CYBERSECURITY BEHAVIOR IN ORGANIZATIONS: A LITERATURE REVIEW

A Thesis

by

RANG YAN

Submitted to the Office of Graduate and Professional Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Chair of Committee,	Olabisi A. Atoba
Committee Members,	Winfred Arthur, Jr.
	Wendy Boswell
Head of Department,	Heather Lench

December 2019

Major Subject: Psychology

ABSTRACT

Cybersecurity have drawn special attention of organizations in the 21st century because of the prevalent use of technology at work. Organizations of all sizes are dependent on computers for storage, management, and transmission of confidential information and any cybersecurity breaches can lead to reputation damages and financial losses for organizations. Consequently, the ubiquitous use of technologies at work leads to a call for attention to cybersecurity. The achievement of cybersecurity goals depends on a number of factors and although many researchers have examined the independent effects of certain factors on individuals' cybersecurity behavior, there is relatively little research that takes an interactional psychology perspective to examine how individual factors, organizational factors, and factors related to methods and measurement intersect to inform and/or facilitate cybersecurity behavior.

Thus, the primary purpose of this thesis was to review the literature on cybersecurity behaviors at work through an intersection of the three areas of I-O (i.e., personnel, organizational, and methods and measurement). A detailed search in GoogleScholar, PsycINFO, ProQuest Dissertations and Theses using the keywords "cybersecurity behavior", "information security behavior", "cyber-CWB" was conducted to retrieve relevant journal articles, book chapters, conference papers, and dissertations on cybersecurity. Specifically, this literature review synthesizes empirical research on (a) individual difference variables that predict cybersecurity behavior (e.g., personality traits, cognitive ability, and intention) and training to improve the knowledge, skills, and attitudes of employees, (b) organizational factors that affect cybersecurity behavior (e.g., leadership and organizational culture), (c) methods for assessing cybersecurity behavior (e.g., self-report questionnaire and simulation test), and (d) a discussion

that integrates the three aforementioned areas. The thesis concludes with a discussion of contributions to science and practice, limitations, future research directions, and recommendations, which provide a framework that organizations can implement to reduce the cybersecurity risks resulting from human factors.

DEDICATION

This is for:

My fiancée, for your love, support, and encouragement.

ACKNOWLEDGEMENTS

I would like to express my appreciation to my family for their unconditional love and support. I would not be able to purse my dreams without them. Special thanks are due to Dr. Olabisi Atoba, my thesis committee chair. She facilitated my independence while consistently offering critical support. I am grateful for her guidance and collaboration. Finally, I would like to dedicate this article to my fiancée who provided constant love, support and encouragement and accompanied me on this journey.

CONTRIBUTORS AND FUNDING SOURCES

Contributors

This work was supervised by the student's thesis committee chair, Dr. Olabisi A. Atoba, with Professor Winfred Arthur, Jr., of the Department of Psychological and Brain Sciences, and Professor Wendy Boswell of the May's Business School as committee members. It also reflects feedback from Professor Stephanie C. Payne.

Funding Sources

There are no outside funding contributors to acknowledge related to this research and compilation of this document.

TABLE OF CONTENTS

LIST OF FIGURES

Page

LIST OF TABLES

Page

1. INTRODUCTION

Information and communication technologies have brought dramatic changes in the way people communicate with others, the way they work, as well as the way organizations do business. The ability to digitize information and to exchange them with anyone around the world via electronic devices now enables humans to connect globally. Such technologies allow people to share information immediately and expansively as 21st century organizations are now more interconnected through file sharing, blogs, and social networking sites, to name a few (Wheeler, 2014; Wingfield, 2016). However, this dependency on the Internet of things has heightened the vulnerability of organizations to cyberattacks, that is deliberate actions that may destroy, disrupt, or degrade data, software, or hardware in computer systems and networks (Denning & Denning, 2010). It could come in the form of viruses or unauthorized user access.

Cybersecurity breaches that occur due to cyberattacks can result in great reputation damage and significant financial losses for organizations (Goel & Perlroth, 2016; Quinn & Arthur, 2011). For example, in 2011, Sony spent around $171 million on cleaning up and remediating its PlayStation Network breach that affected about 77 million online accounts (Quinn & Arthur, 2011). During the second half of 2016, Yahoo disclosed two massive two data breaches that exposed personal information of user account. The first data breach in 2013 was believed to have diclosed more than 1 billion user accounts. The second breach, occurring in late 2014, compromised the account details of 500 million users. These breaches led to an approximate $350 million reduction in Yahoo's sale price (Goel & Perlroth, 2016). Therefore, to ensure continued organizational effectiveness, the issue of cybersecurity is prioritized by modern organizations worldwide.

Because the development of conceptual definitions is a critical step in understanding constructs in psychological science and is necessary for measurement, some definitions are necessary here. Cybersecurity refers to the body of technologies and practices that are designed to protect cyber data from security threats from both internal users and external attackers (Beyer & Brummel, 2015). It is a subset of information security given that the latter focuses on defending both electronic and physical information (Buchy, 2016).

Cybersecurity is important to organizations' success because most organizations collect, process, and store inconceivable amounts of data related to their personnel and their practices and they transmit such data across networks on a daily basis (Gupta & Hammond, 2005). A significant portion of such data are sensitive or confidential such as business information, financial records, personnel information, and trade secrets and illegitimate access to or disclosure of such information can lead to disastrous results. In fact, given the increased volume and sophistication of cyberattacks, James Clapper, the Director of National Intelligence Agency in the United Stated, made an announcement in March 2013 that cybersecurity has become the biggest threat to the national security of the country, surpassing terrorism (Hosenball & Zangerle, 2013).

Granted, cyberattacks are often carried out by external hackers, however, employees within an organization or insiders can pose a greater danger to its information security. For example, in 2010, WikiLeaks publicized hundreds of thousands of U.S. classified military documents and diplomatic cables obtained from a whistleblower Chelsea Manning, a former U.S. Army intelligence analyst. Those files exposed controversial U.S. military war actions in Iraq and Afghanistan and threatened the lives of U.S. soldiers in the field as well as diplomats. Similarly, Vanson Bourne, a consulting firm that specializes in tech research, reported in 2016

that 20% of employees are willing to sell their personal login account details to an outsider. In the 2018 Computer Crime and Security Survey conducted by Computer Security Institute, 44% of 522 computer security practitioners surveyed reported the occurrence of insider abuse of networks in their organizations, which makes insider abuse the second most frequent form of cybersecurity issue, falling behind virus incidents (49 % of respondents). Another survey of employees in global organizations discovered that 59% of employees reported that they had taken sensitive corporate data with them before they left their positions (e.g., customer contact lists) in hopes of converting this into cash (Symantec & Ponemon, 2009). Furthermore, the U.S. Federal Bureau of Investigation investigated the 2014 cyberattack of Yahoo for two years and found that the breach was due to one employee's mistaken click on a link embedded in a phishing email (Williams, 2017).

As employees' behaviors remain the major source of threat to cybersecurity in organizations, more scholars are doing more research on the antecedents of cybersecurity behaviors. Russel, Weems, Ahmed, and Richard (2017) define cyber behaviors as actions that promote (i.e., cyber-secure) or disrupt (i.e., cyber-insecure) the ability to protect the use of cyberspace from cyberattacks. Secure cyber behavior, also known as cybersecurity behavior, involves a wide spectrum of specific behaviors which can be generally categorized into two groups, namely intentional security behavior and unintentional security behavior (Im & Baskerville, 2005). Intentional cybersecurity behavior includes complying with cybersecurity policies and following prescribed procedures. Unintentional cybersecurity behavior is the desired spontaneous behavior that is done unconsciously, which can increase the information security of an organization (Im & Baskerville, 2005), such as locking computer screen displays when not in use, reporting a computer virus when alerted by an anti-virus program, or encrypting the

organization's confidential information during storage and/or distribution. On the other hand, employee's insecure cyber behaviors that are in conflict with the organization's cybersecurity goals can be regarded as a form of counterproductive work behavior (CWB) given its potential harm to the organizations. CWB, in general, refers to undesirable actions and behaviors that harm organization itself and its stakeholders (Ones & Dilchert, 2013). In light of this, cyber-CWB is defined as employee behaviors that directly harm the organization through the use of information communication technology (Mercado, 2017). This definition covers a wide range of behaviors such as intellectual property violations, technological theft, and cyberloafing. Figure 1 illustrates the classification of cyber behaviors.

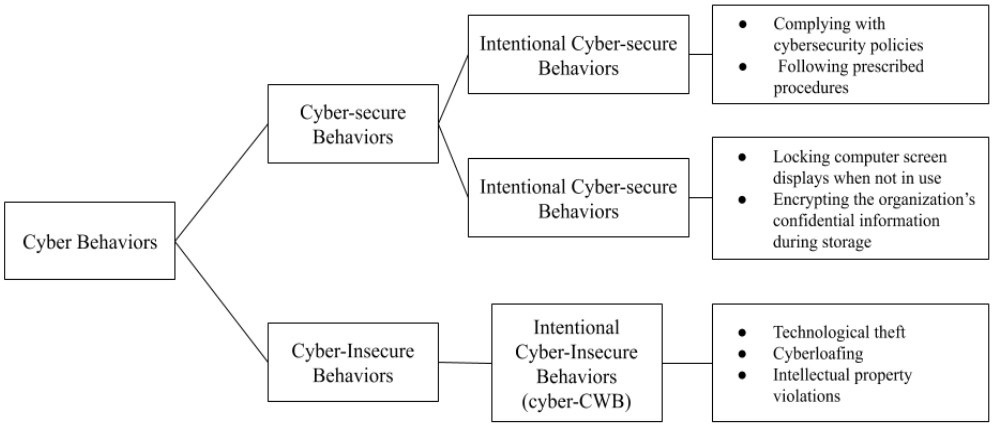

Figure 1. Classification of cyber behaviors.

Given that cybersecurity continues to be an issue that organizations contend with, the objective of this thesis is to (a) summarize the literature that captures the efforts that

organizations have taken to address the cybersecurity crisis, (b) examine the literature through the content domain areas of industrial-organizational (I-O) psychology, namely personnel psychology, organizational psychology, as well as methods and measurement, and (c) a discussion of how the three aforementioned areas of I-O intersect with cybersecurity. The thesis closes with a discussion of scientific and practical implications, limitations, future research directions, and recommendations for organizations.

2. CYBERSECURITY BEHAVIORS THROUGH A PERSONNEL PSYCHOLOGY LENS

The industrial (I) side of I-O psychology, also called personnel psychology, attends to individual differences and the relationship between those differences and job performance (Cascio & Aguinis, 2018). Personnel psychology assesses each individual's knowledge, skills, abilities and other characteristics in order to fit individuals to specific positions. Topics in this area include recruitment, employee selection, training, and performance appraisal and management.

To deal with the current cyber threat environment in which they exist and to achieve their cybersecurity goals, organizations now defend against external threats by utilizing advanced anti-virus software which quarantines viruses that seek to infect computer systems, and firewall protection which blocks unauthorized access from hackers. Although such computer protection systems continue to have some success, organizations also realize that they do not address all cybersecurity issues given that humans are the generators and end-users of data. Thus, organizations depend on developing well-informed computer and mobile device users or employees to keep data and transaction safe. In light of this, this section reviews what previous research has reported concerning how to identify candidates who are more likely to participate in secure computing practices to mitigate the computer vulnerability and how to train employees with the knowledge and skills necessary for performing cybersecurity behaviors.

2.1 Predicting Employee Cybersecurity Behaviors

The recruitment and selection of individuals who are less likely to pose cyber threats to the organization is a critical step in an information security strategy (Shappie, Dawson & Debb,

2019). Although cyberattacks from an outside source are often highlighted in the mainstream media as the primary threat to the cybersecurity, evidence suggests that the majority of data breaches are due to employees inside organizations (Richardson, 2008). As stated in the research conducted by Shred-it (2018), 47% of C-suite executives reported that employee negligence, such as accidental loss of USB devices or computers, accounted for 69% of information leakage. In addition, 42% of small business owners said that 71% of data breaches were caused by employee negligence. Moreover, based on interviews with over 700 IT professionals in 159 organizations across the world, a recent survey conducted by the Symantec Corporation and the Ponemon Institute (2018) revealed that among all 3269 reported cyberattacks, 2081 (64%) attacks were attributed to employee or contractor negligence, and malicious insiders caused another 748 (23%) attacks. Consequently, current employees pose even more danger to organizations' information security than external hackers given their familiarity with the corporate information systems and their access to confidential data during routine work (Johnston & Warkentin, 2010). In fact, in addition to IT professionals, nearly all employees interacting with data play a critical cyber security role in organizations (Beyer & Brummel, 2015). Hence, technological solutions alone are not sufficient and it is necessary for scholars to investigate the predictors associated with an employee's cybersecurity behavior in the context of an organization.

2.1.1 *Personality*

Personality is expected to have a relationship with cybersecurity behaviors in organizations. Personality refers to an individual's relatively stable pattern of thinking, feeling, and behaving in a variety of situations (Gatewood, Field, & Barrick, 2016). It determines how s/he copes with uncertainty, adjusts to obstacles, interact with others, and determines behavior at

work (Gatewood et al., 2016). In fact, many studies have pointed out that personality is a strong antecedent of both cybersecurity awareness and actual cybersecurity behavior (e.g., Bansal, 2011; Hadlington & Murphy, 2018; McCormac et al., 2017). For example, a research study examining the relationship between the Big Five personality factors and information security indicated that individuals who scored high on conscientiousness, emotional stability, and extraversion expressed more concern about privacy and information security at work (Bansal, 2011). The study also found that openness to experience, agreeableness, conscientiousness, and emotional stability were positively related to cybersecurity awareness. Specifically, people high in conscientiousness and/or emotional stability care more about four cybersecurity issues: authentication of the website, privacy of personal information, prevention of personal information corruption while sending it over the web, and disputability of online transaction. Extraverted people were more concerned than introverted people with whether websites can prevent their personal information from getting corrupted. Additionally, openness, agreeableness, conscientiousness, and emotional stability were found to contribute to the prediction of cybersecurity awareness and conscientiousness was the most significant predictor among all Big Five personality factors (McCormac et al., 2017). This is important because individuals with high cybersecurity awareness understand their organizations' cybersecurity policies and guidelines better and have stronger intentions to comply with such polices than individuals with low cybersecurity awareness (Bansal, 2011). The possible explanation is that cybersecurity awareness is positively related to Internet/computer self-efficacy and attitudes towards cybersecurity behaviors, the two determinants of behavioral intention (Flores & Ekstedt, 2016).

With respect to the impact of personality on cybersecurity behaviors, a recent study found that conscientiousness, agreeableness, and openness to experience were closely associated with self-reported cybersecurity behaviors (Hadlington & Murphy, 2018). Specifically, individuals who scored high on these personality dimensions were more inclined to participate in activities that benefit information security systems and comply with cybersecurity policies or keeping anti-virus software up-to-date. Moreover, results from a meta-analytic investigation indicated that conscientiousness and agreeableness related negatively to different forms of cyber-CWB (e.g., cybertheft, cyberloafing, hacking), while emotional stability and openness exhibited small negative relationship with cyber-CWB.

In another study, further evidence suggested that conscientiousness was a significant predictor of individuals' behavioral intentions concerning strong password generation and updating. That is, people high in conscientiousness may be more prone to regularly keep their software up-to-date and generate strong passwords compared to less conscientious people (Gratian, Bandi, Cukier, Dykstra, & Ginther, 2018). A potential explanation for these findings is that because conscientiousness is associated with obedience (Bègue et al., 2015), cautiousness, orderliness, dependability and responsibility for protecting organizations (Connelly, Davies, Ones, & Birkland, 2008), highly conscientious individuals are more likely engage in secure cybersecurity behavior in compliance with company guidelines or policies and go the "extra step" to ensure information security rather than performing cyber-CWB related to negligence.

Concerning agreeableness, results from a meta-analysis demonstrate that agreeableness displays a strong negative relationship with antisocial behaviors as well as both interpersonal and task-based conflicts (Jones, Miller, & Lynam, 2011). Consequently, to build intimate relationship with supervisors, those high in agreeableness are more likely to comply with organizational

cybersecurity rules compared to engaging in deviant behaviors such as hacking and cybercrime. For openness to experience, individuals high on this trait may be more receptive to information security training, and more likely to act out trained behaviors to resist external cyber threats. Finally, a study among university students found that students with low emotional stability are more susceptible to phishing attacks (Halevi, Lewis & Memon, 2013). Perhaps this was so because individuals low on emotional stability may be too anxious to devote enough mental resources to engage in appropriate cybersecurity behavior when facing cyberattacks.

These studies provide evidence that improving cybersecurity practices can be achieved through selecting applicants who are high on the said personality characteristics. Figure 2 illustrates how personality traits are related to cyber behaviors as well as cybersecurity awareness.

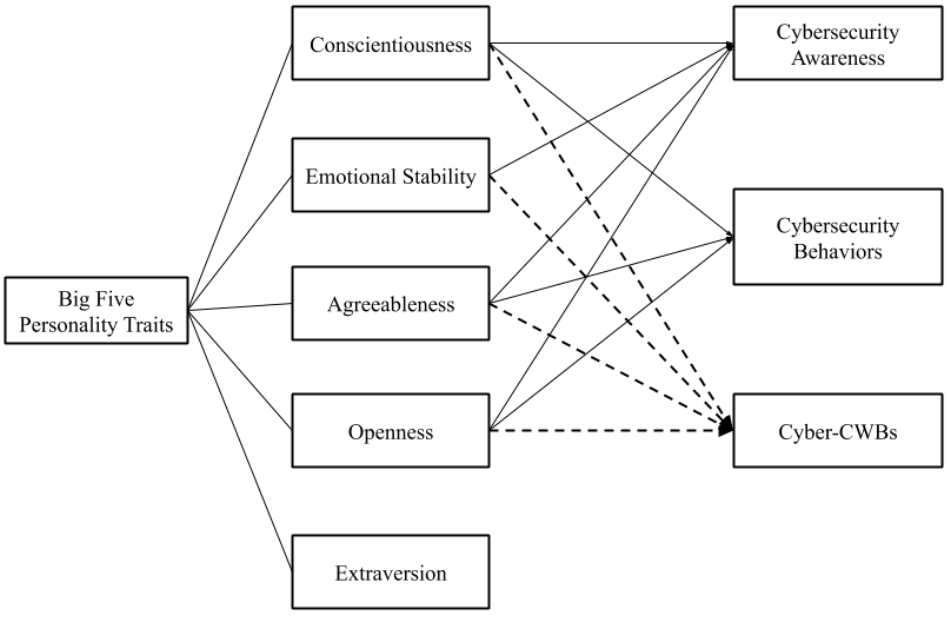

Figure 2. The relationship between personality and cybersecurity awareness and behaviors.

2.1.2 *Cognitive Ability*

Due to their utility for employee selection, researchers have heavily studied the effect of cognitive ability as a predictor of CWBs in general. For example, Dilchert, Ones, Davis and Rostow (2007) have empirically demonstrated a relationship between cognitive ability and CWB. The potential explanation is that individuals with lower cognitive ability might fail to achieve the rewards or compensation they desire from their jobs, therefore, they attempt to acquire desired but unearned resources through engaging in CWB.

Given the existing negative relationship between cognitive ability and CWB, one may expect a similar direction for cyber-CWB. However, an empirical study found that cognitive ability was not related to most forms of cyber-CWB, such as hacking and cybersabotage (Mercado, 2017). Although one may expect that employees who are low on cognitive ability may engage in cyber-CWB due to inability to consider long-term consequences, it should be noted that such employees likely lack the creative thinking and intelligence needed to engage in cyber-CWB behaviors (Mercado, 2017). It is also important to mention that the above results should be considered carefully because cognitive ability in this study was assessed through a test that measured only one fluid ability. Future studies using a more comprehensive measure of cognitive ability is needed to contribute more fully to our theoretically understanding of the relationship between cognitive ability and cyber-CWB.

2.1.3 *Intention*

A rich body of literature exists on the intention-behavior relationship. The theory of planned behavior states that an individual's intentions to perform a behavior has a strong relationship with his/her actual behavior (Ajzen, 2005). Hence, in many studies, behavioral

intentions are measured to represent actual behavior when scholars face practical difficulties in measuring actual behavior (for some examples, see Pavlou & Fygenson, 2006; Siponen & Vance, 2010). Theory of planned behavior model also contends that variance in intentions are explained by three factors, attitudes towards the behavior, subjective norms, and perceived behavioral control. Attitudes are evaluation of behavior that express one's feeling towards and belief about behavior. Subjective norms refer to an individual's perceptions of whether a behavior is accepted and encouraged by others who are in connection with and important to him or her (Ajzen, 2005). Perceived behavior control reflects the perceived ease or difficulty of performing a behavior (Ajzen, 2005). Extending this notion to cybersecurity, an extensive amount of literature about individual behavior in diverse settings has provided strong evidence for the reliability of the TPB in predicting individual intention to comply with cybersecurity policies. (Ajzen, 2005; Dinev & Hu, 2007; Hu et al., 2012; Pavlou & Fygenson 2006). All three antecedents of compliance intention exhibit strong effect and subjective norms are the strongest predictor, whereas attitude is the least strong predictor.

Although the intention-behavior relationship has gained much theoretical support, previous research has also found that employees rarely protect organizational data and take action to follow relevant policies, even when they intend to comply with security policies and practices (Shropshire, Warkentin, & Sharma, 2015). The possible explanation is that intention is a cognitive process while behavior is determined by transient impulsivity that require less cognitive effort (Willison & Warkentin, 2013). Given the intention behavior gap, it is critical to examine other possible predictors in order to better understand cybersecurity behaviors.

2.1.4 *Integrity*

Integrity tests are typically aimed to aid in the selection and identification of job

applicants who are honest, trustworthy and less likely to engage in CWB. Generally, there are two forms of integrity test: (a) overt integrity tests; and (b) personality-oriented measures. Over integrity tests directly ask job applicants about their attitudes toward counterproductive behaviors. Examples of such items includes: "Have you ever overcharged someone for your personal gain?" and "Did you ever think about doing something that, if you had done it, would have been a crime?" (Gatewood et al., 2016). Stanton Survey and Reid Report are two commonly used integrity tests. In contrast, personality-oriented measures do not ask about counterproductive behaviors directly. Instead, they measure personality traits linked to specific organizational delinquency. The Hogan Personality Inventory (HPI) is one such personality-based integrity measure (Hogan & Hogan, 1989). One of its subscales is the reliability scale which measures integrity and honesty.

Ones, Viswesvaran, and Schmidt (1993) published a comprehensive meta- analysis of the integrity test literature which includes 665 criterion-related validity values obtained from over 570,000 test takers. Among their findings, the research demonstrated high validity coefficients for both overt and personality-based integrity tests in predicting CWBs such as theft, absenteeism, and violence. Similarly, an updated meta-analysis conducted by Van Iddekinge, Roth, Raymark, and Odle-Dusseau (2012) provides further support for the integrity-CWB behavior. However, given the high overlap between integrity tests and personality tests, some scholars regarded integrity tests as a personality tests measuring conscientiousness, agreeableness and emotional stability (Sackett & Schmitt, 2012). In contrast, Sackett and Wanek (1996) argued that integrity tests increase the predictive ability of job performance over personality measures as integrity tests include items measuring self-control, which is less likely

to be captured in Big-Five inventories. This is supported by the research study that examines the integrity-job performance relationship while controlling for the impact of conscientiousness (Ones & Viswesvaran, 2007). Therefore, integrity tests contribute independently to the prediction of job performance because of the substantial correlation between self-control and job performance. For cyber-CWBs, a study that examined the cyber-CWBs relationship with personality, integrity, and cognitive ability suggests that integrity is the best predictor of cyber-CWBs such as cybertheft, cybersabotage, and negligent IT practices etc. (Mercado, 2017). Based on the research reviewed, integrity may be a key consideration in the development of practical interventions to avoid and reduce these cyber-CWBs because of its validity in predicting certain undesirable work behavior.

2.1.5 *Other Predictors*

Additional research which focus on different predictors of cybersecurity behavior has found that past security compliance habits, computer/Internet self-efficacy, levels of computer skills and previous experience with cybersecurity practices predict an employee's future cybersecurity behaviors (Hearth & Rao, 2009; Ng, Kankanhalli, & Xu, 2009; Son, 2011; Vance, Siponen, & Pahnila, 2012). Computer/Internet self-efficacy refers to an individual's confidence in his or her skills or ability with regard to computer security (Ng et al., 2009).

Selection is the basis for various types of employee and organizational outcomes such as organizations' effectiveness of cybersecurity initiatives. Through selecting applicants who are more likely to engage in cybersecurity behavior, it may be easier for an organization to develop a culture where cybersecurity behavior is appreciated. With the increasingly connected workplace whereby employees rely on the internet, computing devices have become common tools used by almost all employees. Consequently, it is important for employers to incorporate predictors of

cybersecurity behaviors into the selection system in addition to the knowledge, skills, abilities, and other characteristics necessary for successful task performance. For instance, integrity and personality traits, especially conscientiousness, can be assessed in the selection process for both cybersecurity professionals and end-users who have access to confidential or sensitive data. Generally, Big Five personality traits were assessed using inventories such as the Hogan Personality inventory (Hogan & Hogan, 1995) or the Big Five Inventory (John, Donahue, & Kentle, 1991). Given that empirical evidence with respect to cybervetting is limited, it is recommended that organizations should only take into account job-related information to assess job applicants. Additionally, computer skills and past cybersecurity compliance habits could be assessed through an application blank.

In sum, compared to stated intention, both personality factors and integrity play a more critical role in understanding cybersecurity behaviors and is supported through empirical evidence (e.g., Bansal, 2011; Mercado, 2017; McCormac et al., 2017). Therefore, using personality inventories and integrity tests to identify individuals who have higher propensity for performing cybersecurity behaviors is a promising way for organizations to reduce the number of information security incidents due to human errors. However, further research is needed to examine the effect of other individual predictors (e.g., dark personality, proactive personality) on the cybersecurity behaviors of employees. Figure 3 summarizes the links between the individual-level factors and cybersecurity behavior.

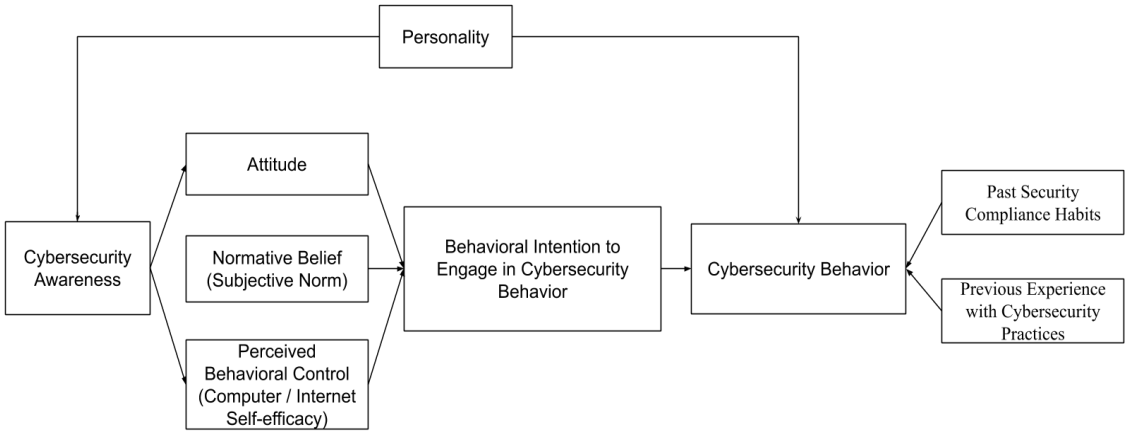

Figure 3. Theoretical framework linking individual predictors with cybersecurity behavior.

2.2 Training to Improve Cybersecurity Behaviors at Work

A large number of the cybersecurity breaches in organizations are due to employees' careless behaviors such as responding to suspicious e-mails and visiting fraudulent web sites. According to 2018 Data Breach Investigations Report conducted by Verizon, 83% of people with email accounts received phishing emails, 30% of phishing emails in the United States were opened, and 66% of security breaches were due to malware installed via malicious email attachments opened by employees. Therefore, not only it is necessary to train cybersecurity professionals, it is also important to train computer end-users on the knowledge, skills, and organizational policies concerning cybersecurity so that they can recognize phishing cues and lures embedded in e-mails and social networks. Puhakainen and Siponen (2010) successfully demonstrated that a well-developed training program could increase employees' levels of compliance with cybersecurity policies through its effect on enhancing their cybersecurity awareness. Thus, this section primarily focuses on certain elements of a cybersecurity training program that seeks to ensure that employees act appropriately during a cyberattack.

Concerning the goals of cybersecurity training, cybersecurity programs are often designed to improve end-users' cybersecurity behaviors through a heightened awareness of cybersecurity issues (Abawajy, 2014). Albrechtsen and Hovden (2010) indicated that information security awareness training is the most cost-effective form of information security control. Many empirical studies on the utility of cybersecurity awareness training provides support for this argument (Dodge, Carver, & Ferguson, 2007). Dodge et al. (2007) showed that awareness training can substantially reduce the number of data breaches. The study revealed that less students fell victim to phishing attacks after training compared to before training. Eminagaoglu, Ucar, and Eren (2010) also found similar results. In their study, weak password usage was significantly decreased after a cybersecurity awareness training course.

In addition to cybersecurity awareness, computer or internet self-efficacy development should be emphasized in a cybersecurity training program to improve cybersecurity behaviors as well as decrease the perceived barriers to cybersecurity practices. In the context of cybersecurity, self-efficacy refers to one's perception of his/her ability to competently use computer in resisting cyberattacks (Ng et al., 2009). As was mentioned in the predictor section, computer or internet self-efficacy is one of the determinants of an end-user's cybersecurity behavior (Ng et al., 2009). To improve computer or internet self-efficacy, training courses can target teaching individuals the necessary computer knowledge and skills related to cybersecurity best practices.

There are various cybersecurity awareness delivery methods such as text-based, game-based, and video-based delivery methods and researchers are examining the effectiveness of these methods (Sheng et al., 2007). For example, a lab experiment conducted at Carnegie Mellon University revealed that the effectiveness of an embedded training approach outperformed that of sending security notices alone (Kumaraguru et al., 2007). The embedded training emails were

designed to look like phishing emails that ask users to go to an unfamiliar website. If users click on the link in that email, they will be immediately redirected to a separate website that provides training about phishing scams. The final results of this study suggested that participants who received training after falling victim to a phishing scam had better knowledge retention and were more likely to successful apply what they had learned from class into practice compared to those who only received text-based training delivered through email. Another research study provides support for the usefulness of interactive game training (Sheng et al., 2007). In this game, participants need to control a small fish, called Phil, to eat worms. Each worm is associated with a URL and the real worms have URLs of legitimate website, while the fake worms (baits) have URLs of phishing websites. Phil has to avoid fake worms and eat all real worms in order to become a big fish. Suggestions on how to identify fake worms are provided during the game. The result indicated that users who participated in an interactive game (i.e., active learning) did better at recognizing phishing websites relative to those who viewed online paper-based tutorials (i.e., inactive learning).

It is important for organizations to develop cybersecurity training programs to increase awareness of cybersecurity among individuals and to equip them with information regarding how to recognize and handle cyber threats. Organizations should invest in implementing cybersecurity training with different goals and through multiple delivery methods that can fit the learning preferences of trainees. This is because the results of a study investigating the effect of sex on perceived computer abilities revealed that, relative to men, women reported lower computer security self-efficacy and computer skills, less past experience with computer security practices, and had lower information security behaviors scores (Anwar et al., 2017). Additionally, another study found that men place less importance on privacy risk when sharing

information on social media. As such, men may be more likely to engage in behaviors that pose cyber threats to their organizations (Hajli & Lin, 2016). In light of this, distinct training programs which focus on different areas of cybersecurity are needed to decrease an organization's susceptibility to external cyber threats.

In conclusion, cybersecurity training should focus on improving end-users' cybersecurity awareness as well as teaching them the requisite knowledge, skills to engage in cybersecurity behavior, which ultimately can improve their computer or internet self-efficacy. Simulations seem to be the most effective delivery method for cybersecurity training because they provide direct cyberattack exposure. Its high fidelity, which duplicates characteristics of a real cyber threat, helps trainees get better prepared to take appropriate defensive action when confronted with cyberattacks (Kumaraguru et al., 2007). However, it is important to note that there is no one-size-fits-all method for cybersecurity training; training implemented through a combination of delivery methods may be the most effective approach to improving cybersecurity awareness as well as actual cybersecurity behaviors (Abawajy, 2014). Finally, it is recommended that organizations devote additional training resources to employees who have special access to sensitive information (e.g., human resources employees and IT professionals).

3. AN ORGANIZATIONAL PSYCHOLOGY VIEW OF CYBERSECURITY BEHAVIORS

The organizational (O) side of I-O psychology integrates research and perspectives from social psychology and organizational behavior, and addresses issues such as motivation, attitudes, fairness, stress, leadership, groups and teams, work-life balance, and diversity (Colquitt, Lepine, Wesson, & Wesson, 2011). This section primarily focuses on how specific organizational psychology variables relate to employees' cybersecurity behavior.

3.1 Job Attitudes and Cybersecurity Behaviors

3.1.1 *Job Satisfaction*

Employee attitudes, especially job satisfaction, have also received scholarly attention among predictors of counterproductive behaviors. Scholars have empirically demonstrated that job satisfaction has long been identified as a precursor of job performance and unethical work behaviors (e.g., Judge, Scott, & Ilies, 2006; Moore, Cappelli & Trzeciak, 2008; Willison & Warkentin, 2009), such as insecure cyber behaviors.

A meta-analysis reported a strong negative relationship between job satisfaction and undesirable work behavior (ρ = -.28; Kish-Gephart, Harrison, & Treviño, 2010). Moore et al. (2008) suggested that employees who were less satisfied with their jobs or organizations attempted to address this dissatisfaction by engaging in retaliatory actions against the organization through theft, sabotage, and fraud, to name a few. Dalal's (2005) meta-analysis also reported comparable results. Relatedly, a recent study examining job satisfaction as a predictor of cyber-CWB also found that job dissatisfaction exhibited a moderate negative relationship with cybergriping (Mercado, 2017). That is to say, employees who were generally dissatisfied with

their jobs were more likely to use social media to publicize their complaints about their supervisors, organizations, or work experience.

3.1.2 *Perception of Organizational Justice*

Justice in one of the central topics of organizational psychology. Perceptions of justice refers to employees' perceptions of the fairness of their organizations (Greenberg, 2011). Colquitt (2001) indicates that justice has four dimensions, namely distributive, procedural, interpersonal, and informational justice. Distributive justice refers to the perceived fairness of outcomes, such as performance evaluation and rewards distributed by an organization. Procedural justice refers to the perceived fairness inherent in the process that was utilized to arrive at the distributions. Interpersonal justice refers to how polite and respectful an individual perceives the way s/he was treated by the organization's agents. Finally, informational justice refers to the extent to which an employee perceives that s/he received sufficient and reasonable explanations regarding work procedures.

Although many research studies on employee perception of justice as a predictor of CWB demonstrated negative relationship between CWB and justice (Cochran, 2014; Colquitt et al., 2013), a recent study (Mercado, 2017) found that only interpersonal and informational justice demonstrate notable negative relationships with overall cyber-CWBs. Specifically, employees who perceive interpersonal or informational injustice are more likely to engage in cyber-CWB.

3.2 Leadership

Yukl and Van Fleet (1992) defined leadership as a process through which a person influences others' actions, the objectives for the group or the organization, and the superior-subordinate communication. It also refers to the ability to guide followers towards a collective

objective (Bryman, 1992). Effective leadership is critical to the success of any organization as it can lead to several desired outcomes at an individual, group, and organizational level.

As stated in the seminal work of Burns (1998), there are two major types of leadership styles, namely transactional leadership and transformational leadership, which substantially influence employees' behavior (such as job performance, employee turnover, and citizenship behaviors). Transactional leaders are more concerned with productivity, whereas, transformational leaders care more about employees' feelings, interpersonal relationship, employee empowerment, and personal improvement (Burns, 1998). Research indicates that transformational leadership is strongly associated with both cybersecurity awareness and perceived information security culture (Flores & Ekstedt, 2016). This awareness and security culture could then be expected to influence employees' attitudes towards cybersecurity policies and facilitate adoption of cybersecurity behaviors.

It has also been reported that compared to large organizations, organizations with 500 or fewer employees are more vulnerable to the evolving threats of cybercrimes due to minimum concern for cybersecurity issues, few professionals who provide cybersecurity assistance, and low resources for mitigating cyberattacks (Ryan, 2000). Given this constraint, it can be said that good leadership is especially critical in small organizations. Nonetheless, in one study that examined cybersecurity issues within small organizations (Bhattacharya, 2011), the author found that a significant relationship existed between leadership styles and concern for information security. Specifically, the results revealed that leaders with a high level of transactional/transformational leadership style were more concerned with the cybersecurity problem than those with low levels of transactional/transformational leadership style. A high level of concern for information security leads to proactive and optimal approaches to deal with

emerging cybersecurity threats and mitigates the vulnerability of cybersecurity systems to external cyberattacks (DeZulueta, 2004).

In Hu, Dinev, Hart and Cooke's (2012) study, the perceived participation of top leaders in establishing, following, and facilitating the information security policies or programs was found to be related to employees' subjective norms and their perceived behavior control. These in turn shaped employees' compliance behavior (Hu et al., 2012). Extending this notion to cybersecurity, an extensive amount of literature on individual behavior in diverse settings has provided strong evidence for the propositions that attitudes, subjective norms, and perceived behavior control significantly influence an employee's intention to comply with cybersecurity policies. (Ajzen, 2005; Dinev & Hu, 2007; Pavlou & Fygenson, 2006). Hu et al. (2012) also found that an employee's perception of top management participation is strongly associated with his/her attitude towards cybersecurity compliance behavior, and this relationship is mediated by organizational culture. To be specific, the extent to which top managers facilitate and follow the established information security policies influences the growth of cybersecurity culture, thereby shaping employees' cybersecurity compliance intention.

Based on the literature reviewed, it can be generalized that leaders hold critical roles in facilitating employee compliance behavior through the shaping of cybersecurity culture and affecting employees' beliefs. Thus, leaders should be highly engaged in cybersecurity initiatives, such as supporting cybersecurity training programs, by serving as executive speakers, trainers, or participating in the training program as a trainee. Leaders can also promote cybersecurity in their organizations by securing and allocating funds for cybersecurity initiatives and through regular communication about cybersecurity.

3.3 A Security-Focused Organizational Culture

Organizational culture refers to a pattern of collective beliefs, values, norms, and basic assumptions that an organization uses to cope with its problems of external adaptation and internal integration (Schein, 1992). These assumptions are passed on to newcomers as the correct way to perceive, think, and feel in relation to those problems through socialization and communication process. Hofstede (2001) defines organizational culture as the shared mental intellect of the people in an organization which substantially impacts the performance of organizations. Culture is relatively stable and can resist manipulation because it is rooted in history and is collectively supported (Dennison, 1996). Investigating the way in which culture influences structure, practices, and policies in the organization helps in the understanding of the role of culture in shaping employee cybersecurity behaviors.

Organizational culture can be categorized based on four fundamental values: support orientation, innovation orientation, goal orientation, and rule orientation (Van Muijen, 1999). Support orientation describes the spirit of sharing, teamwork, and trust; innovation orientation refers to creativity, openness to experience, and exploration; goal orientation is described as rationality, accomplishments, and accountability; while rule orientation reflects a mutual understanding of organization goals, individual responsibility, rational, and discipline elements of the organizational culture.

Evidence from an empirical study (Chang & Lin, 2007) indicates that the cultural values relevant to control (i.e., goal orientation, role orientation) can improve cybersecurity outcomes. This is because cybersecurity compliance behavior is based on following existing policies and best practices and achieving established cybersecurity goals. One research study (Hu et al., 2012), which examined the effect of goal-oriented and rule-oriented organizational culture on

shaping employees' intentions to comply with information security policies, found that an organizational culture of definite goal and strong rule orientations resulted in employees who express great concern about how they are evaluated in terms of the attainment of compliance with policies. Quinn and Rohrbaugh (1983) also found that rule-oriented organizations typically devote a great amount of effort to training employees in cybersecurity skills, as well as developing well-developed cybersecurity policies.

Another study on the role of culture in shaping employees' intentions to resist social engineering found similar results (Hu et al., 2012). Social engineering refers to the cybersecurity threats that psychologically manipulate people to make them divulge confidential information. This often occurs when hackers try to trick an employee into clicking on a malicious email link that will allow them to gain access to the organization's confidential information and personal computer password. Flores and Ekstedt (2016) surveyed 1583 employees from different organizations in Sweden and found that information security culture per se had a weak and indirect effect on employees' intention to resist social engineering; however, it was associated with employees' awareness of information threats such as social engineering or phishing emails. This is important because having the attitude that it is critical to adapt and demonstrate resilient behavior and believing this behavior will help one resist cyber threats was one of the most significant predictors of behavioral intention (Flores & Ekstedt, 2016).

IT and cybersecurity professionals can contribute to a security-focused organizational culture to facilitate organizational adoption of cybersecurity policies, norms, and standards. Meanwhile, both normative beliefs and attitudes showed significant relationships with individuals' behavioral intention (Flores & Ekstedt, 2016). Although culture had a weak and indirect effect on an employee's intention to engage in cybersecurity behavior, it has a

substantial impact on their attitudes towards cybersecurity policies and procedures (Hu et al., 2012). Therefore, establishing a cultural value relevant to control (consistency and effectiveness) is also a key component for organizations to achieve cybersecurity goals.

Relative to leadership and organizational culture, other organizational level constructs as they relate to cybersecurity behaviors have received less scholarly attention. This calls for empirical studies that focus on how organizational commitment, team composition, and norms of reciprocity, for example influence cognitive processes in order to determine other effective methods for increasing secure cyber behaviors in work settings. Research findings in the area of organizational factors are presented in Figure 4.

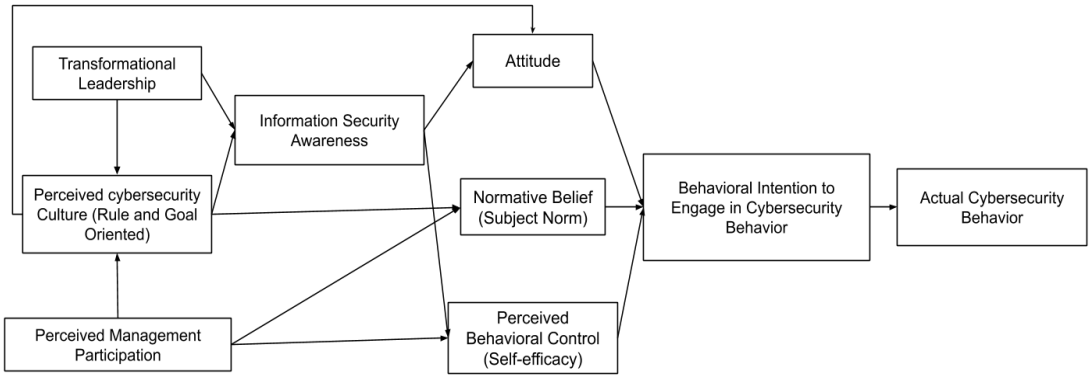

Figure 4. Summary of findings on organizational factors and cybersecurity behavior.

4. CYBERSECURITY BEHAVIORS THROUGH A METHODS AND MEASUREMENT PERSPECTIVE

Although the methods and measurement perspective in behavioral sciences includes both research design and measurement, this thesis focuses on measurement perspective. Measurement is at the heart of I-O psychology because the latter is a behavioral science. If something is not measured or is not measured well, then it cannot be studied via means of the scientific method. Therefore, to gain meaningful and accurate interpretation of research findings, it is essential to evaluate seriously the measurements employed in research (Furr, 2018). Interest in the relationship between individual differences and cybersecurity behaviors has resulted in the development of standardized measures to assess secure/insecure cyber behaviors for use in research and practice. This section examines multiple methods for assessing cybersecurity behavior and what has been done to improve the validity of the measurement.

A challenging area of cybersecurity research and practice is measuring cybersecurity behavior. Given that behavioral science researchers measure behaviors through both direct or indirect methods, previous research on measuring cybersecurity behaviors through self-report measures (direct) and simulated attacks (indirect) is reviewed next.

4.1 Measuring Cybersecurity Behavior through Self-Report Measures

In terms of self-report measures of cybersecurity, respondents are generally asked about their previous experience with online fraud or how they would perform in a specified scenario. For instance, in Davinson and Sillence's (2010) longitudinal study, the Internet Security Risk Questionnaire was used to gather respondents' previous experience of online financial transactions and experience of fraud as a baseline score for their online behavior (e.g., "Did you

only use reputable companies when shopping online"). The same items, framed to reflect intention, were used to measure their intention to behave securely online (e.g., "Do you intend to only use reputable companies when shopping online in the next seven days?"). The author found that presenting end users with threat information promotes secure online behavior (Davinson & Sillence, 2010).

In another study, Anwar et al. (2017) developed five scenarios of different cybersecurity policies violations (e.g., sharing passwords) to measure online security behaviors and beliefs in workplace. Respondents were asked how likely they would behave in the same way as characters in the scenario (e.g., "What is the chance that you would do what [the scenario character] did in the described scenario?"). Their intentions to comply (e.g., "I would act in the same way as [the scenario character] did if I was in the same situation") were also measured. The results of the study suggested that perceived lack of computer/internet skills was a strong negative predictor of secure cyber behaviors.

Self-reports have also been used to measure cybersecurity behavior indirectly by asking about respondents' intention to implement security measures in order to resist cyberattacks rather than actual cybersecurity behaviors. Many scholars demonstrated that intention to compliance in terms of information security policies had a strong and consistent relationship with eventual actions (Ajzen 1991; Venkatesh, Morris, Davis & Davis, 2003). Thus, a person's intention to engage in cybersecurity, to a large extent, determines the actions that s/he will take when confronted with cybersecurity challenges. Based on this rationale, Tsai et al. (2016) measured participants' security intention as an indicator of actual cybersecurity behavior. A sample item on the scale reads: "I will upgrade my security measures to protect myself better online" (Tsai et al.,

2010). All eight items in the survey were rated on a five-point Likert scale to indicate his/her level of agreement with the statement.

Another common approach for measuring information security awareness as an indicator of cybersecurity behavior is the Human Aspects of Information Security Questionnaire (HAISQ) developed by Parsons, McCormac, Butavicius, Butavicius, and Jerram (2014). HAISQ considers two aspects of cybersecurity awareness (McCormac et al., 2014). The first aspect focuses on individuals' understanding of the importance of cybersecurity. The second aspect is the extent to which individuals behave in accordance with the organization's cybersecurity policies and guidelines. The HAISQ is based on the knowledge, attitude, and behavior model (Allport,1935) which, by extension, suggests that a person's knowledge regarding cybersecurity influences his/her attitudes towards cybersecurity and guides the cybersecurity behaviors the individual will perform. The 63-item HAISQ measures seven areas (e.g., email use, internet use, mobile devices) and each dimension is assessed via a combination of a unique knowledge (e.g., "I am allowed to click on any links in emails from people I know"), attitude (e.g., "It is always safe to click on links in emails from people I know") and behavior item (e.g., "I do not always click on links in emails from someone I know"). The result of the validation study indicated that HAISQ was a robust measure of cybersecurity awareness as participants with higher score on the HAISQ did better in the phishing experiment (Parsons et al., 2014).

A new approach to measure and quantify information security behavior is the behavioral threshold analysis technique (Snyman & Kruger, 2016). Initial exploratory studies show that this approach is helpful in determining attitudes of individuals in a group setting on specific information security topics and in determining what should be included in an information security awareness programs (Snyman & Kruger, 2016; 2017). The idea of behavioral threshold

analysis is based on the model presented by Granovetter (1978) in which an individual's awareness of the percentage of other group members that engage in the behavior determines the collective behavior of a group of people. For example, a rumor heard from one person in a group is untrustworthy and lacks merit, whereas a rumor heard from enough numbers of individuals in the group (threshold) is convincing and acceptable and is more likely to become widespread.

Growney (1983) suggests that the questionnaire for assessing individual thresholds for participation should be constructed in a way where participants nominate their threshold values. Based on this guideline, Snyman and Kruger (2016) developed a behavioral threshold questionnaire that simply asked respondents to nominate their threshold value for sharing their passwords with others (e.g., "I will share my passwords when at least "X" percentage of group members share their passwords"). The threshold value refers to the proportion of others in the group that would share their passwords before the respondent would also share. High thresholds indicate that the respondents are sufficiently aware of the associated risks with participating in the behaviors and are less likely to be influenced by others' behavior.

This literature search also retrieved a theoretically informed self-report measure that is commonly used to measure cyber-CWBS (Mercado, 2017). The measure includes 47 items, and 12 subscales assessing the respective homogeneous item clusters (e.g., cybersabotage, cyberloafing, and cybertheft). Measure instructions asked participants to evaluate the frequency of their engagement in cyber-CWBs and respond using a 7-point scale with the anchors ranging from never to once a year. Table 1 summarizes the characteristics of the four self-report measures reviewed in this thesis.

It is worth noting that some scholars (e.g., Crossler et al., 2016) argue that self-reported cybersecurity behavior may be an overestimate of actual cyber actions. For example, Crossler et

al. (2016) found that distribution of scores suggest that the majority of people might be unwilling to admit to engaging in cybersecurity behaviors considered unethical.

Table 1

Summary Characteristics of Cybersecurity Measures

Measure Name	Construct Measured	Dimension Labels	Item Numbers	Response Scale	Reliability Type	Reliability Index
Internet Security Risk Questionnaire (Davinson & Sillence, 2010)	Past Cybersecurity Behavior	Current Behavior	11	Seven-point Likert Scale (1 = Always – 7 = Never)	Internal Consistency (Cronbach's α)	0.83
		Susceptibility	2	Seven-point Likert Scale (1 = Strongly disagree – 7 = Strongly agree)	Internal Consistency (Cronbach's α)	0.73
Security intentions (Tsai et al., 2016)	Cybersecurity Intention	Security Intention	8	Five-point Likert- type Scale (1 = Strongly disagree, 5 = Strongly agree)	Internal Consistency (Cronbach's α)	0.90
Human Aspects of Information Security Questionnaire (Parson et al., 2013)	Cybersecurity Awareness	Knowledge of Policy and Procedures	63	Five-point Likert- type Scale (1 = Strongly disagree, 5 = Strongly agree)	Internal Consistency (Cronbach's α)	0.84
		Attitude towards Policy and Procedures			Internal Consistency (Cronbach's α)	0.88
		Self-reported Behavior			Internal Consistency (Cronbach's α)	0.92
Behavioral Threshold Questionnaire (Snyman, Kruger, 2016)	Cybersecurity Awareness	Inherent Threshold	1	Percentages adjusted to intervals of 10	NA	NA

4.2 Measuring Cybersecurity Behavior through Simulated Cyberattacks

Existing cybersecurity research also reports measuring an individual's behavior with regards to resisting external cyberattacks through simulated attacks or unannounced phishing emails (e.g., Dhamija, Tygar, & Hearst, 2006; Halevi, Lewis, & Memon, 2013). Through simulated attacks, participants' actual actions or behaviors are examined and recorded after a social engineering attack. For example, in a study of the relationship between Big Five personality traits and cybersecurity behaviors (Halevi et al., 2013), experimenters sent phishing emails to a sample of participants and then examined their recorded actions (e.g., did the participants delete or open a phishing email). The result showed that individuals low in emotional stability were more likely to fall victim to phishing emails (Halevi et al., 2013). Similarly, Karakasiliotis, Furnell, and Furnell (2006) assessed individuals' social engineering susceptibility by observing whether they can differentiate legitimate emails from a mix of 20 legitimate and illegitimate emails. The results indicated that only 36 percent of the participants successfully identified legitimate emails. In another simulated study on the factors influencing phishing success, participants were asked to identify the illegitimate ones among 20 websites (Dhamija et al., 2006). The authors found that 91% of the participants fell victim to the phishing website which does not ask for much private information and had animated pictures and other aesthetic design features, such as favicons.

One limitation of these simulated studies mentioned above is that while they provide some information about the reasons why employees fail to resist social engineering, they do not provide data on how individuals behave in real cyberattack situations. Thus, unannounced phishing experiments, in which participants are unaware of the recording of their behavior, have been used by researchers to address this limitation. For instance, Jagatic, Johnson, Jakobsson,

and Menczer. (2007) sent phishing scams to university students in order to acquire students' login information and investigated if including their personal information in the email could increase the probability of a successful attack. The results demonstrated that the percentage of students who submitted their logins increased from 16% to 72% when personal information gathered from social media platforms were used in the emails.

In sum, effectively measuring cybersecurity behavior is critical to a comprehensive understanding of cybersecurity in organizations. It also facilitates being able to determine whether an organization's cybersecurity initiatives are effective (or not).

5. SUMMARY AND CONCLUSIONS

Firms worldwide spend an incredible amount of money on upgrading anti-virus software and firewalls to defend against emerging external cyberattacks (Morgan, 2016). Although those investments are highly prioritized, advanced technology is not a silver bullet that protects organizations from cybercrimes. A higher level of cybersecurity cannot be achieved if organizations rely solely on advanced cybersecurity technologies (e.g., anti-virus software and firewall). Through a systematic review of research on cybersecurity behavior in the I-O psychology literature, it is recommended that attention be directed toward individual and organizational factors that affect employees' attitudes toward cybersecurity and actual cybersecurity behaviors. This is because employees with access to organizational computers or networks play important roles in the achievement of an organization's cybersecurity goals.

This section discusses how three I-O psychology content domains discussed above intersect to facilitate secure cyber behaviors in the workplace. Implications for science and practice, limitations, future research proposals, and recommendations are also discussed. Altogether, they seek to provide a framework that organizations can employ to reduce the cybersecurity risks resulting from human errors which, consequently leads to higher levels of cybersecurity in organizations.

5.1 Intersection of I-O Psychology Content Domains

This section discusses how the three I-O psychology content domains intersect to facilitate secure cyber behaviors in the workplace which not only inform future research ideas but also contributes to the design of cybersecurity interventions.

5.1.1 *Cybersecurity Training and Measurement*

Worldwide spending on cybersecurity training is growing. As reported by Gartner, Inc. in 2018, there has been an increase of 12.4 % from 2017, up to $114 billion, in worldwide cybersecurity market. As companies invest a great deal of resources (e.g., money, time, effort) in training programs, it is necessary for them to know whether their investment is paying off through post-training evaluation. In the context of cybersecurity training, evaluation refers to an assessment of the impact of training on trainee's understanding of cyberattacks and actual cybersecurity behaviors.

It is recommended that a pre-training/post-training evaluation design be implemented. The pre-training/post-training design will allow organizations to observe changes that trainees have undergone with regard to the training goals. Furthermore, this evaluation strategy will account for threats to internal validity such as history, maturation, mortality, testing, and instrumentation (Noe, 2017). The typical pre-training/post-training evaluation design process includes two steps. First, collect information on previous cybersecurity behaviors (and/or current knowledge, skills, and attitudes about cybersecurity) from trainees prior to training. Next, immediately following the cybersecurity training program or after a period of time, cybersecurity behavior (and/or current knowledge, skills, and attitudes about cybersecurity) are again measured to determine learning and behavior change, for example. One can estimate whether there is a significant improvement is the result of training by using analysis of variance to compare score differences between pre-training measures and post-training measures.

5.1.2 *Leadership Support and Training Effectiveness*

Although a well-developed training program can increase employees' levels of cybersecurity awareness and future cybersecurity behaviors, training intervention alone, cannot

guarantee that organizations will achieve their cybersecurity goals. This is because it is difficult to know how an employee will learn content and/or acquire skills during training and a comprehensive understanding of a concept during training does not always transfer to job success if trainees have few opportunities to practice what they learned on the job and receive feedback. Thus, to maximize the utility of cybersecurity training, the significance of leadership support cannot be understated. For example, leaders hold critical roles in facilitating employee compliance behavior. Leadership styles determine the business strategy to handle cyber threats and how many resources organizations invest in cybersecurity training. Perceived participation of top leaders was found to be related to employees' subjective norms and their perceived behavior control (Hu et al., 2012). Finally, the extent to which top managers facilitate and follow the established information security policies and initiatives, such as training, contributes to the development of a cybersecurity culture, which affects employee attitudes toward information security policies and procedures and willingness to transfer what they learned during training.

5.2 Implications

The present literature review contributes to the scientific effort to understand cybersecurity behaviors in organizations. As previous research on cybersecurity behaviors tend to focus on either individual-level or organizational-level factors affecting employees' cybersecurity behavior, they often do not synthesize most studies on cybersecurity behavior. In contrast, the present literature review takes a holistic approach and looks beyond the independent effects of specific constructs by examining the intersection between three content domains of I-O psychology. This approach may inform the development of theoretical models for examining employees' cybersecurity behavior and serve as a catalyst for future empirical cybersecurity behavior research that is holistic in nature.

This review also has practical implications for cybersecurity management in organizational settings. Organizations can use personality traits, especially conscientiousness, together with computer skills and past cybersecurity compliance habits during the selection process to determine applicants, including those applying for leadership positions, who are more likely to abuse their work computer privileges. In addition, organizations can use this information to design training programs, which improves employees' cybersecurity awareness and facilitates secure cyber behaviors. Cybersecurity awareness training is challenging to design because such training for end users is often too broad to result in relevant content knowledge about secure use of cyber resources (Beyer & Brummel, 2015).

Furthermore, a concern with cybersecurity training programs in most organizations is that the training function often taken on by IT professionals alone. Therefore, interdisciplinary collaboration among HR professionals, IT specialists, and instructional designers (which may include I-O psychologists) is necessary for an effective training program. As IT and cybersecurity specialists have a thorough knowledge of diverse cyberattacks and vulnerabilities of the organization's existing cybersecurity system, they easily become aware of end users' knowledge gaps. HR practitioners are positioned to gain management support for cybersecurity training and act as a liaison between instructors and trainees to ensure the training content is relevant and that trainees are motivated to learn. Furthermore, instructional designers such as I-O psychologists are uniquely qualified on training program and/or course design and to measure whether training is well-developed, job-related, and has achieved desired outcomes.

I-O psychologists can impact modern organizational life and contribute to the achievement of cybersecurity goals through their unique role in assisting individuals, teams, and organizations. The findings of the research summarized in this thesis provide organizations with

practical guidelines for making best selection decision for positions that have unrestricted access to sensitive information, developing an effective cybersecurity training program, and fostering a cybersecurity culture. It is anticipated that this thesis will motivate scholars to investigate further antecedents of cybersecurity behavior such that the results lead practitioners in the right direction on how to build a workforce that is resistant to emerging cyberattacks.

5.3 Limitations and Future Directions for Research

Although this literature review synthesized almost all accessible research findings on cybersecurity as it is related to I-O psychology, limitations still exist. Due to time constraint, the literature search may have not captured all cybersecurity papers. There was no attempt to limit bias and there exists the possibility that papers that were unintentionally excluded may contradict the arguments and conclusions of this review. Furthermore, there is still limited research exploring the complicated interconnections among leadership, organizational culture, intentions, personal characteristics, and cybersecurity behavior. Hence, this review is limited because a number of key constructs have a relationship with cybersecurity behaviors, especially due to the intuitive appeal of such constructs in this context, are not incorporated. As shown in Table 2, such factors include negative affect, person-organization fit, organizational commitment, and workplace mistreatment.

Additional research should explore other individual and organizational predictors of cybersecurity behaviors in addition to the aforementioned predictors as well as developing a comprehensive theoretical model of cybersecurity behavior. This also warrants a call for a new stream of research, which examines the measurement tools used in cybersecurity studies. Some research questions include: How is an organization's cybersecurity effectiveness measured? Which cybersecurity indicators could be included in the performance appraisal of all employees

and IT professionals? How is cybersecurity culture measured? What issues exist in the measurement of cybersecurity behaviors? How do organizations select for leaders who will facilitate a positive cybersecurity culture?

Furthermore, despite the fact that research has found empirical support for the linkage between organizational culture and employee compliance behavioral intentions, organizational culture may simply alter the internal cognitive schema rather than behavioral intentions or actual behavior towards specific policies. Existing literature (e.g., on cybersecurity in the workplace has focused more efforts on the human element of cybersecurity management (e.g., security awareness, belief, and subjective norms) than organizational factors (e.g., leadership styles and organizational culture). Thus, more empirical studies which focus on how organizational level factors influence the cognitive processes are needed to determine other methods for increasing individual cybersecurity awareness in work settings.

Table 2
Predictors of Cybersecurity Behavior

Individual-level factors		Organizational-level factors		Measurement	
Mentioned	Not Mentioned	Mentioned	Not Mentioned	Mentioned	Not Mentioned
Personality	Proactive Personality	Leadership Styles	Commitment	Self-report Questionnaire	Response distortion (faking and social desirability)
Behavior Intention	P-O fit	Rule and Goal Oriented Culture	Workplace mistreatment (e.g., cyber-incivility)	Simulated and unannounced attack	Response distortion (faking and social desirability)
Computer/Internet Self-Efficacy	Dark personality	Transformational / Transactional Leadership	Team composition		Balance scorecards
Past Security Compliance Habits	Employment testing (e.g., Assessment Center)	Management Participation	Breach of psychological contracts		Cost-benefit analysis
Perceived Barriers		Job Satisfaction	Ethical leadership		
Cognitive Ability		Perception of Organizational Justice	Reciprocity norms		
Training					

5.4 Conclusion

The primary objective of this thesis was to review the literature on cybersecurity behaviors at work through an intersection of three areas of I-O (i.e., personnel, organizational, methods and measurement). The thesis summarizes research on predictors of cybersecurity behavior, training to improve the knowledge, skills, and attitudes of employees, organizational factors that affect cybersecurity behavior, methods for assessing cybersecurity behavior, and an intersection of the reviewed I-O psychology content areas.

In cybersecurity management, the success of cybersecurity cannot be achieved without placing emphasis on factors affecting cybersecurity behaviors such as personal characteristics, leadership, and organizational culture. This is because the number and frequency of cyberattacks designed to exploit human related vulnerabilities is increasing at rapid rates. Selecting individuals who are more likely to engage in cybersecurity behaviors is the first step to resisting unintentional cybersecurity attacks that occur due to human factors.

Next, a well-developed cybersecurity training program should be implemented to provide employees with a clear understanding of cyberattacks and necessary skills and attitudes needed to effectively resist them. To facilitate transfer of learning and curtail counterproductive computer usage among employees, leaders should be highly engaged in cybersecurity initiatives, such as supporting cybersecurity training programs, by serving as executive speakers, trainer, or participating in the training program as a trainee. Finally, a security-focused organizational culture can facilitate an organization's adoption of cybersecurity policies, norms, and standards through shaping employees' intentions to resist cyberattacks.

REFERENCES

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*, 237-248.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*, 179-211.

Ajzen, I. (2005). *Attitudes, personality, and behavior*. Milton-Keynes, England: Open University Press & Chicago, IL: Dorsey Press.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security, 29*, 432-445.

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of Economic Perspectives*, *31*, 211-236.

Allport, G. W. (1935). Attitudes. In C. A. Murchinson (Ed.), *Handbook of social psychology* (pp. 798-844). Worchester, MA: Clark University Press.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*, 613-643.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69,* 437-443.

Back, M. D., Stopfer, J. M., Vazire, S., Gaddis, S., Schmukle, S. C., Egloff, B., & Gosling, S. D. (2010). Facebook profiles reflect actual personality, not self-idealization. *Psychological Science, 21*, 372-374.

Bansal, G. (2011, December). *Security concerns in the nomological network of trust and Big 5: First order vs. second order.* Paper presented at the 32th Annual International Conference on Information Systems, Shanghai, China.

Bègue, L., Beauvois, J. L., Courbet, D., Oberlé, D., Lepage, J., & Duke, A. A. (2015). Personality predicts obedience in a Milgram paradigm. *Journal of Personality, 83*, 299-306.

Berkelaar, B. L. (2010). *Cyber-vetting: Exploring the implications of online information for career capital and human capital decisions* (Unpublished doctoral dissertation). Purdue University, West Lafayette, IN.

Beyer, R. E., & Brummel, B. J. (2015). Implementing effective cyber security training for end-users of computer networks. *SHRM-SIOP Science of HR Series: Promoting Evidence-Based HR*. Retrieved from https://www.shrm.org/hr-today/trends-and-forecasting/special-reports-and-expert-views/Documents/SHRM-SIOP%20Role%20of%20Human%20Resources%20in%20Cyber%20Security.pdf on July 13, 2019.

Bhattacharya, D. (2011). Leadership styles and information security in small businesses. *Information Management & Computer Security*, *19*, 300-312.

Bryman, A. (1992). *Charisma and leadership in organizations.* London, UK: Sage.

Burns, J. M. (1998). Transactional and transforming leadership. *Leading Organizations*, *5*, 133-134.

Cascio, W. F., & Aguinis, H. (2018). *Applied psychology in talent management*. Thousand Oaks, CA: Sage Publications.

Cochran, M. N. (2014). *Counterproductive work behaviors, justice, and affect: A meta-analysis* (Unpublished doctoral dissertation). University of Central Florida, Orlando, FL.

Colquitt, J.A., Lepine, J. A., Wesson, M. J., & Gellatly, I. R. (2011). *Organizational behavior: Improving performance and commitment in the workplace*. New York, NY: McGraw-Hill Irwin.

Colquitt, J. A., Scott, B. A., Rodell, J. B., Long, D. M., Zapata, C. P., Conlon, D. E., & Wesson, M. J. (2013). Justice at the millennium, a decade later: A meta-analytic test of social exchange and affect-based perspectives. *Journal of Applied Psychology*, *98*, 199-236.

Connelly, B., Davies, S., Ones, D., & Birkeland, A. (2008). Conscientiousness: Investigation of its facet structure through meta-analytic factor analysis. *International Journal of Psychology, 43*, 553-553.

Dalal, R. S. (2005). A meta-analysis of the relationship between organizational citizenship behavior and counterproductive work behavior. *Journal of Applied Psychology*, *90*, 1241-1255.

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior*, *26*, 1739-1747.

Denison, D. R. (1996). What is the difference between organizational culture and organizational climate? A native's point of view on a decade of paradigm wars. *Academy of Management Review*, *21*, 619-654.

Denning, P. J., & Denning, D. E. (2010). Discussing cyber attack. *Communications of the ACM, 53*, 29-31.

DeZulueta, M. (2004). *A novel neural network based system for assessing risks associated with information technology security breaches* (Unpublished doctoral dissertation). Florida International University, Miami, FL.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006, April). *Why phishing works.* Paper presented at 24th Annual International Conference on Human Factors in Computing Systems, Montreal, Quebec, Canada.

Dilchert, S., Ones, D. S., Davis, R. D., & Rostow, C. D. (2007). Cognitive ability predicts objectively measured counterproductive work behaviors. *Journal of Applied Psychology, 92*, 616-627.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, *8*, 386–408.

Dodge Jr, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security*, *26*, 73-80.

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies–A case study. *Information Security Technical Report, 14*, 223-229.

Ernest Chang, S., & Lin, C. S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems*, *107*, 438-458.

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, *59*, 26-44.

Furr, R. M. (2018). *Psychometrics: An introduction.* Thousand Oaks, CA: Sage Publications.

Gatewood, R., Feild, H. S., & Barrick, M. (2016). *Human resource selection* (7th ed.). Boston, MA: Cengage Learning

Goel, V., & Perlroth, N. (2016). Yahoo says 1 billion user accounts were hacked. Retrieved from https://www. nytimes.com/2016/12/14/technology/yahoo-hack. html on July 13, 2019.

Granovetter, M. (1978). Threshold models of collective behavior. *American Journal of Sociology*, *83*, 1420-1443.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, *73*, 345-358.

Greenberg, J. (2011). Organizational justice: The dynamics of fairness in the workplace. In Zedeck S. (Ed.), *APA handbook of industrial and organizational psychology: Maintaining, Expanding, and Contracting the Organization* (Vol. 3, pp. 271–327). Washington, DC: American Psychological Association.

Growney, J. S. (1983). *I will if you will: individual thresholds and group behavior: applications of algebra to group behavior*. Bedford, MA: COMAP Inc.

Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. I*nformation Management & Computer Security*, *13*, 297-310.

Hadlington, L., & Murphy, K. (2018). Is media multitasking good for cybersecurity? Exploring the relationship between media multitasking and everyday cognitive failures on self-reported risky cybersecurity behaviors. *Cyberpsychology, Behavior, and Social Networking*, *21*, 168-172.

Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics, 133*, 111-123.

Halevi, T., Lewis, J., & Memon, N. (2013). *Phishing, personality traits and Facebook.* Cornell University Library. Retrieved from http://arxiv.org/abs/1301.7643 on July 13, 2019.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems, 18*, 106-125.

Hofstede, G. (2001). *Culture's consequences: Comparing values, behaviors, institutions and organizations across nations*. Thousand Oaks, CA: Sage Publications.

Hogan, J., & Hogan, R. (1989). How to measure employee reliability. *Journal of Applied Psychology*, *74*, 273-279.

Hogan, R., & Hogan, J. (1995). *Hogan Personality Inventory Manual* (2nd ed.). Tulsa, OK: Hogan Assessment Systems.

Hosenball, M., & Zangerle, P. (2013). Cyber-attacks are leading threat against US: spy agencies. *NBC News.* Retrieved from https://www.reuters.com/article/us-usa-threats-idUSBRE92B0LS20130312 on July 17, 2019

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*, 615-660.

Im, G. P., & Baskerville, R. L. (2005). A longitudinal study of information system threat categories: The enduring problem of human error. *DATA BASE for Advances in Information Systems*, *36*, 68-79.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*, 94-100.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS Quarterly*, *34*, 549-566.

Judge, T. A., Scott, B. A., & Ilies, R. (2006). Hostility, job attitudes, and workplace deviance: test of a multilevel model. *Journal of Applied Psychology*, *91*, 126-138.

Kish-Gephart, J. J., Harrison, D. A., & Treviño, L. K. (2010). Bad apples, bad cases, and bad barrels: Meta-analytic evidence about sources of unethical decisions at work. *Journal of Applied Psychology*, *95*, 1–31.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007, April). *Protecting people from phishing: The design and evaluation of an embedded training email system.* Paper presented at the 25th Annual International Conference on Human Factors in Computing Systems, San Jose, CA.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, *69*, 151-156.

Mercado, B. K. (2017). *Cyber counterproductive work behaviors: Measurement, prediction, and means for reduction* (Unpublished Doctoral Dissertation). City University of New York, New York, NY.

Moore, A. P., Cappelli, D. M., & Trzeciak, R. F. (2008). The "big picture" of insider IT sabotage across US critical infrastructures. In S. J. Stolfo, S. M. Bellovin, S. Hershkop, A. D. Keromytis, S. Sinclair, & S. W. Smith, (Eds.), *Insider Attack and Cyber Security* (pp. 17-52). Springer: Boston, MA.

Morgan, S. (2016). Cybersecurity spending outlook: $1 trillion from 2017 to 2021. *CSO Cybersecurity Business Report* (June 15). Retrieved from www.csoonline.com/article/3083798/security/cybersecurity-spending-outlook-1-trillionfrom-2017-to-2021.html on July 13, 2019.

Ng, B. Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior using the health belief model. *Decision Support Systems*, *46*, 815-825.

Noe, R. A. (2017). *Employee training & development* (7th ed.). New York: McGraw Hill.

Ones, D. S., & Dilchert, S. (2013). Counterproductive work behaviors: Concepts, measurement, and nomological network. In K. F. Geisinger (Ed.), *APA handbook of testing and assessment in psychology* (pp. 643–659). Washington, DC: American Psychological Association.

Ones, D. S., & Viswesvaran, C. (2007). A research note on the incremental validity of job knowledge and tests for predicting maximal performance. *Human Performance*, *20*, 293–303.

Ones, D. S., Viswesvaran, C., & Schmidt, F. L. (1993). Comprehensive meta-analysis of integrity test validities: Findings and implications for personnel selection and theories of job performance. *Journal of Applied Psychology*, *78*, 679-703.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, *66*, 40-51.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security*, *42*, 165-176.

Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly*, *30*, 115-143.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*, 757-778.

Quinn, B., & Arthur, C. (2011). PlayStation Network hackers access data of 77 million users. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data on July 15, 2019.

Quinn, R. E., & Rohrbaugh, J. (1983). A spatial model of effectiveness criteria: Towards a competing values approach to organizational analysis. *Management Science*, *29*, 363-377.

Richardson, R. (2008). *CSI computer crime and security survey*. Retrieved from http://www.kwell.net/doc/FBI2008.pdf on July 13, 2019.

Russell, J. D., Weems, C. F., Ahmed, I., & Richard III, G. G. (2017). Self-reported secure and insecure cyber behaviour: Factor structure and associations with personality factors. *Journal of Cyber Security Technology*, *1*, 163-174.

Ryan, J. J .C. H. (2000), *Information security practices and experiences in small businesses* (Unpublished doctoral dissertation). The George Washington University, Columbia, CA.

Sackett, P. R., & Schmitt, N. (2012). On reconciling conflicting meta-analytic findings regarding integrity test validity. *Journal of Applied Psychology*, *97*, 550-556.

Sackett, P. R., & Wanek, J. E. (1996). New developments in the use of measures of honesty integrity, conscientiousness, dependability trustworthiness, and reliability for personnel selection. *Personnel Psychology*, *49*, 787-829.

Schein, E. H. (1992). How can organizations learn faster? The challenge of entering the green room. *Sloan Management Review*, *34*, 85–92

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2019). Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media Culture*. Advance online publication. http://dx.doi.org/10.1037/ppm0000247

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007, July). *Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish.* Paper presented at the 3rd Symposium on Usable Privacy and Security, Pittsburgh, PA.

Shred-it (2018). S*tate of the Industry Information Security*. Retrieved from https://www.shredit.com/getmedia/b5de58fd-7e17-4d18-b718-9eca8d0665a6/Shred-it-2018-North-America-State-of-the-Industry.aspx on September 12, 2019.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177-191.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*, 487-502.

Snyman, D. P., & Kruger, H. A. (2016). Behavioural Thresholds in the Context of Information Security. *In Proceedings of the 10th International Symposium on Human Aspects of Information Security & Assurance* (HAISA 2016, pp. 22–32). Frankfurt, Germany: Plymouth University.

Snyman, D. P., & Kruger, H. A. (2017). The application of behavioural thresholds to analyse collective behaviour in information security. *Information & Computer Security*, *25*, 152–164.

Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, *48*, 296-302.

Symantec Coporation & Ponemon Institute (2009). *More than half of ex-employees admit to stealing company data according to new study.* Press release by Symantec Corporation and Ponemon Institute. Retrieved from http://www.symantec.com/about/news/release/article.jsp?prid=20090223_01 on September 10, 2019.

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138-150.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*, 190-198.

Van Iddekinge, C. H., Roth, P. L., Raymark, P. H., & Odle-Dusseau, H. N. (2012). The criterion-related validity of integrity tests: An updated meta-analysis. *Journal of Applied Psychology*, *97*, 499-530.

Van Muijen, J. J. (1999). Organizational culture: The focus questionnaire. *European Journal of Work and Organizational Psychology*, *8*, 551-568.

Vanson Bourne. (2016). *2016 SailPoint Market Pulse Survey*. Retrieved from https://docs.sailpoint.com/pdf/?file=https://docs.sailpoint.com/wpcontent/uploads/SailPoint-Market-Pulse-Survey-Results-2016.pdf on September 13, 2019.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*, 425-478.

Widup, S., Spitler, M., Hylender, D., & Bassett, G. (2018). *2018 Verizon Data Breach Investigations Report*. Retrieved from http://www.verizonenterprise.com/de/DBIR/ on September 12, 2019.

Williams, M. (2017). *Inside the Russian hack of yahoo: How they did it*. Retrieved from https://www.csoonline.com/article/3180762/data-breach/inside-the-russian-hack-of-yahoo-how-they-did-it.html on September 13, 2019.

Willison, R., & Warkentin, M. (2009, May). *Motivations for employee computer crime: understanding and addressing workplace disgruntlement through the application of organizational justice*. Paper presented at the 1st International Workshop on Information Systems Security Research, Cape Town, South Africa.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, *37*, 1-20.

Yukl, G., & Van Fleet, D. D. (1992). Theory and research on leadership in organizations. In M. D. Dunnette & L. M. Hough (Eds.), *Handbook of industrial and organizational psychology* (pp. 147–197). Palo Alto, CA: Consulting Psychologists Press.