

2019

An Examination of User Detection of Business Email Compromise Amongst Corporate Professionals

Shahar Sean Aviv

Follow this and additional works at: https://nsuworks.nova.edu/gscis_etd



Part of the [Computer Sciences Commons](#)

Share Feedback About This Item

This Dissertation is brought to you by the College of Computing and Engineering at NSUWorks. It has been accepted for inclusion in CCE Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

An Examination of User Detection of Business Email Compromise Amongst
Corporate Professionals

by

Shahar Sean Aviv

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

College of Computing and Engineering
Nova Southeastern University

2019

We hereby certify that this dissertation, submitted by Shahar S. Aviv conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.



Yair Levy, Ph.D.
Chairperson of Dissertation Committee

12/3/2019
Date



Ling Wang, Ph.D.
Dissertation Committee Member

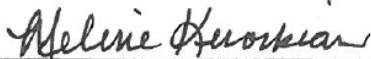
12/3/2019
Date



Nitza Geri, Ph.D.
Dissertation Committee Member

December 3, 2019
Date

Approved:



Meline Kevorkian, Ed.D.
Interim Dean, College of Computing and Engineering

12/3/19
Date

College of Computing and Engineering
Nova Southeastern University

2019

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial
Fulfillment of the Requirements for the Degree of Doctor of Philosophy

An Examination of User Detection of Business Email Compromise Amongst Corporate Professionals

By
Shahar Sean Aviv
November 2019

With the evolution in technology and increase in utilization of the public Internet, Internet-based mobile applications, and social media, security risks for organizations have greatly increased. While corporations leverage social media as an effective tool for customer advertisements, the abundance of information available via public channels along with the growth in Internet connections to corporate networks including mobile applications, have made cyberattacks attractive for cybercriminals. Cybercrime against organizations is a daily threat and targeting companies of all sizes. Cyberattacks are continually evolving and becoming more complex that make it difficult to protect against with traditional security methods. Cybercriminals utilize email attacks as their most common method to compromise corporations for financial gain. Email attacks on corporations have evolved into very sophisticated scams that specifically target businesses that conduct wire transfers or financial transactions as part of their standard mode of operations. This new evolution of email driven attacks is called Business Email Compromise (BEC) attacks and utilize advanced social engineering, phishing techniques, and email hacking to manipulate employees into conducting fraudulent wire transfers that are intended for actual suppliers and business partners. One of the most common types of BEC attacks is the Chief Executive Officer (CEO) fraud, which are highly customized and targeted attacks aimed to impersonate corporate users that have authority to approve financial transactions and wire transfers in order to influence an employee to unknowingly conduct a fraudulent financial wire transfer. Thus, the main goal of this research study was to assess if there are any significant differences of corporate users' detection skills of BEC attacks in a simulated test environment based on their personality attributes, using the Myers-Briggs Type Indicator® (MBTI®)' 16 personalities® framework. BEC attacks have attributed to over \$26 billion in corporate financial losses across the globe and are continually increasing. The human aspect in the cybersecurity has been a known challenge and is especially significant in direct interaction with BEC attacks. Furthermore, this research study analyzed corporate users' attention span levels and demographics to assess if there are any significant differences on corporate users' BEC attack detection skills. Moreover, this research study analyzed if there are any significant differences for BEC detection skills before and after a BEC awareness training. This research study was conducted by first developing an experiment to measure BEC detection and ensure validity via cybersecurity subject matter experts using the Delphi process. The experiment also collected qualitative and quantitative data for the

participants' performance measures using an application developed for the study. This research was conducted on a group of 45 corporate users in an experimental setting utilizing online surveys and a BEC detection mobile test application. This research validated and developed a BEC detection measure as well as the BEC awareness training module that were utilized in the research experiment. The results of the experiments were analyzed using analysis of variance (ANOVA) and analysis of covariance (ANCOVA) to address the research questions. It was found that there were that no statistically significant mean differences for Business Email Compromise Detection (BECD) skills between personality attributes of corporate professional participants, However, results indicated that there was a significant mean difference for BECD skills and span attention with a $p < .0001$. Furthermore, there was a significant mean difference for BECD skills and span attention when controlled for gender with a $p < 0.05$. Furthermore, the results indicated that the BEC detection awareness training significantly improved the participant BEC detection skill with a $p < .0001$. Moreover, following the training, it was found that female BEC detection test scores improved by 45% where the men BECD score improved by 31%. Recommendations for research and industry stakeholders are provided, including to corporations on methods to mitigate BEC attacks.

Acknowledgements

Completing my Ph.D. has been a personal goal of mine that I knew I would work towards and achieve it. The journey has been long, and I could not have done it without the support and love of my family and mentors.

I would like to thank my wife Aurit, and three amazing children Ariel, Maya, And Lia. My wife has worked tirelessly over the years taking care of the family to allow me time to focus on my Ph.D. I didn't realize how much time my Ph.D. studies would consume, but thanks to my wife who worked hard taking care of the family which allowed me to focus on my studies.

I would like to thank my parents Noga and Avi for their continuous lifelong support to drive me to excel in everything I do. To this day, my mother continues to be such a positive force in my life and motivates me to always improve, develop, and succeed in my goals. I am grateful and very lucky to have such amazing parents who have been such a tremendous positive impact from a young age and to this day continue with the same passion, love, and dedication.

I would like to thank my dissertation committee, Dr. Nitza Geri and Dr. Ling Wang who I have the utmost respect for. The knowledge and guidance that Dr. Geri and Dr. Wang and provided me throughout my dissertation has been nothing short of amazing. I am very proud to have such an amazing and professional committee to work with.

I would like to say a special thank you to my mentor and dissertation chair, Dr. Yair Levy. Over the course of my Ph.D. studies, I have had numerous classes with Dr. Levy, and I cannot express in words how highly I think of him. I truly believe that Dr. Levy is one of the most intelligent and knowledgeable people that I have had the honor of meeting. Every minute in his classrooms and every conversation we have had brought new perspectives, knowledge, and so much value to me. I have learned so much from Dr. Levy and his contribution to my growth as a person and a professional is something that I will carry with me for the rest of my life.

A few words of advice to my children, Ariel, Maya, and Lia. Always aim high, follow your dreams, and work hard to achieve them. One thing I have learned in life, is that you are always learning new things. Always look for ways to improve yourself, be the best person you can be, and be true to yourself. Most importantly, be happy, be positive, and be smart as you start your journey.

Table of Contents

Abstract **iv**

Acknowledgements **vi**

List of Tables **ix**

List of Figures **x**

Chapters

1. Introduction **1**

Background 1

Problem Statement 3

Dissertation Goal 8

Research Questions 13

Relevance and Significance 14

 Relevance 14

 Significance 15

Barriers and Issues 16

Limitations and Delimitations 17

 Limitations 17

 Delimitations 18

Definition of Terms 19

Summary 20

2. Review of the Literature **22**

Introduction 22

Business Email Compromise in the Cybersecurity Space 23

 Cybersecurity in Corporations 23

 Cyberattack methods in the Business Sector 26

Evolution of Business Email Compromise Attacks 29

 Phishing Attacks 29

 Social Engineering 32

 Business Email Compromise Defined 36

 Anatomy of Business Email Compromise 38

Corporate Users' Detection Skill of Business Email Compromise Attacks 41

 User Personality Impact on Cybersecurity 41

 User Attention Span Impact on Cybersecurity 44

Summary of What is Known and Unknown	46
3. Methodology	47
Overview of Research Design	47
Instrument Development	50
Business Email Compromise Detection Skill	50
User Personality Type	53
Attention Span Level	54
Business Email Compromise Awareness Training	54
Expert Panel	55
Reliability and Validity	56
Reliability	56
Validity	56
Population and Sample	57
Data Collection	58
Pre-analysis Data Screening	60
Data Analysis	60
Resources	62
Summary	63
4. Results	65
Overview	65
Qualitative Research and Expert Panel (Phase 1)	65
Qualitative and Quantitative Research (Phase 2)	71
BEC detection measure	70
BEC Detection Mobile Application	72
Pre-Analysis Data Screening	74
Demographic Analysis	75
Data Analysis	78
Summary	82
5. Conclusions, Implications, Recommendations, and Summary	85
Conclusions	85
Discussions	86
Implications	87
Recommendations and Future Research	88
Summary	89
Appendices	
A. Expert Recruitment Email	95

B. Expert Panel Instrument	96
C. Participant Experiment Recruitment Letter	105
D. Participant Instruction & Survey Instrument (Segment 1)	107
E. Participant Experiment Initial Instruction Email (Segment 2)	113
F. Research Study Informed Consent Form	114
G. Institutional Review Board Approval Letter	117
References	118

List of Tables

Tables

1. Summary of Cybersecurity in Corporations	25
2. Summary of Cyberattacks in the Business Sector	28
3. Summary of Phishing Attacks	31
4. Summary of Social Engineering	35
5. Summary of Business Email Compromise Defined	38
6. Summary of Anatomy of Business Email Compromise	41
7. Summary of User Personality in Cybersecurity	43
8. Summary of User Attention Span in Cybersecurity	45
9. Summary of Research Questions Statistical Analysis	62
10. Descriptive Statistics of SMEs (N=30)	66
11. BEC Detection Measure Components	68
12. Phishing Detection (PD) components	69
13. Mobile Device Malware (MDM) components	70
14. BEC Awareness Training Module Components	70
15. Descriptive Statistics of the Population (N=44)	76
16. ANOVA Results for Personality Attributes	79
17. ANOVA Results for Attention Span	79
18. ANCOVA Results for BECD skills before and after BEC awareness training	80
19. ANCOVA Results for Attention Span When Controlled for Demographics	81

List of Figures

Figures

1. BEC Attack Steps	40
2. Overview of the Research Design Process	49
3. Conceptual Design for Business Email Compromise Detection Level	53
4. Business Email Compromise Detection (BECD) Scoring Equation	53
5. BECD measure score aggregation	71
6. BECD mobile test application login and test initiation screens	73
7. BECD test mobile application login and test initiation screens	74
8. BECD test score statistics by gender	82
9. BECD test score improvement percentage by gender	82

Chapter 1

Introduction

Background

The tremendous advancement of Internet connectivity has enabled an attractive global platform for cyberattacks to surge into the marketplace (Jang-Jaccard & Nepal, 2014). Cyberattacks are continually evolving and becoming more sophisticated, which make them difficult to prevent (Lin, Tien, Chen, Tien, & Pao, 2015). As emails have become a standard method of communication via the connected world, cybercriminals utilize email systems to conduct cyberattacks on businesses for financial gains (Deshmukh, Shelar, & Kulkarni, 2014). Moreover, almost all companies allow emails to directly enter their network for business communication purposes, which make it an especially appealing attack method for hackers (Deshmukh et al., 2014). Social engineering is defined as “the psychological manipulation of people in order to gain access to a system for which the attacker is not authorized” (Bhakta & Harris, 2015, p. 424). The sophistication of business email attacks utilizes social engineering methods to craft customized emails in order to compel corporate users to trust and act on the malicious emails (Kotson, 2015). Furthermore, Kotson (2015) stated that email attacks are the primary method that hackers use to compromise businesses and organizations. Business Email Compromise (BEC) scams are reported in 100 countries around the world

as well as in all 50 states in the United States (U.S.) where businesses of all sizes are being targeted (Security Week News, 2016). Guardian Analytics (2016) has reported that BEC attacks have attributed to \$2 billion in corporate losses from 12,000 businesses globally, while the Federal Bureau of Investigations (FBI) reports it to be over \$5 billion in scam in less than two years (FBI, 2017). FBI (2019) stated that BEC scams have exceeded to \$26 billion in losses through to July of 2019.

This study has addressed the need for additional experimental investigation of the continued growth of BEC attacks on businesses and corporate users (Hinchliffe, 2017; Wilkerson, Levy, Kiper, & Snyder, 2017). The results of this study have contributed to the Information Systems (IS) body of knowledge by providing researchers with insight into corporate users' personality attributes, attention span, demographic attributes, and job characteristics that affect susceptibility to be victimized by malicious BEC email attacks. Human interaction with cyber threats is the predominant flaw in the cybersecurity space for some time now and there is a recognized lack of research in the area of user personality attributes, along with its impact on user susceptibility to business email attacks (Stembert, Padmos, Bargh, Choenni, & Jansen, 2015). Moreover, computer and mobile device user attention span is a key factor in human information processing within computing systems (Bulling, 2016). Therefore, corporate users' attention span has been included in this research. Additionally, the results of this study are aimed to help improve industry cybersecurity practices related to the mitigation of BEC attacks. The remainder of this dissertation is organized to describe the problem statement, dissertation goals, research questions, research significance, research limitations, review of the literature, and research methodology.

Problem Statement

The research problem that this study has addressed is the growing cyberattacks targeting businesses via email and social engineering methods that amount to massive financial loss for companies around the globe (Osuagwa & Chukwudebe, 2015). Choeje, Fung, Wong, Murray, and Sonam (2015) defined cybersecurity as “preservation of confidentiality, integrity, and availability of information” (p. 1). Cyberattacks are defined as “the disruption of computers’ normal functioning and the loss of sensitive information through malicious network events” (Ben-Asher & Gonzalez, 2015, p. 51). Social engineering is a technique used to manipulate users into disclosing information or conducting an action to enable a cyberattack through various forms for example, malicious software such as key loggers to record user credentials, fraudulent phone calls, and the most used form, which is fraudulent email links that hijack the users email account (Osuagwa & Chukwudebe, 2015). Moreover, cybercriminals are increasingly utilizing social engineering in order to surpass security controls (Jakobsson, 2019). Furthermore, corporations are increasingly implementing software systems to optimize their business efficiencies and reduce costs, however cybercriminals are also increasingly targeting these systems to gain information and conduct comprehensive cyberattacks on these organizations (Alotibi, Clarke, Fudong, & Furnell, 2018). One of the main contributing human factors that enable the successful cyberattacks is the user’s limited attention span, which requires ongoing training to maintain an acceptable level of situational awareness related to cybersecurity (Campen, 2009). Attention span is defined as the amount of time that individuals can concentrate on a single task without getting distracted with other tasks (Bulling, 2016). The research conducted by Microsoft Canada

(2015) stated that the average human attention span levels in using computers have decreased from 12 seconds in the year 2000 to just eight seconds in the year 2013.

Moreover, Microsoft Canada (2015) stated that the volume of media consumption, social media usage, multi-screen behavior, and the adoption of technology are most impacting to users on remaining focused on a single task. Therefore, to effectively interact with computing applications such as email, managing the mobile device user' attention span levels are critical (Bulling, 2016).

The massive growth of the Internet, business connectivity, and network vulnerabilities have attributed to the exponential growth in cyberattacks on a global scale (Jang-Jaccard & Nepal, 2014). Additionally, Osuagwa and Chukwudebe (2015) stated that cybercrime is the fastest growing crime method in the world where new sophisticated email attacks are amongst the most dangerous due to the human nature tendency to trust and assist. When it comes to cybersecurity, email attacks specifically are difficult to detect just by utilizing today's email filtering technologies, therefore, humans need to be able to detect legitimate and fraudulent emails that reach their inbox (Ferreira & Lenzini, 2015). The FBI stated that the emerging BEC attacks are more sophisticated than ever seen before and posing a significant threat of financial losses to global corporations of any size (FBI, 2017). BEC attacks are also referred to as "whaling" scams and "Chief Executive Officer (CEO) fraud" (Jakobsson & Leddy, 2016). The FBI Internet Crime Complaint Center (IC3) (2015) stated that BEC attacks are sophisticated email scams that target businesses of any size that often conduct wire transfers, where cybercriminals are closely monitoring and studying their business emails prior to the BEC attack. Furthermore, to conduct the sophisticated BEC attacks, cybercriminals accurately

identify the business environment and employees through many methods, which may include email phishing attacks, as well as professional social networking sites (i.e. LinkedIn) to attain relevant information (FBI IC3, 2015). Moreover, when conducting BEC attacks, hackers profile their victims and learn the payment methods they authorize for business transactions in order to drive a successful attack (Security Week News, 2016). Phishing scams have long been used to gain sensitive information through email messages that seem to be trustworthy and authentic to the corporate users (Thakur, Qui, Gai, & Ali, 2015). The most common types of phishing involve manipulating corporations and users for financial gain and include additional attack vectors such as social engineering, text, and voice conversations to increase the attack success rate (Furnell, Millet, & Papadaki, 2019). Standard phishing attacks have attributed to over \$1.6 billion in losses globally (Konradt, Schilling, & Werners, 2016). Additionally, the cost for corporations to take cybersecurity measures is expected to continue to greatly increase as cyberattacks continue to evolve and drive financial gain for the attackers (Konradt et al., 2016). A more advanced form of phishing attacks are spear-phishing attacks that are more direct attacks on a specific organization and appear to be genuine emails to that organization in order to attain confidential information that is used for malicious intent (Osuagwa & Chukwudebe, 2015). BEC scams have begun since late 2013 where over 69,000 U.S. based businesses have been attacked with reported losses of over \$10 billion (FBI, 2019). Furthermore, the FBI (2017) stated that since 2015 there has been a 2370% increase in BEC attacks globally with a combined dollar loss of over \$5 billion from 40,203 businesses in 131 countries. Since June of 2016 through to July of 2019, BEC attacks have attributed to a combined total of over 166,000 incidents within

domestic and international business have accumulated to over \$26 billion in total financial losses (FBI, 2019). Specific BEC attacks include the business Mega Metals Inc. which was manipulated into wiring \$100,000 into an unknown account utilizing a fraudulent email account with a similar domain name and posing as one of their German based vendors in which they have an existing relationship with (Simon, 2015). A much larger BEC attack was conducted on Ubiquiti Networks where cybercriminals were able to manipulate employees into wiring \$47 million out of their Hong Kong subsidiary, which resulted in the resignation of their Chief Accounting Office (CAO) (Murphy, 2015). Moreover, a Toyota subsidiary in Europe was a victim of a BEC attack where the firm's executive leadership email accounts were hacked, and a \$37 million loss was reported (Lindsay, 2019). It is found that human factor components in cybersecurity are very important in gaining insight around actual security risks and loss outcomes (Shropshire, Warkentin, & Sharma, 2015). Moreover, recent research has found that personality attributes influence users' behavior and perception of risk to cyber threats (Shropshire et al., 2015). Stembert et al. (2015) stated that users' personality attributes are suspected to have an impact on their susceptibility to malicious email attacks. Furthermore, Stembert et al. (2015) stated that business email attacks are increasingly becoming more difficult to detect with automated detection tools, therefore, there is a need for users' ability to detect and react to malicious email attacks. Harrison, Vishwanath, and Rao (2016) defined user detection of email attacks as the user's ability to recognize a deceptive email through cognitive processing of perceived information insufficiency, user's trust personality attributes, and perceived self-efficacy levels. Additionally, user's attention span, while conducting activities such as reading emails, is

greatly reduced due to distractions that drive a pattern of continuous partial attention and lead to the limited user processing of information from the activity at hand (Bulling, 2016). Cyber threats are defined as “any type of malicious activity or actor that leverages computers and networks to adversely affect other computers and networks, to include everything from well-known forms of malware to malicious insiders and targeted attacks” (Cyberedge, 2015, p. 4). Security risks are defined as “the level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring” (Kissel, 2013, p. 161). There is a grave concern within the cybersecurity professionals’ community as well as a highly recognized challenge for organizations regarding corporate users’ lack of cybersecurity knowledge that is jeopardizing corporate data and finances (Greitzer, Strozer, Moore, Mundie, & Cowley, 2014). BEC attacks are a very serious large-scale global threat to businesses of all sizes and have been tracked by the FBI since 2013 (FBI, 2015). The CEO of ValiMail stated that the reason BEC attacks are on the rise, is due to the fact the companies rely too heavily on their email security systems and the cybercriminals are sending sophisticated, impersonation emails that are not detected as suspicious by these systems or employees themselves (Loten, 2016). Therefore, further research is needed on the organizational cybersecurity practices and contributing human factors that drive unintentional employee actions that increase cyberattack susceptibility including those initiated through malicious business emails (Greitzer et al., 2014).

Dissertation Goal

The main goal of this research study was to assess if there are any significant differences of corporate users' detection skills of BEC attacks or signs of actions that can lead to BEC attacks in a simulated test environment based on their personality attributes, using the Myers-Briggs Type Indicator® (MBTI®) 16 personalities® framework. Moreover, this research study assessed if there are any significant differences on the measured detection skills of BEC attacks or signs of actions that can lead to BEC attacks in a simulated test environment based on corporate mobile device users' attention span levels. Additionally, this research study assessed if there are any significant differences on the measured detection skills to BEC attacks or signs of actions that can lead to BEC attacks in a simulated test environment based on demographic indicators such as age, gender, years of computer experience, years of mobile device experience, years of mobile device email use, years of experience in a professional job, the number of employees that are under the supervision of the mobile device user, the job level, the job travel requirement, and the number of email devices used in a simulated test environment. The need for this research is demonstrated by Stembert et al. (2015), which stated that email attacks are gradually getting more sophisticated with customized attacks directed toward individuals and organizations. Furthermore, one of the most advanced manipulation scams is BEC attack, which have cost corporations billions of dollars due to unaware corporate employees (Jakobsson & Leddy, 2016). Human personality attributes and behaviors are a known challenge with email attacks and, therefore, there is need to research specific user personality attributes and user behaviors that enable the success of

email attacks within corporations (Stembert et al., 2015). Furthermore, social engineering deception tactics make BEC attacks very difficult to detect and prevent as they exploit employee tendency to trust, so the attackers successfully manipulate victims into taking actions such as conducting wire transfers (Meinert, 2016). Moreover, due to the growing sophisticated email attacks, automated methods and tools to detect email attacks are increasingly becoming more unsuccessful in mitigating these attacks (Stembert et al., 2015). Cybercriminals are continually finding newer and more creative methods to attack individuals as well as organizations, where email attacks are amongst the most preferred method utilized by hackers today, which make it difficult to defend against (Lin et al., 2015).

The exponential increase utilization of mobile device in the workplace has greatly extended reach to employees beyond the traditional work hours and places where business communication is typically conducted (David, Bieling, Bohnstedt, Ohly, Robnagel, Schmitt, Steinmerz, Stock-Homburg, & Wacker, 2014). In addition, corporate user attention span is a major limiting factor in the individuals' effectiveness when conducting communications via mobile devices (David et al., 2014). Moreover, prior research shows that human actions due to lack of attention span caused by high stress or fatigue impacted employee performance and increases cybersecurity risk (Greitzer et al., 2014). Human attention span is limited and is reduced by distractions such as interruptions, noise, and any emotional interference (Jorm & O'Sullivan, 2012). Sheng, Holbrook, Kumaraguru, Cranor, and Downs (2010) stated that conducting training around email attacks has shown to improve users' susceptibility to become victims. Bulling (2016) stated that limited amount of research has been conducted around the

effect of user attention span on applications such as email. Moreover, in addition to human factors, there is a need to consider organizational factors such as security policies and job pressure (Greitzer et al., 2014). Furthermore, lack of cybersecurity knowledge and skills contribute to the enablement of up to 95% of cybersecurity threats, which lead to significant financial loss to businesses (Carlton & Levy, 2015). This research study was well aligned to expand upon current research of human factors that affect social engineering cyberattacks on organizations and add focus specifically on corporate Business Email Compromise Detection (BECD) amongst corporate users. BECD is defined as the discovery of a BEC breach or signs that may lead to a BEC breach in the future (Verizon, 2017). While, BECD skills are defined as the combination of knowledge, experience, and ability that enables an individual to discover BEC attack or signs that may lead to a BEC attacks in the future (Carlton & Levy, 2015; Verizon, 2017).

This work builds on prior research by developing an experiment that measures whether there are any significant differences between various human components such as personality, attention span, and user demographics on BECD. Uebelacker and Quiel (2014) developed a five-factor social engineering personality framework based on Cialdini's principles of influence theory. Their framework provides the correlation between user personality traits, such as consciousness, extraversion, and openness to the success or failure of principles of influence used by social engineering cyberattacks (Uebelacker & Quiel, 2014). Cialdini's (2009) theory stated that there are six principles of persuasion: (1) consistency, (2) reciprocation, (3) social proof, (4) authority, (5) liking, and (6) scarcity. Frauenstein and Flowerday (2016) mention that social engineering email attacks leverage these six principles of persuasion as psychological triggers to influence

users to perform certain actions. This work also builds on prior research by expanding personality attributes, assessing attention span levels, expanding demographic attributes, as well as developing a BEC awareness training module to assess if there are any changes to significant mean differences with detection of BEC attacks in a simulated test environment. Karjalainen and Siponen (2011) stated that employee non-compliance with security policies are amongst the largest threats, especially in social engineering attacks, and should be resolved through training. Moreover, Karjalainen and Siponen (2011) stated that user cybersecurity training is an underdeveloped area of research. Furthermore, in today's highly open Internet environment, there is a growing problem with cyber attackers persuading users to make fraudulent online electronic payments, and user cybersecurity training will help reduce susceptibility to cyberattacks (Williams, Beardmore, & Joinson, 2017).

Large corporations have sustained high financial losses due to cyberattacks including Nortel Networks, which filed for bankruptcy in 2009 greatly due to hacking of executive computers, servers, and emails (Srinidhi, Yan, & Tayi, 2015). Other malicious email attacks have also included the spear-phishing email attack on the large retailer Target that was forced to pay \$67 million to VISA due to credit card information compromise (Laszka, Lou, & Vorobeychik, 2016). Financial losses are expected to reach \$20 trillion by the year 2020 due to cyberattacks around the globe (Srinidhi et al., 2015). BEC related financial losses have already exceeded \$12 billion in 2018 (Trend Micro, 2018). The need for this research is also demonstrated by Akhunzada et al. (2014), which focuses on the concept that cyberattacks are initiated by humans, therefore, requires a human factor to address these cybersecurity threats. Additionally, Vahdati and Yasini

(2015) analyzed how internal corporate employees address external security threats and found that employee personality attributes can influence the increase or reduction of successful cyberattacks within an organization.

The six specific goals of this research study were as follows. The first specific goal of this research study developed an experiment to measure BECD and validated the experimental protocol utilizing cybersecurity Subject Matter Experts (SMEs) via the Delphi process. The second specific research goal developed, utilized cybersecurity SMEs, a BEC knowledge and awareness training session for the mobile device users. The experiment validation process has utilized 30 SMEs to gain an accurate experiment structure and protocol for this research study. Brown, Levy, Ramim, and Parrish (2015) indicate that using the Delphi process requires multiple interactions with SMEs using methods such as questionnaires to eliminate conflicting data and produce accuracy where human judgment input is critical. The experimental protocol was then implemented in this research study and utilized a group of 45 corporate professional participants who conducted the Myers Briggs Type Indicator® (MBTI®)'s 16 personalities® test and completed the BEC experimental protocol. The third specific research goal assessed whether there are any significant differences on BEC detection based on the different personality attributes. The fourth research goal analyzed the experimental results and assessed whether there are any significant differences between mobile device user attention span, utilizing the Psychology Today® attention span online test and BECD. The experiment then conducted a training exercise that was aimed to improve mobile device user attention span around BEC awareness and ran the experiment a second time which assessed whether there was change to the significant mean difference of BECD

and attention span after the BEC awareness training. The fifth specific research goal assessed whether there are any significant differences between mobile device user BECD skills before and after the BEC awareness training session. The sixth specific research goal analyzed the experimental results and assessed whether there are any significant differences on the BECD based on the demographic indicators: (a) age; (b) gender; (c) years of computer experience; (d) years of mobile device experience; (e) years of mobile device email use; (f) years of experience in a professional job; (g) number of employees that are under the supervision of the mobile device user; (h) job level; (i) job travel requirement; and (j) number of email devices used.

Research Questions

The six research questions that this study addressed are:

RQ1: *What are the Subject Matter Experts' (SMEs) approved components of the experiment to measure BECD skills and its experimental protocol using the Delphi methodology?*

RQ2: *What are the SMEs' approved components of the mobile device users' BECD knowledge and awareness training program using the Delphi methodology?*

RQ3: *Are there any statistically significant mean differences for BECD skills between personality attributes as measured by the 16 personalities® test of corporate professional participants?*

RQ4: *Are there any statistically significant mean differences for BECD skills between attention span as measured by the Psychology Today® test of corporate professional participants?*

RQ5: *Are there any statistically significant mean differences for BECD skills of corporate professional participants before and after BEC awareness training session?*

RQ6: *Are there any statistically significant mean differences for BECD skills and attention span of corporate professional participants when controlled for demographic indicators: (a) age; (b) gender; (c) years of computer experience; (d) years of mobile device experience; (e) years of mobile device email use; (f) years of experience in a professional job; (g) number of employees that are under the supervision of the mobile device user; (h) job level; (i) job travel requirement; and (j) number of email devices used.*

Relevance and Significance

Relevance

This research study was relevant as it seeks to improve the understanding of the corporate users' BECD skills in a simulated test environment. The FBI (2016) has stated that BEC attack continue to grow on a global scale and victims range anywhere from small businesses to large enterprises, within all business markets. In recent years, email driven attacks have become one of the most rapidly growing and most widely used cyberattack methods for financial gain where BEC attacks are the most dominant amongst all email driven cyberattacks (Gupta, Tewari, Jain, & Agrawal, 2016). There has been a steady increase over the last five years utilizing malicious email attacks and social engineering techniques targeting corporations as well as employees (Symantec, 2016). The Verizon (2016) data breach investigative report found that 30% of social engineering malicious email attacks were opened by the targeted employees in under two minutes,

12% continued with actually opening the malicious attachment in under four minutes, and only 3% of targeted employees notified their management of the potential cyberattack. Moreover, there has been a 270% rise in BEC attacks alone since early 2015, however, due to large numbers of unreported attacks, the actual increase in BEC attacks is most likely much greater (Jakobsson & Leddy, 2016). BEC attacks are increasingly attractive to cybercriminals due to the immediate return on investment from wire transfers derived from successful attacks on corporations (Solutionary, 2016). Moreover, BEC attacks are complex social engineering attacks, which are difficult to detect as they are not as technical as other forms of malicious cyberattacks (Solutionary, 2016). BEC attacks have proven to be very successful with multiple agencies reporting massive financial losses including reports by the FBI claiming over 40,000 BEC incidents with \$5.3 billion in losses, French authorities are reporting that 15,000 business have fallen to BEC scams with a loss of over €465 million, and the United Kingdom (U.K.) authorities reporting 994 BEC scams where the largest was for a loss of £18.5 million (Mansfield-Devine, 2016). As corporations increasingly continue to utilize the open Internet, social networks, and a multitude of Internet driven applications, the risk of successful BEC attacks grow in parallel. The understanding and knowledge of corporate email users' attributes that influence the success of BEC attacks is crucial. The relevance of this research study is substantial.

Significance

This research study was significant. This study enhanced existing research focused on cyberattacks in the businesses segment, and more specifically corporate users' BECD skills in a simulated test environment. While automated security solutions have

been effective in reducing email driven cyberattacks, the growing complexity and sophistication of these attacks require corporate email users to possess cybersecurity skills, which continue to be a difficult challenge in the cybersecurity space (Stembert et al., 2015). Mansfield-Devine (2016) stated that while there are certain security solutions, such as anti-malware systems and digital signing of emails can help reduce risks of spoofed emails. However, hackers with access to a genuine email account or whom are utilizing similar domain names can successfully conduct a BEC attack by surpassing the technology triggers (Mansfield-Devine, 2016). Prior research indicated that user awareness and education pertaining to phishing based cyberattacks are factors in reducing attacks, yet for 20 years since phishing has been identified, it is still an effective and growing attack method (Gupta et al., 2016). Moreover, Mansfield-Devine (2016) claimed that potentially the strongest BEC defenses are strong user procedures and policies in place. Insight into the human aspects that influences the detection of BEC attacks can greatly help reduce risk of massive financial losses for organizations. Research shows that there is a need for corporate users' assessment of attributes that can help mitigate cyberattack risks, especially when it comes to sophisticated phishing attacks such as BEC. Therefore, the significance of this research study is substantial.

Barriers and Issues

There were several potential barriers for this research study around the development as well as the execution of a successful and meaningful experiment around BEC detection among corporate users. The first potential barrier was the development and validation of measurement indicators of users' BECD ability utilizing SMEs via the Delphi method. The development and validation of a BECD skills measurement is a

lengthy and complex process, which consists of multiple rounds of direct collaboration with the SME panel to attain a consensus that is meaningful for this research study (Kermanshachi, Dao, Shane, & Anderson, 2016; Dupuis, Crossler, & Endicott-Popovsky, 2016). In addition, appropriate panel of SMEs was needed to ensure valid research outcomes (Okoli, & Pawlowski, 2004). For this research study, an SME panel in the field of information security and cybersecurity was needed to be selected accordingly. The second potential barrier is attaining an Institutional Review Board (IRB) approval for conducting an experimental research study utilizing human participants. This research study required an IRB approval in order to measure BECD skills amongst corporate users. To ensure an ethical study where the research participants were protected and are not at risk in any way during the study. An IRB application was submitted and approved prior to beginning the research study (Musoba, Jacob, & Robinson, 2014). The third barrier was conducting and maintaining a valid experiment in a controlled environment. Experiments in Information Systems (IS) can be limited as it is difficult to control all the variables that may influence the research (Ellis & Levy, 2009). Thus, this study also used the SME panel in order to help validate the experimental setting, requirements, and the actual components of the BECD skills measure.

Limitations and Delimitations

Limitations

This research study developed a new measure for BECD skills and utilized a panel of SMEs leveraging the Delphi process to generate a consensus, which is ultimately the goal and requirement within the process to validate the measure (Dupuis et al., 2016). A potential limitation of the Delphi process is that it can vary within different studies

(Dupuis et al., 2016). Therefore, a consensus threshold of 75% or greater was achieved for the measurement instrument which deemed the Delphi process results acceptable for the study to mitigate potential variability from other studies. Additionally, there was a possible limitation of this research study that the participants may choose to withdraw from the study experiment, which would have potentially led the study to have limitations when it comes to be generalized to a larger population (Ellis & Levy, 2009). Therefore, it was important that this research study mitigate this risk and provided an incentive for the participants to complete the experiment.

During the software development of the mobile application, there was a limitation that was discovered on certain version of iPhones, where certain mobile malware behaviors could not be simulated. The more recent Apple IOS versions generate user alert for certain cybersecurity SME identified mobile malware behaviors such as high CPU usage and high CPU temperatures. Therefore, in order to maintain identical mini-experiments and a seamless user experience, this research study did not simulate malware behaviors, and rather conducted a participant 7-point scale based mini-experiment on the SME identified mobile malware behaviors.

Delimitations

A potential delimitation of this research study was the accuracy of the relevancy of the participant demographic selection for the overall population sample. It was critical to maintain external validity of the experimental results (Ellis & Levy, 2009). This research study needed to maintain generalizability through proper sample selection around all aspects that were assessed including the multiple demographics being assessed for significant mean differences with BEC detection.

Definition of Terms

The following represents the definition of terms:

Attention Span – The time a user can focus on a certain task without diverting attention to another task (Bulling, 2016).

Business Email Compromise (BEC) – A sophisticated cyberattack that is aimed at businesses that conduct wire transfers on a regular basis and leverage social engineering fraudulent emails to persuade an employee to conduct a wire transfer (FBI Internet Crime Complaint Center, 2015).

Business Email Compromise Detection (BECD) – The discovery of a BEC attack or signs that may lead to a BEC attack in the future (Verizon, 2017).

BECD Skills – The combination of knowledge, experience, and ability that enables an individual to discover BEC attack or signs that may lead to a BEC attacks in the future (Carlton & Levy, 2015; Verizon, 2017)

Cyberattack – Any fraudulent task conducted by an individual or group to a computer information system or network (Gupta et al., 2016).

Cybercriminal – Individuals or groups that carry out cyberattacks such for fraudulent reasons such as financial gain, destruction, and terror (Arora, 2016).

Cybersecurity – “A computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It draws from the foundational fields of information security and information assurance; and began with more narrowly focused field of computer security” (JTF on Cybersecurity Education, 2017, p. 16).

Cybersecurity Skills – An individual's competence and technical expertise around Information Technology (IT) that is needed to protect an IT environment against unauthorized use damage, or exploitation (Carlton & Levy, 2015).

Hacker – An unauthorized user who tried to achieve information or access to a system (Kissel, 2013, p. 81).

Phishing – A form of a social engineering cyberattack with the intention of attaining sensitive information via emails consisting of malicious software or fraudulent online website or form (Osuagwu & Chukwudebe, 2015).

Security Risks – The risk to a company or organization's disclosure, disruption, change, or elimination of information or information systems (Kissel, 2013, p. 96).

Spear-phishing – Email based social engineering cyberattacks that are customized and targeted toward specific individuals and organization in order to attain confidential information that is used for fraudulent purposes (Osuagwa & Chukwudebe, 2015).

Social Engineering – The act of psychological manipulation conducted by a cybercriminal to a targeted victim to gain sensitive information or conduct a task (Alazri, 2015)

Spoofing – The process of impersonating or masquerading as someone else for malicious reasons (Osuagwu & Chukwudebe, 2015).

Summary

BEC attacks on companies and organizations of all sizes continue to grow, become more complex, and are significantly financially impacting (FBI, 2017).

Throughout 2017, BEC attacks were one of the top threats that affected organizations and have already reached \$5.3 billion in global financial losses since 2013 (Trend Micro,

2017). The challenge with BEC attacks is that they have evolved into complex social engineering attacks to where security systems are limited in ability to detect these attacks and are more so dependent on the employees to be able to identify BEC attempts (Trend Micro, 2017). Furthermore, cybercriminals utilize email spoofing for BEC attacks to impersonate an executive corporate user request for money transfers in order to pressure the employees to comply with the request (Secureworks, 2017). While there have been some studies conducted around phishing and social engineering email attacks, there is very limited research on individuals' BECD skills related to cyberattacks focused on financial transaction through social engineering tactics. Thus, this research addressed the BEC threats to organizations by assessing corporate user's BECD skills. Furthermore, this research assessed users' personality attributes, attention span, and demographic indicators and tested if there are any significant differences on corporate users' BECD skills in a simulated test environment based on such constructs. Moreover, as cybersecurity training is an underdeveloped area in research and is a crucial component in overcoming social engineering attacks, thus, this research study conducted a user BEC knowledge and awareness training which assessed its implications on corporate users' BECD skills in a simulated test environment.

Chapter 2

Review of the Literature

Introduction

In this chapter, a literature review was conducted to provide a theoretical foundation for this research study pertaining to corporate users' detection of BEC attack signs. The literature review determined that there is a very limited research in the area of BEC attacks. While there is research around corporate user characteristics that attribute to cybersecurity attacks, there is a significant research gap when it pertains specifically to detection of BEC attacks. Moreover, it appears that there is no established measure found in literature for users' BECD skills. As this literature review found that there is a significant lack of research on the user characteristics related to detection of BEC attacks within corporations, this literature review determined that there is a need to further assess corporate user attributes' and test if there are any significant differences on BECD skills based on such constructs. Moreover, the continued growth of BEC attacks is an indicator that current research methodologies are insufficient and affirm that additional research is needed (Wilkerson, 2017).

The literature review has also found that there is a lack of research around corporate user skills to identify mobile malware and other mobile cyberthreats that relates to BECD via mobile device use. Moreover, it has also been determined that the inclusion

of BEC knowledge and awareness training as part of this research study was required. Current regulations and training within corporations are inadequate and do not detect nor prevent BEC attacks (Zweighaft, 2017).

Research has also shown that the user attributes of personality types and attention span relates to users' detection of cybercrime, however, here too there is a gap in research specifically to detection of BEC attacks. For this reason, this research study has focused on assessing if any significant differences exist on corporate mobile device users' BECD skills in a simulated test environment when controlled for the characteristics of personality attributes, attention span levels, and demographic attributes. This in turn, provides organizations a tool to reduce BEC attacks within their companies. This research utilized a systematics literature examination of existing research around BEC and contributes new value to the body of knowledge (Levy & Ellis, 2006).

Business Email Compromise in the Cybersecurity Space

In this section of the literature review, a systematic review of the literature was conducted on the evolution of how BEC attacks have become such a dangerous cyberattack method in the corporate environment and why it is important to enhance the BEC knowledgebase in research. It is important to understand the exponentially increasing landscape of cyberattacks on corporations and how cybercriminals are leveraging social engineering and phishing tactics to conduct the relatively new as well as advanced BEC attack method for financial gain.

Cybersecurity in Corporations

The evolution of technology and the ongoing increase in the utilization of public Internet based services such as cloud computing, social networks, as well as online

money transaction services have greatly increased cyberattack risks for organizations (Bendovschi, 2015). Corporations are becoming increasingly more connected to the open Internet, which in turn has increased the number of cyberattacks that have already affected seven million businesses including high profile attacks on corporations such as Target and JPMorgan Chase & Co. (Nandi, Medal, & Vadlamani, 2016). Similarly, an India based subsidiary of Tecnimont, an Italian engineering firm, reported \$18.6 million in financial losses due to BEC which included hackers impersonating the company's CEO (Goswami, 2019). Cyberattacks have become the second most reported economic crime that has impacted 32% of corporations (PricewaterhouseCoopers, 2016). Therefore, is it important to continue to conduct research around corporate cybersecurity and add value in this research area. Cyberattacks on businesses are increasingly becoming more complex and require a focus not only on the technical security aspects, but the organizational policies and human aspects as well (Roumani, Fung, & Choeje, 2015). When it comes to corporate cyberattacks and business information security risks, the human factor is the weakest link, which is why corporate procedures and policies are critical for organization (Tsohou, Karyda, & Kokolakis, 2015). Therefore, it is important to focus on the human attributes that may be related to the mitigation of corporate cybersecurity risks. Ernst and Young (2015) stated that the top security vulnerabilities for cyberattacks within organizations are carelessness and lack of security awareness of their employees. Tsohou et al. (2015) developed a theory based conceptual framework in the area of corporate user's information security policy compliance and stated that further empirical investigation is needed through experimental studies to fully understand all the factors that enable cyberattacks on organizations. PricewaterhouseCoopers (2016) stated

that only 37% of corporations have a cyberattack response plan in place. The annual costs of cybercrime to the global economy is estimated to be over \$400 billion and could be as high as \$575 billion in total for cost of defense, recovery initiatives, and financial losses (Intel Security, 2014). In recent years, corporate cyberattacks have quickly evolved toward email-based attacks that are posing a massive global threat to corporate cybersecurity, which has spiked a great interest in the research community (Gupta et al., 2016). Therefore, this research study focused on corporate user detection of BEC attacks, which are sophisticated email-based cyberthreats that bring a new and complex financial risk to organizations (FBI, 2017).

Table 1

Summary of Cybersecurity in Corporations

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Gupta et al., 2016	Literature review and analysis	Online datasets comprised of 50,000 spam and 43,000 ham emails	Phishing attacks	Demonstrated the importance of protecting organizations both from a technology as well as user awareness perspective. The growth of Phishing email attacks as the most used type of malicious attack for financial gain.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Nandi et al., 2016	Experimental study via synthetic attack and defend algorithms	200 synthetic nodes (network size)	Cyberattacks	Developed an approach to optimize security countermeasures via attack graph method which analyzes organizational network vulnerabilities
Roumani et al., 2015	Quantitative Analysis study via simulation software and mathematical equations.	Simulated set of cyberattacks	Various information systems variables including perceived value of target, attractiveness of target, and time to penetrate	Current corporate processes are insufficient for loss risk due to lack of cybersecurity threat measures
Tsohou et al., 2015	Literature Review & Analysis of security practices	NA	Conceptual framework of users' intention to comply with information security policies	The impacts influence of corporate users' information security Behaviors impact on corporate policy compliance and the importance of corporate user security awareness training programs

Cyberattack Methods in the Business Sector

Cybercriminals in the business sector are individuals or groups that conduct cyberattacks against corporations, governments, and other organizations, which primarily

have malicious purposes for financial gain, theft of Intellectual Property (i.e. IP), or for destructive purposes (Hughes, Bohl, Ifran, Margolese-Malin, & Solorzano, 2016).

Technological advancements and the growing use of the public Internet have enabled cybercriminals to increasingly become more sophisticated in cyberattack methods (Hemphill & Longstreet, 2016). Moreover, with this development of new tools and techniques, cybercriminals are also consistently increasing in terms of number of attacks and higher level of damage caused to its victims (Bendovschi, 2015). Furthermore, the global public Internet and advanced hacking methods also enable cybercriminals to conduct attacks from anywhere around the globe, while maintaining anonymity by making it very challenging to detect the source of the cyberattacks (Alazab, 2015). The primary motive for cybercriminals to conduct an attack on an organization is for financial gain (Verizon, 2016). Furthermore, the most utilized attack methods used by cybercriminals on corporate networks are email based cyberattacks, such as phishing and BEC social engineering attacks (Trustwave, 2016). In the emerging global threat of BEC, cybercriminals are not only spoofing emails, but are utilizing malware to gain access to actual email threads pertaining to billing in order to conduct successful BEC attacks (FBI, 2015). The increasing cyberattack complexity on corporate users utilizing malicious email-based attacks in the business segment, which warrants additional research in this on the users' ability to detect malicious email attacks (Stembert et al., 2015).

Table 2

Summary of Cyberattack Methods in the Business Sector

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Alazab, 2015	Experimental analysis using software tools	Dataset of 66,703 executable files where 51,223 contain malware	Malware variants	Current security mechanisms are incapable of detecting malware cyberattacks due to growing attack sophistication
Bendovschi, 2015	Literature Review	Aggregated literature data of over 15 million cyberattacks	Cyberattack trends	The strong correlation between cyberattacks and the business sector
Hemphill & Longstreet, 2016	Literature Review	NA	Corporate cybercrime trends	Business segment cybercrime is on an upward trajectory and cyberattack sophistication requires new methods to attacks
Hughes et al., 2016	Literature Review	NA	Security costs and business benefits of information and communication technologies	The global landscape of security spending versus business benefits remains poorly understood
Stembert et al., 2015	Qualitative research via video camera while interacting with email client mockup	24 participants	Malicious email mockups and data capture of behavior, facial expression, and eye movements	Security automation tools are insufficient and user security decisions are required to reduce business email attacks.

Evolution of Business Email Compromise Attacks

Phishing Attacks

Phishing attacks utilize malicious email messages that appear to be reputable emails and are aimed to attain information such as personal or bank account information from individuals or corporations (Thakur et al., 2015). The primary driver in conducting phishing attacks is for financial gain through exploiting system vulnerabilities and user unawareness (Gupta et al., 2016). A common phishing attack method is to drive the email recipient to a fraudulent Website to complete an online form that collects personal or sensitive information that then can be leveraged to gain access to various systems such as email accounts (Osuagwu & Chukwudebe, 2015). These phishing attacks rely heavily on unsuspecting users entering private information into malicious Websites that appear to be genuine and associated with a legitimate organization such as bank entity, but the actual Website's Uniform Resource Locator (URL) is not authentic and use tactics such as misspelled business name within the URL (Jang-Jaccard & Nepal, 2014). While phishing attacks are a global threat, 77% of phishing attacks targeted the U.S. in 2015 and that trend continues to increase (Phishlabs, 2016). Phishing attacks have reached an all-time high in the second quarter of 2016 alone where over 466,000 phishing sites were found and over 315,000 reported phishing email attacks (APWG, 2016). Kaspersky Lab (2016) stated that in the third quarter of 2016 they have identified over 37 million phishing attacks globally, which was 5.2 million (~14%) higher than the second quarter of 2016.

A more evolved and advanced form of phishing attacks are spear-phishing attacks, where more customized attacks on targets are conducted by utilizing social engineering methods which make it difficult for both security systems and end users to

detect (Laszka et al., 2016). Thus, BEC attacks leverage phishing and spear-phishing attack methods to attain confidential information that is used to enable a successful BEC attack (FBI Internet Crime Complaint Center, 2017). Spear-phishing is increasingly targeting corporate users and corporations at an annual rate of 55% increase in 2015 from the previous year (Symantec, 2016). Cybercriminals recognize the financial benefits of spear-phishing attacks on businesses, which by far exceed other phishing methods, therefore, the increase in spear-phishing attacks on the business segment (Sun, Yu, Lin, & Tseng, 2016). Fireeye (2016) stated that 84% of companies acknowledged that they were successfully attacked by spear-phishing attacks. Moreover, Fireeye (2016) also stated that the average successful spear-phishing attack has a \$1.6 million impact on companies. BEC attacks utilize phishing emails to impersonate corporate users in executive positions to attain information and request wire transfers from corporate users (Trend Micro, 2017). Therefore, this research study assessed the corporate users' ability to detect phishing email attacks or signs that lead to such attacks as part of the BECD skill measure. Furthermore, the increase in mobile device use and mobile applications has led to an increase in mobile malware (Jang-Jaccard & Nepal, 2014). BEC attacks also utilize malware to attain information such as the victim's data, passwords, and financial account information (FBI Internet Crime Complaint Center, 2017). Moreover, Jang-Jaccard and Nepal (2014) stated that there is a proactive need for mobile device security measures. Therefore, this research study also included the measure of corporate mobile device users' skill to detect mobile malware as part of the BECD skills measure.

Table 3

Summary of Phishing Attacks

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Jang-Jaccard & Nepal, 2014	Literature Review & Survey Analysis	NA	Emerging cybersecurity threats	Growth of the Internet, business connectivity, and mobile device use have greatly contributed to the exponential growth of cyberattacks. Phishing and malware are amongst the most used and difficult to stop
Laszka et al., 2016	Conceptual paper	NA	Spear-phishing attacks	Spear-phishing attacks are customized social engineering attacks based on targets which make it difficult for both security systems and end users to detect

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Osuagwa & Chukwudebe, 2015	Literature Review	NA	Social engineering cyberattacks	Due to the importance of email communications in business, cybercriminals leverage this medium for social engineering attacks to phish for sensitive information. This has become one of the most dangerous threats of our time for information disclosure and financial loss
Sun et al., 2016	Empirical Study via classroom questionnaires	434 University students	Anti-phishing self-efficacy	Anti-phishing self-efficacy positively impacts the occurrence of anti-phishing behavior. In addition, further research is needed around effectiveness of anti-phishing training
Thakur et al., 2015	Literature Review	NA	Cyber Security Threats	There is a lack of research around users' email password security

Social Engineering

Social Engineering is a modern-day form of the confidence scam where cybercriminals are conducting a psychological manipulation of people through phishing, spear-phishing, vishing (voice solicitation), and impersonation attacks in order to attain

sensitive information or convince the user to conduct a key task in alignment with the attack agenda (Bhakta & Harris, 2015). When it comes to spear-phishing attacks, the more effective ones are those where the fraudulent emails contained real information, such as colleague names and addresses utilizing as much of a social presence as possible in order to persuade the user of email authenticity (Ferreira & Lenzini, 2015). There are multiple social engineering methods that cybercriminals utilize to gain sensitive information to conduct successful cyberattacks including pretexting, spoofing, and phishing (Alazri, 2015). Pretexting is a social engineering method where the hacker is pretending to be another person to gain information usually via phone call, phishing utilizes fraudulent emails, and spoofing is the act of impersonating an email or Website to gain information (Osuagwu & Chukwudebe, 2015). Social engineering can also include leveraging social media platforms to gain information, either using fake social networking accounts and connecting to targeted users or leveraging publicly available social media information as part of the overall social engineering cyberattack (Symantec, 2016). The growth of corporate employees using social media has driven an increase of cybercriminals that leverage social engineering in the social networking space as an attack medium, which further increases corporate cyberattack risks and is a rising concern for businesses (Wilcox & Bhattacharya, 2016). Kunwar and Sharma (2016) stated that cybercriminals strategically social engineer corporate users via online social media outlets such as LinkedIn, Twitter, and Facebook by creating fake profiles with an untraceable fake email address. These cybercriminals then utilize these fake social media accounts to connect to companies and with mutually connected targeted employees for optimal positioning as an authentic user (Kunwar & Sharma, 2016).

Social engineering has evolved to a sophisticated attack method that utilizes comprehensive psychological techniques of influence and persuasion on corporates to perform an action that is not in their best interest (Uebelacker & Quiel, 2014). Key psychological attributes of persuasion such as trust, fear, and commitment have a strong positive correlation to user susceptibility of phishing email attacks (Goel, Williams, & Dincelli, 2017). Thus, social engineering malicious emails are highly utilized in BEC attacks to persuade unsuspecting business email users by impersonating corporate users in executive positions or corporates with authorization to approve wire transfers (Trend Micro, n.d.). Therefore, this research study assessed the corporate user's ability to authenticate their sent emails as part of the BEC detection measure where business executive email accounts have been hacked. Greitzer et al. (2014) conducted a case study analysis of social engineering susceptibility and determined that organization should examine their management practices influence by employee stress, employ effective user trainings, limit access of corporate information externally, and improve employee security awareness around email authenticity. Frauenstein and Flowerday (2016) conducted a theoretical analysis of how information updates on social networking platforms have driven users to become accustomed to easily sharing information, which has led to the increase of user susceptibility to social engineering attacks. This literature review found that additional research is required on the corporate users' behaviors and attention span level around social engineering cyberattacks (Frauenstein & Flowerday, 2016). Moreover, BEC attacks are largely carried out utilizing social engineering methods (FBI, 2017). Furthermore, Greitzer et al. (2014) found that there is a lack of research on the human contributing factors of unintentional insider threats of corporate

users as it pertains to social engineering malicious email attacks. This further validated the need for this research study.

Table 4

Summary of Social Engineering

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Alazri, 2015	Theoretical	NA	Social engineering techniques	Corporate user trainings in social engineering cyberattacks have shown to be effective
Bhakta & Harris, 2015	Experimental data via software algorithm	545 lines of email text	Social engineering detection	Incorrect English grammar is a potential indicator of a malicious email
Ferreira & Lenzini, 2015	Empirical study via phishing email data	52 Phishing emails	Principles of persuasion in social engineering	Principles of persuasion including authority, social proof, consistency, and distraction impact phishing effectively
Frauenstein & Flowerday, 2016	Theoretical	NA	Social Network Phishing	The increased usage of social media has driven users to share information online and be more susceptible to social engineering attacks.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Goel et al., 2017	Experimental research via online survey and phishing email	7,225 undergraduate students	Human vulnerability to phishing attacks	Contextualizing emails to exploit human emotions and appeal to recipients' psychological weaknesses increases their susceptibility to phishing attacks
Kunwar & Sharma, 2016	Literature review & analysis	NA	Cyberattacks in social media	Individuals and companies are exposed to increased cybersecurity risks due to social network utilization and human tendency to trust social media
Wilcox & Bhattacharya, 2016	Conceptual paper	NA	Social engineering mitigation in business	Proposed a framework for businesses to reduce social engineering attack risk

Business Email Compromise Defined

BEC attacks are sophisticated email scams that target businesses, which conduct wire transfers as part of their standard operations (FBI Internet Crime Complaint Center, 2015). These BEC attacks leverage legitimate business email accounts through hacking and social engineering methods to scam the victims into conducting wire transactions (FBI Internet Crime Complaint Center, 2015). Social engineering is a key component

within BEC attacks, where cybercriminals have been very successful in defrauding businesses and employees worldwide (Mansfield-Devine, 2016). There has been an immense increase in BEC attacks throughout 2015 and 2016, while increasingly becoming more complex (Phishlabs, 2016). One of the earlier victims of BEC attacks is Xoom, which transferred \$31 million to a fraudulent account (Verizon, 2016). One of Boeing's suppliers in Austria named FACC has been a victim of a BEC attack, which consisted of multiple wire transfers totaling €41.9 million and has led to the termination of their CEO Walter Stephan (Tung, 2016). Mansfield-Devine (2016) stated that training and ensuring that corporate users are well informed are important factors in BEC attack mitigation as well as user detections skill. Therefore, this research study included BEC awareness training and assessed corporate users' BECD before and after the training. Derouet (2016) stated that it is challenging for organizations to rely on their employees to identify malicious emails, and therefore, have focused on email authentication technologies such as domain keys identified mail (DKIM) to block incoming phishing and BEC attacks. However, Derouet (2016) have added that these malicious email identification methods cannot block all the attacks and even less so, for domains that are outside of the organization. Companies such as Microsoft and Cloudmark have developed products utilizing big data analytics and artificial intelligence programming that aim to protect against BEC attacks, however, have not been successful due to the highly dynamic and shifts in attack strategy of the cybercriminals (Jakobsson & Leddy, 2016). Furthermore, traditional security methods, such as spam filters, have not been successful in blocking BEC attacks as they are custom and have not been detectable via technical security solutions (Jakobsson & Leddy, 2016). Human behavior remains a challenge for

phishing email attacks in the business sector and needs to be further assessed (Stembert et al., 2015). Therefore, the current organizational challenges and lack of success in mitigating BEC attacks warrant the need for additional research of the human attributes that are enabling BEC attack success.

Table 5

Summary of Business Email Compromise Defined

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Derouet, 2016	Theoretical	NA	Spear-phishing & BEC mitigation	For corporate domains, email authentication mechanisms are a sophisticated defense for malicious emails
Jakobsson & Leddy, 2016	Experimental research via scam email messages	Over 200,000 scam email messages	Malicious email attack mitigation	This research study developed an algorithm that looks at email addresses and risk content language to reduce malicious email attack risk
Mansfield-Devine, 2016	Theoretical	NA	Business email compromise methods	BEC training and user policies are potentially the optimal defense against BEC attacks

Anatomy of Business Email Compromise

When it comes to BEC attacks, cybercriminals impersonate a trusted colleague within the organization, such as the CEO and request that the targeted employee conduct

a wire transfer in a fashion that seems to be a legitimate task (Jakobsson & Leddy, 2016). BEC attacks utilize several forms of email configurations in order to successfully deploy the attack, such as a fake email account that could be passed off as a colleagues personal account, a closely mimicked domain alias of the organization that may pass as a legitimate corporate email account, or it may be an actual corporate email account where access was gained through various other attacks that consisted of malware to gain the credentials (Mansfield-Devine, 2016). Prior to the BEC wire transfer request stage, the cybercriminal studies the target through phishing and social engineering methods to be able to accurately depict the specific corporate processes, employees, and business partners associated with the wire transfer request (FBI, 2016).

The FBI has identified five BEC attack versions: (1) the bogus invoice scheme, (2) CEO fraud, (3) account compromise, (4) attorney impersonation, and (5) data theft (FBI, 2017). In the bogus email scheme, the targeted business is requested to wire funds to a known supplier via spoofed email address and clone the process as accurately as possible to legitimize the transaction, but to a fraudulent bank account (Anderson, 2016). The CEO scheme is where the CEO or other business executive's email account is either hacked or spoofed and leveraging that account to request a wire transfer to the fraudulent account (Anderson, 2016). The third scheme of account compromise is where the employee's personal account is hacked and invoice payment requests are sent to vendors in the contact list (Anderson, 2016). The fourth scheme is similar where the cybercriminal impersonates an attorney and pressures the employee to complete a wire transfer (Anderson, 2016). The final BEC attack scheme that has been identified by the FBI is where the attacker sends an email request from an executive spoofed email

account to employees requesting private information and financial statements such as tax statements that are collected prior to the BEC wire transfer request (Anderson, 2016). This research study focused on the CEO scheme, where a business executive's credentials are utilized to authorize a fraudulent wire transaction. The specific steps in which BEC financial fraud is executed are (1) identifying the business target utilizing online information (2) leveraging spear phishing emails and phone calls to exploit corporate users within the company (3) once the victim is convinced of the legitimacy, wire transfer details are provided to the corporate user (4) the wire transfer is executed to the fraudulent bank account controlled by the attacker (FBI Internet Crime Complaint Center, 2017). The BEC attack steps are shown in Figure 1, whereas Table 7 lists a summary of research studies defining anatomy of BEC.

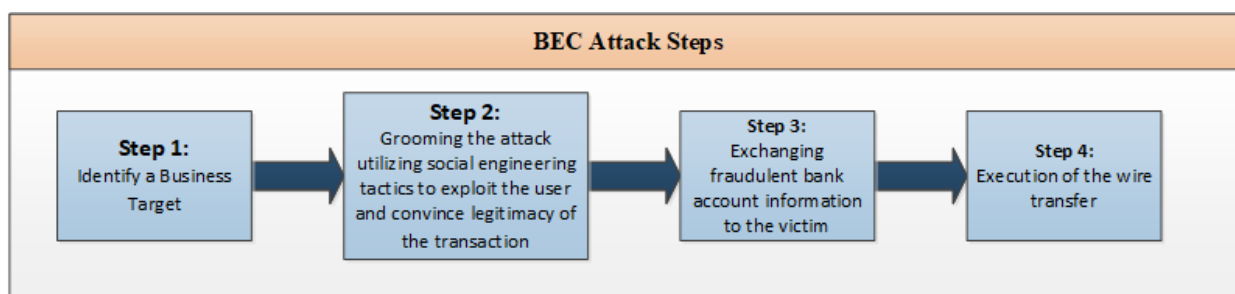


Figure 1: The BEC Attack Steps

BEC attacks, in the form of CEO fraud, are customized and targeted attacks utilizing social engineering to impersonate corporate users in leadership positions to conduct wire transfers (Symantec, 2017). There are numerous BEC attack methods utilized in CEO fraud including gaining access to the corporate network through spear-phishing and malware attacks (FBI, 2017). Moreover, cybercriminals utilize the corporate users' email

style and travel schedule to customize as well as time the BEC attack targeting employees at the office, while the business executive user is not available in order to enhance the attack success rate (FBI, 2017). Thus, there is a need to research BECD capabilities from the business executive's perspective.

Table 6

Summary of Anatomy of Business Email Compromise

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Anderson, 2016	NA	Over 17,600 Reports from Victims in 79 countries	Business Email Compromise attacks	BEC attack examples and mitigation recommendations.
FBI, 2017	NA	Over 40,000 BEC attack reports	Business email compromise methods	BEC attack scenarios, trends, and suggested policies to reduce risk of BEC attacks

Corporate Users' Detection of Business Email Compromise Attacks

User Personality in Cybersecurity

Personality characteristics have been identified as critical factors that affect user detection of cyberattacks such as phishing (Neupane, Saxena, Maximo, & Kana, 2016). User behavior is one of the main concerns in security threat risk and remains to be the weakest component in cybersecurity (Stembert et al., 2015). In cybersecurity within the business sector, there is limited research around the employees' attitude and personality characteristics, which are critical components in managing cyberattack risk and must be taken into consideration by organizations (Safa, Sookhak, Solms, Furnell, Ghani, &

Herawan, 2015). Personality traits such as impulsivity, anxiety, and trust have shown to influence the detection of phishing emails (Neupane, 2016). Maasberg, Warren, and Beebe (2016) proposed a theoretical model that aims to identify employee personality traits that influence motivation for insider cybersecurity threats. Stembert et al. (2015) proposed a human centered integrated framework for phishing detection based on user intelligence and stated that the proposed model as well as current research lacks user personality traits in phishing attacks. The way users perceive, process, and respond to cyberattacks will differ based on their attitudes as well as personalities (Renaud & Weir, 2016). Therefore, there appears to be a need to research user personality attributes in other areas of cybersecurity such as detection of BEC attacks. Uebelacker and Quiel (2014) have developed a user personality framework around social engineering cyberattacks, where the user personality traits: consciousness, extraversion, agreeableness, openness, and neuroticism are directly correlated with Cialdini's principles of influence that are leveraged by the social engineer to drive user behavior. Moreover, Tamrakar, Russell, Ahmed, Richard, and Weems (2016) have determined that the personality traits of anxiety and callousness to have an effect on susceptibility of social engineering attacks and have developed a software system for researchers that simulates email attacks to further explore additional user personality traits that are susceptible to social engineering attacks. This further validates the need to assess the corporate users' personality attributes and how it relates to their detection of BEC attacks in a simulated test environment.

Table 7

Summary of User Personality in Cybersecurity

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Maasberg et al., 2016	Theoretical	NA	Personality traits effect on insider threat.	Developed a theoretical model for insider threat detection through user profiling and employee triggers
Neupane et al., 2016	Experimental study utilizing a survey questionnaire and psychology software tools and neurological imaging	25 university students	Users detection of phishing and malware cyberattacks	Personality attributes (i.e. impulsivity) may result in poor security decisions. Brain activity in the decision-making process for detecting cyberthreats does not indicate a correct decision in mitigating the attack
Renaud & Weir, 2016	Empirical study via survey	110 small and medium business employees	Perceived Security risk	Small and medium sized businesses are not securing their environment in a sufficient manner
Safa et al., 2015	Empirical study via survey questionnaire	212 participants	Corporate user security behavior	Security awareness has a significant impact on corporate users' information security attitude towards conscious care behavior

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Tamrakar et al., 2016	Concept paper	NA	Corporate user personality traits	Development of a configurable software to determine relationships between user cyber behavior and personality traits
Uebelacker & Quiel, 2014	Literature review	NA	Personality traits	There is a correlation between personality traits and social engineering attacks

User Attention Span in Cybersecurity

User attention span has been defined as the concentration time on a single task without shifting attention away from that task (Bulling, 2016). In addition to user attitudes and personalities, the user attention span levels are behavior impacting as well as affect the response to cybersecurity threats (Neupane et al., 2016). User attention span is limited and interruptions such as instant messaging while conducting a computer or mobile task will degrade the memory of the previous task (Jorm & O'Sullivan, 2012). Decreased attention span has been found in numerous studies to gear user attention away from suspicious fraud factors in phishing attacks such as the email source and grammatical errors, but rather on the urgency of the response (Greitzer et al., 2014). Moreover, Greitzer et al. (2014) stated that employee workload and pressures can have a negative impact in user attention span, while causing the user to overlook malicious activity and cyberattacks. Furthermore, the use of smartphones reduces cognition

(Wilmer, Sherman, & Chein, 2017). Therefore, this research study assessed the corporate user attention span specifically to the detection of BEC attacks in a simulated test environment.

Table 8

Summary of Computer User Attention Span in Cybersecurity

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Bulling, 2016	Literature review	NA	User attention	Managing user attention is a major concern in the human-computer interaction field and there is a gap in research around user attention in an everyday setting.
Greitzer et al., 2014	Case study analysis	28 cases derived from news articles, journals, and blogs	Unintentional business insider threats	There is an immaturity in business security reporting as well as a lack of research in contributing factors to email attacks on organization especially the human aspects
Jorm & O'Sullivan, 2012	Literature review	NA	Human attention span	Mobile devices have potential effects on user attention span
Wilmer, Sherman, & Chein, 2017	Literature review	NA	Cognition (attention, memory, and delay of gratification)	there is growing evidence of a significant relationship between smartphone technology and cognitive performance

Summary of What is Known and Unknown

A literature review of BEC in the cybersecurity research field has been conducted to provide a foundation for this research study. A layout of what is known, and unknown is depicted in this literature review. BEC attacks are a relatively new form of cyberthreats to corporations and it was found that limited amount of research has been conducted in this area. Furthermore, there was a lack of research found for an established measure that focuses on corporate users' BECD skill and BEC attack susceptibility in the literature review. Literature does show that there is a need to further research users' ability to detect malicious email attacks (Stembert et al., 2015). Moreover, Flores and Ekstedt (2016) stated that there is a lack of research around phishing email attacks within organizations as well as a gap in the examination of corporate user behavior and relates to social engineering attack detection. This further validated the need for this research study. This literature review did find that there are affecting attributes of user personality and attention span on user ability to detect cyberthreats, however, there was limited research found in this area specifically to BECD and threat mitigation. In addition, this literature review found that there are fast growing cyberattacks utilizing mobile device malware (Jang-Jaccard & Nepal, 2014). Thus, this research study expanded upon the existing body of knowledge in several key focus areas of research. This study developed a set of experiments to measure BECD amongst corporate mobile device users and assessed which of the personal attributes is related to BEC detection.

Chapter 3

Methodology

Overview of the Research Design

This study was an experimental research aimed to determine corporate users' detection of BEC attacks in a simulated test environment. An experimental research aims to determine the differences in the user's BECD based on a set of factors and measures participant performance (Ellis & Levy, 2009; Creswell & Creswell, 2018). Furthermore, there was increased importance in leveraging experimental research designs in the field of information systems and enhanced knowledge in this field (Levy & Ellis, 2011). This study developed an experiment that measures corporate users' detection of BEC attacks in a simulated test environment and empirically assessed if there are any significant differences based on user personality attributes, attention span levels, and demographic attributes. As required for experimental research using human subjects, this research study was conducted following an Institutional Review Board (IRB) approval (Creswell & Creswell, 2018). Figure 2 illustrates the research design that this study followed. In phase 1, this experimental research study developed the BEC measure for the experiment, leveraging a cybersecurity SME panel review and analysis process utilizing the Delphi method. The SME panel recruitment email is shown in Appendix A and the SME panel instrument is depicted in Appendix B. Phase 1 also developed a BEC awareness and

knowledge training module for the participants. The SME panel consisted of 30 cybersecurity SMEs who conducted the BEC measure review. The Delphi method is a proven and effective technique in the field of information systems in the development of the experiment via SMEs (Ramim & Lichvar, 2014). Following Phase 1, adjustments to the experiment tasks and experimental protocols were made. Once validation of the BEC measurement and the training module were achieved, Phase 2 of this research study began with the participant sample selection of 45 corporate users. This phase of the research study initiated a controlled experiment starting with the data collection phase consisting of a qualitative and quantitative data collection utilizing Google® Forms electronic survey to gather participant requirements criteria, demographic data and work experience information as shown in Appendix D. Once the participants were selected, Phase 2 then proceeded with the data gathering utilizing online analysis tests leveraging 16 personalities® test for the user personality assessment and Psychology Today® attention span test for user attention span levels. The next phase of the experiment assessed the participant's BECD skills in a simulated test environment. The experiment was developed with a focus on corporate users in executive positions and was comprised of four mini-experiments that addressed: (1) email authenticity of sent items, (2) the detection of signs of malicious mobile applications, (3) the detection of signs of phishing emails, and (4) the detection of signs of mobile device malware. These mini-experiments were customized per participant and based on the data collection with attributes around sent email screenshots, type of mobile devices used, and email software client used by each participant. These mini-experiments were conducted via custom developed mobile-based simulation application. Upon data gathering completion, a pre-analysis data

screening for reliability followed by a data analysis utilizing linear statistical models Analysis of Variance (ANOVA) and Analysis of Covariance (ANCOVA) to measure the statistical differences of user factors and BECD performance were conducted. The final step in Phase 2 conducted a BEC knowledge and awareness training exercise, then repeated the BECD skills mini-experiments for a second time and assessed whether there was a change in the significant mean difference between the corporate users' BECD performance, along with the measured user factors post BEC knowledge and awareness training.

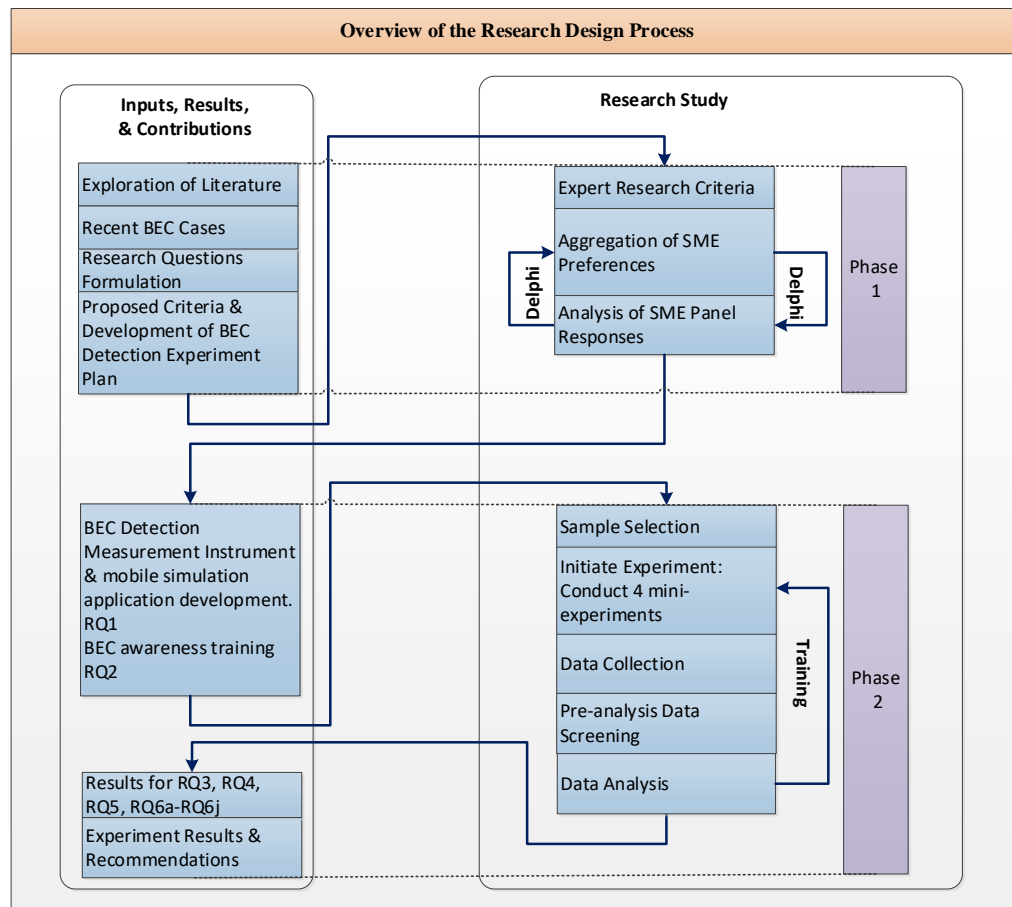


Figure 2: Overview of the Research Design Process

Instrument Development

Business Email Compromise Detection Skills

This research study developed an instrument to measure BECD skills amongst corporate users. FBI (2017) stated that a BEC attacks can arise in several forms including the following scenarios:

Scenario 1: A fraudulent supplier or vendor invoice is sent via spoofed email to a corporate user.

Scenario 2: A compromised executive corporate user email account leads to a fraudulent executive corporate user requests a second employee to conduct a fraudulent wire transfer via spoofed or hacked executive corporate user email.

Scenario 3: An employee business account is hacked or spoofed and sent to vendors requesting payment to fraudulent bank accounts.

Scenario 4: Fraudulent emails from hacked or spoofed impersonating attorneys that are claiming to be handling funds.

The focus of this research was on corporate users in executive leadership roles such as Chief Executive Officers (CEO), Chief Financial Officers (CFO), and any corporate leader that utilizes mobile device-based email communications that has authority to approve payments or financial money transfers to 3rd party vendors. As indicated above, such individuals are the key targets of BEC by cybercriminals. The instrument was developed utilizing cybersecurity SMEs via the Delphi process. The Delphi method is an effective approach in achieving an SME panel consensus in designing a measurement instrument (Ramim & Lichvar, 2014). Prior research has leveraged the Delphi method to

identify user cybersecurity skillsets (Carlton & Levy, 2015). The experiment in this study was conducted utilizing four mini-experiments that are focused on BEC threats on the executive corporate users' mobile device. The FBI (2017) stated that BEC attacks are derived from spoofed or hacked email accounts where hackers use tactics such as malicious links, malware, and phishing emails to gain access to the victim's data. Furthermore, mobile malware indicators include behaviors such as slow performance, reported text messages that were not sent by the mobile user, and the mobile device battery is draining quicker than in the past (Eddy, 2013; Steinberg, 2016). Therefore, the four mini-experiments which consumed approximately five to 10 minutes per experiment and focused on the following areas are:

Mini-experiment 1: Email Authenticity (EA) experiment of sent items. This experiment utilized the collection of the participants' own mobile device screen capture of 20 recently sent items. The experiment required the participants to identify which emails are authentic, and which are fraudulent emails.

Mini-experiment 2: Malicious Mobile Application (MMA) detection. It was critical that mobile device users are familiar with credible and known mobile applications on mobile devices. This experiment simulated the participants' mobile environment to include authentic mobile applications as well as malicious application icons placed in random order within the application icon pages. The participants were then required to identify which application icons are potentially malware

applications within the mobile simulation of their application layout.

Mini-experiment 3: Phishing Detection (PD) experiment. This experiment was comprised of a list of incoming email to the participants in the form of a screen image. The participants were required to identify which emails are credible and which are fraudulent.

Mini-experiment 4: Mobile Device Malware (MDM) detection. In this experiment, the mobile simulation application simulates mobile malware indicators such as impacting the phone's performance, generate pop-ups, increase data usage, drain the phone battery quicker, heat phone, generate fraudulent text messages from known contacts, and switch on the phones Wi-Fi. The participants were then asked to identify any phone performance and concerns they may have experienced during the experiment. The participant's score was determined on the number of identified mobile malware indicators.

The combined score across all four mini-experiments provided a total score indicating the BECD measure as depicted in Figure 3 below.

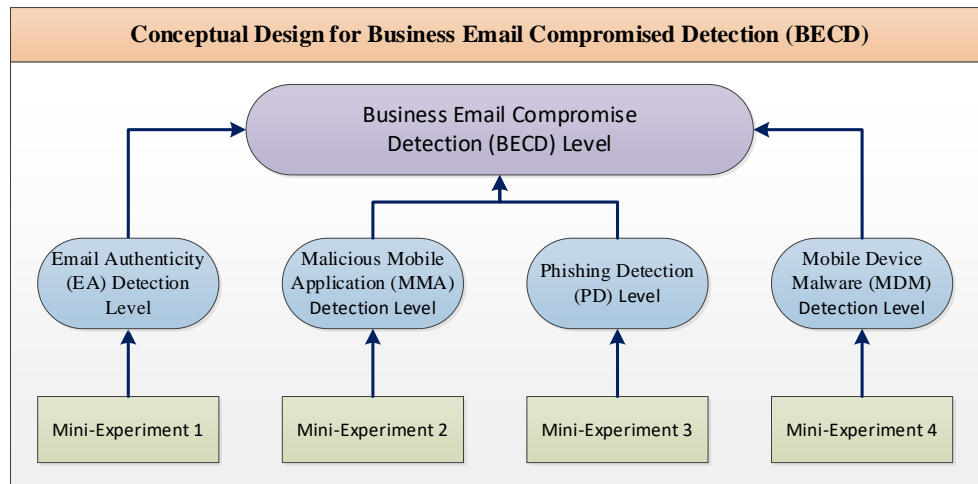


Figure 3: Conceptual Design for Business Email Compromise Detection (BECD)

Level

Each of the four mini-experiments have been scored on a scale of one to 10 and the sum of the scores generated the BECD score as shows in Figure 4. The total BECD score indicated a range from a low BECD skill to an extremely high BECD skill amongst corporate mobile device users.

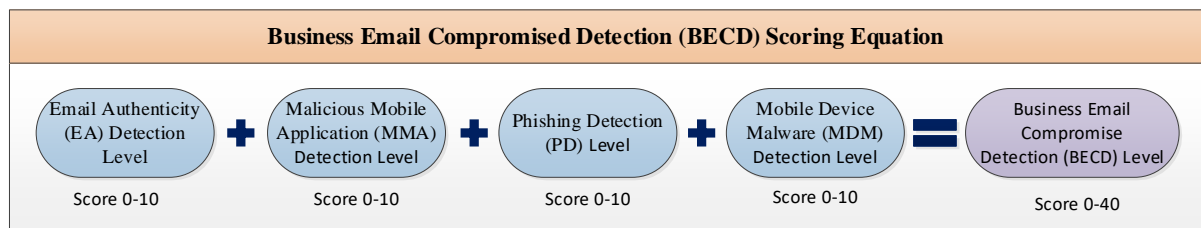


Figure 4: Business Email Compromise Detection (BECD) Scoring Equation

User Personality Type

This study conducted a personality assessment which identified the corporate user personality attributes and assessed whether there are any significant mean differences with BECD. Personality attributes affect user perception of cybersecurity risk as well as security compliance behaviors that impact cyberattack outcomes (Shropshire et al.,

2015). Furthermore, research shows that the Myers Briggs Type Indicator® (MBTI®) is the most popular and widely used personality assessments in the world (Amar & Mullaney, 2017). Therefore, this research study utilized the Myers Briggs based personality online assessment by 16 Personalities® (n.d.). This is a 60-question online web-based assessment utilizing a 7-point Likert scale.

Attention Span Level

This study measured the corporate users' attention span level and assessed whether there are any significant mean differences with BECD. Research shows that there are multiple factors that affect attention span levels, including age and noisy environment conditions (Mani et al., 2004). Furthermore, the use of smartphones has shortened user attention span (Gowthami & VenkataKrishnaKumar, 2016). Therefore, since attention span is a limited resource and can impact user activity, this research study measured attention span levels (David et al., 2014). This research utilized the online web-based attention span level test by Psychology Today® (n.d.) which is comprised of a 10-question multiple choice test.

Business Email Compromise Knowledge and Awareness Training

This research study conducted a BEC knowledge and awareness training module with the goal of enhancing BEC detection skills. Osuagwa and Chukwudebe (2015) stated that security training is a crucial component in raising cyberthreat awareness to ensure information assets are protected as well as a mitigation method of potential cyberattacks. Corporate employee trainings in social engineering cyberattacks have been productive in safeguarding internal corporate information and reducing security threats (Alazri, 2015). This experiment assessed whether BECD training improved the corporate

user BEC detection by conducting the BEC detection experiment for a second-time post training module as shown in Figure 1. There was a 25-minute online virtual BEC awareness training video delivered to the user via the BEC detection test mobile application. The video training consisted of four main modules and included: BEC best practices training conducted, mobile malware detection, known malware training, and phishing detection training

Expert Panel

This research study utilized cybersecurity SME panel to develop the BECD measurement index. A preliminary measurement instrument was created and distributed via email to the expert panel for modification, further development, and ultimately approval. To maintain reliability and validity of the BECD measure, the Delphi method was leveraged for this research study (Carlton & Levy, 2015; Ramim & Lichvar, 2014). The Delphi method is a highly effective tool that has a long history of accuracy and validity in research (Okoli, & Pawlowski, 2004). Moreover, the Delphi method is specifically designed for group communication and developed to avoid confrontation and achieve consensus across an expert panel (Ramim & Lichvar, 2014). Upon development completion and consensus approval of the BECD index measure which used the Delphi method, the BECD index was incorporated into the mini-experiment testing methods and structure that derived the final BECD index. The next steps conducted the experiment and assessed users for BECD performance levels.

Reliability and Validity

Reliability

A reliability assessment was conducted in this research study measure to ensure stability and consistency (Sekaran & Bougie, 2016; Creswell & Creswell, 2018).

Reliability can be measured with internal consistency around the level of agreement within the components of the measurement instrument used (Ellis & Levy, 2009). This research study utilized Cronbach's Alpha test for reliability utilizing Statistical Package for the Social Sciences® (SPSS) Statistics™ version 25. Cronbach's Alpha is the most used consistency and reliability test used for multi-point-scaled constructs (Sekaran & Bougie, 2016; Hair, Sarstedt, Hopkins, & Kuppelwieser, 2014). Moreover, to further enhance the study reliability, every test score as well as the overall BECD scores were manually calculated for each participant. If the manual calculations equated to the scores calculated by the mobile BECD test application, then validity and reliability was established.

Validity

Research findings' validity is critical in order to attain useful and meaningful inferences from the instrument scores (Creswell & Creswell, 2018). Moreover, research validity was important to ensure that the degree to which the instrument measures what is intended as well as that the results are relatable to a real-world setting (Ellis & Levy, 2009). Therefore, a literature review was conducted to ensure content validity as well as construct validity. Goodness of measure was achieved through validation of content validity, construct validity, and criterion-related validity (Sekaran & Bougie, 2016). Moreover, prior research has utilized the Delphi method to ensure validity of the

experiment leveraging SMEs to converge and streamline the measurement components (Carlton & Levy, 2015). Therefore, this research utilized the Delphi method to develop a valid instrument to measure BEC detection capabilities.

Population and Sample

The research study evaluated the BECD performance level amongst corporate users. This research utilized 45 corporate user participants which were selected based on specific criteria that was collected via the initial research study survey shown in Appendix D. Sekaran and Bougie (2016) stated that a sample size of over 30 participants is an appropriate size for research studies. While there are benefits to random sample method in research to ensure equal probability of being selected as well as ensuring that the sample is generalizable to the population, this research required purposeful sampling to target a specific group (Creswell & Creswell, 2018). Therefore, this research study leveraged judgement sampling to target corporate users in executive positions and qualified them using a survey questionnaire via Google[®] Forms and selected participants with the right experience and qualifications in order to ensure that the research study findings are generalizable to the population (Sekaran & Bougie, 2016). The selected participants were required to have experience in utilizing corporate email applications via mobile device and have corporate authorization to approve financial transactions or vendor payments via wire transfer. The focus of this research was on the corporate user in executive roles and employees with authority to approve financial transactions. BEC attack success rate are driven by hacked email accounts, phishing attacks, as well as malware, therefore, it was critical that this study population requirements included participant utilization of business email communications regularly as part of their daily

operational tasks. This research study also gathered key demographic characteristics such as age range, gender, years of experience in using mobile devices, and job travel requirements to ensure that the data collected is a strong representation of the study population.

Data Collection

The data collection for the research study was conducted in several stages. There were several data collection methods used including survey research and experimental research to collect participant data (Creswell & Creswell, 2018). The participants followed two segments in order to complete the research study data collection process as follows:

(1) Segment 1: Online assessment and survey instrument completion

- a. Completion of a 12-minute online personality type assessment consisting of 60 questions on a 7-point scale.
- b. Completion of a 5-minute online attention span test consisting of 10 multiple choice questions.
- c. Enter the test results via online survey and complete the remainder of the survey via Google® Forms.

(2) Segment 2: Experiment and training completion

- a. Conducted four 5-minute mini-experiments via mobile simulation application.
- b. Attended a 25-minute online virtual BEC awareness training via mobile test application.

c. Repeated the four 5-minute mini experiments post training.

Initially the participants were sent a recruiting email as shown in Appendix C with instructions. Upon participant approval, the participants were provided an online survey via Google® Forms that was distributed via email that included instructions to complete the online personality assessment and online attention span tests. The participants were provided online links to the personality test via 16 Personalities® and an attention span test via Psychology Today® via URL that was provided within the survey instrument instruction as shown in Appendix D. Once the participants completed the two assessments, they entered those results along with demographic information directly in the survey instrument. This survey provided critical data for the experiment as well as functioned as the initial participant assessment and qualification requirement gathering which was used to determine whether the participant was a good fit for this research study. Once the participant selection stage was complete and Segment 1 was complete, the participants received the initial instructions for Segment 2 via email as shown in Appendix E. This initiated the request from the participants to provide mobile device screen captures of their email sent items as well as several screenshots of their main application icon screen that was required in the customization of the mini-experiments. After the development of the completion of the customized mini-experiment tests, the participants then conducted the mini-experiments via a custom developed mobile based simulation application for the BEC detection results. In the final step the participants conducted a BEC knowledge and awareness training, which was followed by a second experiment session to measure the post training BEC knowledge and awareness training.

The results of both mini-experiment iterations were captured in the BEC detection test application database.

Pre-analysis Data Screening

A pre-analysis data screening was conducted to ensure the quality of the data collected. It was strongly recommended to check the data reliability and accuracy using pre-analysis checks for data inconsistencies such as missing data and statistical outliers (Buchanan & Scofield, 2018). This research study analyzed the data reliability utilizing Mahalanobis Distance via SPSS® Statistics™ version 25 to detect multivariate outliers and missing data. The next phase in the pre-analysis data screening process, the outliers were assessed and removed from the data that was analyzed, as well as the missing data records were removed prior to the final research data analysis.

Data Analysis

Upon completion of the pre-analysis data screening, this research study utilized the linear statistical models Analysis of Variance (ANOVA) and Analysis of Covariance (ANCOVA) to address the study's research questions utilizing SPSS® Statistics™ version 25. The statistical analysis one-way ANOVA was used to assess for significant mean differences between variables being studies (Sekaran & Bougie, 2016; Sethi & Willis, 2017). In addition, the statistical analysis ANCOVA extends the ANOVA linear model to include more than one continuous variable, referred to as covariates, to determine whether there are significant differences with the dependent variable (Field, A., 2018). Therefore, this search study utilized the ANOVA model to analyze RQ3 and RQ4 as depicted in Table 9.

RQ3: *Are there any statistically significant mean differences for BEC detection between personality attributes as measured by the 16 personalities® framework of corporate users?*

RQ4: *Are there any statistically significant mean differences for BEC detection between attention span as measured by the Psychology Today® attention span test of corporate users?*

Furthermore, to address RQ5 and RQ6, which include covariates, this research study utilized ANCOVA for identifying statistically significant differences between the variables:

RQ5: *Are there any statistically significant mean differences for BEC detection of corporate users before and after BEC awareness training session?*

RQ6: *Are there any statistically significant mean differences for BEC detection and attention span of corporate users when controlled for demographic indicators: (a) age; (b) gender; (c) years of computer experience; (d) years of mobile device experience; (e) years of mobile device email use; (f) years of experience in a professional job; (g) number of employees that are under the supervision of the mobile device user; (h) Job Level; (i) Job travel requirement; (j) Number of email devices used.*

Table 9

Summary of Research Question Statistical Analysis

Research Question Number	Research Question Description	Statistical Analysis
RQ3	Significant mean differences for BEC detection between personality attributes	ANOVA
RQ4	Significant mean differences for BEC detection between attention span	ANOVA
RQ5	significant mean differences for BEC detection of corporate users before and after BEC awareness training session?	ANCOVA
RQ6	statistically significant mean differences for BEC detection and attention span of corporate users when controlled for demographic indicators	ANCOVA

Resources

This research study required and attained IRB approval to conduct the experiment utilizing human participants. This research also accessed security subject matter expert which developed the BEC detection measurement instrument via the Delphi method. Furthermore, this research study consisted of human participants for the BEC experiment and data collection phases. Forty \$10 Gift cards were provided to the participants as a motivational reward for participating in the research experiment. In addition, thirty \$10 gift cards were provided to the security expert panel for their effort in developing the BEC measurement instrument. Once the data collection was completed, the data collection surveys utilizing Google® Forms and was distributed via email. Once the sample was selected, the BEC attack detection experiment utilized a custom mobile simulation application download link and instructions were distributed via email as well.

For the statistical analysis the software packages SPSS® Statistics™ version 25 was utilized.

Summary

Chapter Three consisted of an overview of the quantitative research design and methodology that was conducted. This research design was an experimental research which assessed corporate users' personality attributes and attention span levels on user BEC detection capabilities. As discussed, there were a total of six research questions where RQ1 and RQ2 utilized the Delphi method to determine the approved components of the experiment which measured the BEC detection as well as mobile device user BEC awareness. As discussed RQ3 utilized the ANOVA statistical analysis method to determine whether there are significant mean differences between the corporate users' personality attributes and BEC detection. RQ4 also utilized ANOVA to determine whether there are significant differences between the corporate users' attention span levels and BEC detection. Moreover, the ANCOVA statistical analysis method was used to analyze RQ5 for statistically significant differences between corporate users' BEC detection skills before and after the BEC awareness training. ANCOVA was utilized for RQ6 to analyze the significant differences between demographic attributes and BEC detection. Furthermore, this research study utilized four mini-experiments where the sum of the mini-experiment scores generated an overall BEC detection score amongst corporate mobile device users. The four mini experiments were comprised of:

Mini-experiment 1: Email authenticity experiment of sent items.

Mini-experiment 2: Malicious mobile application detection.

Mini-experiment 3: Phishing detection experiment.

Mini-experiment 4: Mobile device malware detection.

This research utilized Google® Forms, to collect participant data via an online survey instrument. Furthermore, this study utilized the 16 personalities® online test to assess users' Myers Briggs Type Indicator® (MBTI®) for personality attributes. Moreover, the users' attention span levels were collected utilizing the Psychology Today® attention span online test. In addition, the BEC detection experiments were delivered via custom mobile simulation application. Once the data collection phase was complete, this study has utilized the software packages SPSS® Statistics™ version 25 to conduct a linear statistical analysis to answer the research questions and determine the factors contributing to user BEC detection amongst corporate mobile device users.

Chapter 4

Results

Overview

The results of the data analysis for this research study are presented in this chapter. The research study results were completed in two phases, where the details of each of the phases are presented in the order in which they were conducted. Phase 1 details the expert panel data collection utilizing the Delphi method that utilized SMEs to develop the BEC detection measure as well as the BEC awareness and knowledge training module. The results of this phase addresses RQ1 and RQ2. Phase 2 details the results of the main experimental study which utilized a custom mobile application via App Store[®] and Google Play[®]. The results of this phase address RQ3, RQ4, RQ5, and RQ6.

Qualitative Research and Expert Panel (Phase 1)

In phase 1, the research study utilized the Delphi method with a panel of 42 cybersecurity experts that was targeted in order to identify the SME opinion and consensus around the cybersecurity areas for BEC detection (Carlton & Levy, 2015; Ramim & Lichvar, 2014). There were two Delphi rounds, where 30 SME responses were received which represents a 71% SME response rate. The descriptive statistics of the cybersecurity expert panel are provided in Table 10. This research utilized the Delphi

process recommendations from Ramim and Lichvar (2014), upon expert panel agreement to participate in this research study, the BEC measurement instrument questions and components were distributed via anonymous online form to the expert panel for feedback and consensus. These questionnaires were then refined throughout the Delphi rounds until consensus amongst the expert panel was achieved.

Table 10

Descriptive Statistics of SMEs (N=30)

Demographic Item	Frequency	Percentage
<i>Age Group:</i>		
21-30	2	6.7%
31-40	6	20.0%
41-50	7	23.3%
51-60	13	43.3%
61-70	1	3.3%
71 and above	1	3.3%
<i>Gender:</i>		
Male	21	70.0%
Female	9	30.0%
<i>Education Level:</i>		
High School	2	6.7%
Associate Degree	0	0.0%
Bachelors	12	40.0%
Masters	14	46.7%
Doctoral	2	6.7%
<i>Level at Organization:</i>		
Entry Level	0	0.0%
Sr. Individual Contributor	14	46.7%
Supervisor	3	10.0%
Manager	0	0.0%
Director / VP	3	10.0%
Executive/C-Level	8	26.7%
Academic	1	3.3%
System Administrator	1	3.3%
<i>Years in the Information Security field:</i>		
Under 1	1	3.3%
1-4	1	3.3%

5-10	8	26.7%
11-15	7	23.3%
16-20	9	30.0%
21 years and above	4	13.3%
<i>knowledge in Business Email Compromise Attacks:</i>		
Not Familiar	0	0.0%
Somewhat Familiar	3	10.0%
Very Familiar	22	73.3%
Expert in the Field	5	16.7%

In the first round of the Delphi process, the cybersecurity experts were requested to provide opinions and feedback on the cybersecurity components required to measure BEC detection amongst corporate professionals as well as feedback on a BEC awareness training module. Typically, Delphi consensus thresholds range between 51% to 100%, however 75% or greater consensus is standard and therefore an acceptable threshold (Dupuis et al., 2016). There was a total of two sequential Delphi rounds conducted which were refined based on SME feedback. The first Delphi round included capturing of SME demographics, BEC detection measure components, and BEC awareness training module components. This first round asked the SMEs to validate the relevant cybersecurity components for the BEC detection measure and training module for corporate professional mobile device users based on the utilized BEC scam techniques depicted by the FBI (2017) as well as prior research. The cybersecurity SMEs indicated which components for the BEC detection measure and BEC awareness training module that should be included, provided their level of agreement via 7-point Likert scale, and asked for additional recommendations. The cybersecurity experts found the majority of BEC detection components and training awareness module components relevant and important, the sub-component of mobile malware for unexplained or suspicious text

messages was found irrelevant. The second Delphi round consisted of the refined BEC detection measure components and training module components to provide validation. Consensus was achieved for all BEC detection measure components and training module components within the two Delphi rounds. There was a very high agreement amongst the experts at a threshold range of 86.7% to 96.7% as shown in that was achieved for the measurement instrument which deemed the Delphi process results above the standard and acceptable for the study. In view of the above standard consensus achieved, no additional Delphi rounds were required. The SME feedback around the research components were analyzed and validated a high consensus on each component. The cybersecurity SME approved components for the BECD measure are provided in Table 11. These SME approved BEC detection measure components address RQ1.

Table 11

BEC Detection Measure Components

BEC Detection Measure	SME Responses	SME Consensus
Email Authenticity (EA)	30	93.3%
Malicious Mobile Application (MMA)	30	90.0%
Phishing Detection (PD)	30	96.7%
Mobile Device Malware (MDM) detection	30	86.7%

The BECD measure components that derived from the Delphi process are email authenticity detection, malicious mobile application detection, Phishing Detection, and mobile device malware detection. These are the key components for the CEO fraud that focuses on the business executive's that use mobile devices for business purposes and that have the authority to approve financial transactions (FBI, 2017). The BECD measure

component EA refers to the corporate users' capability to recognize and identify the authenticity of their sent emails. The MMA detection component refers to users' detection skill and familiarity with credible and malicious mobile applications. The PD component is the users' ability to detect credible and fraudulent incoming emails. Lastly, the MDM component refers to mobile device behaviors that indicate potential mobile malware on the device. Further SME input was gathered around the sub-components for the BECD components of phishing detection and mobile device malware detection. The cybersecurity SME approved components for the sub-component PD are provided in Table 12.

Table 12

Phishing Detection (PD) Components

Phishing Detection (PD)	SME Component Consensus
Requesting to fill in personal information.	87.0%
Suspicious, unrecognized URL, or URL mismatch	100.0%
The "From" address is an imitation of a legitimate address	97.0%
Pressure tactic to click and/or enter information (i.e. urgent matter, threatening emails, etc.)	86.7%
The mail contains suspicious or unexpected attachments	93.0%
The URL or link shows as unsecure (http://)	87.0%
Poor spelling and grammar	90.0%
Mis-spelled or slightly different URL or email address domain than expected on email	93.0%
Email from unknown sender making big promises	93.0%
Request for money for business reason (i.e. expense, bill payment, etc.)	97.0%
Suspicious Email claiming to be from a government agency	87.0%
Password reset email from a known social network or financial institution	100.0%

The cybersecurity SME approved components for the sub-component MDM are provided in Table 13.

Table 13

Mobile Device Malware (MDM) Components

Mobile Device Malware (MDM)	SME Component Consensus
Mobile Device performance is slow	87.0%
Battery drains quickly	97.0%
Screen Freezes	93.0%
Spike in data usage	97.0%
Popups Ads	87.0%
Wifi/Bluetooth turn on automatically	87.0%
Phone overheats	100.0%
Unexplained phone charges	90.0%
Unrecognized Outgoing calls/texts	87.0%
Application crashes	100.0%

According to Zweighaft (2017), there is a critical need to enhance corporate professional trainings around BEC which will lead to lower BEC incidents within organizations. Therefore, SMEs were also asked to validate a list of BEC awareness training module components and were requested to provide additional training suggestions. Table 14 provides a list of the key training module components utilized in this research study. These SME approved training components for BEC Awareness address RQ2.

Table 14

BEC Awareness Training Module Components

BEC Awareness Training Module Components	SME Component Consensus
BEC Detection Best Practices Training	100.0%
Mobile Malware Detection Training	93.0%
Known Mobile Malware Application Training	93.0%

Qualitative and Quantitative Research (Phase 2)

BEC Detection Measure

In phase 2, the BEC detection instrument was developed. The SME consensus from phase 1 of the four main indicators that make up BECD measure instrument validated the experimental protocol. Each approved BECD indicator was given an equal weight, where the sum of the scores of each BECD indicator determined the users total BEC detection skill level. The BECD measure was then integrated into a custom developed BEC detection mobile application inclusive of pre-training assessment, the BEC awareness training, and the post-training assessment. Figure 8 depicts the overall score aggregation of the BECD measure.

$$\text{Eq. 1 } \text{BECD} = \sum (\text{EA}_i) + \sum (\text{MMA}_j) + \sum (\text{PD}_k) + \sum (\text{MDM}_l)$$

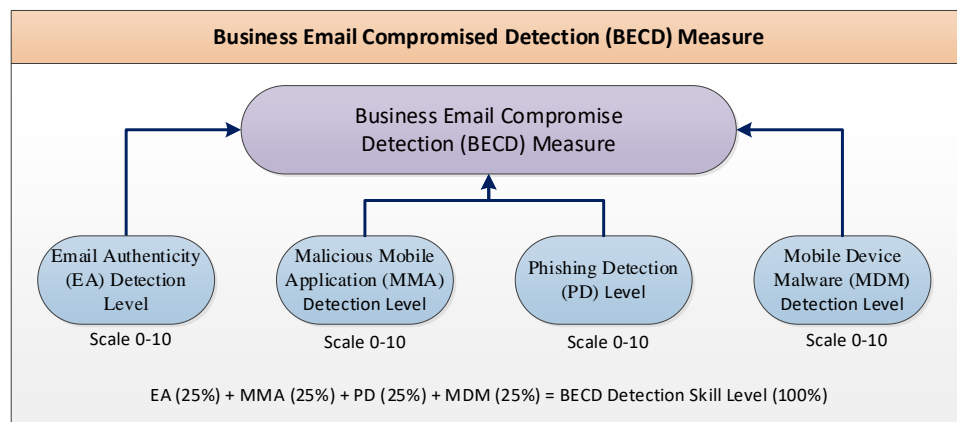


Figure 5: BECD Measure Score Aggregation

BEC Detection Mobile Application

Utilizing the BEC detection measure, a custom mobile application was developed and utilized in this research study to assess the participants BECD skill levels, to train the users via mobile application training video, and to conduct a second post-training BECD skill level assessment. The mobile application was developed utilizing Ionic framework, a cross-platform development system for fast deployment across both iOS and Android mobile platforms. The BEC detection test mobile application was developed with multi-factor authentication mechanisms to ensure participant data protection and a flexible architecture to allow participants to log back in and continue each of the three test sections within the application from where they left off previously, Once a section test has begun, the participant must complete that section within the allotted time. Figure 6 displays screenshot of the BECD test mobile application login and initial start screens. The BEC detection test mobile app consisted of the following three sections:

- Section 1: Pre-training BECD assessment (Four, 5-minute mini-experiments)
 - Pre-training Mini-experiment 1: Email authenticity experiment of sent items.
 - Pre-training Mini-experiment 2: Malicious mobile application detection.
 - Pre-training Mini-experiment 3: Phishing detection experiment.
 - Pre-training Mini-experiment 4: Mobile device malware detection.
- Section 2: BECD Awareness Training
 - A 25-minute in-app training video
- Section 3: Post-training BECD assessment (Repeat the four, 5-minute mini-experiments)

- Post-training Mini-experiment 1: Email authenticity experiment of sent items.
- Post-training Mini-experiment 2: Malicious mobile application detection.
- Post-training Mini-experiment 3: Phishing detection experiment.
- Post-training Mini-experiment 4: Mobile device malware detection.

The mini experiments were delivered to the user as mobile application tests. Each mobile application test was conducted and scored based on the developed BECD measure instrument which the application scored on a range of 0-10 for each test and calculated a total BECD skill level score ranging from 0-40 which derived from the sum of the four mobile app tests.

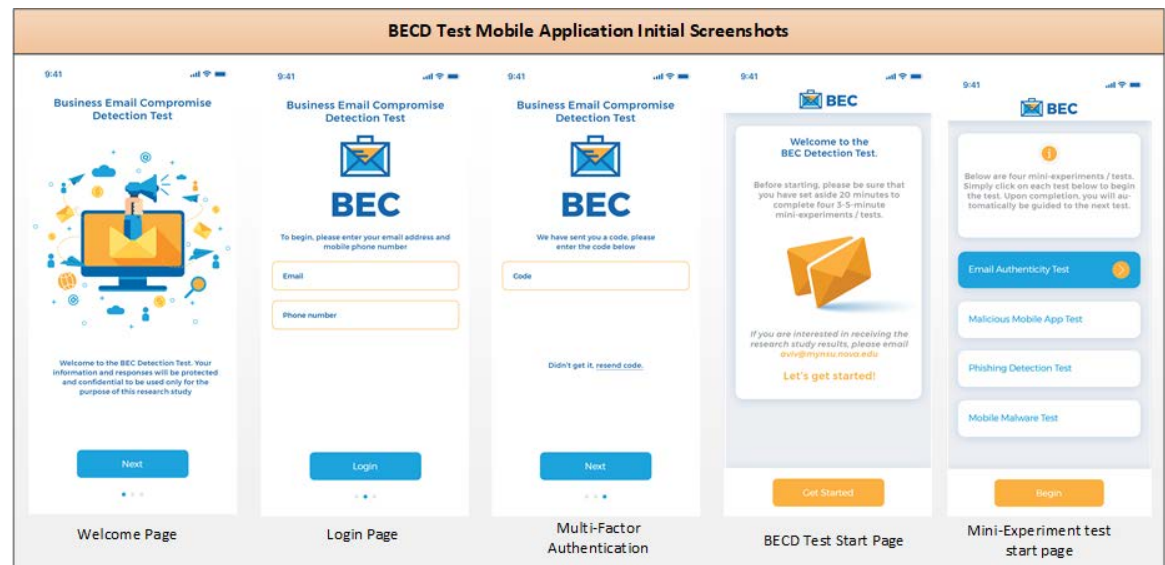


Figure 6: BECD mobile test application login and test initiation screens

In order to develop an effective test for email authentication and malicious mobile application detection, participants were required to provide mobile screenshots as these tests were customized per participant. The EA mini experiment required that each

participant send mobile screenshots of mobile device sent items folder within their mobile email client. This was required in order to test the user's ability to recognize and detect authentic and fraudulent emails that were sent from their email accounts. The MMA mini experiment required that participants send screenshots of their mobile desktop screens where malicious applications were embedded within their own mobile environment via a simulated desktop in the BECD mobile test application. Figure 7 provides the screens of the BECD mobile application of each mini experiment as well as the BEC awareness training video screen.

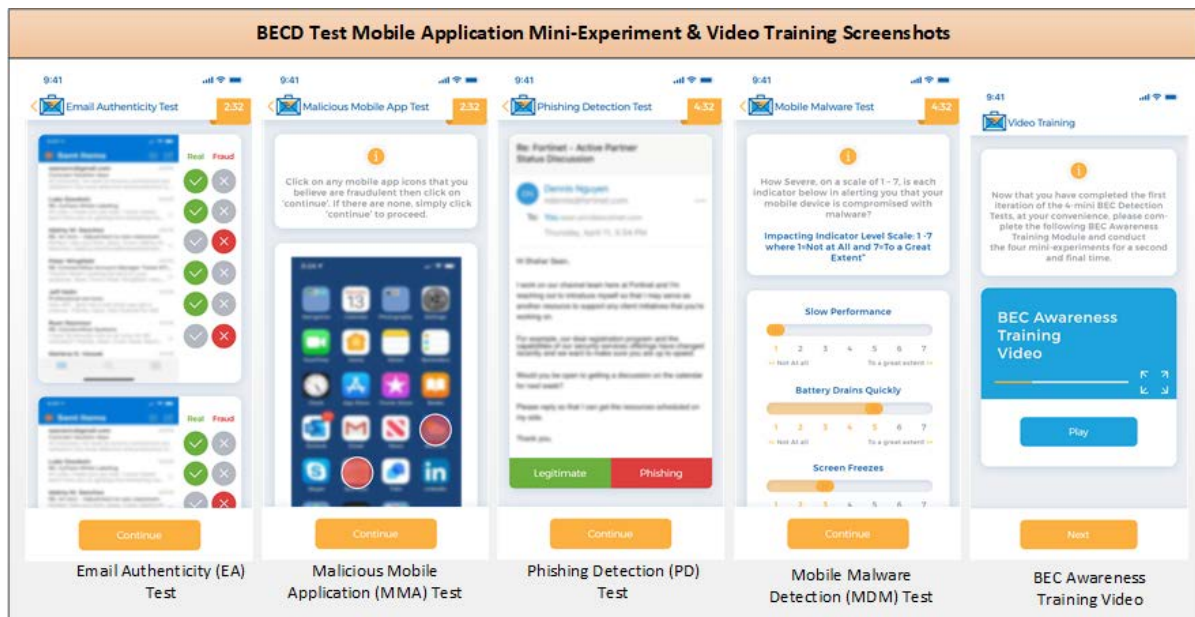


Figure 7: BECD test mobile application login and test initiation screens

Pre-Analysis Data Screening

In Phase 2, corporate professional participants were recruited via recruitment email as shown in Appendix C to the BEC detection research study experiment.

Participants were requested to complete two segments 1) Online personality assessment, online attention span test, online survey via Google Forms®, and provide screenshot captures from their mobile device 2) The research study experiment & training module. The participants that were invited also received a \$10 Amazon digital gift card as a token of appreciation for participating in this research study. There was a total of 78 corporate professionals that were invited to participate, 47 responses were collected, generating a response rate of 60.3%. For relevancy and accuracy purposes, there were 2 participants that responded to not having authority to approve financial transactions and, therefore, were removed from the data collected, leaving a total of 45 participants in the research study experiment.

The data sets collected via Google® Form and the BECD mobile test application were consolidated and imported into SPSS® Statistics™ version 25 for pre-analysis data screening. The participant data was analyzed for response-set issues to address any risk of identical responses to all response values. There were no occurrences of such as case. Moreover, to ensure the accuracy and reliability of the data, a multivariate reliability analysis was conducted utilizing Mahalanobis Distance via SPSS® Statistics™ version 25 to detect multivariate outliers and missing data. Participant ID 25 was removed, resulting in total of 44 participants in the dataset (N=44). The remaining 44 participants were within the acceptable ranges. Therefore, this represents a response rate of 56.4%.

Demographic Analysis

After the completion of the pre-analysis data screening, there were 44 participant responses remaining for data analysis. Of these participants, 40 or 88.9% were male and 5 or 11.1% were completed by females. An analysis of the participant age groups

indicated that 33 or 75% were between the ages of 35 and 54. Furthermore, the analysis indicated that 43 or 97.7% of the participants had over 10 years of computer experience and 41 or 93.2% had over 10 years of smartphone experience. Furthermore, the participant data analysis also revealed that 36 or 81.8% had 10 or more years of experience using mobile device-based email clients and 44 or 100% of the participants had a minimum of two devices that are used for business email communications. This is reflective of today's corporate environment where employees access business application from any location, at any time, via multiple devices. The participant data analysis also indicated that 40 or 90.9% of the participants were 10 or more years in a professional job where 27 or 61.4% were supervising between 6 and 50 employees. Moreover 39 or 88.6% had either no travel or up to 25% travel requirements for work. Moreover, 25 or 56.8% had were at a C-Level job (i.e. Chief Executive Offer, Chief Information Offer, Chief Financial Officer, etc.) and the other 19 or 43.2% were at a manager or above role within their organization. Table 15 presents the participant demographic detail of the study population.

Table 15

Descriptive Statistics of the Population (N=44)

Demographic Item	Frequency	Percentage (%)
<i>Age Group:</i>		
18 and under	0	0.0%
19-24	0	0.0%
25-29	2	4.5%
30-34	1	2.3%
35-39	5	11.4%
40-44	10	22.7%
45-54	18	40.9%
55-59	2	4.5%

60 or older	6	13.6%
<i>Gender:</i>		
Male	39	88.9%
Female	5	11.1%
<i>Computer Experience Years:</i>		
Under 1	0	0.0%
1-3	0	0.0%
4-6	0	0.0%
7-9	1	2.3%
10 and above	43	97.7%
<i>Mobile Device or Smartphone Experience Years:</i>		
Under 1	0	0.0%
1-3	0	0.0%
4-6	0	0.0%
7-9	3	6.8%
10 and above	41	93.2%
<i>Years using a mobile device-based email client:</i>		
Under 1	0	0.0%
1-3	0	0.0%
4-6	1	2.3%
7-9	7	15.9%
10 and above	36	81.8%
<i>Number of devices used for business email communications:</i>		
None	0	0.0%
1	0	0.0%
2	26	59.1%
3	12	27.3%
4	3	6.8%
5 and above	3	6.8%
<i>Years of experience do you have in a professional job:</i>		
Under 1	0	0.0%
1-3	0	0.0%
4-6	2	4.5%
7-9	2	4.5%
10 and above	40	90.9%
<i>Number of Employees under supervision:</i>		
None	0	0.0%
1-5	14	31.8%
6-10	10	22.7%
11-20	12	27.3%
21-50	5	11.4%
51 or above	3	6.8%

***Job travel frequency
requirement:***

None	21	47.7%
Up to 25%	18	40.9%
26% to 50%	3	6.8%
51% to 75%	2	4.5%
Above 75%	0	0.0%

Job Level:

Individual Contributor	0	0.0%
Manager	7	15.9%
Director	11	25.0%
VP	1	2.3%
C-Level	25	56.8%

Data Analysis

Subsequent to the pre-analysis data screening as well as the descriptive analysis were completed, Cronbach's Alpha test for reliability was conducted, an Analysis of variance (ANOVA), and an analysis of covariance (ANCOVA) were used to assess the remaining four research questions. The results of the reliability of the instrument was measured using Cronbach's Alpha was .686. The ANOVA utilizing SPSS® Statistics™ version 25 was then conducted to answer RQ3 and RQ4. For RQ3, the responses were analyzed to determine if there were any significant mean differences for BECD skills between personality attributes as measured by the 16 personalities® test of corporate professional users. The participants completed a pre-test, the BECD awareness training, and then a post-test. The results of the ANOVA indicated that there was no statistically significant mean difference for BECD skills by personality attributes of corporate professional participants, $F(1, 87) = 3.787, p = 0.055$.

Table 16

ANOVA Results for BECD skills by Personality Attributes (N=44)

RQ#	Variable	Mean	St. Dev	F	Sig.	*	Comments
RQ3	Personality Attributes	8.23	4.533	3.787	0.055		No significant mean difference for BECD skills and personality attributes

* $p < .05$, ** $p < .01$, *** $p < .0001$

To answer for RQ4, the responses were analyzed to assess whether there were any significant differences for BECD skills between attention span as measured by the Psychology Today® attention span test of corporate users. The results of the ANOVA indicated that there was a strong significant difference between BECD skills by corporate user attention span, $F(1, 87) = 20.348$, $p < 0.0001$.

Table 17

ANOVA Results for Attention Span (N=44)

RQ#	Variable	Mean	St. Dev	F	Sig.	*	Comments
RQ4	Attention Span	71.55	13.103	20.342	0.000	***	This is a significant mean difference for BECD skills and attention span

* $p < .05$, ** $p < .01$, *** $p < .0001$

To address RQ5 and RQ6, the ANCOVA utilizing SPSS® Statistics™ version 25 was conducted. To address RQ5, analyzing for significant differences for BEC detection skill of corporate users before and after the BEC awareness training session. The results

of the ANCOVA indicated that there was a significant difference $F(1, 86) = 110.97, p < 0.0001$.

Table 18

ANCOVA Results for BECD skills before and after BEC awareness training (N=44)

RQ#	Variable	Pre Training		Post Training		F	Sig.	*
		Mean	St. Dev	Mean	St. Dev			
RQ5	BECD Skill (pre vs. post)	22.87	3.691	30.45	3.017	110.97	0.000	***

* $p < .05$, ** $p < .01$, *** $p < .0001$

To address RQ6, analyzing for significant mean differences for BECD skills and attention span of corporate users when controlled for demographic indicators: (a) age; (b) gender; (c) years of computer experience; (d) years of mobile device experience; (e) years of mobile device email use; (f) years of experience in a professional job; (g) number of employees that are under the supervision of the mobile device user; (h) job level; (i) job travel requirement; and (j) number of email devices used. The results of the ANCOVA indicated that there were no significant differences for attention span when controlled for demographic, aside from gender. For attention span when controlled for gender, indicate a significant difference, $F(1, 87) = 5.414, p = 0.027$. Table 18 presents the ANCOVA results for attention span when controlled for demographic indicators.

Table 19

ANCOVA Results for BECD Skills by Attention Span When Controlled for Demographic Indicators (N=44)

RQ6		BECD Skills by Attention Span			
Variable	F	Sig.		Mean	St. Dev
Age	2.054	0.162		6.61	1.45
Gender	5.414	0.027	*	-	-
Years of computer experience	2.115	0.156		4.98	0.151
Years of mobile device experience	0.109	0.744		4.93	0.255
Years of mobile device email use	0.739	0.396		4.80	0.462
Years of experience in a professional job	0.01	0.922		4.86	0.462
Number of employees under supervision	1.698	0.202		3.38	1.23
Job level	0.266	0.61		1.68	0.80
Job travel requirements	0.541	0.468		3.00	1.22
Number of email devices used	0.013	0.91		3.62	0.886

* $p < .05$, ** $p < .01$, *** $p < .001$

Moreover, for the significant demographic gender, the research study results also indicated that the females mean score improved at a high level than the males after the BECD awareness training. The men BECD score improved by 31.82% where the females improved by 45.24% on their overall BECD test score. As depicted in Figure 8 and Figure 9, while men are less prone to BEC attacked, females have shown to improve at a high level than men via BECD awareness training.

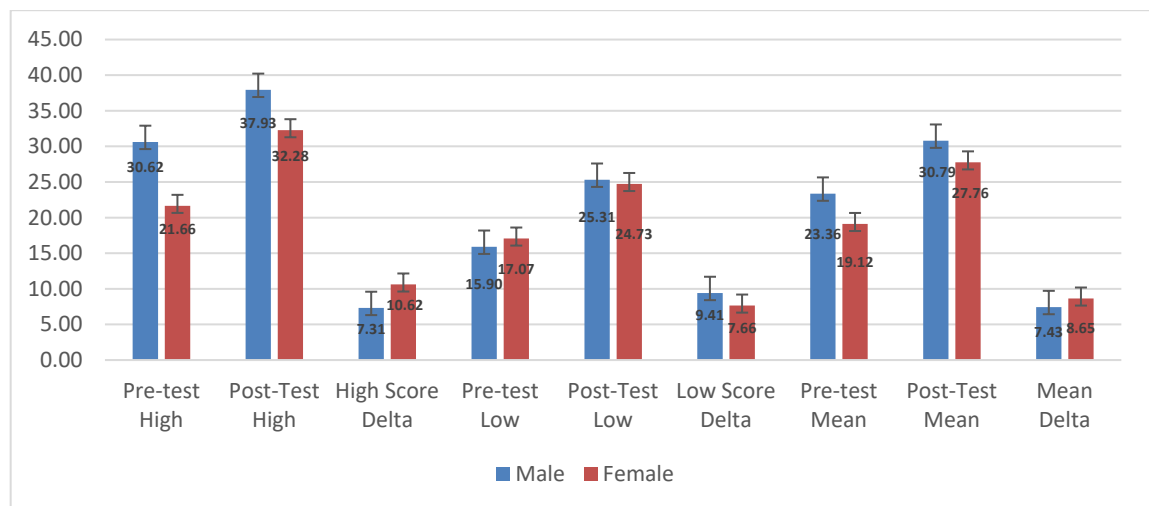
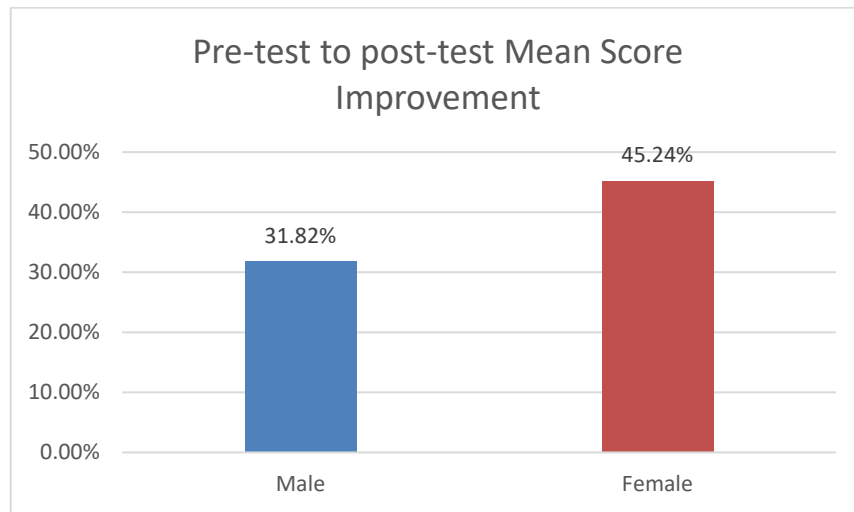


Figure 8: BECD test score statistics by gender**Figure 9:** BECD test score improvement percentage by gender

Summary

In this chapter, the results of the research study were presented in the sequence in which the study was performed. There were two phases as part of this research design that were utilized to address the six research goals. The first section discussed Phase 1 of this research study that addressed a qualitative research that was used to develop the BECD measure instrument and BEC awareness training utilizing cybersecurity experts via the Delphi process. The results consisted of the assessment of the approved BEC detection measure components as well as the approved BEC awareness training module components. Moreover, after two Delphi rounds a consensus was reached amongst the SMEs and both a BECD measure was developed as well as the BEC awareness training module. The main BEC detection measure components were, email authenticity detection, malicious mobile application detection, phishing detection, and mobile device

malware detection. This portion of the study address the first and second specific goals of this research study.

The additional four specific goals were addressed in Phase 2 of this research study. In Phase 2, BECD detection measure and BEC awareness module were integrated into a custom developed mobile application that was used in this research study to assess BEC detection. Moreover, the third specific goal of this research study was addressed in Phase 2. Using the personality attribute data results of the BECD detection scores, to assess if there were significant differences in BECD and personality attributes. ANOVA was utilized for the data analysis to test for differences. The results were presented in Table 16. This phase also addressed the fourth specific goal using the attention span test data as well as the results of the BECD detection score to assess if there were significant differences for BECD skill and attention span. The data analysis for the fourth goal utilized ANOVA. The results for the fourth specific research goal were presented in Table 17. Moreover, the fifth specific research goal to determine if there were significant differences for BECD skills before and after the BEC awareness training which utilized ANCOVA was conducted in this phase. The results for the fifth specific research goal were presented in Table 18. The sixth specific goal was also addressed in Phase 2 which was assessed using ANCOVA for significant differences in BECD and attention span when controlled for demographic indicators. The results were presented in Table 19. After the completion of the data analysis, it was found that while there was no significant difference for BEC detection skills and personality attributes, it was found that there was a significant difference for BEC detection skills and attention span. Furthermore, it was found that there was a significant difference for BEC detection skill before and after the

BEC awareness training module. Moreover, it was found for the sixth research goal that there was a significant difference for BECD skills and attention span when controlled for gender.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusions

The reliance of businesses on the open internet has enabled cyber-criminality to become the fastest growing crime globally and is increasingly becoming more complex and difficult to mitigate (Osuagwa & Chukwudebe, 2015). One of the fastest growing attack methods targeting businesses, is the BEC attack which has a very high success rate by evading detection by both humans and machines and has proven to deliver extremely high financial gains for cybercriminals (Jakobsson, 2019). There has been over \$26 billion in financial losses reported in 177 countries due to BEC attacks and continues to grow (FBI, 2019). Moreover, human behaviors and personality attributes are known challenges in cybersecurity and user susceptibility to cyberattacks, including email-based attacks which impact organizations (Stembert et al., 2015). Therefore, the main goal of this research study was to assess if there are any significant differences of corporate users' BEC detection skill and personality attributes. This research study achieved the six goals with a two-phased approach. First, an expert panel utilizing the Delphi method was used to develop and validate the BEC detection measure instrument and the BEC awareness training module. Second, the developed BEC detection measure and BEC awareness training were integrated into a custom developed mobile application for IOS and Android smartphones that was used to assess the BEC detection skills of corporate

professional users. Lastly, the main study consisted of 44 corporate professional participants that conducted the experiment and utilized the BECD test mobile application for pre-test, BEC awareness training, and post-test.

Discussions

The first result of this research study was the development of a validated and reliable measure of BECD which add significant value to the body of knowledge, as there is limited research specific to the BEC space that is relatively new and limited measure for BEC detection. Furthermore, due to the lack of employee BEC awareness, the advanced nature of the attack, and lack of corporate procedures to mitigate BEC attacks, the second result of this research study adds additional value to the body of knowledge in the development of BEC awareness training module components (Jakobsson & Leddy, 2016). The third result indicate that there was no significant difference found for BECD skill based on personality attributes. The fourth result indicated that there was a significant difference for BECD skills between attention span. Moreover, the fifth result indicated a significant mean difference for BECD skills before and after a BEC awareness training session. The sixth results, while indicated that there were no significant differences found for BEC detection skills and attention span when controlling for age, years of computer experience, years of mobile device experience, years of mobile device email use, years of experience in a professional job, number of employees that are under the supervision, job level, job travel requirement, and number of email devices used, it did find that for the sixth goal there was a significant difference for attention span when controlling for gender.

Overall the corporate professional population of 44 participants demonstrated a pre-training BECD mean score of 57.19% with no corporate professional scoring a perfect 100%. Furthermore, the post-test demonstrated an increase in BECD mean score to 76.12%. Moreover, the study found a significance for BECD skills and BEC awareness training, which further indicates that there is a need for corporate BEC awareness training. While it was found that males were less prone to fall victim to BEC attacks with a pre-test mean BECD score of 58.40% and a mean post-test BECD score of 76.98, the training improvement among males indicate 31.82% improvement. Moreover, it was found that the females received a mean pre-test BECD score of 47.79% and a mean post-test BECD score of 69.41%, indicating a training improvement in females of 45.24% increased improvement.

A limitation in this study was that the BECD test mobile application, simulated the participants mobile phone email and desktop environment. Some of the malware behaviors would not be simulated due to newer enhancements on IOS versions that generate user alert for certain SME identified mobile malware behaviors, for example, higher than normal CPU utilization, higher phone temperatures, and battery drainage. Instead a 7-point scale based mini-experiment was conducted to identify and rate the level of agreement for the different mobile malware behaviors.

Implications

The findings of this research study significantly contributed to the body of knowledge and has several implications for providing both researchers and practitioners additional insight into the development of both BECD measure and BECD awareness training components. The validated BECD measure can be utilized by organizations

globally to assess their employee capability to detect BEC attacks and provide BEC detection skill level scores for employees. Moreover, the validated BEC awareness training components can be utilized to improve employee BECD skill and reduce risk of financial losses due to BEC attacks. The results indicate that the BEC awareness training significantly improved the participant BEC detection skill. Moreover, The BECD measure and BEC awareness training provide tools that can help organizations make informed decisions on employee access to systems and financial authority to mitigate information security and financial loss risks due to BEC attacks. Furthermore, the results indicate that attention span levels amongst corporate professionals impacts the users' ability to detect BEC attacks. Moreover, the results also indicated that there was significant difference for BECD skill levels and attention span levels when controlling for gender. This study also found that female corporate professionals improved at a high level than men in the post-test after the BECD awareness training. This finding enables organizations to an additional layer of focus as well as potential training customization to further optimize and improve employee BEC detection skills based on gender. However, since the sample included only 5 women, this issue should be examined in further research.

Recommendations and Future Research

The research study was to develop and validate a measure for BEC detection, to develop a BEC awareness training module, and to assess corporate professionals for BEC detection skill levels. While not all the goals of this research study were met, there are several areas for expansion and additional future research in the BEC space. BEC is relatively a new cyberattack which is very specific to targeting businesses that conduct

wire transaction and is a cyberattack with the goal of financial gain. In the area BEC, there is limited research and a need to further research in this space. This research study was focused on a specific type BEC attack called CEO fraud. Based on the FBI (2017), there are five types of BEC scams that require further research including (1) the bogus invoice scheme, (2) CEO fraud, (3) account compromise, (4) attorney impersonation, and (5) data theft. Moreover, while this research study found no significant differences for BECD skills and personality attributes for BEC attack type CEO fraud, further research around expanding personality attributes to other types of BEC attack is warranted. Another area that can be improved upon is the attention span assessment around BEC detection. This research study conducted a web-based attention span online test; however, attention span is reduced by distractions such as interruptions, noise, and any emotional interference (Jorm & O'Sullivan, 2012). This warrants additional research around an in-person experiment to enhance the attention span aspect and simulate a real corporate work environment. Finally, due to the highly custom aspect of this research study, scaling this research to a higher population size was restricted. By automating the BECD measure testing tool and expanding the population size to increase the generalizability is recommended.

Summary

This dissertation study has addressed the research problem of the growing cyberattacks targeting businesses via email and social engineering methods that accumulate to massive financial loss for companies worldwide (Osuagwa & Chukwudebe, 2015). The technology evolution that is driving corporations to becoming increasingly more connected to the open Internet and dependent on these connections to

operate their businesses, are also increasing their risk exposure to cybercrime. Moreover, cyberattacks are continually evolving, becoming more complex, and are highly sophisticated. This evolution in cybercrime is making it very difficult for organization to prevent cyberattacks. Corporate cyberattacks have evolved toward email-based cyberattacks that are posing a global threat to corporations and has raised concern and interest within the research community. One of the most successful and dangerous email-based attacks on corporations is a Business Email Compromise (BEC) attack. BEC attacks are highly complex in nature and consists of a multitude cyberattacks methods such as phishing, social engineering, malware, and other hacking methods, which have proved very successful to cybercriminals. The BEC attack landscape has continually increased over the years since it was first identified in 2013. BEC attacks are now attributed to over 166,000 BEC incidents globally with over \$26 billion in reported financial losses to organizations of all sizes (FBI, 2019). While there is research around corporate user characteristics that attribute to cybersecurity attacks, there is limited research specifically around the detection of BEC attacks as it is relatively a new type of attack. Furthermore, it appears that there is no established measure for user BEC detection skill. Therefore, the first specific goal aof this research study was to develop and validate a BEC detection measure and then to develop a BEC awareness training module.

In cybersecurity, the human aspect has been a challenge and is especially significant in when it comes to complex cyberattacks such as BEC. The perception of risk to threats are attributed to user personality attributes. Moreover, user personality attributes as suspected to have an impact on susceptibility to cyberattacks, including

malicious email-based attacks such as BEC. In addition, attention span is a key factor in human information processing within the technology realm. Human interaction with cyberthreats is a known flaw in cybersecurity and is a recognized gap in research around human aspects such as personality attributes and attention span in corporate cybersecurity. Moreover, BEC is one of the fastest growing cyberattacks that is targeting businesses. The sophistication of BEC attacks has a high success for massive financial losses to businesses due to its ability to surpass both network security measures and humans (Jakobsson, 2019). Therefore, this study contributed to the body of knowledge by assessing if corporate professional users are susceptible to be victimized by malicious BEC email attacks based on personality attributes, attention span, awareness training, demographic attributes, and job characteristics. A two-phased approach was utilized to address the goals of this research study as well as answering six research questions.

In Phase 1, a panel of cybersecurity Subject Matter Experts (SMEs) was utilized to review and validate the Business Email Compromise Detection (BECD) measure as well as to review and validate the BEC awareness training module components. This phase used the Delphi methodology to ensure reliability and validity of the BECD measure instruments that was developed. This phase was used to answer the first two research questions as follows:

RQ1: What are the Subject Matter Experts' (SMEs) approved components of the experiment to measure BECD skills and its experimental protocol using the Delphi methodology?

RQ2: What are the SMEs' approved components of the mobile device users' BECD knowledge and awareness training program using the Delphi methodology?

Phase 2 of this research study achieved answers to the remainder of the research questions. This phase utilized 44 participants to conduct the research experiment. The main study was conducted utilizing a BECD test mobile application where four mini-experiments were conducted and make the BECD test scores. Moreover, the mobile test application also conducted a BEC awareness training video. The study data was collected from both a pre- and post-test integrated with the mobile test application. A pre-analysis data screening was completed prior to the statistical data analysis. The next two research questions utilized the statistical model Analysis of Variance (ANOVA) as follows:

RQ3: Are there any statistically significant mean differences for BECD skills between personality attributes as measured by the 16 personalities® test of corporate professional participants?

RQ4: Are there any statistically significant mean differences for BECD skills between attention span as measured by the Psychology Today® test of corporate professional participants?

The results indicated that there was no significant difference for BECD skills between personality attributes of corporate user. However, the results indicated that there was a significant difference between BECD skills and corporate user attention span with a $p < .0001$. The next two research questions utilized the statistical model Analysis of Covariance (ANCOVA) as follows:

RQ5: Are there any statistically significant mean differences for BECD skills of corporate professional participants before and after BEC awareness training session?

RQ6: Are there any statistically significant mean differences for BECD skills and attention span of corporate professional participants when controlled for demographic indicators: (a) age; (b) gender; (c) years of computer experience; (d) years of mobile device experience; (e) years of mobile device email use; (f) years of experience in a professional job; (g) number of employees that are under the supervision of the mobile device user; (h) job level; (i) job travel requirement; and (j) number of email devices used.

The results also indicated that there was a significant difference for BECD of corporate professional user before and after BEC awareness training session with a $p < .0001$.

Moreover, the results also indicated that there was a significant mean difference for BECD skills and span attention when controlled for gender with a $p < 0.05$.

In conclusion, this research made several contributions to the body of knowledge, including providing insights into the development of a BECD measure instrument which can be utilized for to expand and conduct additional research in the area of BEC.

Moreover, this research designed and validated a BEC awareness training module component list which can further be utilized for future research. The training module indicated significant improvements in participant post-test BEC detection skill results.

These tools provide corporations the ability to assess employee BEC detection skill and mitigate BEC risks via the BEC assessment instrument as well as BEC training components. Additionally, the results indicated that there was significant difference for

BECD skill levels and attention span levels which provide organizations insight into impacting factors for BEC detection skills. Moreover, the research the results indicated that there was significant difference for BECD skill levels and attention span levels when controlling for gender, providing additional insights in the BEC area which can further assist in strategies to mitigate risk of financial loss due to BEC attacks.

Appendix A

Expert Recruitment Email

Dear Information Security Subject Matter Expert (SME),

I am conducting a research study that focuses on user detection of Business Email Compromise (BEC) attacks amongst corporate professionals for my dissertation work. I am a PhD candidate in Information Systems at the College of Engineering and Computing of Nova Southeastern University. My dissertation is chaired by Dr. Yair Levy and this work is part of the Levy CyLab Projects (<http://CyLab.nova.edu/>). My research study is seeking to develop the components of the experiment to measure the BEC detection as well as BEC awareness training module that will be presented to the research participants.

The experiment that I am seeking assistance with is aimed to develop a BEC detection instrument that is comprised of 4 mini-experiments. My initial proposed Business Email Compromised Detection (BECD) index score which is comprised of these 4 mini-experiments as follows:

- (1) Mini-experiment 1: Email Authenticity (EA) experiment of sent items.
- (2) Mini-experiment 2: Malicious Mobile Application (MMA) detection.
- (3) Mini-experiment 3: Phishing detection (PD) experiment.
- (4) Mini-experiment 4: Mobile Device Malware (MDM) detection.

By participating in this research study, you agree and understand that your responses are voluntary. All responses are anonymous and no personal identifiable information will be collected or traced back to anyone. Of course, you may stop your participation at any time. If you agree to participate, please reply to this email with your approval. As a token of appreciation for your security expert contribution to this research study you will receive a \$10 Amazon digital gift card to your email address upon completing the survey instruments required to initiate this research study.

Thank you in advance for your consideration. I appreciate your assistance and contribution to this research study. If you wish to receive the findings of the study, feel free to contact me via email and I will be more than happy to provide you with the information about the academic research publication resulting from this study.

Best Regards,

Shahar (Sean) Aviv, PhD Candidate in Information Systems and Cybersecurity

Nova Southeastern University

Email: aviv@mynsu.nova.edu

Appendix B

Expert Panel Instrument

An Examination of User Detection of Business Email Compromise Amongst Corporate Professionals

Dear Information Security Subject Matter Expert (SME),

Thank you for agreeing to contribute to this important cybersecurity research study that focuses on user detection of Business Email Compromise (BEC) attacks amongst corporate professionals. I am a PhD candidate in Information Systems at the College of Engineering and Computing of Nova Southeastern University. My dissertation is chaired by Dr. Yair Levy and this work is part of the Levy Cylab Projects (<http://CyLab.nova.edu/>). My research study is seeking to develop the components of the experiment to measure the BEC detection as well as BEC awareness training module that will be presented to the research participants.

The experiment that I am seeking assistance with is aimed to develop a BEC detection instrument that is comprised of 4 mini-experiments. My initial proposed Business Email Compromised Detection (BECD) index score which is comprised of these 4 mini-experiments as follows:

- (1) Mini-experiment 1: Email Authenticity (EA) experiment of sent items.
- (2) Mini-experiment 2: Malicious Mobile Application (MMA) detection.
- (3) Mini-experiment 3: Phishing detection (PD) experiment.
- (4) Mini-experiment 4: Mobile Device Malware (MDM) detection.

By participating in this research study, you agree and understand that your responses are voluntary. All responses are anonymous and no personal identifiable information will be collected or traced back to anyone. Of course, you may stop your participation at any time. As a token of appreciation for your security expert contribution to this research study you will receive a \$10 Amazon digital gift card to your email address upon completing the survey instruments required to initiate this research study.

I appreciate your assistance and contribution to this research study. If you wish to receive the findings of the study, feel free to contact me via email and I will be more than happy to provide you with the information about the academic research publication resulting from this study.

Best Regards,
Shahar (Sean) Aviv, PhD Candidate in Information Systems and Cybersecurity
Nova Southeastern University
Email: aviv@mynsu.nova.edu

* Required

Email address *

Your email _____

Business Email Compromise Detection Components

You are asked to evaluate the Business Email Compromise Detection (BECD) measure components. Below please find a list of indicators, and as an Information Security SME, please rate the level of agreement that you find for each to be a good fit as a measure of BECD amongst corporate mobile device users.

Instructions: The items below are related to the BECD experiment components. Please indicate the level of agreement for each component for the questions with a 7-point scale, where 1 indicated that you strongly disagree and 7 indicates that you strongly agree.

Please rate the level of agreement that Email Authenticity (EA) of sent items is a good fit as a measure of BECD amongst corporate mobile device users.

1 2 3 4 5 6 7

Strongly Disagree Strongly Agree

Please rate the level of agreement that Malicious Mobile Application (MMA) detection is a good fit as a measure of BECD amongst corporate mobile device users. (example: An unfamiliar application is found on the users' mobile device)

1 2 3 4 5 6 7

Strongly Disagree Strongly Agree

Please rate the level of agreement that Phishing detection (PD) detection is a good fit as a measure of BECD amongst corporate mobile device users.

1 2 3 4 5 6 7

Strongly Disagree Strongly Agree

Please rate the level of agreement that Mobile Device Malware (MDM) detection is a good fit as a measure of BECD amongst corporate mobile device users. (Example: The user is experiencing slower performance on their mobile device)

1 2 3 4 5 6 7

Strongly Disagree Strongly Agree

Are there any other critical components that you feel should be included as a mini-experiment for BECD?

Your answer

Mini-Experiments components and methods

You are asked to evaluate the 4 mini-experiment components and methods.

Instructions: The items below are related to the BECD mini-experiment components. Please indicate the level of agreement for each component for the questions with a 7-point scale, where 1 indicated that you strongly disagree and 7 indicates that you strongly agree.

Mini-experiment 1: Email Authenticity (EA) experiment of sent items: This experiment will begin with the collection of the participants mobile device screen capture of 20 recently sent items. The experiment will require the participants to identify which emails are authentic, and which are fraudulent emails. As an Information Security SME, please rate the level of agreement with this method.

1 2 3 4 5 6 7

Strongly Disagree Strongly Agree

Mini-experiment 1: Email Authenticity (EA) experiment of sent items:
Are there any suggestions or recommendations for this mini-experiment?

Your answer

Mini-experiment 2: Malicious Mobile Application (MMA) detection. This experiment will simulate the participants' mobile environment to include authentic mobile applications as well as malicious application icons placed in random order within the application icon pages. The participant will then be required to identify which application icons are potentially malware applications within the mobile simulation of their application layout. As an Information Security SME, please rate the level of agreement with this method.

1 2 3 4 5 6 7

Strongly Disagree Strongly Agree

Mini-experiment 2: Malicious Mobile Application (MMA) detection. Are there any suggestions or recommendations for this mini-experiment?

Your answer _____

Mini-experiment 3: Phishing detection (PD) experiment. This experiment will be comprised of a list of incoming email to the participants in the form of a screen image. The participants will be required to identify which emails are credible and which are fraudulent. The experiment will utilize known phishing tactics and identifying attributes such as requests for credentials. As an Information Security SME, please rate the level of agreement with this method.

1 2 3 4 5 6 7

Strongly Disagree ☐ ☐ ☐ ☐ ☐ ☐ ☐ Strongly Agree

Mini-experiment 3: Phishing detection (PD) experiment. As an Information Security SME, please check all phishing attributes that you feel should be included in mini-experiment 3, leave the ones that you feel should not be included unchecked.

- ☐ Requesting to fill in personal information.
- ☐ Suspicious, unrecognized URL, or URL mismatch displays when mouse hover over link
- ☐ The "From" address is an imitation of a legitimate address
- ☐ The formatting / Layout are different from what is usually received
- ☐ Pressure tactic to click and/or enter information (i.e. urgent matter, threatening emails, etc.)
- ☐ The mail contains suspicious or unexpected attachments
- ☐ The URL or link shows as unsecure (http://)
- ☐ Poor spelling and grammar
- ☐ Mis-spelled or slightly different URL or email address domain than expected on email
- ☐ Email from unknown sender making big promises
- ☐ Request for money for business reason (i.e. expense, bill payment, etc.)
- ☐ Suspicious Email claiming to be from a government agency
- ☐ Other: _____

Mini-experiment 3: Phishing detection (PD) experiment. Are there any suggestions or recommendations for this mini-experiment?

Your answer _____

Mini-experiment 4: Mobile Device Malware (MDM) detection skill. In this experiment, the mobile simulation application will simulate mobile malware behaviors such as impacting the phone's performance or generate random pop-ups that the participant will need to identify. As an Information Security SME, please rate the level of agreement with this method.

1 2 3 4 5 6 7

Strongly Disagree ☐ ☐ ☐ ☐ ☐ ☐ ☐ Strongly Agree

Mini-experiment 4: Mobile Device Malware (MDM) detection. As an Information Security SME, please check all mobile malware identifiers that you feel should be included in mini-experiment 4, leave the ones that you feel should not be included unchecked.

- ☐ Mobile Device performance is slow
- ☐ Battery drains quickly
- ☐ Screen is frozen for elongated period of time
- ☐ Data usage increases while phone is idle
- ☐ Random pop-ups on the mobile device
- ☐ Unexpected or suspicious text messages
- ☐ Wi-Fi turns on automatically
- ☐ Other: _____

Mini-experiment 4: Mobile Device Malware (MDM) detection. Are there any suggestions or recommendations for this mini-experiment?

Your answer _____

Training Module 5: Overview of how to detect phishing emails utilizing the experiment such as suspicious URLs, request for personal information, etc. As an Information Security SME, please rate the level of agreement with this training module.

	1	2	3	4	5	6	7	
Strongly Disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly Agree

Training Module 6: Overview of how to detect mobile device operational events that impact the mobile device such as battery drainage and frozen screens. As an Information Security SME, please rate the level of agreement with this training module.

	1	2	3	4	5	6	7	
Strongly Disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly Agree

Are there any suggestions or recommendations for the BEC awareness training?

Your answer _____

Please tell us about yourself

What is your age group? *

- ☐ (1) 21-30
- ☐ (2) 31-40
- ☐ (3) 41-50
- ☐ (4) 51-60
- ☐ (5) 61-70
- ☐ (6) 71 and above

What is your Gender? *

- ☐ Male
- ☐ Female

What is your Education Level? *

- ☐ High School
- ☐ Associate Degree
- ☐ Bachelors
- ☐ Masters
- ☐ Doctorate

Level at your organization *

- ☐ Entry Level
- ☐ Sr. Individual Contributor
- ☐ Supervisor
- ☐ Manager
- ☐ Director / VP
- ☐ Executive/C-Level
- ☐ Academic
- ☐ Other: _____

How many years of experience do you have in the Information Security field? *

- ☐ under 1
- ☐ 1-4
- ☐ 5-10
- ☐ 11-15
- ☐ 16-20
- ☐ 21 years and above

How would you rate your knowledge in Business Email Compromise Attacks? *

- ☐ Not familiar
- ☐ Somewhat familiar
- ☐ Very familiar
- ☐ Expert in the field
- ☐ Other: _____

SUBMIT

Page 1 of 1

Never submit passwords through Google Forms.

Appendix C

Participant Recruitment Letter

Dear Participants,

My name is Shahar (Sean) Aviv. I am a PhD candidate at Nova Southeastern University. I am conducting a research study that focuses on user detection of Business Email Compromise (BEC) attacks amongst corporate professionals for my dissertation work. The results of this research study will provide researchers and practitioners additional insight into BEC attack detection and mitigation approaches.

I would appreciate your time in participating in this research study. This study is comprised of several 2 segments as follows:

- (1) Segment 1: Online assessment, Survey, and Screenshot captures
 - a. Complete a 12-minute online personality type assessment (60 7-point scale questions)
 - b. Complete a 5-minute online attention span test (10 multiple choice questions)
 - c. Email screenshot of each online assessment results to: aviv@mynsu.nova.edu
 - d. Complete the online survey via Google Forms.
 - e. Email smartphone screenshots of your sent items email folder containing 20 sent items to: aviv@mynsu.nova.edu
 - f. Email smartphone screenshots of your mobile desktop screens to: aviv@mynsu.nova.edu
- (2) Segment 2: Experiment & Training
 - a. Conduct four 3-5-minute mini-experiments via mobile simulation application.
 - b. Attend a 25-minute online virtual BEC awareness training
 - c. Upon completion of the training, you will be asked during the following day or few days later to repeat the four 5-minute mini experiments.

Your participation is voluntary, and all responses will be confidential. All information and data collected as part of this study will be protected and used only for the purpose of this research study. Moreover, this research and surveys do not collect personal identifiable information and is fully anonymous. Per the above, the research requires that you send mobile screenshots of your mobile email sent items folder for 20 recent emails (just the sent folder view, not the individual emails) as well as several screenshots for your smartphone desktop screens / icons. This information will remain confidential. You may stop your participation at any time. If you agree to participate, please reply to this email with your approval. As a token of appreciation for your participation in this

research study you will receive a \$10 Amazon digital gift card to your email address upon completing of the 2 segments mentioned above.

Thank you,

Shahar Sean Aviv, PhD Candidate in Information Systems and Cybersecurity
College of Engineering and Computing, Nova Southeastern University

Appendix D

Participant Instruction & Survey Instrument (Segment 1)

Business Email Compromise (BEC) attacks to Corporate Professionals

Dear Participants,

My name is Shahar (Sean) Aviv. I am a PhD candidate at Nova Southeastern University. Thank you for agreeing to participate in this important cybersecurity research study which focuses on user detection of Business Email Compromise (BEC) attacks amongst corporate professionals. The results of this research study will provide researchers and practitioners additional insight into BEC attack detection and mitigation approaches.

I would appreciate your time in participating in this research study. This study is comprised of two segments as follows:

- (1) Segment 1: Online assessment, Survey, and
 - a. Complete a 12-minute online personality type assessment (60 questions)
 - b. Complete a 5-minute online attention span test (10 questions)
 - c. Email screenshot of each online assessment results to: aviv@mynsu.nova.edu
 - d. Complete the online survey via Google Forms.
 - e. Email smartphone screenshots of your sent items email folder containing 20 sent items to: aviv@mynsu.nova.edu
 - f. Email smartphone screenshots of your mobile desktop screens to: aviv@mynsu.nova.edu
- (2) Segment 2: Experiment & Training
 - a. Conduct four 5-minute mini-experiments via mobile simulation application that will be provided to you after completing segment 1 (as noted above).
 - b. Attend a 25-minute online virtual BEC awareness training Video.
 - c. Upon completion of the training, you will be asked to repeat the four 5-minute mini-experiments.

Your participation is voluntary, and all responses will be confidential. All information and data collected as part of this study will be protected and used only for the purpose of this research study. Moreover, this research and surveys do not collect personal identifiable information. You may stop your participation at any time. As a token of appreciation for your participation in this research study you will receive a \$10 Amazon digital gift card to your email address upon completing of the 2 segments mentioned above.

Thank you,

Shahar Sean Aviv, PhD Candidate in Information Systems and Cybersecurity
College of Engineering and Computing, Nova Southeastern University

* Required

Email address *

Your email

Tell us about yourself.

Mobile Phone Number *

Your answer

What is your age group? *

- ☐ 18 and under
- ☐ 19-24
- ☐ 25-29
- ☐ 30-34
- ☐ 35-39
- ☐ 40-44
- ☐ 45-54
- ☐ 55-59
- ☐ 60 older

What is your Gender? *

- ☐ Male
- ☐ Female

How many years have you been using a computer? *

- ☐ under 1
- ☐ 1-3
- ☐ 4-6
- ☐ 7-9
- ☐ 10 and above

How many years have you been using a mobile device or smartphone? *

- ☐ under 1
- ☐ 1-3
- ☐ 4-6
- ☐ 7-9
- ☐ 10 and above

How many years have you been using a mobile device based email application? *

- ☐ under 1
- ☐ 1-3
- ☐ 4-6
- ☐ 7-9
- ☐ 10 and above
- ☐ Never

How many devices do you use for business email communications? *

- ☐ None
- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5 and above

How many years of experience do you have in a professional job? *

- ☐ under 1
- ☐ 1-3
- ☐ 4-6
- ☐ 7-9
- ☐ 10 and above
- ☐ Never

What is the number of employees that are under your supervision? *

- ☐ None
- ☐ 1-5
- ☐ 6-10
- ☐ 11-20
- ☐ 21 - 50
- ☐ 51 and above

What is your Job travel frequency requirement for work? *

- ☐ None
- ☐ up to 25%
- ☐ 26% - 50%
- ☐ 51% - 75%
- ☐ Above 75%

What is your Job level? *

- ☐ Individual Contributor
- ☐ Manager
- ☐ Director
- ☐ VP
- ☐ C-Level

In your current position, do you authorize financial payments and/or wire transfers? *

- ☐ Yes
- ☐ No

Which mobile device manufacturer(s) & device model(s) do you use for work related email (example: Apple iPhone 6, Apple iPhone X, Samsung Galaxy 8, etc.) *

Your answer _____

Which mobile email client are you using (example: Gmail, Office365/Outlook, etc.) *

Your answer

What is your job title? *

Your answer

Online Test Results Input

Please enter your online test results below and email a screenshot of the online results screen to:
aviv@mynsu.nova.edu:

Please enter the personality type you have received via the online personality type assessment
(<https://www.16personalities.com/free-personality-test>) [Example: Entertainer (ESFP-a)] *

Your answer

Please enter the attention span score that you have received via the online assessment
(<https://www.psychologytoday.com/us/tests/personality/attention-span-test>). [Note: Score
range is 0 - 100] *

Your answer

Submit

Page 1 of 1

Appendix E

Participant Experiment Initial Instruction Email (Segment 2)

Dear Participants,

Thank you for completing the online assessments and survey. For the next portion of the research study of BECD, we proceed into the 2nd and final segment of the experiment and training, as follows:

- Conduct four, 3-5-minute mini-experiments via mobile simulation application.
- Attend a 25-minute online virtual BEC awareness training
- Upon completion of the training, you will repeat the four 5-minute mini experiments.

Prior to starting segment 2, you will need to send the following via email to aviv@mynsu.nova.edu :

- Mobile screenshots of 20 sent items from your email application.
- 2-3 screenshots of your mobile device application / main screen icon layout

Once received, you will receive an email with further instructions to begin the mini-experiments. You will use that link to download the mobile application and follow the instructions directly on the application.

Once the 1st iteration of the experiments are completed, you will receive an email with a link to the online BEC awareness training where you will complete a 15-minute online training. Upon completion of the training, you will receive another email notification with a link to conduct the 4 mini-experiments for a second time during the following day or few days later.

Reminder, once this segment is complete, as token of appreciation for your participation in this research study you will receive a \$10 Amazon digital gift card to your email address.

Thank you,

Shahar Sean Aviv, PhD Candidate in Information Systems and Cybersecurity
College of Engineering and Computing, Nova Southeastern University

Appendix F

Research Study Informed Consent Form



NOVA SOUTHEASTERN UNIVERSITY
College of Engineering and Computing

Research Study Informed Consent Form

Consent Form for Participants in the Research Study Entitled: *An Examination of User Detection of Business Email Compromise Amongst Corporate Professionals*

Funding Source: None/Unfunded

IRB Protocol #: TBD

Principal Investigator:
Shahar Sean Aviv, Ph.D. Candidate of
Information Systems and Cybersecurity
Email: aviv@mynsu.nova.edu

Co-Investigator & Dissertation Chair:
Yair Levy, Ph.D.
Professor of Information Systems and
Cybersecurity
College of Engineering & Computing
The DeSantis Building – Room 4058
3301 College Avenue
Fort Lauderdale, Florida 33314
Phone: (954) 262-2006
Email: levy@nova.edu

Site Information:

Remotely via online surveys, online training, & online mini-experiment via mobile application.

What is this study about?

You are invited to participate in this research study to be submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Information Systems in the Department of Information Systems & Cybersecurity at Nova Southeastern University. The goal of this research is to develop a Business Email Compromise Detection (BECD) index and to measure the factors impacting BECD amongst corporate professionals using a mobile device application. The results of this research study will provide researchers and practitioners additional insight into BEC attack detection as well as mitigation approaches.

Why are you asking me to be in this research study?

You are being asked to be in this research study because of your interest demonstrated by responding to the posted announcement. You are a corporate professional utilizing mobile device for business email communications, have wire transfer or other digital payments authority within your organization, and are 18 years of age or older. There will be a minimum of 50 participants in this research study.

Are there any benefits for taking part in this research study?

There are no direct benefits aside from the ability to receive a copy of the research findings once it's published in peer-reviewed outlet.

Will I be paid or be given compensation for being in the study?

Upon completion of this research study, you will receive a \$10 Amazon digital gift card to your email address as token of appreciation for your participation.

I
Initials: _____ Date: _____

Page 1 of 3

Will it cost me anything?

There are no costs to you for taking part in this research study.

What will I be doing if I agree to be in this research study?

While you are taking part in this research study, there will be two segments. During the first segment you are asked to complete two online assessments. A 12-minute online personality type assessment consisting of 60, 7-point scale questions and a 5-minute online attention span test consisting of 10 multiple-choice questions. Once both assessments are complete, you will send your online results screen capture via email to aviv@mynsu.nova.edu, and complete a 10-minute online survey via Google Forms (link provided via e-mail). The Second segment is the experiment and training session. In this segment you will conduct four 5-minute mini-experiments via mobile simulation application. The following day or few days later, you will be asked to attend a 15-minute online virtual BEC awareness training, and upon completion of the training, you will repeat the four 5-minute mini experiments. Segment 1 should take approximately 20 minutes to complete. Segment 2 experiments include custom testing that requires you to send mobile screenshots of your 'Sent folder' that includes 20 'sent items' from your email application and 2-3 screenshots of your mobile device applications / main screen icon layout, which will take approximately 15 minutes. This is done in order for us to develop the customized mini-experiments base on your own sent items and mobile device applications / main screen icon layout. Segment 2 should take approximately 90 minutes in total. This will bring the total research study time to approximately 110 minutes. Thank you!

How will you keep my information private?

Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law and will be limited to people who have a need to review this information (the student & overseeing professor only). The responses and data submitted will be collected via Google Forms, Email, and mobile experiment application. This data will be available to the researcher, the Institutional Review Board and other representatives of this institution. When the results of the study are published in a scientific peer-reviewed conference, journal, or book, we will not identify you or any information about you, rather provide information in aggregated form only across all participants of the study. At the end of the data collection period, all information will be removed from online mechanisms and saved to a local USB drive. The USB drive will be kept in a locked file cabinet for 36 months from the end of the research study and destroyed after that time by formatting the USB drive.

Are there possible risks to me?

This research study involves minimal risk to you. To the best of our knowledge, the things you will be doing have no more risk of harm than you would have in everyday life.

What happens if I do not want to be in this research study?

You are welcome to leave this research study at any time, or not be in it. If you do decide to leave or you decide not to be in the study anymore, you will not get any penalty or lose any services you have a right to get. If you choose to stop being in the study, any information collected about you **before** the date you leave the study will be kept in the research records for 36 months from the end of the study, but you may request that it not be used.

Initials: _____ Date: _____

Whom can I contact if I have questions, concerns, comments, or complaints?

If you have questions now, feel free to ask us. If you have more questions about the research, your research rights, or have a research-related inquiry, please contact:

Primary contact:

Shahar (Sean) Aviv can be reached at 561-843-1811 or aviv@mynsu.nova.edu

Research Participants Rights

For questions/concerns regarding your research rights, please contact:

Institutional Review Board
Nova Southeastern University
(954) 262-5369 / Toll Free: 1-866-499-0790
IRB@nova.edu

You may also visit the NSU IRB website at www.nova.edu/irb/information-for-research-participants for further information regarding your rights as a research participant.

Research Consent & Authorization Signature Section

Voluntary Participation - You are not required to participate in this study. In the event you do participate, you may leave this research study at any time. If you leave this research study before it is completed, there will be no penalty to you, and you will not lose any benefits to which you are entitled.

If you agree to participate in this research study, sign this section. You will be given a signed copy of this form to keep. You do not waive any of your legal rights by signing this form.

SIGN THIS FORM ONLY IF THE STATEMENTS LISTED BELOW ARE TRUE:

- You have read the above information.
- Your questions have been answered to your satisfaction about the research.

Adult Signature Section

I have voluntarily decided to take part in this research study.

Printed Name of Participant

Signature of Participant

Date

Printed Name of Person Obtaining
Consent and Authorization

Signature of Person Obtaining Consent &
Authorization

Date

Appendix G

Institutional Review Board Approval Letter



MEMORANDUM

To: **Shahar Sean Aviv**

From: **Ling Wang, Ph.D.,
Center Representative, Institutional Review Board**

Date: **October 26, 2018**

Re: **IRB #: 2018-546; Title, "An Examination of User Detection of Business Email Compromise
Amongst Corporate Professionals"**

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under **45 CFR 46.101(b) (Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies)**. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

- 1) **CONSENT:** If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.
- 2) **ADVERSE EVENTS/UNANTICIPATED PROBLEMS:** The principal investigator is required to notify the IRB chair and me (954-262-5369 and Ling Wang, Ph.D., respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.
- 3) **AMENDMENTS:** Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Yair Levy, Ph.D.
Ling Wang, Ph.D.

References

- 16 Personalities (n.d.). *Free personality test*. Retrieved from <https://www.youtube.com/watch?v=LfGaDd7-dlk>
- Akhunzada, A., Sookhak, M., Anuar, N. B., Gani, A., Ahmed, E., Shiraz, M., Furnell, S., Hayat, A., & Khan, M. K. (2014). Man-at-the-end attacks: Analysis, taxonomy, human aspects, motivation and future direction. *Journal of Network and Computer Applications*, 48, 69-76. doi: 10.1016/j.jnca.2014.10.009
- Alazab, M. (2015). Profiling and classifying the behavior of malicious codes. *Journal of Systems and Software*, 100, 91-102. doi: 10.1016/j.jss.2014.10.031
- Alazri, A. S. (2015). The awareness of social engineering in information revolution: Techniques and challenges. *Institute of Electrical and Electronic Engineers International Conference for Internet Technology and Secured Transactions*, 198-201. doi: 10.1109/ICITST.2015.7412088
- Alotibi, G., Clarke, N., Fudong, L., & Furnell, S. (2018). The current situation of insider threat detection: An investigative review. *Institute of Electrical and Electronic Engineers Saudi Computer Society National Computer Conference*. doi: 10.1109/NCG.2018.8592986
- Amar, A.D., & Mullaney, K. (2017). Employee ability to innovate: How can organizations recognize it. *Proceedings of the First International Conference on Intelligent Computer in Data Sciences*, 122, 494-501. doi: 10.1016/j.procs.2017.11.398
- Anderson, V. D. (2016, March 29). FBI warns of rise in schemes targeting businesses and online fraud of financial officers and individuals. *FBI Cleveland News*. Retrieved from <https://www.fbi.gov/contact-us/field-offices/cleveland/news/press-releases/fbi-warns-of-rise-in-schemes-targeting-businesses-and-online-fraud-of-financial-officers-and-individuals>
- APWG. (2016), *Phishing activity trending report*. Retrieved from: http://docs.apwg.org/reports/apwg_trends_report_q2_2016.pdf

- Arora, B. (2016). Exploring and analyzing Internet crimes and their behaviors. *Journal of Perspectives in Science*, 8, 540-542. doi: 10.1016/j.pisc.2016.06.014
- Ben-Asher, N & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *International Journal of Critical Infrastructure Protection*, 48, 51-61. doi: 10.1016/j.chb.2015.01.039
- Bendovschi, A. (2015). Cyber-attacks – Trends, patterns and security countermeasures. *Procedia Economics and Finance*, 28, 24-31.
- Bhakta, R. & Harris, I. G. (2015). Semantic analysis of dialogs to detect social engineering attacks. *Institute of Electrical and Electronic Engineers International Conference on Semantic Computing*, 424-427. doi: 10.1109/HICSS.2015.422
- Bhatnagar, N., Madden, H., & Levy, Y. (2017). Initial empirical testing of potential factors contributing to patient use of secure medical teleconferencing. *Journal of Computer Information Systems*, 57(1), 89-95. doi: 10.1080/08874417.2016.1181504
- Billion-dollar scams: The numbers behind business email compromise. (2016, June 9). *Trend Micro Security News*. Retrieved from: <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/billion-dollar-scams-the-numbers-behind-business-email-compromise>
- Brown, S. D., Levy, Y., Ramim, M., & Parrish, J.L. (2015). Pharmaceutical companies' documented and online privacy practices: Development of an index measure and initial test. *Online Journal of Applied Knowledge Management*, 3(2), 68-88.
- Buchanan, E.M., Scofield, J.E. (2018). Methods to detect low quality data and its implication for psychological research. *Journal of Behavior Research Methods*, 50(1), 1-11. doi: 10.3758/s13428-018-1035-6
- Bulling, A. (2016). Pervasive attentive user interface. *Institute of Electrical and Electronic Engineers Computer Journal*, 49(1), 94-98. doi: 10.1109/MC.2016.32
- Campen, A. D. (2009). Take me to your cyber leader. *Armed Forces Communication and Electronics Association Signal Magazine*, 64(3), 60-62.
- Carlton, M., & Levy, Y. (2015). Expert assessment of top platform independent cybersecurity skills for non-IT professionals. *Proceedings of the Institute of Electrical and Electronic Engineers Southeast Conference* (pp. 1-6). doi: 10.1109/SECON.2015.7132932
- Cialdini, R. B. (2009). *Influence: The psychology of persuasion*. Retrieved from: <https://books.google.com/books?id=5dfv0HJ1TEoC>

- Choejey, P., Fung, C. C., Wong, K. W., Murray, D., & Sonam, D. (2015). Cybersecurity challenges for Bhutan. *Institute of Electrical and Electronic Engineers International Conference on Electrical Engineering/Electronics, Computer, Telecommunications, and Information Technology* (pp. 1-5). doi: 10.1109/ECTICon.2015.7206975
- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches*. Los Angeles, CA. Sage Publications, Inc.
- Creswell, J. W. & Creswell J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches*. Los Angeles, CA. Sage Publications, Inc.
- Cyberedge Group. (2015). *2015 Cyberthreat defense report: North America & Europe*. Retrieved from: https://www.bluecoat.com/sites/default/files/documents/files/CyberEdge_2015_CDR_Report.pdf
- Cyberedge Group. (2016). *2016 Cyberthreat Defense Report: North America, Europe, Asia Pacific, & Latin America*. Retrieved from: http://images.machspeed.bluecoat.com/Web/BlueCoat/%7B43e0b80d-8e85-45a3-bcfd-19f9ca0b0577%7D_CyberEdge_2016_CDR_Report.pdf
- David, K., Bieling, G., Bohnstedt, S. J., Ohly, S., Robnagel, A., Schmitt, A., Steinmerz, R., Stock-Homburg, R., & Wacker, A. (2014). Balancing the online life: Mobile usage scenarios and strategies for a new communication paradigm. *Institute of Electrical and Electronic Engineers Computer Vehicular Technology Magazine*, 9(3), 72-79. doi: 10.1109/MVT.2014.2333763
- Derouet, E. (2016). Fighting phishing and securing data with email authentication. *Journal of Computer Fraud & Security*, 10, 5-8. doi: 10.1016/S1361-3723(16)30079-3
- Deshmukh, P., Shelar, M., & Kulkarni, N. (2014). Detecting of targeted malicious email. *Institute of Electrical and Electronic Engineers Global Conference on Wireless Computing and Networking*, 199-202. doi: 10.1109/GCWCN.2014.7030878
- Dupuis, M. J., Crossler, R. E., & Endicott-Popovsky, B. (2016). Measuring the human factor in information security and privacy. *Institute of Electrical and Electronic Engineers Hawaii International Conference on System Sciences*, 3676-3685. doi: 10.1109/HICSS.2016.459
- Eddy, M. (2013, April 3). Five signs your Android device is infected with Malware. *PC Magazine*. Retrieved from <https://securitywatch.pcmag.com/mobile-security/309980-five-signs-your-android-device-is-infected-with-malware>

- Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology*, 6, 323-337.
- Ernst and Young. (2015), *Creating trust in the digital world: EY's global information security survey*. Retrieved from: [http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/\\$FILE/ey-global-information-security-survey-2015.pdf](http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf)
- Federal Bureau of Investigations. (2015). *Business e-mail compromise*. Retrieved from: <https://www.fbi.gov/news/stories/2015/august/business-e-mail-compromise/business-e-mail-compromise>
- Federal Bureau of Investigations. (2017, February 27). *Business e-mail: Cyber-enabled financial fraud on the rise globally*. Retrieved from <https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise>
- Federal Bureau of Investigations Internet Crime Complaint Center. (2015). *Business e-mail compromise public service announcement*. Retrieved from: <https://www.ic3.gov/media/2015/150827-1.aspx>
- Federal Bureau of Investigations Internet Crime Complaint Center. (2016). *Business e-mail compromise: The 3.1 billion dollar scam*. Retrieved from: <https://www.ic3.gov/media/2016/160614.aspx>
- Federal Bureau of Investigations Internet Crime Complaint Center. (2017). *Business e-mail compromise: E-mail account compromise the 5 billion dollar scam*. Retrieved from: <https://www.ic3.gov/media/2017/170504.aspx>
- Federal Bureau of Investigations Internet Crime Complaint Center. (2019). *Business Email Compromise The \$26 Billion Scam*. Retrieved from: <https://www.ic3.gov/media/2019/190910.aspx>
- Ferreira, A., & Lenzini, G. (2015). An analysis of social engineering principles in effective phishing. *Institute of Electrical and Electronic Engineers International Workshop on Socio-Technical Aspects in Security and Trust*, 9-16. doi: 10.1109/STAST.2015.10
- Field, A. (2018). *Discovering statistics using IBM SPSS statistics*. Thousand Oaks, CA. Sage Publications, Inc.
- Fireeye. (2016), *Spear-phishing attacks: Why they are successful and how to stop them*. Retrieved from: <https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/wp-fireeye-how-stop-spearphishing.pdf>

- Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture awareness. *Journal of Computers and Security*, 59, 26-44. doi: 10.1016/j.cose.2016.01.004
- Frauenstein, E. D., & Flowerday, S. V. (2016). Social network phishing: Becoming habituated to clicks and ignorant threats?. *Institute of Electrical and Electronic Engineers International Journal of Information Security for South Africa*, 98-105. doi: 10.1109/ISSA.2016.7802935
- Furnell, S., Millet, K., & Papadaki, M. (2019). Fifteen years of phishing: Can technology save us? *Journal of Computer Fraud and Security*, 7, 11-16. doi: [https://doi.org/10.1016/S1361-3723\(19\)30074-0](https://doi.org/10.1016/S1361-3723(19)30074-0)
- Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems*, 18(1), 22-44.
- Goswami, S. (2019, January 11). BEC scam leads to theft of \$18.6 million. *Information Security Media Group*. Retrieved from <https://www.bankinfosecurity.com/bec-scam-leads-to-theft-186-million-fraud-a-11930>
- Gowthami, S., & VenkataKrishnaKumar, S. (2016). Impact of smartphone: A pilot study on positive and negative effects. *International Journal of Scientific Engineering and Applied Science*, 2(3), 473-478.
- Greitzer, F. L., Strozer, S. C., Moore, A. P., Mundie, D., & Cowley, J. (2014). Analysis of unintentional insider threats deriving from social engineering exploits. *Institute of Electrical and Electronic Engineers Conference on Security and Privacy*, 236-250. doi: 10.1109/SPW.2014.39
- Guardian Analytics (2015, December 8). *BEC best practices video*. Retrieved from <https://www.youtube.com/watch?v=LfGaDd7-dlk>
- Guardian Analytics. (2016), *Guardian Analytics Fraud Update: Business Email Compromise (BEC)*. Retrieved from: http://info.guardiananalytics.com/rs/850-VFT-328/images/FraudUpdate_BusinessEmailCompromiseScam.pdf
- Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2016). Fighting against phishing attacks: state of the art and future challenges. *Journal of Neural Computing and Applications*, 1-26. doi: 10.1007/s00521-016-2275-y
- Hair, J.F, Sarstedt, M., Hopkins, L., & Kuppelwieser, V.G. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *European Business Review*, 26(2), 106-121. doi: 10.1108/EBR-10-2013-0128

- Harrison, B., Vishwanath, A., & Rao, R. (2016). User-centered approach to phishing susceptibility: The role of a suspicious personality in protecting against phishing. *Institute of Electrical and Electronic Engineers International Workshop on System Sciences*, 5628-5634. doi: 10.1109/HICSS.2016.696
- Hemphill, T. A., & Longstreet, P. (2016). Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards. *Journal of Technology and Society*, 44, 30-38. doi: 10.1016/j.techsoc.2015.11.007
- Hinchliffe, A. (2017). Nigerian princes to kings of malware: the next evolution in Nigerian cybercrime. *Journal of Computer Fraud & Security*, 5, 5-9. doi: doi.org/10.1016/S1361-3723(17)30040-4
- Hughes, B. B., Bohl, D., Ifran, M., Margolese-Malin, E., & Solorzano, J. R. (2016). ICT/Cyber benefits and costs: Reconciling competing perspectives on the current and future balance. *Journal of Technological Forecasting and Social Change*, 1-14. doi: 10.1016/j.techfore.2016.09.027
- Intel Security. (2014), *Net Losses: Estimating the Global Cost of Cybercrime: Economic Impact of Cybercrime II*. Retrieved from: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf
- Jakobsson, M. (2019). The rising threat of launchpad attacks. *Institute of Electrical and Electronic Engineers Security & Privacy Journal*, 17(5), 68-72. doi: 10.1109/MSEC.2019.2922865
- Jakobsson, M., & Leddy, W. (2016). Could you fall for a scam? Spam filters are passe. What we need is software that unmasks fraudsters. *Institute of Electrical and Electronic Engineers Spectrum Magazine*, 53(5), 40-55. doi: 10.1109/MSPEC.2016.7459118
- Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973-993. doi: 10.1016/j.jcss.2014.02.005
- Joint Task Force on Cybersecurity Education. (2017). *Cybersecurity curricula 2017: Curriculum guidelines for post-secondary degree programs in cybersecurity*. Retrieved from: https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf
- Jorm, C. M., & O'Sullivan, G. (2012). Laptops and smartphones in the operating theatre - how does our knowledge of vigilance, multi-tasking and anaesthetist performance

help us in our approach to this new distraction? *Journal of Anaesthesia and Intensive Care*, 40(1), 71-78.

Karjalainen, M., & Siponen, M. (2011). a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, 12(8), 518-555.

Kaspersky Lab. (2016), *Spam and Phishing in Q3 2016*. Retrieved from:
https://securelist.com/files/2016/11/Spam-report_Q3-2016_final_ENG.pdf

Kermanshachi, S., Dao, B., Shane, J., & Anderson, S. (2016). Project complexity indicators and management strategies- A Delphi study. *Procedia Engineering*, 145, 587-594. doi: 10.1016/j.proeng.2016.04.048

Kissel, R. (2013). *Glossary of key information security terms* (NIST IR 7298r2). Retrieved from National Institute of Standards and Technology Website:
<http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>

Konradt, C., Schilling, A., & Werners, B. (2016). Phishing: An economic analysis of cybercrime perpetrators. *Journal of Computers and Security*, 58, 39-46. doi: 10.1016/j.cose.2015.12.001

Kotson, K. C. (2015). Characterizing phishing threats with natural language processing. *Institute of Electrical and Electronic Engineers Conference on Communications and Network Security*, 308-316. doi: 10.1109/CNS.2015.7346841

Kunwar, S. M., & Sharma, P. (2016). Social media: A new vector for cyber attack. *Institute of Electrical and Electronic Engineers International Conference on Advances in Computing, Communication, & Automation*, 1-5. doi: 10.1109/ICACCA.2016.7578896

Laszka, A., Lou, J., & Vorobeychik, Y. (2016). Multi-defender strategy filtering against spear-phishing attacks. *Association for the Advancement of Artificial Intelligence Conference on Artificial Intelligence*, 1-8.

Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science Journal*, 9(1), 181-212.

Levy, Y., & Ellis, T. J. (2011). A guide for novice researchers on experimental and quasi-experimental studies in information systems research. *Interdisciplinary Journal of Information, Knowledge, and Management*, 6, 151-161.

Lin, C. H., Tien, C. W., Chen, C. W., Tien, C. W., & Pao, H. K. (2015). Efficient spear-phishing threat detection using hypervisor monitor. *Institute of Electrical and*

Electronic Engineers International Conference on Security Technology, 299-303.
doi: 10.1109/CCST.2015.7389700

Lindsay, N. (2019, September 20). Toyota subsidiary loses \$37 million due to BEC scam. *CPO Magazine*. Retrieved from <https://www.cpomagazine.com/cyber-security/toyota-subsi-dary-loses-37-million-due-to-bec-scam/>

Lord, J. (2016). Fifty shades of fraud. *Journal of Computer Fraud & Security*, 6, 14-16.
doi: 10.1016/S1361-3723(15)30047-6

Losses from business email compromise scams top \$3.1 billion: FBI. (2016). *Security Week News*. Retrieved from <http://www.securityweek.com/losses-business-email-compromise-scams-top-31-billion-fbi>

Loten, A. (2016, June 16). FBI says corporate email ‘impersonation’ scams growing. *Wall Street Journal*. Retrieved from <http://blogs.wsj.com/cio/2016/06/16/fbi-says-corporate-email-impersonation-scams-growing/>

Maasberg, M., Warren, J., & Beebe, N. L. (2015). The dark side of the insider: Detecting the insider threat through examination of dark triad personality traits. *Institute of Electrical and Electronic Engineers Hawaii International Conference on System Sciences*, 3518-3526. doi: 10.1109/HICSS.2015.423

Mani, T. M., Bedwell, J. S., & Miller, L. S. (2004). Age-related decrements in performance on a brief continuous performance test. *Archives of Clinical Neuropsychology*, 20(5), 575-586. doi: doi:10.1016/j.acn.2004.12.008

Mansfield-Devine, S. (2016). The imitation game: How business email compromise scams are robbing organizations. *Journal of Computer Fraud & Security*, 11, 5-10. doi: 10.1016/S1361-3723(16)30089-6

McAfee Labs. (2016), *Threats Report*. Retrieved from:
<http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-sep-2016.pdf>

Meinert, M. C. (2016). Social engineering: The art of human hacking. *American Bankers Association Banking Journal*, 108(3), 49.

Microsoft Canada. (2015), *Attention span*. Retrieved from:
<https://advertising.microsoft.com/en/WWDocs/User/display/cl/researchreport/31966/en/microsoft-attention-spans-research-report.pdf>

Murphy, M. (2015, August 7). CFO-less Ubiquiti tricked into wiring hackers large sums of money. *Wall Street Journal*. Retrieved from
<http://blogs.wsj.com/cfo/2015/08/07/cfo-less-ubiquiti-tricked-into-wiring-hackers-large-sums/>

- Musoba, G. D., Jacob, S. A., & Robinson, L. J. (2014). The institutional review board (IRB) and faculty: Does the IRB challenge faculty professionalism in the social sciences? *The Qualitative Report*, 19(51), 1-14.
- Nandi, A. K., Medal, H. R., & Vadlamani, S. (2016). Interdicting attack graphs to predict organizations from cyberattacks: A bi-level defender-attacker model. *Journal of Computers & Operations Research*, 24-31. doi: 10.1016/j.cor.2016.05.005
- Neupane, A., Saxena, N., Maximo, J. O., & Kana, R. (2016). Neural markers of cybersecurity: An fMR study of phishing and malware warnings. *Institute of Electrical and Electronic Engineers Journal of Transactions on Information Forensics and Security*, 11(9), 1970-1983. doi: 10.1109/TIFS.2016.2566265
- Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: an example, design, considerations and applications. *Journal of Information and Management*, 42(1), 15-29. doi: 10.1016/j.im.2003.11.002
- Osuagwu, E. U., & Chukwudebe, G. A. (2015). Mitigating social engineering for improved cybersecurity. *Institute of Electrical and Electronic Engineers International Conference on Cyberspace Governance*, 91-100. doi: 10.1109/CYBER-Abuja.2015.7360515
- Phishlabs. (2016). 2016 *Phishing trends & intelligence report: Hacking the human* . Retrieved from [https://pages.phishlabs.com/rs/130-BFB-942/images/PhishLabs 2016 Phishing Trends and Intelligence Report Hacking the Human.pdf](https://pages.phishlabs.com/rs/130-BFB-942/images/PhishLabs%202016%20Phishing%20Trends%20and%20Intelligence%20Report%20Hacking%20the%20Human.pdf)
- PricewaterhouseCoopers (PwC). (2016). *Global economic crime survey*. Retrieved from <http://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf>
- Psychology Today. (n.d.). *Attention span test*. Retrieved from: <https://www.psychologytoday.com/tests/personality/attention-span-test>
- Ramim, M. M., & Lichvar, B. T. (2014). Elicit expert panel perspective on effective collaboration in system development projects. *Online Journal of Applied Knowledge Management*, 2(1), 122-136.
- Renaud, K., & Weir, G. R. S. (2016). Cybersecurity and the unbearability of uncertainty. *Institute of Electrical and Electronic Engineers Conference on Cybersecurity and Cyberforensics*, 137-143. doi: 10.1109/CCC.2016.29
- Roumani, M. A., Fung, C. C., & Choeje, P. (2015). Assessing economic impact due to cyber attacks with system dynamics. *Institute of Electrical and Electronic*

Engineers International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, 1-6. doi: 10.1109/ECTICon.2015.7207084

- Safa, N. S., Sookhak, M., Solms, E.V., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behavior in organizations. *Journal of Computers and Security*, 53, 65-78. doi: 10.1016/j.cose.2015.05.012
- Secureworks. (2017), *2017 State of cybercrime report: Exposing the threats, techniques, and markets that fuel the economy of cybercriminals*. Retrieved from: <https://www.secureworks.com/~media/Files/US/Reports/SecureworksSECO1150N2017StateofCybercrimeReport.ashx>
- Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *International Association for Computer Machinery Conference on Human Factors in Computer Systems*, 373-382. doi: 10.1145/1753326.1753383
- Sethi, A., & Willis, G. (2017). Expert-interviews led analysis of EEVi – A model for effective visualization in cyber-security. *Institute of Electrical and Electronic Engineers Symposium on Visualization for Cyber Security*, 1-8.
- Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Journal of Computers and Security*, 49, 177-191. doi: 10.1016/j.cose.2015.01.002
- Simon, R. (2015, July 29). Hackers trick email systems into wiring them large sums. *Wall Street Journal*. Retrieved from <http://www.wsj.com/articles/hackers-trick-email-systems-into-wiring-them-large-sums-1438209816?mg=id-wsj>
- Solutionary. (2016), *Security engineering research team: Quarterly threat intelligent report Q2*. Retrieved from: https://www.solutionary.com/_assets/pdf/research/sert-q2-2016-threat-report.pdf
- Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill-building approach* (7th Ed.). West Sussex, United Kingdom: John Wiley & Sons Ltd.
- Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Journal of Decision Support Systems*, 75, 49-62. doi: 10.1016/j.dss.2015.04.011
- Steinberg, J. (2016, October 31). *Mobile malware: How to detect it*. Retrieved from <https://www.youtube.com/watch?v=i3fTFBv9UDE>

- Steinberg, J. (2016, November 1). 14 signs your smartphone or tablet has been hacked. *Inc Magazine*. Retrieved from <https://www.inc.com/joseph-steinberg/14-signs-your-smartphone-or-tablet-has-been-hacked.html>
- Stembert, N., Padmos, A., Bargh, M. S., Choenni, S., & Jansen, F. (2015). A study preventing email (spear) phishing by enabling human intelligence. *Institute of Electrical and Electronic Engineers International Conference on Intelligence and Security Informatics*, 113-120. doi: 10.1109/EISIC.2015.38
- Sun, J. C., Yu, S., Lin, S. S. J., & Tseng, S. (2016). The mediating effect of anti-phishing self-efficacy between college students' Internet self-efficacy and anti-phishing behavior and gender difference. *Journal of Computers in Human Behavior*, 59, 249-257. doi: 10.1016/j.chb.2016.02.004
- Symantec. (2016), *Internet security threat report*. Retrieved from: <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>
- Symantec. (2017), *Worried about business email compromise? Lacking visibility into advanced attacks? Look no further*. Retrieved from: <https://www.symantec.com/connect/blogs/worried-about-business-email-compromise-lacking-visibility-advanced-attacks>
- Tamrakar, A., Russell, J. D., Ahmed, I., Richard, G. G., & Weems, C. F. (2016). SPICE: A software tool for bridging the gap between end-user's insecure cyber behavior and personality traits. *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy*, 124-126. doi: 10.1145/2857705.2857744
- Thakur, K., Qui, M., Gai, K., & Ali, M. L. (2015). An investigation on cyber security threats and security models. *Institute of Electrical and Electronic Engineers International Conference on Cyber Security and Cloud Computing*, 307-311. doi: 10.1109/CSCloud.2015.71
- Trend Micro. (n.d.), *Business Email Compromise (BEC)*. Retrieved from: [https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-\(bec\)](https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec))
- Trend Micro. (2017), *2017 Midyear security roundup: The cost of compromise*. Retrieved from: <https://documents.trendmicro.com/assets/rpt/rpt-2017-Midyear-Security-Roundup-The-Cost-of-Compromise.pdf>
- Trend Micro. (2017), *Security 101: Business email compromise schemes*. Retrieved from: <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/business-email-compromise-bec-schemes>

- Trend Micro. (2018), *Year-end review: Business email compromise in 2018*. Retrieved from: <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/year-end-review-business-email-compromise-in-2018>
- Trustwave. (2016), *Trustwave global security report*. Retrieved from: <https://www2.trustwave.com/rs/815-RFM-693/images/2016%20Trustwave%20Global%20Security%20Report.pdf>
- Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Journal of Computers and Security*, 52, 128-141. doi: 10.1016/j.cose.2015.04.006
- Tung, L. (2016, May 26). CEO fired after 'fake CEO' email scam cost firm \$47m. *CSO Online*. Retrieved from <http://www.cso.com.au/article/600535/ceo-fired-after-fake-ceo-email-scam-cost-firm-47m>
- Tuttle, H. (2017). The 2017 cyberrisk landscape. *Journal of Risk Management*, 64(1), 4-7.
- Uebelacker, S., & Quiel, S. (2014). The social engineering personality framework. *Institute of Electrical and Electronic Engineers Workshop on Socio-Technical Aspects in Security and Trust*, 24-30. doi: 10.1109/STAST.2014.12
- Vahdati, S., & Yasini, N. (2015). Factors affecting Internet frauds in private sector: A case study in cyberspace surveillance and scam monitoring agency of Iran. *Journal of Computers in Human Behavior*, 51, 180-187. doi: 10.1016/j.chb.2015.04.058
- Verizon. (2016), *Data breach investigations report*. Retrieved from: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf
- Verizon. (2017), *Data breach investigations report*. Retrieved from: http://www.verizonenterprise.com/resources/reports/2017_dbir_en_xg.pdf
- Wilcox, H., & Bhattacharya, M. (2016). A framework to mitigate social engineering through social media within the enterprise. *Institute of Electrical and Electronic Engineers Conference on Industrial Electronics and Applications*, 1039-1044. doi: 10.1109/ICIEA.2016.7603735
- Wilkerson, S., Levy, Y., Kiper, J.R., Snyder, M. (2017). Toward a development of a social engineering exposure index (SEXI) using publicly available personal information. *2017 Kennesaw State University Conference on Cybersecurity Education, Research and Practice*, 1-9.

- Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Journal of Computers in Human Behavior*, 72, 412-421. doi: 10.1016/j.chb.2017.03.002
- Wilmer, H. H., Sherman, L. E., & Chein, J. M. (2017). Smartphones and cognition: A review of research exploring the links between mobile technology habits and cognitive functioning. *Frontiers in psychology*, 8, 605. doi: doi.org/10.3389/fpsyg.2017.00605
- Zweighaft, D. (2017). Business email compromise and executive impersonations: are financial institutions exposed? *Journal of Investment Compliance*, 18(1), 1-7. doi: 10.1108/JOIC-02-2017-0001