is the only significant predictor for determining the knowledge of security terms and concepts, with males scoring significantly higher in their responses to the security concepts questions. When the company factors were added in step two, sex remains significant while one's job role is also significantly correlated with security knowledge. However, when accounting for background skills and perceived knowledge (step three), these factors fall out of the model and no variable emerges as significant.

The adjusted R^2 for the full model is quite low (predicting only 6.5% of the DV), which is not surprising as none of the variables emerged as a significant predictor of security knowledge and concepts. This is especially surprising for the skills variables; future research should try to unpack these relationships.

5.3 Knowledge of Current Security Policies

Knowledge of current security policies variable measures the averaged employee knowledge of general and password related company policies as outlined in Table 5 above. Demographic, company-specific and skills-based variables were evaluated to determine which factors affect the employees' knowledge of current security policies. One-way ANOVA was run to see the difference between various groups for each independent variable. ANOVA findings are listed in Table 19 below (significant findings are bolded).

Table 19. ANOVA findings for the knowledge of current security policies.

Variable Categories	Independent Variables	Mean Comparison
Demographic variables	Sex	$t(137)=-0.413$, *ns*
	Age	***F*(3,229)=2.746, *p*<.05**
	Education	$F(2,246)=1.462$, *ns*
Company-specific variables	Security training (Yes/No)	$t(194)=-1.529$, *ns*
	Employment time	$F(3,249)=1.372$, *ns*
	Job role	$F(2,244)=0.129$, *ns*
	Industry sector	$F(5,226)=0.198$, *ns*
Skill-based variables	Internet skills	$F(3,247)=0.481$, *ns*
	Tech background	$t(245)=0.672$, *ns*
	Time in tech role	***F*(3,203)=4.492, *p*<.01**
	Perceived tech knowledge	$F(2,244)=0.390$, *ns*
	Perceived security awareness	***F*(3,248)=4.96, *p*<.01**
	Perceived security policy knowledge	***F*(3,247)=9.224; *p*<.001**

ANOVA findings show that from demographic variables, age is the only variable with significant results. Employees from age group 18-28 have the lowest knowledge of company's security policies while employees of age 48+ have the highest knowledge (no significant differences found between particular groups).

Even though none of the company-specific variables show significant results for determining the knowledge of the current company's policies, some of the skills-based variable do; namely, the number of years in a technical role, perceived security awareness and perceived security policy knowledge.

Findings shows that the longer the employees work in a technical role, the higher the knowledge of company's security policies. Specifically, employees working in a technical role for less than five years have lower knowledge of company's security

policies than employees working in a technical role for 20+ years ($p<.01$). This significance stems from differences between these two groups in company's password-related policies ($p<.05$).

Surprisingly, the number of years employed at the company didn't show significant results which could imply, considering the above findings, that instead of considering the employment duration at one company, the total employment time of an employee could be a better estimate of their security policies knowledge (this could stem from the fact that some companies enforce it more than the others).

Perceived security awareness and perceived security policy knowledge also have a significant effect on one's knowledge of company's security policies. The higher the perceived awareness score, the higher the knowledge of company's security policies ($p<.01$), mainly when it comes to the knowledge of general security policies (excluding password policy) ($p<.001$). This is the same for the perceived security policy knowledge as well. Employees who have higher perceived security policy knowledge have a higher knowledge of general security policies (excluding password policy) ($p<.001$).

Even though security training doesn't show significance for the combined policy variable, significance is shown when it comes to general security policy. Employees who received security training have a higher knowledge of company's general security policies than employees without training ($p<.05$).

Once all the individual factors were tested in ANOVA, the whole model was tested via OLS regressions to see what the major predictors are for determining employees' knowledge of current security policies. Regression findings can be found in Table 20 below (significant findings are bolded).

Table 20. Regression findings for the knowledge of current security policies.

Independent variables	Model 1: Demographic Factors		Model 2: Company factors		Model 3: Skill based factors	
	ß	**p-value**	**ß**	**p-value**	**ß**	**p-value**
Sex	.061	.391	.068	.350	.038	.621
Age	**.227**	**.001**	**.207**	**.006**	**.145**	**.050**
Education	.031	.659	.032	.656	.040	.558
Security training			.110	.116	.034	.620
Employment time			.069	.354	.041	.569
Job role			.004	.949	.038	.621
Industry sector			.069	.329	.049	.477
Internet skills					-.003	.974
Tech background					-.079	.334
Perceived tech knowledge					-.044	.676
Perceived security awareness					.143	.101
Perceived security policy knowledge					**.234**	**.004**
F test	$F(3,204)=3.69$, $p<.05$		$F(7,204)=2.11$, $p<.05$		$F(12,204)=3.14$, $p<0.001$	
Adjusted R^2	**.038**		**.037**		**.112**	

In step one of the regression model, which only looks at demographic variables, age is the only significant predictor for determining the knowledge of company's security policies. Then, step two of the regression model, which looks at all of the demographic and company-specific variables together, shows that age is still a significant predictor (more important than company-specific variables). Finally, step three of the regression model, which looks at all of the demographic, company-specific and skills-based variables together, shows that age and perceived security policy knowledge are the significant predictors. This implies that the older an employee gets (which means more work experience too) the higher the perceived security policy knowledge, and then it turn the higher the knowledge of companies security policies.

In contrast to the analyses looking at knowledge of security concepts, the skills factors significantly increased the R^2 in this model, suggesting they are positively correlated with knowledge of company security policies.

6. Discussion

The following sections provide a deeper discussion of organizational security and are grouped by the dependent variables.

6.1 Phishing

Previous research has found that phishing susceptibility varies mainly with people's age and gender but that those can be mediated using control variables such as education level, Internet activity, tech savviness, job roles and exposure to phishing training [21]. For example, Sheng et al. found that individuals ages 18-25 were most vulnerable to phishing attacks because younger people have less number of years of education, less number of years on the Internet and less exposure to security training [21]. In addition, research has found that women are significantly more susceptible to phishing attacks than men due to their lower technical knowledge [21], more agreeable personality and their Internet usage (mainly online shopping) [28]. Education level and income didn't affect phishing susceptibility between men and women [21].

Unlike previous findings, the current study didn't find any significant differences for any of the demographic, company-specific or skills-based variables when each variable was tested separately (ANOVA) and when all the variables were combined (regressions). These findings could be due to the uneven study sample characteristics when it comes to gender, education, and technical background. The sample is male-dominated (70%), well-educated (97% with Bachelor's degree or higher), with the majority of employees having a technical background (85% total; 92.9% of males and 68.1% of females have a technical background).

Furthermore, as there were no differences between employees who have recently received security training and those who haven't (neither when it comes to any security training nor phishing training specifically), it appears that other factors are at play in predicting phishing vulnerability that were not captured in this study. Those could include more details around the training such as the relevance and quality of training, mode of training and employee comprehension as, for example, previous findings [21] show, that simulated phishing attacks decrease phishing susceptibility by 40%.

6.2 Passwords

Previous literature looked at various password characteristics, such as length, composition, lifetime, selection and storage [33] as well as people's password sharing [41, 44] and re-using habits [35, 41], all mainly through demographic and company-specific factors. This study extends the literature reviewed by a) adding additional password characteristics such as password priority and the use of random password generators for creating passwords, b) creating a combined averaged variable of all the password characteristics c) adding skills-based variables to test password habits against and d) performing a more-in-depth analysis of each of the demographic and company-specific variables as they relate to specific password characteristics and e) performing analysis with all variables (demographic, company-specific and skills-based) combined against the averaged password variable.

Similar to the CSID study on password length [35], this study found that the majority of employees (76%) create passwords between 8 and 10 characters in length while 24% of employees create passwords over 11 characters. Since the company's minimum password length is 8 characters, and the survey item listed was a password

between 8-10 characters, it is unclear exactly how many employees only stick to minimum password requirements and how many go beyond that. Future studies should investigate this finding further.

Compared to previous research finding that 56% of employees reuse passwords across their corporate and personal accounts [46], this study found that only 20% of employees engage in this practice. More specifically, females (not significant), employees ages 18-28, and employees with lower perceived Internet knowledge and security awareness are most likely to reuse work passwords for personal use. Also in line with earlier research [41], findings indicate that younger employees mainly choose passwords that are easy to remember. However, in contrast to research suggesting that females tend to forget their passwords [41], female employees in this study also use passwords that are easy to remember, which reduces one's likelihood of forgetting a password (even if this is a riskier behavior than choosing more complex passwords).

When it comes to employees' password sharing habits, previous studies have found that 20% of employees share passwords with others [46], while this was quite rare in the current study with only 2% of employees are doing that. Unlike previous findings that specify people in office management roles and of age 22 and under to be the most likely group to share passwords with others [41. 44], current findings (significant only) show that females and employees without a Bachelor's degree are most likely to share passwords. Interestingly, compared to previous findings that employees in financial sectors have good password management habits [44], current findings show that employees working in financial sector are more likely to share passwords with others than employees working in other sectors. As this group of employees is likely to be

working with sensitive company and customer data, this is especially concerning from a management perspective.

Even though the current study didn't find significant differences for password sharing habits among various job roles (as was case in previous studies [41, 44]), when controlling for demographic and company-specific variables, employees' job role is associated with their password habits. Employees working in office management roles have worse password habits than employees working in IT roles.

Surprisingly, unlike previous studies [44], the employment time didn't effect employees' password habits. When controlling for demographic, company-specific and skills-based variables, employees' job role and perceived technical knowledge are associated with their password habits. This further implies that no matter the number of years employed at the company, the technical skills and day-to-day work employees do affect their password habits the most.

6.3 BYOD and Company-Issued Laptops

Previous studies have found that the number of employees connected to organizational networks is on the rise, up 19% from 2013 to 2014 [50]. In line with these findings, current study found that 80% of company employees use their smartphones to check work emails. Also, with the increased user-base, the number of different devices connecting to corporate networks is on the increase too [53]. The most commonly used devices are Apple iPhones and iPads, Samsung Galaxy smartphones and Microsoft Windows tablets [51]. The current study only considered smartphones. Company employees mainly use iPhones (48.5%) and Android devices (42.4%), while Windows phone use is rare (7.2%). Even though previous findings show that Blackberries and

iPhones are more secure than Androids (and Windows phones are even less secure), these articles all argue that in a BYOD environment, any device exposes the company to same risks without user education [57, 58].

Previous research highlights that employees have poor security hygiene when using company devices such as work laptops and smartphones that have network access. For example, one study found that 40% of employees did not password protect their devices or apply updates to the mobile and laptop applications, even though it is widely known that mobile apps are not always very secure in their initial releases [47, 51]. The present study found that 15% of employees do not lock their smartphones and the lock question was not asked for laptops as all company-supplied laptops require passwords.

Interestingly, the current study found that 47% of employees report updating apps on both their smartphones and company-supplied laptops as soon as they see the updates available. This finding, together with a smaller percentage of employees without phone PINs or passwords, could result from a) a very technical workforce (85% of employees) and b) peer pressure in work settings. Findings from this study show that employees who have higher Internet skills, technical background and perceived security awareness generally update apps more frequency than employees with less knowledge in these areas. Additionally, Herath and Rao [59] found that one's immediate environment in the workplace affects employees' security behaviors; for example, if an employee sees her coworkers adopting security policies, she will be more likely to also adopt them.

This study extends previous research by a) looking at various BYOD and laptop characteristics and averaging them each into a separate variable (as described in Section 4.2.1 of the methods) and b) looking at various demographic, company-specific and

skills-based variables to determine how those separately and combined affect each of the BYOD and laptop characteristics as well as the final averaged variables.

Younger and less tech-savvy employees in this sample were the most likely BYOD victims. Additionally, employees in office management roles check their work emails on the phone significantly more frequently than employees in IT roles. On the contrary, employees in IT roles (60% of them) mainly use pins or sliding patterns to lock their smartphones (which are 4-digit) while employees in office management and BA/PM roles (~50% of both groups) use passwords and/or biometrics. This is interesting as employees in office management roles are less tech savvy than employees in IT roles.

When it comes to being a laptop victim, female employees place themselves at a higher risk than males specifically when it comes to applying laptop updates; that is, 15.5% of females never apply updates compared to 10.1% of males (X^2=15.6, p<.05, p<.01). Also, 31% of females only run updates when forced to compared to 15.4% for males. Like women, younger employees also update significant less often than older employees: 41% of employees 18-28 never run updates or only run them when they are forced to compared to 23% of employees in age group 29-37 and 30% of employees of age 37+. Finally, when controlling for these and other factors, perceived knowledge of security policies emerges as the most significant predictor for becoming a laptop victim.

Furthermore, as there were no differences between employees who have recently received security training and those who have not (except for relation between laptop training and frequency of usage), it appears that other factors are at play in predicting BYOD/laptop vulnerability that were not captured in this study. Those could include more details around the training such as the amount of a topic covered, quality of the

training, mode of training and employee comprehension, as findings show that no matter the devices' OS used, without user education, each and very device could put the company at the same risks [57, 58].

6.4 Security Threats Combined

To expand on previous studies, the current work looked at the four security threats both separately and combined to determine the likelihood of an employee becoming a security victim when all those factors are looked at together. This extends the current literature by giving a more detailed (analyzed across demographic, company-specific and skill-based variables) and holistic view of the most important factors companies should focus on when implementing training and other programs to reduce the likelihood of security breaches.

So what are the most likely characteristics of a security victim based on the current findings? The security victim would most likely be a female, young (age 18-28), without a technical background, and with low perceived knowledge in Internet-related technologies, technical areas, company security policies, and general security awareness. The more of these characteristics a person has, the higher the likelihood they will become a security victim. However, while all of these variables have an effect on employees' likelihood of being a security victim, some are more prominent than others. Specifically, the perceived knowledge of security policies is the most significant predictor, followed by sex and age.

Interestingly, attending one or more security training sessions in the last year did not impact an employee's likelihood of falling victim to security threats. There are a number of potential reasons for this finding including the training topic relevance and

quality, training mode, and employee comprehension. First, even though the survey asked employees about the topic and types of training attended, it was hard to determine how much of the topic-relevant information, and of what quality, were included as part of the training. As a result, some respondents may have reported attending sessions that were unrelated to these threats.

Second, out of 89 employees who attended any security training, 66 reported it as mandatory online training, 36 as self-initiated online training and only 5 as in-classroom training.[12] The high number of mandatory online training reports could be a result of employees' tendency to include the reading of the security policy as part of the security training. This is interesting especially since the perceived knowledge of the security policies is the major predictor of an employee being a security victim.

None of the employees mentioned receiving training that resembled real-life scenarios (e.g., simulated phishing attacks), which security experts and security studies have shown to be the most effective at decreasing security breaches [21]. Even though security experts, interviewed in the study, are divided on the best modes to deliver security training in the organizational environment, they all agree that training must be relevant, to the point, and employee-engaging. Also, for a training to be effective, it must clearly show a benefit to an employee.

Third, as these training sessions do not include metrics to measure comprehension, it is impossible to evaluate how effective they were. Hence, security experts suggest that every training end with a quiz or questionnaire as well as to

[12] Employees were able to select multiple answers which causes higher sum than the total who received training

frequently perform short incentive-based security tests to measure employees' comprehension of previous training material on the on-going basis.

To summarize, in order to better understand how security training effects employee's likelihood of being a security victim, the training topic relevance and quality, training mode and employee comprehension should be considered in future studies.

6.5 Knowledge of Security Terms and Concepts

Unlike any literature reviewed, this study measured the average knowledge of a company employee as it relates to the four security threats to determine what variables (demographic, company-specific and skills-based) affect employees' knowledge of security terms and concepts. This extends the current literature by measuring and combining the employee knowledge of all four security areas instead of just one.

So based on the findings, which employees are likely to have the most knowledge about good security practices? Based on the data, these employees are likely to be males with technical backgrounds and high levels of perceived knowledge about Internet and technical topics. These employees are most likely to be working in IT roles, where these skills are being put to use on a daily basis, as compared to many other roles where the only technical skill requirements are basic word processing and Internet knowledge. This further shows that employees' sex and job role are the most significant variables to consider when determining employee's knowledge of security terms and policies. Interestingly, security training didn't show any significant effects on the security knowledge of employees. See section 6.4 for details about security training.

6.6 Knowledge of Current Security Policies

Unlike any literature reviewed, this study measured the average knowledge of a company employee as it relates to the knowledge of current company security policies (including general security policies and password policies) through a quiz-style multiple choice question format that tested employees' knowledge of various security policies.

Findings show that younger employees have the least knowledge of company's security policies; age has a strong linear relationship to security policy knowledge with oldest employees (48+) exhibiting the most knowledge. In contrast to the analyses looking at security threat victims, security training was positively correlated with knowledge of company security policies (could be due to the fact that security policy was considered as a training); future studies should work to unpack the relationship between knowledge gained through training, and becoming a victim of a security breach.

When demographic, company-specific and skills-based variables were considered together, perceived security policy knowledge was the only significant predictor (age only marginal) for employees' knowledge of current security policies. One reason why employment duration did not show significant differences in employees' knowledge of company security policies could be because of similarities in policies across companies (as explained by the significant positive correlation between employee age and perceived knowledge of the policies).

7. Recommendations

Based on the survey findings, reported by 250 company employees (>10% of total employees in organization) and interviews with security experts from educational, government, and private sectors, the following set of recommendations is presented below with the goal to help companies improve their security policies and practices, especially in regards to human-related security threats.

Recommendations are grouped by security threat area: phishing, passwords, BYOD and laptop usage. After those, recommendations about security training and user awareness programs are listed as critical components for improving the security culture of an organization.

Security experts universally agreed that the vast majority of security incidents that companies face are related to human factors, mainly the introduction of malware due to social engineering techniques (phishing, spear-phishing, etc.), employees' download and browsing habits, and lost or stolen devices. When asked about minimum requirements companies must meet to operate securely, all experts agreed that first, companies must ensure that all the technical controls (firewalls, IDSs, network segregation, access controls, patch policies, etc.) are in place and working properly before "user controls" can be considered. Let's review security experts' recommendations in these areas.

7.1 Phishing

Phishing is still one of the major problems companies face as it depends largely on human factors—a single employee who falls for a phishing campaign can compromise an entire company's data security. Even though security experts urge companies to implement spam filters to block and filter out potentially suspicious emails, there are no

filters that can block every variation of malicious email. Furthermore, there are currently no filters available to block phishing phone calls (i.e., vishing), piggyback rides, tailgating and related strategies. Hence, educating employees on how to deal with unfiltered emails, phone calls, and people around them becomes a critical factor in securing the organizational network. This is because "there is no patch for user doing a wrong thing. There is no user firewall," according to John Linkous, founder and CEO of InterPoint Group, LLC. Education becomes the only "user firewall" that protects the organization's boundary when it comes to phishing (vishing, piggyback rides, tailgating) attacks.

Security experts agree that the most effective way to fight against phishing attacks is through implementing real-life scenario-based trainings such as simulated phishing attacks. Previous research [21] supports this assertion, finding that simulated phishing attacks decreased phishing susceptibility by 40%. Additionally, annual trainings might be a good refresher, but such trainings should be based on recent stories, real data and real impacts so that employees can connect the more abstract concepts with real-world outcomes. Frequent reminders (e.g. one in few weeks) about phishing threats are crucial (through simulated attacks, emails, newsletters, posters, discussions, inceptive-based competitions, etc.) to keep employees aware that phishing threats are real and are daily causing business impacts.

7.2 Passwords

When it comes to mitigating threats related to user passwords, security experts agree that complex password policies must exist, that proper technical tools must be leveraged to enforce those policies, and that appropriate access controls (i.e., identity

management) must be well defined and enforced. Specifically, experts recommend the use of:

1. two-factor authentication (use of tokens, smart cards, biometrics, etc.) as a requirement for external access (for internal access preferred)
2. passphrases (multiple words together) that are 15+ characters in length
3. password complexity (alphanumeric, uppercase and lowercase characters, symbols)
4. a limited number of password attempts when accessing the network to protect against brute force attacks
5. computer-generated passwords that are randomized and more secure (could be used for various server access)

While security experts were proponents of password expirations based on 30-, 60- or 90-day intervals, John Linkous mentions that "changing a crappie password with another crappie password is not security." This statement is in line with research that questions password expirations due to the predictability of a new password based on the old one [60].

Interestingly, Raymond Gabler, founder and CEO of RGS Specialists, suggests that for all the web-based applications that list exact password requirements on the websites, passwords requirements should be specified as *suggested* instead of *required* to minimize the number of known password characteristic for an attacker.

Finally, experts argue that there must be a balance between security and usability. If passwords are too complicated, employees are more likely to forget them and hence write them down. When it comes to password-storing mechanisms, the majority of

security experts recommend the use of password-manager tools (e.g., KeePass, 1Password, Password Safe, Cyber Ark) as a good option compared to everything else; however, they come with disadvantages too (e.g., a single point of failure).

Just like with phishing, once all the technical controls are in place, continuous education becomes a "user firewall" against password-related attacks, especially in circumstances when two-factor authentication is not implemented.

7.3 BYOD

When it comes to BYOD policies, security experts argue that companies have three choices to make:

1) No personal devices and no company-issued devices allowed on the network
2) Only company-issued devices allowed on the network
3) Both personal and company-issued devices allowed on the network

Obviously, not allowing any external devices or company-issued mobile devices to connect to the network is the most secure way to protect the organization; however, as previous research found, allowing employees to stay connected improves satisfaction and productivity [49, 61]. Capgemini consulting reports that employees who use their own devices for both work and personal matters put in 240 more hours a year than those who do not [61]. However, companies need to be careful when deciding on BYOD use as initial cost savings (from not providing a device) can be very costly if the BYOD solutions are not implemented properly [61].

When companies want employees connected, security experts argue that going with a company-issued device is the easier and more secure option to choose. That is because there is a clear owner of the device data (i.e., the company), the device is on the

network (which means that is secured, audited and monitored as any other device), and if the device is lost or stolen, remote wipe is always possible. However, parts of the network that the device can access depend on company's network segregation. Hence, before the devices are issued to employees, they should be verified for appropriate network segment access.

In situations where companies allow employees to use their own devices, security experts note there are a lot more factors to consider. Even though companies might save money on the device itself, implementing MDM (Mobile Data Management) solutions is expensive and hard to set up. First, before allowing a device to connect to the network, the device should be scanned for viruses and malware and device password requirements enforced. Some level of monitoring, if possible, should be set up. Well-written device use policy must exist that clearly defines data ownership (what part of device data is used by the company and what by the user), user rights and responsibilities and agreement for remote wipe in case of a lost or stolen device (which could remove personal data depending on the MDM solution). However, parts of the network that the device can access depend on company's network segregation. Hence, before employees are allowed to use their personal devices, the devices should be verified for appropriate network segment access.

No matter which choice a company makes (company-supplied vs. personal devices), the less segregated the network is or the more company data the user has on the device, the greater the responsibility on the end-user. That is, employees need to ensure that password requirements are met, device OS and apps are updated regularly (for personal devices), and devices are not lost or stolen. But do employees or even

companies really think about all this? Yet again, continuous education becomes the "user firewall" in securing the companies' end-points, especially when considering the intertwined nature between user's passwords and apps update habits and personal devices used on corporate networks.

7.4 Company-Supplied Laptops

Companies often provide laptops to their employees to increase workplace flexibility, allowing employees to access the network and complete tasks when outside the office. On questions around company-supplied laptops, security experts argue that laptops should be locked down (i.e., employees should not have Admin rights), have encrypted drives, have proper monitoring in place (e.g., disabling access if user is inactive for an extended period of time), proper patch management practices and a well-defined acceptable use policy.

The IT manager from the surveyed company said that malware infections significantly dropped since locking down company laptops. On the other hand, company employees reported a lot of productivity issues since the lock-down, which had the unintended consequence of some employees using their own personal laptops to get work done. Using personal laptops brings similar risks as using personal smartphones as mentioned in section 7.3 above. This shows how improving laptop security without allowing for employee convenience or ease of access can actually have opposite effects.

Additionally, as part of acceptable use policy, employees should be aware that these laptops are for work purposes only, so allowing their children or family members to access them (i.e. to play games or access various websites) should be forbidden. Also, employees should be cautious not to leave their laptops unattended and should always

lock their laptops when stepping away from them (e.g., during a break). A security expert who works in higher education suggested randomly walking through work areas and checking on employees' locking habits to increase compliance with this practice.

Additionally, encrypted drives and two-factor authentication should be instituted for all the company-issued devices to minimize risks in case of unattended, lost or stolen laptops when the only obstacles for criminals is to crack the employee password [63]. Implementing encrypted-drives and two-factor authentication becomes extremely important as employees who deal with the most sensitive data (office management employees), based on this study, are most likely to be password victims.

Finally, continuous education in this area would help employees tremendously in understanding the true reasons behind laptop lock-downs and various use policies (e.g., show the number of incidents and impacts prior to lock down and post lock-down initiatives). Only after users understand the true reasons behind the changes that are impactful for them (e.g. locked-down laptops), they would be able to serve as "user firewalls" in protecting companies' endpoints.

7.5 Training

There is no doubt that employees should be trained in every security area, but what constitutes a good user awareness program? Security experts recommend the following components be included in any employee security training programs:

1) Use of real-world scenarios - simulated phishing attacks, simulated password cracking attacks, etc.

2) Use of real world, real data, real people – include interesting current examples that show facts (other events in the news, or company events like monitoring reports and trends)
3) Emphasize the intertwined nature of the four security threats (e.g. poor password habits can cause employees being BYOD or laptop victims)
4) Make it personal and important – engage employees, show an example on one of their personal accounts (e.g. let's hack your FB account or let's see what people can find out about you based on your data online) and how can that affect them and their families
5) Classroom setting preferred but engaging online training rated high as well
6) Mandatory training enforced (people who don't complete training lose network access)
7) Must be fresh and new – new examples, new ideas, new concepts (adapt to new threats available)
8) Must be continuous (always in employee's minds) – it can be yearly online training, but with frequent emails, newsletters, security meet-ups, posters, boot-camps, competitions (with incentives), meetings that start with a security message, etc.
9) Incentive based (part of being important for employees as bottom line always matters) – regularly check employees' knowledge in various security areas (e.g. through timed online surveys), score and average them every few months and award the employees with highest scores with additional monetary funds (similar to referrals)

10) Emphasize education (that can help them personally) and not testing – there is nothing to lose but much to gain.
11) Stop and feel the pain – refers to a practice of simulating impacts of an attack, for example, shut down one of your (web) services and see how fast you can recover. This is just to show (mainly to decision-makers) that attacks can happen and if recovery, business continuity, and incident-handing plans are not in place and tested regularly, companies can experience big and very expensive consequences.
12) Start early – this implies to companies, educational institutions and individuals alike. Companies should train their employees early and often (e.g. don't allow network access until training is done). Education system, from elementary school to college and higher education, should be adjusted to raise awareness of security risks and protect youngster from being victims. Parents should know about security and the associated risks to be able to teach their kids early and often.

8. Limitations and Future Work

There are several limitations to this study. First, survey data was collected from a single IT company. On a related note, as the studied company is in the IT business, the workforce is heavily male-dominated and employees likely have higher overall technical and security knowledge than non-IT companies. Selection bias could have been also possible as this study could have attracted more tech-savvy employees compared to non tech-savvy ones. It is expected that because of these company features and possible selection bias, the number of employees who reported giving credentials on malicious sites or opening malicious attachments (15 out of 250) is not representative of companies at large. The results of the study might not hold true for other companies in different sectors that have a more diversified user base, which should be considered in future studies.

Second, since the survey was online and not timed, for questions measuring knowledge of general and company-specific security policies, employees could have searched for answers online which could skew the results of the study. In future studies, it would be worthwhile checking the knowledge questions through a timed survey or in a lab-based isolated environment to see if similar results are found.

Third, because of the point-in-time nature of data collection through a single survey, causality cannot be established. Future work should consider alternative methods to establish causality, such as longitudinal studies or experiments that capture baseline knowledge, then use a treatment such as various types of training, then measure knowledge again at a later time. Capturing data at least another survey six months or

longer from the first data collection would help establish reliability and validity of results (assuming everything else is constant).

Fourth, a surprising finding was that security training was unrelated[13] to all three major dependent variables, namely (1) being a security victim, (2) knowledge of security terms and concepts, and (3) knowledge of security policies. This could stem from the fact that various training characteristics such as the topic relevance and quality, mode of delivery and employee comprehension were not taken into consideration when determining the effects of security training on dependent variables (e.g. reading of the security policy could have been reported as security training). Additionally, there were measures not captured in this study (e.g., to capture the type of training received, when it was received, and the effectiveness of that training). Various training characteristics should be considered in future work.

Finally, the adjusted R^2 values, predicting all of the dependent variables (including sub-variables), are relatively low, ranging from ~3% to ~20%. This means that there are other factors at play (e.g., involving detailed security training) in predicting the likelihood of being a security victim, the knowledge of security terms and concepts, and the knowledge of security policies. Future work should consider finding additional factors to increase predictability for these dependent variables.

[13] That is, significant differences were not found neither with ANOVA nor with regressions

9. Conclusion

As employees are the weakest link in securing the organizational endpoints, the present study achieved its goal of determining the most common characteristics of employees who are a) most likely to be security victims, b) most knowledgeable about security concepts and c) most aware of the security policies when four different, yet intertwined, security risk areas (phishing, passwords, BYOD and laptop usage) are taken into account.

Being aware of employee characteristics—who the literature and experts agree pose the biggest security risks for organizations—can help companies tailor their security awareness programs to ensure that "riskier" employees are given special attention when it comes to organizational security. This especially becomes important, as pointed out by security experts interviewed, as security victims are often the same people over and over again.

Security experts interviewed pointed out that *continuous education* is the only "user firewall" that keeps organizations secure when it comes to their endpoints. One unintended consequence of this study is that the mere act of surveying employees has helped this process. The survey increased employees' awareness around the most prominent human-related security threats as employees already started discussions about these topics among themselves and pointed out that they hope to see improvements in these areas as those are very much needed[14]. To further highlight that training is needed, 82% of employees mentioned that the security training should be mandatory and 33.6%

[14] This has been reported in the survey comment section.

of them emphasized that employees' lack of education is the biggest threat in ensuring the security of corporate data.

However, for security awareness programs, this is just the beginning [62]. Ideally, companies would look at recommendations and apply them but in real life, that is never the case. Security experts interviewed point out that often time security is an afterthought and is looked upon only after the incidents happen. Also, funding and staffing around security is always scarce and as one of the experts from educational sector points out: "There is always a lot of work but never enough people." This further shows that management support and buy-in are very low, which can be proven by SANS Institute study that shows that only 5% of companies work on their security awareness programs full-time and spend less than $10,000 (or < $5,000 for smaller companies) per year on security awareness programs which is less than what is collected through bake sales [62].

Hence, for an organization to be truly security-oriented, the whole organizational culture needs to change and that needs to start from the top. Michael S. Huhn[15] even suggested sending CEOs and top-level management to attend major security conferences, as that would provide valuable education to help them make decisions that would be in line with the security best practices. As security experts interviewed point out, when it comes to security attacks and breaches, it is the matter of *when* not *if*.

Hopefully the literature reviewed, findings and recommendations from this study help organizations improve their security practices and help them see how important it is to invest in security matters, especially when it comes to the organizations' most important assets—the employees.

[15] Michael S. Huhn is an adjunct cybersecurity instructor at UMBC holding the following security certifications CISSP, ISSEP, BAP, CAP, CEH.

10. Appendix

Appendix A: Survey Questions

Section 1: Current Security Awareness

1) Security awareness refers to your awareness of security concerns that people and organizations face nowadays including phishing, passwords and the use of personal devices (smartphones, tablets, etc.) in everyday life. Overall, how would you rate your general information security awareness? (Slider: 1=very low, 5=very high)

2) Security policy refers to a company document that outlines the expected security behavior to be followed in the organizational setting. How would you rate your knowledge of your employer's security policies? (Slider: 1=very low, 5=very high)

[new page]

The following set of questions will ask you about specific aspects of your employer's security policy. **Please answer to the best of your knowledge.**

3) Does your employer have a security newsletter?
   a) Yes
   b) No

4) **If yes to 3**, how often does the company security newsletter come out?
   a) About once a week
   b) About once a month
   c) About once a quarter
   d) About once a year
   e) I am not sure

5) Does your company have a security policy?
   a) Yes
   b) No

6) **If yes to 5**, how long has it been since your employer last updated its security policy?
   a) About one month
   b) About three months

c) About six months
d) About a year
e) I am not sure

7) **If yes to 5**, how do you, MOST OFTEN, hear about the security policy updates?
   a) Security newsletter as part of corporate communication
   b) Colleagues
   c) Management
   d) Other (please list)

8) **If yes to 5**, have you read the most current security policy?
   a) Yes, thoroughly
   b) I skimmed through it
   c) No, but I plan to read it
   d) No, and I hadn't planned to read it

9) **If yes or skimmed to 8**, did you understand the security policy?
   a) Yes, it is all straight forward
   b) So-so, I could use some explanations to better understand it
   c) No, I need help to understand it

10) Have you received any security awareness training (HIPAA, phishing, passwords, etc.) in 2015?
   a) Yes
   b) No

11) **If yes to 10,** what kind of training have you received? (check all that apply)
   a) Self-interested online training
   b) Mandatory online training (e.g. HIPAA)
   c) In-person classroom training
   d) Other (please list)

12) **If yes to 10**, what was the training topic? (check all that apply)
   a) Social engineering (phishing, spear phishing, etc.)
   b) HIPAA
   c) Password requirements
   d) Bring Your Own Device (BYOD) policies

e) Proper use of the company supplied laptop (passwords, patches, updates, downloads, etc.)
f) Other (please describe)

13) What is the current password expiration timeframe based on your employer's password policy?
    a) 30 days
    b) 60 days
    c) 90 days
    d) 120 days
    e) There is no expiration

14) What is the maximum number of password retries before your employer account (laptop, emails) gets locked?
    a) 3
    b) 5
    c) 10
    d) 20
    e) Unlimited

15) What is the current **minimum** password length for your organization?
    a) There is no minimum
    b) 5 characters
    c) 8 characters
    d) 10 characters
    e) 15 characters

16) When you change your password on your employer-supplied laptop, what is the minimum number of characters you need to change?
    1) 0
    2) 1
    3) 4
    4) 6
    5) 8
    6) I am not sure

[new page]

The following questions ask about your security-related experiences while working at your employer.
Please answer to the best of your knowledge.

17) A malicious site is any site used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Have you ever clicked on a link in the email from your employer-supplied laptop or client PC that took you to a malicious site?
    a) Yes, I clicked on the link in the email
    b) No, I never click the links I don't trust
    c) I am not sure

18) **If yes to 17**, did you provide your credentials on the site you were re-directed to?
    a) Yes
    b) No
    c) No credentials were requested

19) **If yes to 17**, was there any impact to you, your organization or the client after clicking the link in the email?
    a) Yes (please describe)
    b) Not to my knowledge

20) Malware is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Have you ever opened an attachment on your employer-supplied laptop or client PC that installed malware?
    a) Yes
    b) No
    c) I am not sure

21) **If yes to 20**, was there any impact to you, your organization or the client after opening the attachment?
    a) Yes (please describe)
    b) Not to my knowledge

22) How long is your current employer password (laptop, email)?
    a) 5 -7 characters
    b) 8 - 10 characters
    c) 11 - 15 characters

d) 15+ characters

23) Where do you **generally** store the passwords for various organizational systems (laptop, email, time entry, social collaboration, etc.)? (check all that apply)
   a) In my head (memory only)
   b) Sticky notes visible to others
   c) Sticky notes hidden from others
   d) Text file on the computer
   e) In the email received
   f) On my USB or external hard drive
   g) Password-protected document (Excel sheet)
   h) Password manager software (e.g., KeePass, 1Password)
   i) Other (please list)

24) How do you **mainly** choose your password for various organizational systems?
   a) Meaningful detail (e.g. name, date, street, registration number, geographic location)
   b) Combination of meaningful details (e.g. Bill2000, 4jun84)
   c) Pronounceable password (e.g. one4you, 2Bfree)
   d) Random combination of characters (e.g. car8&t, CoLL186+)
   e) Not chosen by me. Please specify who chose it (e.g. work, provider)
   f) Other (please list)

25) Have you ever used a random password generator for any of your organizational passwords (email, laptop, time entry, social collaboration)?
   a) Yes
   b) No

26) When creating a password in a work environment, what is your **top** priority?
   a) Strength and security
   b) Easy to remember
   c) Easy to enter
   d) Meeting password requirements

27) Have you ever used your company password for any other personal accounts (emails, banking, etc.)?
   a) Yes
   b) No

28) Have you ever shared your company password with someone else (colleagues, family, etc.)
    a) Yes
    b) No

29) Do you access work emails on your phone?
    a) Yes
    b) No

30) **If yes to 29**, generally, how often do you access work emails on your phone?
    a) All the time
    b) Few times a day
    c) Once a day
    d) Few days a week
    e) Less than few days a week

31) **If yes to 29**, how do you access work emails on your phone?
    a) Through the Outlook app
    b) Through Outlook webmail
    c) Other (please list)

32) **If yes to 29,** what is the operating system on your smartphone?
    a) iOS
    b) Android
    c) Windows
    d) Blackberry
    e) Other (please list)

33) **If yes to 29,** how do you protect (lock) your smartphone?
    a) Biometrics only
    b) Biometrics/pin or password
    c) Sliding pattern only
    d) Pin only
    e) Password only
    f) I do not lock my smartphone

34) **If 33=b,c,d,e,** how many characters does your smartphone pin/password/pattern have?
    a) 4 digit numeric pin/pattern

b) 4+ digit numeric pin/pattern
c) 0-5 character password
d) 6-10 character password
e) 10+ character password

35) **If 33=b,c,d,e,** does your smartphone pin/password/pattern contain any of the below (check all that apply):
   a) Initial of, or full, your first name, last name or both
   b) Any or all parts of your birth date: day, month, year
   c) Initial of, or full, family member's first name, last name or both
   d) Any or all parts of family member's birth date: day, month, year
   e) None of the above

36) **If yes to 29**, how often do you update the apps on your smartphone?
   a) As soon as updates are available
   b) Once a week or longer interval
   c) Once a month or longer interval
   d) Only when apps are updated automatically
   e) Never

37) **If yes to 29,** do you use an Antivirus software for your smartphone?
   a) Yes
   b) No

38) How often do you use your employer supplied laptop?
   a) Every day
   b) Every work day
   c) Few times a week
   d) Once a week or less
   e) Once a month or less

39) How often do you apply updates to your employer-supplied laptop, for applications which are NOT updated automatically by the employer?
   a) As soon as I see them
   b) Once a week or longer interval
   c) Once a month or longer interval
   d) Only when forced to update
   e) Never

Section 2: Security Skills

1) What is the goal of encrypted data transmission?
    a. The data can't be eavesdropped
    b. The data is protected against viruses
    c. The data is not corrupted during transmission
    d. Only the user herself can see the data

2) What is malware?
    a. Software which is not working properly
    b. Software which is automatically updating itself
    c. Software which is unwanted and might be harmful
    d. A faulty technical device

3) What is phishing?
    a. The analysis of user's browsing behavior
    b. The sending of unwanted ads
    c. The uninstalling of software that needs too much resources
    d. A form of deception using email or messaging in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy entity

4) What is social engineering?
    a. Distribution of software-testing tasks to several engineers in order to find security leaks
    b. Psychological manipulation of people into performing actions or divulging confidential information
    c. The development of software for social networks
    d. The development of charitable apps which are free of charge

5) How can you recognize malicious emails (i.e., emails with suspicious links or attachments)? (check all that apply)
    a) By email sender
    b) By email subject
    c) By email content
    d) By the seeming urgency
    e) None of the above
6) What helps you recognize a suspicious website? (check all that apply)
    a) Checking the URL
    b) Using toolbar tools like McAfee Site advisor or similar

c) Checking website safety ratings and reputation
d) Checking the site's digital certificate
e) None of the above

7) What makes the password strong? (check all that apply)
   a) Length
   b) Randomness
   c) Avoidance of dictionary words
   d) The use of alphanumeric and special characters
   e) None of the above

8) How can a device (laptop, smartphone) be protected from viruses? (Check all that apply)
   a) Always keep software and OS up-to-date
   b) Avoid downloading unknown software (apps) from the Internet
   c) Use antivirus to scan your device often
   d) Avoid visiting unfamiliar or unknown websites
   e) Avoid using unsecured wireless networks
   f) None of the above

9) How confident are you in your responses to above questions (1-8)?
   (Slider: 1=not confident at all, 5=very confident)

Section 3: Challenges in securing corporate data and improving user awareness

1) What do you see as the **biggest** challenge in ensuring the security of corporate data?
   a) Lack of employee education
   b) Lack of corporate communication (not being aware of things)
   c) Improper use of personal devices (e.g. smartphones, tablets, etc.) in the organizational setting
   d) Improper use of the company supplied laptop (passwords, patches, updates, downloads, etc.)
   e) Poor, or difficult to understand, security policy
   f) Other (please list)

2) Please explain why you made the above selection.
3) Which of the below security areas do you think are important to have employees trained on? (check all that apply)
   a) Social engineering (phishing, spear phishing, tailgating, piggy back rides, etc.)

b) Password requirements
c) Proper use of personal devices (e.g. smartphones, tablets, etc.) in the organizational setting
d) Proper use of the company supplied laptop (passwords, patches, updates, downloads, etc.)
e) None of the above

4) Do you think that the security training should be mandatory?
   a) Yes
   b) No

5) What would be the preferred method for you to receive security training? (check all that apply)
   a) Online self-learning (watching videos online, reading links from the Security newsletter, etc.)
   b) In person classroom training
   c) Real-world scenarios training (e.g. simulated phishing attacks)
   d) Other (please list)

6) How often should the security training be offered?
   a) Every month
   b) Every 3 months
   c) Every 6 months
   d) Every year
   e) Less than once a year

Section 4: Demographics and Conclusion

1) Approximately how long have you been employed by your current employer?
   ___Months ___ Years

2) What best describes the job role that you currently have?
   What describes the best your current job role?
   a) Finance
   b) Accounting
   c) Human Resources
   d) Office Management and Administration
   e) Sales
   f) Security
   g) Project Management

h) Business Analysis
i) Testing
j) IT (development, systems analysis and support, production support, etc.)
k) Other (please list)

3) What industry sector do you work in?
   a) Financial
   b) Healthcare
   c) Utilities
   d) Retail
   e) Other (please list)

4) What is your age today?

5) What is your sex?
   a) Male
   b) Female

6) What is the highest degree you received?
   a) None
   b) Elementary school diploma
   c) High school diploma or equivalent (GED)
   d) Associate degree
   e) Bachelor's degree
   f) Master's degree
   g) Professional degree (MD, DDS, DVM, LLB, JD, DD)
   h) Doctorate degree (Ph.D., Ed.D.)

7) Do you have a technical background (education, work experience, etc.)?
   a) Yes
   b) No

8) If yes to 7, how many years of work experience do you approximately have working in a technical field (where technical work comprises a significant portion of your job)?
   ____ None ____Months ____Years

9) How would you rate your overall technical knowledge (e.g. related to hardware and software components of the system)?
(Slider: 1=very low, 5=very high)

10) How would you rate your overall Web skills (e.g. searching and locating information, shopping online, online banking, etc.)?
(Slider: 1=very low, 5=very high)

11) How would you rate your knowledge of Internet-specific concepts (e.g. cache, cookies, phishing, digital certificates, trusted sites, etc.)?
(Slider: 1=very low, 5=very high)

12) Is there anything else that you would want to add, suggest or comment on?

[new page]

Below are the questions that you marked as "I am not sure" as your answer. To help us understand your selection, could you please briefly explain what made you choose that as your answer? [Note: SurveyGizmo will pull those questions in and list them for the participant]

[new page]

Thank you for your participation in this survey. Your responses will help to identify areas where the company needs to provide additional information and/or training on issues of organizational security.

Appendix B: Interview Questions

1) What are the most common types of security incidents that your company/clients are facing? What percentage of incidents on average are related to human factor (phishing, passwords, BYOD, laptop/computer maintenance, etc.)?
2) What do you see nowadays as the biggest challenges in ensuring the security of corporate data?
3) What are some of the biggest challenges your company or clients face?
4) Do you see phishing as a big threat to companies nowadays and in upcoming future? Why or why not?
5) How can phishing threats be mitigated or prevented?
6) What do you consider as a strong password policy? How can that be enforced?
7) Do you think that employee password choices often times put a company at risk?
8) How can password related threats be mitigated? (Password length, complexity, random passwords)
9) Do you think BYOD policy is a threat to organizational security? Why or why not?
10) How can BYOD policy be enforced? (How can you check that your employees actually have pins/passwords on the smartphone?)
11) How can threats related to BYOD be mitigated and prevented?
12) When an organization gives you a laptop to use (new laptops are lockdown, older one not), what are your biggest concerns related to security?
13) How can those concerns be mitigate and prevented?

14) Based on your experience, how are user awareness programs implemented within various organizations?
15) What are the characteristics of good user awareness programs? What are the characteristics of bad ones?
16) How can company employees see the benefit of the security awareness programs and be actively involved in creating the security culture?
17) What are the few things that companies must do at a minimum do operate securely? How critical is the user awareness program for a company to have?

Appendix C: Correlation Matrix for Dependent and Independent Variables

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. Security Victim Likelihood (DV)	1														
2. Actual Security Knowledge (DV)	-.11	1													
3. Security Policy Knowledge (DV)	-.09	.06	1												
4. Sex	.21**	-.20**	.03	1											
5. Age	-.16*	-.05	.19**	-.17*	1										
6. Education	.06	.08	.02	-.22**	.11	1									
7. Security Training	-.01	.06	.09	.01	.04	.08	1								
8. Years Employed	.01	-.08	.12	-.01	.33**	-.05	-.17**	1							
9. Job Role	-.13*	.19**	-.02	-.17**	-.10	.01	.07	-.19**	1						
10. Industry Sector	-.11	.08	.02	-.16*	-.03	-.11	-.02	-.16*	.00	1					
11. Internet Knowledge	-.27**	.23**	.01	-.25**	.04	.17**	.09	-.11	.31**	.09	1				
12. Technical Background	-.12	.18**	-.04	-.32**	.05	.14*	.04	-.10	.52**	.05	.44**	1			
13. Perceived Technical Knowledge	-.28**	.28**	.03	-.46**	.14*	.13*	.09	-.05	.41**	.11	.65**	.53**	1		
14. Perceived Security Awareness	-.30**	.09	.23**	-.16*	.19**	.12	.18**	.00	.15*	.07	.49**	.21**	.40**	1	
15. Perceived Security Policy Knowledge	-.36**	-.04	.33**	.05	.23**	.04	.26**	.01	-.05	.02	.19**	-.05	.15*	.52**	1

Note: * p<.05 ** p<.01

11. References

[1] Ponemon Institute Releases 2014 Cost of Data Breach: Global Analysis. (n.d.). Retrieved February 18, 2015, from http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis

[2] Top 10 Social Engineering Tactics | #10. Social Engineering in Reverse | InformIT. (n.d.). Retrieved February 17, 2015, from http://www.informit.com/articles/article.aspx?*p*=1350956

[3] The new users' guide: How to raise information security awareness (EN) — ENISA. (n.d.). Retrieved January 28, 2015, from https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide

[4] ThreatTrack Security. (n.d.). *2015 Predictions from the Front Lines: Cybersecurity Professionals Very Confident in Their Ability to Fight Data Breaches in 2015*. Retrieved from http://www.threattracksecurity.com/resources/white-papers/2015-predictions-from-the-front-lines.aspx

[5] Olavsrud, T. (2014, December 10). 5 Information Security Trends That Will Dominate 2015. Retrieved from http://www.cio.com/article/2857673/security0/5-information-security-trends-that-will-dominate-2015.html

[6] Ellyat, H. (2015, January 5). Top 5 cybersecurity risks for 2015. Retrieved from http://www.cnbc.com/id/102283615

[7] Pescatore, J. (2014). *2014 Trends That Will Reshape Organizational Security*. Retrieved from http://www.sans.org/reading-room/whitepapers/analyst/2014-trends-reshape-organizational-security-34625

[8] Davis, G. (2014, December 29). 2014: Security Year in Review. Retrieved from https://blogs.mcafee.com/consumer/2014-security-year-review

[9] Blue, V. (2014, November 19). 10 top security threats of 2014 (so far). *ZDNet.* Retrieved from http://www.zdnet.com/article/10-top-security-threats-of-2014-so-far/2/

[10] Symantec. (2011). *Advanced Persistent Threats: A Symantec Perspective Preparing the Right Defense for the New Threat Landscape*. Retrieved from http://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf

[11] Hayes, S., Shore, M., & Jakeman, M. (2012). The Changing Face of Cybersecurity. *ISACA Journal*, *6*, 29.

[12] Ferrillo, P. (2015, January 20). Changing the Cyber Security Playing Field in 2015. Retrieved from http://blogs.law.harvard.edu/corpgov/2015/01/20/changing-the-cyber-security-playing-field-in-2015/

[13] Social Engineer, INC. (n.d.). What is Social Engineering? Retrieved from http://www.social-engineer.org/

[14] Parrish Jr, J. L., Bailey, J. L., & Courtney, J. F. (2009). A Personality Based Model for Determining Susceptibility to Phishing Attacks. *Little Rock: University of Arkansas*. Retrieved from http://www.swdsi.org/swdsi2009/Papers/9J05.pdf

[15] Whitaker, A. (2009, June 11). Top 10 Social Engineering Tactics. Retrieved from http://www.informit.com/articles/article.aspx?*p*=1350956

[16] VERACODE. (2013, March 6). Hacking the Mind: How & Why Social Engineering Works. Retrieved from http://www.veracode.com/blog/2013/03/hacking-the-mind-how-why-social-engineering-works

[17] Trend Micro. (n.d.). Targeted Attacks. Retrieved from http://www.trendmicro.com/vinfo/us/security/definition/targeted-attacks#

[18] Ragucci, J. W., & Robila, S. A. (2006). Societal aspects of phishing. In *Technology and Society, 2006. ISTAS 2006. IEEE International Symposium on* (pp. 1–5). IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4375893

[19] Kessem, L. (2013, January 15). Laser Precision Phishing — Are You on the Bouncer's List Today? Retrieved from https://blogs.rsa.com/laser-precision-phishing-are-you-on-the-bouncers-list-today/

[20] APWG. (2014). *Phishing Activity Trends Report*. Retrieved from http://docs.apwg.org/reports/apwg_trends_report_q1_2014.pdf

[21] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 373–382). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=1753383

[22] Trend Micro, TrendLabs APT Research Team. (2012). *Spear-Phishing Email: Most Favored APT Attack Bait*. Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf

[23] Srikwan, S., & Jacobsson, M. (n.d.). *A Phishing Cartoon Collection*. Retrieved from http://www.securitycartoon.com/

[24] Bull, D. (2015, January 26). Don't Let Cybercriminals Go Phishing in Email Inboxes. Retrieved from https://blogs.mcafee.com/business/security-connected/cybercriminals-go-phishing-in-email-inboxes

[25] Statista. (2014). *Phishing: most targeted industries 2014*. Retrieved from http://www.statista.com/statistics/266161/websites-most-affected-by-phishing/

[26] Moore, J. (2014, December 4). Health Care Industry To See Phishing, Malware Attacks Intensify in 2015. *iHealthBeat*. Retrieved from http://www.ihealthbeat.org/insight/2014/health-care-industry-to-see-phishing-malware-attacks-intensify-in-2015

[27] ID Experts. (2014). *Criminal Attacks on Healthcare Organizations Increase 100 Percent*. Retrieved from https://www2.idexpertscorp.com/press/single/criminal-attacks-on-healthcare-organizations-increase-100-percent

[28] Darwish, A., Zarka, A. E., & Aloul, F. (2012). Towards understanding phishing victims' profile. In *Computer Systems and Industrial Informatics (ICCSII), 2012 International Conference on* (pp. 1–5). Retrieved from http://www.researchgate.net/profile/Fadi_Aloul/publication/261384277_Towards_understanding_phishing_victims%27_profile/links/0deec53a48323b308d000000.pdf

[29] Identity Theft Resource Center. (n.d.). *Identity Theft Resource Center Breach Report Hits Record High in 2014*. Retrieved from http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html

[30] Hardekopf, B. (2015, January 13). The Big Data Breaches of 2014. *Forbes*. Retrieved from http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/

[31] EC-Council. (2012, September). *Ethical Hacking and Countermeasures*. Retrieved from http://www.slideshare.net/th3prodeveloppер/th3-professional-developper-ceh-social-engineering

[32] Ponemon Institute. (2014). *2014 Cost of Data Breach Study: Global Analysis*. Retrieved from http://www-935.ibm.com/services/multimedia/SEL03027USEN_Poneman_2014_Cost_of_Data_Breach_Study.pdf

[33] Zviran, M., & Haga, W. J. (1999). Password security: an empirical study. *Journal of Management Information Systems*, 161–185.

[34] Riley, S. (2006). Password security: What users know and what they actually do. *Usability News*, *8*(1), 2833–2836.

[35] CSID. (2012). Consumer Survey: Password Habits. Retrieved from http://www.csid.com/wp-content/uploads/2012/09/CS_PasswordSurvey_FullReport_FINAL.pdf

[36] Ross, J. (2014). *How To Change Employees' Poor Password Habits*. Retrieved from https://www.privacyassociation.org/news/a/how-to-change-employees-poor-password-habits

[37] Winder, D. (2011, December 2). Top ten password cracking techniques. Retrieved from http://www.pcpro.co.uk/features/371158/top-ten-password-cracking-techniques/page/0/1

[38] Mitchell. (n.d.). Password Cracking. Retrieved from http://web.cs.du.edu/~mitchell/forensics/information/pass_crack.html

[39] Condliffe, J. (n.d.). The 25 Most Popular Passwords of 2014: We're All Doomed. Retrieved from http://gizmodo.com/the-25-most-popular-passwords-of-2014-were-all-doomed-1680596951

[40] Password length limits in history of operating systems and popular web sites. (2013). Retrieved from http://security.stackexchange.com/questions/22721/password-length-limits-in-history-of-operating-systems-and-popular-web-sites

[41] Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., … Cranor, L. F. (2010). Encountering stronger password requirements: user attitudes and behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (p. 2). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=1837113

[42] Kelley, P. G., Komanduri, S., Mazurek, M. L., Shay, R., Vidas, T., Bauer, L., et al.445654654546 (2012). Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In *Security and Privacy (SP), 2012 IEEE Symposium on* (pp. 523–537). IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6234434

[43] Gibson Research Corporation. (2012, March 28). How Big is Your Haystack? ... and how well hidden is YOUR needle? Retrieved from https://www.grc.com/haystack.htm

[44] Stanton, J. M., Mastrangelo, P., Stam, K. R., & Jolton, J. (2004). Behavioral Information Security: Two End User Survey Studies of Motivation and Security Practices. In *10th Americas Conference on Information Systems, AMCIS 2004, New York, NY, USA, August 6-8, 2004* (p. 175). Retrieved from http://www.researchgate.net/publication/220890851_Behavioral_Information_Security_Two_End_User_Survey_Studies_of_Motivation_and_Security_Practices

[45] Gott, A. (2014, July 14). 6 Mistakes Employees Are Making with Passwords. Retrieved from https://blog.lastpass.com/2014/07/6-mistakes-employees-are-making-with-passwords.html/

[46] Cunningham, K. (n.d.). Password Management Problems: Employees Significantly Increasing Risk of Security Breaches. Retrieved from https://www.sailpoint.com/blog/2015/01/survey-password-management/

[47] Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security*, *42*, 56–65. http://doi.org/10.1016/j.cose.2014.01.005

[48] Ponemon Institute. (2012). *2013 State of the Endpoint*. Retrieved from http://www.ponemon.org/local/upload/file/2013%20State%20of%20Endpoint%20Security%20WP_FINAL4.pdf

[49] Thayer, J. (2013, November 15). Why The BYOD Trend Is So Popular. Retrieved from http://www.cyber-knowledge.net/blog/why-the-byod-trend-is-so-popular/

[50] Barker, C. (2014, October 29). BYOD: Why the biggest security worry is the fool within rather than the enemy without. *ZDNet*. Retrieved from http://www.zdnet.com/article/byod-why-the-biggest-security-worry-is-the-fool-within-rather-than-the-enemy-without/

[51] McAfee. (2014). Smarter BYOD Do it right. Retrieved from http://www.mcafee.com/us/resources/solution-briefs/sb-byod-mobile.pdf

[52] Phifer, L. (2013, January). Allowing employee-owned mobile devices doesn't have to mean accepting all BYOD risks. Infosec pros share their BYOD security strategies. *TechTarget*. Retrieved from http://searchsecurity.techtarget.com/feature/BYOD-security-strategies-Balancing-BYOD-risks-and-rewards

[53] Blevins, B. (2013, June 13). Enterprise BYOD offers mixed bag for enterprise endpoint security. *TechTarget*. Retrieved from http://searchsecurity.techtarget.com/news/2240186008/Enterprise-BYOD-offers-mixed-bag-for-enterprise-endpoint-security

[54] Johnston, C. (2013, April 29). Why your password can't have symbols—or be longer than 16 characters. *Ars Technica*. Retrieved from http://arstechnica.com/security/2013/04/why-your-password-cant-have-symbols-or-be-longer-than-16-characters/

[55] Scarfone, K., & Souppaya, M. (2009). Guide to Enterprise Password Management (Draft). *NIST Special Publication 800-118*. Retrieved from http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

[56] TechNet Magazine. (n.d.). Best Practices for Enforcing Password Policies. Retrieved from https://technet.microsoft.com/en-us/magazine/ff741764.aspx

[57] iOS No More Secure Than Android When It Comes To Enterprise Security. (n.d.). Retrieved July 25, 2015, from http://www.phonenomena.com.au/blog/2014/07/01/enterprise-mobility-ios-vs-android-byod-security-threat/

[58] Most Secure Mobile Operating System | INFOSEC MAESTROS Awards 2015 | Recognising Security Excellence. Redefining Security Leadership. (n.d.). Retrieved July 25, 2015, from http://www.infosecmaestros.com/blog/most-secure-mobile-operating-system

[59] Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165. http://doi.org/10.1016/j.dss.2009.02.005

[60] Zhang, Y., Monrose, F., & Reiter, M. K. (2010). The security of modern password expiration: an algorithmic framework and empirical analysis. In *Proceedings of the 17th ACM conference on Computer and communications security* (pp. 176–186). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=1866328

[61] Capgemini Consulting. (2013). Bring Your Own Device It's all about Employee Satisfaction and Productivity, not Costs!. Retrieved from https://www.capgemini-consulting.com/resource-file-access/resource/pdf/bringyourowndevice_29_1.pdf

[62] Spitzner, L., & Rudis, B. (2015, March 27). 2015 Security Awareness Report! SANS Securing The Human!. Security Awareness @ SANS Webcast. Webcast retrieved from https://www.sans.org/webcasts/99782

[63] Best Practices for Data Security: Part 2 - Hypersecu Information Systems,Inc. (n.d.). Retrieved July 25, 2015, from https://www.hypersecu.com/blog/115-best-practices-for-data-security-part-2

[64] Kraus, L., Hirsch, T., Wechsung, I., Poikela, M., & Möller, S. (2014). Poster: Towards an Instrument to Measure Everyday Privacy and Security Knowledge. In *Unpublished, accepted for publication at the Symposium on Usable Privacy and Security (SOUPS), Menlo Park, CA, USA*. Retrieved from http://cups.cs.cmu.edu/soups/2014/posters/soups2014_posters-paper16.pdf