

2020

Development of Criteria for Mobile Device Cybersecurity Threat Classification and Communication Standards (CTC&CS)

Emmanuel Jigo

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.

Development of Criteria for Mobile Device Cybersecurity Threat
Classification and Communication Standards (CTC&CS)

by


Emmanuel Jigo

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

2020

We hereby certify that this dissertation, submitted by Emmanuel Jigo 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

Nov 10, 2020

Date



Steve Furnell, Ph.D.
Dissertation Committee Member

Nov 10, 2020

Date




Laurie P. Dringus, Ph.D.
Dissertation Committee Member

Nov 10, 2020

Date

Approved:



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

Nov 10, 2020

Date

College of Computing and Engineering
Nova Southeastern University

2020

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

Development of Criteria for Mobile Device Cybersecurity Threat
Classification and Communication Standards (CTC&CS)

By
Emmanuel Jigo
November 2020

The increasing use of mobile devices and the unfettered access to cyberspace has introduced new threats to users. Mobile device users are continually being targeted for cybersecurity threats via vectors such as public information sharing on social media, user surveillance (geolocation, camera, etc.), phishing, malware, spyware, trojans, and keyloggers. Users are often uninformed about the cybersecurity threats posed by mobile devices. Users are held responsible for the security of their device that includes taking precautions against cybersecurity threats. In recent years, financial institutions are passing the costs associated with fraud to the users because of the lack of security.

The purpose of this study was to design, develop, and empirically test new criteria for a Cybersecurity Threats Classification and Communication Standard (CTC&CS) for mobile devices. The conceptual foundation is based on the philosophy behind the United States Occupational Safety and Health Administration (OSHA)'s Hazard Communication Standard (HCS) of Labels and Pictograms that is mainly focused on chemical substances. This study extended the HCS framework as a model to support new criteria for cybersecurity classification and communication standards.

This study involved three phases. The first phase conducted two rounds of the Delphi technique and collected quantitative data from 26 Subject Matter Experts (SMEs) in round one and 22 SMEs in round two through an anonymous online survey. Results of Phase 1 emerged with six threats categories and 62 cybersecurity threats. Phase 2 operationalized the elicited and validated criteria into pictograms, labels, and safety data sheets. Using the results of phase one as a foundation, two to three pictograms, labels, and safety data sheets (SDSs) from each of the categories identified in phase one were developed, and quantitative data were collected in two rounds of the Delphi technique from 24 and 19 SMEs respectively through an online survey and analyzed. Phase 3, the main data collection phase, empirically evaluated the developed and validated pictograms, labels, and safety data sheets for their perceived effectiveness as well as performed an analysis of covariance (ANCOVA) with 208 non-IT professional mobile device users.

The results of this study showed that pictograms were highly effective; this means the participants were satisfied with the characteristics of the pictograms such as color,

shapes, visual complexity, and found these characteristics valuable. On the other hand, labels and Safety Data Sheets (SDS) did not show to be effective, meaning the participants were not satisfied or lacked to identify importance with the characteristics of labels and SDS. Furthermore, the ANCOVA results showed significant differences in perceived effectiveness with SDSs with education and a marginal significance level with labels when controlled for the number of years of mobile device use. Based on the results, future research implications can observe discrepancies of pictogram effectiveness between different educational levels and reading levels. Also, research should focus on identifying the most effective designs for pictograms within the cybersecurity context. Finally, longitudinal studies should be performed to understand the aspects that affect the effectiveness of pictograms.

Acknowledgments

Pursuing a Ph.D. has demanded an incredible amount of time, concentration, and motivation. These past five years have been a challenge of perseverance with missed time and events with those close to me. On many occasions, the idea of completing this dissertation seemed bleak. Nevertheless, those close to me offered inspiration and encouragement. Words cannot express my gratitude for their support, and I wish I could acknowledge everyone that positively influenced my life towards achieving this goal. Although I would like to recognize those, I am incredibly grateful and to whom this is work is dedicated.

To my wife Joykrystyna Alyse Mance, my most tremendous appreciation belongs to you. I cannot thank you enough for the sacrifices you made while I was focused on my studies. Above all, thank you for your support and love.

To my parents Oti and Bregidita Jigo, you both have been great examples of self-determination and strong work ethics and have taught me to face difficulties and challenges with confidence and courage. Thank you both for your unwavering love and confidence in me. I know completing the Ph.D. will make you both proud.

To my dissertation committee members, Dr. Steven Furnell and Dr. Laurie Dringus, thank you very much for the reviews of this dissertation. Your feedback and guidance were instrumental in the progress and immeasurability of the quality of this work. Also, thank you, Dr. Ling Wang, for your course and assistance during the IRB process.

To my dissertation chair Dr. Yair Levy, I was fortunate to have the opportunity to work with you both in my master's and doctoral level classes, as well as within the dissertation process. Accomplishing this would not be possible without your guidance, wisdom, and rigor. I also appreciate your patience during the tough times. It has been a great honor to work with you. I will be forever grateful for the leadership and counsel you provided throughout this dissertation process.

Table of Contents

Abstract	ii
Acknowledgment	iv
List of Tables	v
List of Figures	vi

Chapters

1. Introduction	1
Background	1
Problem Statement	3
Dissertation Goal	5
Research Questions	10
Relevance and Significance	11
Relevance	11
Significance	12
Barriers and Issues	14
Assumptions, Limitations, and Delimitations	15
Definition of Terms	15
Summary	17
2. Review of Literature	1919
Introduction	19
Threat classification	19
Attack Techniques	19
Threat Impacts	21
Hazard communication	30
Safety Data Sheets	32
Labels	33
Pictograms	33
IS Effectiveness	53
Summary of what is Known and Unknown	57
3. Methodology	60
Overview of Research Design	60
Instrument Development	62
Expert Panel	62
CTC&CS development	65
User-perceived effectiveness of CTC&CS	71
Reliability and Validity	72
Reliability	72

Validity	73
Population and Sample	75
Data Collection	75
Data Analysis	76
Resources	77
Summary	77
4. Results	77
Overview	77
Expert Panel – Phase One (RQ1, RQ2, & RQ3)	78
Pre-analyses data screening	79
Demographics	79
Data Analysis	80
Expert Panel – Phase Two (RQ4 & RQ5)	81
Pre-analyses data screening	83
Demographics	84
Data Analysis	85
Main Data Collection – Phase Three (RQ6 & RQ)	84
Pre-analyses data screening	86
Demographics	87
Data Analysis	93
5. Conclusions, Implications, Recommendations, and Summary	96
Conclusions	96
Discussions	97
Implications	98
Recommendations and Future Research	99
Summary	100
Appendices	
A. Sample Safety Data Sheet	107
B. Expert Panel Instrument – Phase 1 draft	115
C. Expert Panel Instrument – Phase 2 draft	134
D. Study Participants’ Recruitment Announcement	139
E. Initial Draft Study Participants’ Survey Instrument	140
F. IRB Approval Letter	147
G. SME Identified Categories and Threats	139
H. SUS Raw scores	143
I. SUS Inflated Scores and Adjective rating	149
References	155

List of Tables

Tables

1. Summary of classifications based on attack techniques 24
2. Summary of classifications based on impact 30
3. Summary of safety data sheet studies 33
4. Summary of labels studies 35
5. Summary of studies on interactions with safety data sheets (SDS) and labels 38
6. Summary of studies on pictogram characteristics 43
7. Summary of studies on pictogram development 52
8. Summary of studies on Effectiveness 55
9. Cybersecurity Threat Categories 63
10. Proposed mobile cybersecurity threats for CTC&CS 64
11. Summary of Phase One Demographics(N=48) 79
12. Summary of Threat categories 81
13. Summary of Phase Two Demographics (N = 43) 83
14. Summary of Phase Three Demographics (N= 208) 86
15. Summary of SUS scores 90
16. ANCOVA Summary Table – Pictograms 92
17. ANCOVA Summary Table – Labels 92
18. ANCOVA Summary Table – SDS 93

List of Figures

Figures

1. Overview of the Research Design Process 61
2. Sample label 69
3. Effectiveness Formula 88
4. Final list of pictograms 90
5. Satisfaction means 90
6. Value means 91
7. Effectiveness means 91
8. Number of respondents for each corresponding SUS adjective 99

Chapter 1

Introduction

Background

Mobile device usage has presented opportunities to all groups of individuals and businesses. Almost all communication and processes can be carried out through a mobile device facilitating an individuals' daily life (McFarland & Ployhart, 2015). The number of mobile-cellular subscriptions worldwide has increased ten times, from 738 million to over seven billion (International Telecommunication Union, 2017a). Cellular mobile connections surpass the world's population, and smartphone penetration in developed nations amounts to over 50% globally (International Telecommunication Union, 2017b). The highest use of mobile devices in the private sector includes commercial training providers at 90%, manufacturing, science, and engineering at 79%, professional and technical services at 72%, as well as finance and insurance at 69% (Fahlman, 2017). There are little differences in the uptake of mobile devices among those working in the not-for-profit (74%), public (73%), and private (69%) sectors. Analyst forecast 5.6 billion smartphones by 2020 and 90% of growth will come from low to middle-income countries (GSM Association, 2018).

Mobile threats are everywhere. In 2017, Apple and Google released a record number of security patches (Mitre Corporation, 2017). Zimperium Global threat intelligence found two out of three mobile devices are running vulnerable operating systems, while an

additional 10% of devices have experienced man-in-the-middle attacks (Zimperium mobile threat defense, 2017). The mobile malware, copycat, infected more than 14 million devices by taking advantage of out-dated devices. The attackers made \$1.5 million in fake ad revenues in under two months. ExpensiveWall, a new variant of Android malware, registered mobile device users for paid services without their permission and was discovered in the Google Play Store. Over 300 apps in the Google Play Store contained malware and were downloaded by over 106 million users. Moreover, it is predicted that by 2019, mobile malware will amount to one-third of total malware (Zumerle & Girard, 2017).

The increasing scale of mobile devices brings along a variety of threats. Cisco's 2018 annual cybersecurity report identified mobile devices as the most challenging area to defend. Different security threats can affect mobile devices. Some threats target the physical device at the hardware or Operating System (OS) level, while others use mobile apps to gain a footing on the device and from the organizational network. Other areas under threat are WiFi, cellular, and Bluetooth. Additionally, how a device is deployed or how the device is used creates its own set of challenges. There is a growing danger from fraudulent websites and emails that prey on users to access sensitive organizational resources (Jones & Towse, 2018).

Mobile devices are rife with security vulnerabilities that can put users and organizations at risk (Watson & Zheng, 2017). Notably, users face the risk of data loss, degraded functionality, financial losses, and the invasion of privacy. These risks are apparent when criminals or malicious agents exploit vulnerabilities in the operating system of third-party applications. Data on the device can be stolen, tampered, held for ransom, or outright deleted (Yalew, Maguire, Haridi, & Correia, 2017), which is

especially harmful to the user since mobile devices are used to store personal information, access banking, medical, and shopping services. User credentials stored on the mobile device can be stolen then used to access additional accounts and services. If the device is used for organizational purposes, the stolen credentials can lead to financial hardships for both the user and the organization. Mobile device security is a growing concern given the large number of users who use their own devices for work purposes (Harris, Furnell, & Patten, 2014; Hasan, Rajski, Gómez, & Kurzhöfer, 2016; Penning, Hoffman, Nikolai, & Wang, 2014; Vecchiato, Vieira, & Martins, 2016).

The goal of this study was to develop a classification system for cybersecurity threats and communication guidelines for mobile device users. The projected outcome was to advance the security practices of mobile device users, specifically, to assist users in recognizing and avoiding potential cybersecurity threats and exploits of mobile device use.

Problem Statement

The problem that this research addressed is that cybersecurity threat classifications and communication standards criteria are lacking for mobile device users, while mobile device compromises are on the rise (Hovav & Gray, 2014; Peha, 2013). The remote access and popularity of mobile devices coupled with valuable and private information that devices hold make users and their devices vulnerable to new threats to cybersecurity (Bertino, 2016; Bitton et al., 2018; Patten & Harris, 2013). The increasing use of mobile devices has brought about the need for assistance in protecting user privacy due to the high degree of user malleability (Acquisti, Brandimarte, & Loewenstein, 2015). Researchers have been searching for preventative measures to help overcome the

insufficient knowledge of cybersecurity threats by users and the lack of awareness of potential threat consequences (Abraham & Chengalur-Smith, 2010; Kritzinger & von Solms, 2010; 2013).

The forms of cybersecurity threats to mobile devices are increasing, such as public information sharing on social media, user surveillance (e.g., geolocation, camera, etc.), phishing, malware, spyware, trojans, as well as keyloggers (Rocha Flores, Holm, Svensson, & Ericsson, 2014). For example, McAfee (2018) saw an increase in malicious banking. Attackers would take advantage of auto-install vulnerabilities in the Android platform that victimized millions of Google Play users. The attack was done through the impersonation of a legitimate app (e.g., video players, flash players, games, & system utilities). Cybersecurity threats to the mobile device also target large and small banks using specially crafted mobile apps or phishing campaigns. For instance, android malware MoqHao targeted major Korean banks. The threat spread through Short Message Service (SMS) using social engineering lures that asks the recipient to verify a picture of themselves (McAfee, 2018). Once verified, a fake banking app is installed and then scans for and deletes legitimate banking apps on a user's mobile device (McAfee, 2018). With the increasing interest in cryptocurrencies and exponential growth in cryptocurrency prices, attacks have targeted mobile wallets of workers in the cryptocurrency industry (McAfee, 2018; Rauchs & Hileman, 2017). The year 2017 saw an 80% increase in malware related to bitcoin mining (McAfee, 2018).

Issues surrounding the end-user as threats to cybersecurity are continually growing following the growing volume of personal information over the Internet (Jang-Jaccard & Nepal, 2014). End-users increasingly find themselves having to make security decisions,

such as the configuration of security-related settings, responding to security-related events and messages, or enforce specific policy and access rights (Jang-Jaccard & Nepal, 2014). An IBM report found that over 95% of security incidents investigated recognized human error as a contributing factor (IBM global technology services, 2014). The state-sponsored attacks on Equifax and the American electoral system started because of poor decisions and actions from end-users. End-users need focused security mechanisms where users can identify and use them without complexity to protect their information (Jang-Jaccard & Nepal, 2014). Thus, it appears that further research into cybersecurity threat classifications and communication methods of cybersecurity threats to users is warranted (Alhabeeb, Almuhaideb, & Srinivasan, 2010; Shillair et al., 2015).

Dissertation Goal

The main goal of this study was to design, develop, and empirically test a set of criteria, which enables the validation of a Cybersecurity Threats Classification and Communication Standard (CTC&CS) for mobile devices. Similarly, the chemical industry developed hazard communication standards. The Occupational Safety and Health Act (OSHA) was passed in 1970 to “assure so far as possible every working man and woman in the nation safe and healthful working conditions” (29 U.S.C. § 651). OSHA promulgated the Hazard Communication Standard (HCS) in 1983 (Carle, 1987). The purpose of the standard is to inform employees of the hazards associated with the chemical substances they are exposed to in the workplace (OSHA, 2016). Chemical manufacturers and importers are required to follow specific criteria when evaluating hazardous chemicals and when communicating the hazards (OSHA, 2016). Moreover, designed to protect chemical-source injuries and illnesses by ensuring that employers and

employees are provided with sufficient information to anticipate, recognize, evaluate, control chemical hazards, and to take appropriate protective measures (OSHA, 2016). These standards are made up of a classification of the hazards, development of labels, safety data sheets, and the dissemination of information as well as training to facilitate understanding (Boelhouwer, Davis, Franco-Watkins, Dorris, & Lungu, 2013). OSHA follows a standardized approach to classifying chemicals and developing Safety Data Sheets (SDSs), labels, and pictograms. These standards have increased the quality and consistency of information provided to employers and their workers, which further improved understanding and workers' health and safety. Standardized pictograms, labels, and SDSs have reduced the compliance burden and helped workers exposed to chemicals access and understand hazard information more efficiently (OSHA, 2016). In 2016, construction, manufacturing, wholesale trade, and retail trade industry sectors experienced a significant decline in the rate of occupational injuries and illnesses. Industry employers reported 48,500 fewer injuries and illness cases in 2016 compared to a year earlier (Bureau of Labor Statistics, 2017).

The direct effect of hazard communication on millions of people exposed to chemicals in the workplace is the focus of businesses and regulators (Brooks, Bryan, & Ivan, 2017). HCS is preventing work-related injuries and is estimated that the standard has created \$550 million in monetized benefits annually (Brooks et al., 2017). Benefits found from implementing HCS include improved quality and consistency of hazard information in the workplace, enhanced worker comprehension of hazards, provided workers a quicker, more efficient access to information and Safety Data Sheets, as well as cost savings for American businesses of \$475 million due to productivity improvements (OSHA, 2012).

Likewise, the cybersecurity field can experience similar benefits that emerge from the development of a CTC&CS for mobile devices. A threat communication standard can help improve the quality and consistency of cybersecurity threat information, enhance comprehension of threats primarily for low to limited-literacy users, reduce confusion in the workplace, facilitate training, provide safer handling and use of mobile devices, and provide users quicker and more efficient access to information (See Figure 2 & Appendix A).

The need for this work was demonstrated by the work of Alhabeeb et al. (2010), Davinson and Sillence (2010), as well as Shillair et al. (2015). Shillair et al. (2015) noted that policymakers face problems of communicating cybersecurity threats, as well as their severity and procedures to alleviate the threats. Davinson and Sillence (2010) found that tailored warning messages can increase end-users' intention to act securely online, regardless of whether the messages showed high or low risk. Alhabeeb et al. (2010) noted the need for adequate threat classification, which included sources of threats and the organization's IS areas that may be highly affected by the threats. Furthermore, Alhabeeb et al. (2010) identified the importance of classifying threats to protect assets in advance.

Several types of threat classifications have been developed. Classifications have involved: threats to organizational assets (Ruf, Thorn, Christen, Gruber, & Portmann, 2008), cloud computing (Jouini, Rabai, & Aissa, 2014; Masetic, Hajdarevic, & Dogru, 2017), bluetooth, radio-frequency identification, and wireless sensors (Panigrahy, Jena, & Turuk, 2011). Currently, it appears that there is limited research conducted into cybersecurity threats classification and communication for mobile devices. Therefore,

this study designed, developed, and tested criteria for a cybersecurity threats classification and communication standard for mobile devices.

This study builds on previous research from Ruf et al. (2008), Loch et al. (1992), Yeh and Chang (2007), Alhabeeb et al. (2010), Jouini et al. (2014), as well as Gerić and Hutinski (2007). This research first identifies common cybersecurity threats and common categories of threats to mobile devices to develop a cybersecurity threat classification. A classification provides an enhanced understanding of the phenomenon under study (Lindqvist & Jonsson, 1997). The grouping and classification of threats have been used to understand threats and their necessary countermeasures. Classifications exist for computer-based threats and telecommunications, although these studies were concerned with managers' perceptions of IS threats for the microcomputer, mainframe computers, and network environments (Masetic et al., 2017).

Ruf et al. (2008) proposed an orthogonal threat model with three dimensions of top-level threats: (1) motivation, (2) localization, and (3) agent. Ruf et al.'s (2008) model provided a foundation of comparability for threat exposures but only dealt with IS architectures. Yeh and Cheng (2007) developed a list of security baselines, which assessed several firms' countermeasures to protect IS assets. However, Yeh and Cheng's (2007) study identified threats across four industries: general manufacturing, high tech firms, bank/finance, and retailing/service. Alhabeeb et al. (2010) designed a method of classifying deliberate threats dynamically. Alhabeeb et al.'s (2010) model provided a means to represent each threat in different areas of the organization's IS. Hybrid classifications have been developed, which address different criteria of IS threats classifications (Gerić & Hutinski, 2007; Jouini et al., 2014). However, the hybrid

classification models were mainly based on a review of previous classifications. Previous literature has developed several classifications for threats. Classifications have involved threats to computers, networks, or IS, but it appears none specifically for cybersecurity of mobile devices. Additionally, none were focused on developing standardized warning pictograms, labels, and safety data sheets, which is the focus of this study.

This study also builds on the United States (U.S.) OSHA's well-established HCS that has been in place since 2012 (OSHA, 2016). OSHA has established hazard communication standards for manufacturers, importers, and employers that transport, use, and store chemicals. OSHA's HCS utilizes specific criteria to evaluate hazardous chemicals and communicate the hazards through labels and safety data sheets. The HCS involves classification and communication of hazards, which involve four steps: (1) selection of chemicals to evaluate, (2) collection of data, (3) analysis of the collected data, and (4) record keeping of rationale behind the results obtained (OSHA, 2016). After a completed classification process, manufacturers, importers, or distributors must ensure that each container of hazardous chemicals leaving the workplace is labeled. Labels include information on the product (signal words, hazard statements, precautionary statements, pictograms), as well as the name, address, and telephone number of the chemical manufacturer, importer, or the responsible party. This study identified threats and hazards as synonymous. This study sought to establish pictograms, labels, and safety data sheets best suited for each of the Subject Matter Experts' (SME) validated classified most common cybersecurity threats.

Seven goals of the study were as follows: (1) Identify, using SMEs, the most common cybersecurity threats to mobile devices. SMEs need to be involved in the identification of

the most common threats and threat categories. SMEs possess expert knowledge and experience on cybersecurity threats and can confirm the viability of measures (Sekaran & Bougie, 2013, p. 226). (2) Identify, using SMEs, the most common categories of cybersecurity threats to mobile devices. Identifying threats and threat categories is required to show the range of threats under a general identified category. For example, a category could be identified as Wifi while the threats under that category would include a rogue access point, Wi-Fi Service Set Identifier (SSID) tracking, client Media Access Control (MAC) address tracking, etc. (3) Develop a classification of the SMEs identified most common threats and categories by identifying the level of severity for each threat as well as the category. (4) Develop pictograms, labels, and safety data sheets best suited for each of the previously validated, classified most common cybersecurity threats. (5) Validate, using SMEs, the developed pictograms, labels, and safety data sheets. (6) Assess the users perceived effectiveness on pictograms, labels, and safety data sheets in warning mobile device users against cybersecurity threats. (7) Assess the perceived effectiveness of the pictograms, labels, and safety data sheets when controlled for demographics.

Research Questions

The main research question that this study addressed is: What is the perceived effectiveness of validated pictograms, labels, and safety data sheets of the most common cybersecurity threats in warning mobile device user's against cybersecurity threats? Also, this study addressed seven specific research questions:

RQ1: What are the specific Subject Matter Experts' (SMEs) identified most common cybersecurity threats to mobile devices?

RQ2: What are the specific SMEs' identified most common categories of cybersecurity threats to mobile devices?

RQ3: How can the SMEs' identified most common cybersecurity threats be classified and to what degree of severity?

RQ4: What pictograms, labels, and safety data sheets can be assigned to represent the previously validated, classified most common cybersecurity threats?

RQ5: What are the SMEs' validated pictograms, labels, and safety data sheets?

RQ6: What is the perceived effectiveness of pictograms, labels, and safety data sheets in warning mobile device user's against cybersecurity threats?

RQ7: What are the perceived effectiveness of pictograms, labels, and safety data sheets in warning mobile device user's against cybersecurity threats when controlled for (a) age, (b) gender, (c) years of education, (d) years of work experience, and (e) years of mobile device use?

Relevance and Significance

Relevance

This study sought to mitigate the cybersecurity threats to end-users mobile devices due to a lack of classification and communication standards. The proliferation of mobile devices has seen increased attention by adversaries as a point of attack (McAfee, 2018). In a 2018 report by McAfee, pay-per-download campaigns were identified in 144 apps on Google Play. It estimated that 17.5 million mobile android devices downloaded apps from the campaign before being taken down (McAfee, 2018). Further, Apple's practice of silently removing apps from the app store after security or privacy-related discovery (called "dead apps") leaves millions of users at risk of malware which targets

development workflow, as well as source code leaks that can provide attackers the opportunity to gain a better understanding on how to create exploits (McAfee, 2018).

Global cybercrime is estimated at \$600 billion in 2018 (McAfee, 2018). With banking Trojans, which generate millions of dollars in revenue, click fraud, as well as crypto mining latent apps flooding online stores, increased exploitation is expected in the future (McAfee, 2018). There has been a variety of research studies focused on threat classifications (Alhabeeb et al., 2010; Gerić & Hutinski, 2007; Jouini et al., 2014; Loch et al., 1992; Ruf et al., 2008; Yeh & Cheng, 2007). However, a literature review reveals limited research that has focused on cybersecurity threats as it relates to mobile devices. Cybersecurity threats to mobile devices are a continually growing threat today (McAfee, 2018). A single successful cyber-attack may result in financial and information losses (Carlton, 2016).

Mobile devices increasingly face various types of threats (Leavitt, 2011). As individuals continue to rely on their mobile devices for everyday tasks such as store personal information to connecting to organizational networks, classifying cybersecurity threats to mobile devices and communicating these threats through pictograms, labels, and safety data sheets is critical in protecting the users, organizations, as well as the government. Given the documented increase in the importance of cybersecurity in everyday activity, this study's relevance is substantial.

Significance

This research advanced current research in cybersecurity and advanced the body of knowledge regarding mobile devices as it relates to the standardized classification and communication of cybersecurity threats. Prior threat classifications did not classify

cybersecurity threats specific to mobile devices (Alhabeeb et al., 2010; Gerić & Hutinski, 2007; Jouini et al., 2014; Loch et al., 1992; Ruf et al., 2008; Yeh & Chang, 2007).

According to Alhabeeb et al. (2010), the classification of threats is necessary to protect assets in advance. Additionally, limited research in the cybersecurity field has sought to develop communication standards. Cybersecurity communication standard can potentially increase user awareness of threats, comprehension of threat information, and provide the needed steps to alleviate a cybersecurity threat (Boelhouwer et al., 2013; Nayar et al., 2016). There is an ongoing need for cybersecurity threats classification and communication standards. The development of a Cybersecurity Threat Classification and Communication (CTC&CS) standard for mobile devices would benefit the cybersecurity field. The proliferation of mobile devices has increased use due to the enhanced personal services that a mobile device offers, such as store payments, Global Positioning System (GPS), storing airline boarding passes. However, the threats to these devices are unknown to users (Mylonas, Kastania, & Gritzalis, 2013).

Mobile devices present numerous security challenges due to users storing and accessing personal or workplace data on their devices. Further, studies have shown that users are unable to make security decisions nor use security controls adequately (Furnell, 2005, 2007; Furnell, Jusoh, & Katsabas, 2006; Sheng, Broderick, Koranda, & Hyland, 2006). This remains a problem in current research (Breitinger, Tully-Doyle, & Hassenfeldt, 2019). Breitinger et al. (2019) conducted an online survey that explored user choices, awareness, and education regarding cybersecurity and found users, whether a novice or advanced, had poor security practices. The lack of standardization of cybersecurity threats on mobile devices has caused a slump in knowledge on required

actions to avoid threats posed by mobile devices. Like the chemical industry, HCS is used to protect workers in contact with hazardous chemicals and allow for proper classification of chemicals. The CTC&CS aims to protect users against application-based, web-based, network-based, and physical threats to mobile devices by providing users with sufficient information to anticipate, recognize, evaluate, and control cybersecurity threats as well as take appropriate protective measures. Moreover, threat communication standards appear absent in cybersecurity literature, therefore, developing a cybersecurity threat classification and communication standard will directly affect users exposed to cybersecurity threats on their mobile devices. Communication standard for the CTC&CS will include labels that warn mobile users of exposure to cybersecurity threats, which will increase user awareness to the threats they face; the use of pictograms in addition to the labels will provide increased comprehension of labels (Boelhouwer et al., 2013). Additionally, safety data sheets will give mobile users information and steps to alleviate the cybersecurity threat (Nayar, Wehrmeyer, Phillips, Crankshaw, & Marsh, 2016). This study focused mainly on users of mobile devices for their everyday use.

Barriers and Issues

It is necessary to address the barriers and issues that can be met in this study. One potential barrier of this study was obtaining permission to validate the threats classification and test the SDS, labels, and pictograms with non-IT professional participants. Institutional Review Board (IRB) approval was needed to work with users to validate and test the criteria. Another potential issue was collecting a comprehensive list of mobile device threats. The current literature of threats classification provides non-

exhaustive lists of threats; additionally, these classifications either lacked applicability or slightly apply to mobile devices' domain.

Another issue that the researcher faced was the development of SDSs, labels, and pictograms. These types of threats communication methods have not been used in the cybersecurity field, identifying appropriate information to include in the SDS, choosing appropriate labels for each category of classification, and developing the appropriate pictogram representation of each category was challenging to this study.

Assumptions, Limitations, and Delimitations

Research limitations can be defined as the study's potential weakness (Leedy & Ormrod, 2019). One limitation of this study related to the expert opinions collected during the Delphi technique. The opinions of the experts were limited to the recruited members (Ellis & Levy, 2010). Thus, collating the Delphi technique along with the review of literature, mitigated to some extent this limitation.

Definition of Terms

The following represent terms and definitions.

Classification. "process in which ideas and objects are recognized, differentiated, and understood" (Kalmegh & Deshmukh, 2014, p. 132).

Cybersecurity. "A computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries" (CSEC2017, 2017, p. 16).

Cybersecurity threat. An event or a set of circumstances, if left uncontrolled, could present a potential to cause serious harm to IS Security.

Hazard. “The inherent capacity of a substance to cause an adverse effect” (OSHA, 2016, p. 21)

Hazard Communication Standard (HCS). “ensure that the hazards of all chemicals produced or imported are classified and that the information on the hazardous chemicals is transmitted to employers and workers” (Brooks, 2014, p. 27).

Information Systems (IS). “A discrete set of information resources [i.e., personnel, equipment, funds, and information technology] organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Also includes specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems” (NIST, 2006, p. 3).

Label. “A appropriate group of written, printed or graphic information elements concerning a hazardous chemical that is affixed to, printed on, or attached to the immediate container of a hazardous chemical, or the outside packaging” (OSHA Standard 29 CFR 1910.1200(f)).

Mobile Device. A small form factor that provides data communication (Wifi, cellular networking, etc.), non-removable data storage, an operating system, applications available through multiple methods, network services (Bluetooth, NFC, voice communications, GPS), digital cameras/video recording, microphone, and built-in features for synchronizing local data with different locations. (Souppaya & Scarfone, 2013).

Occupational Safety and Health Act (OSHA). “assure so far as possible every working man and woman in the nation safe and healthful working conditions” (OSHA, 2016, p. 1).

Pictogram. “graphic symbols used to communicate specific information about the hazards of a chemical” (OSHA Standard 29 CFR 1910.1200(f)(1)(iv)).

Safety Data Sheet (SDS). provides comprehensive information about a substance or mixture for use in workplace chemical management (OSHA Standard 29 CFR 1910.1200(g)).

Threat. “any circumstance or event with the potential to adversely impact organizational operations, assets, individuals, other organizations, or the Nation through an IS via unauthorized access, destruction, disclosure, modification of information, or denial of service” (NIST, 2006, p. 8).

User-perceived value. “belief about the level of importance that users hold for IS characteristics” (Levy et al., 2009, p. 94).

Summary

Chapter one discussed the problem statement, research goals, research questions, relevance and significance, barriers and issues, limitations, and the definition of terms. The research problem addressed was the lack of cybersecurity threats classification and communication standards for mobile devices, while mobile device compromises are on the rise. This main goal of the study was to design, develop, and empirically test criteria that enable the validation of a Cybersecurity Threats Classification and Communication Standard for mobile devices. Chapter one also defined the research questions that this study addressed. The main research question this study addressed was: What is the

perceived effectiveness of validated pictograms, labels, and safety data sheets of the most common cybersecurity threats in warning mobile device user's against cybersecurity threats? Chapter one presented the relevance and significance of the study, as well as issues and barriers. Finally, limitations of the study, as well as a list of definitions of key terms, are provided.

Chapter 2

Review of Literature

Introduction

In this chapter, a literature review is presented to provide a synopsis of the relevant literature on threat classifications, labels, safety data sheets, and pictograms as well as lay the theoretical foundation for this study. The literature review is an essential step toward developing a theoretical foundation for a study (Paré, Trudel, Jaana, & Kitsiou, 2015, p. 183). Furthermore, a systematic literature review should analyze and synthesize quality peer-reviewed, and secondary IS literature, which substantiates the existence of a research problem, establish a foundation for a research methodology, and demonstrate the contributions of this study to the overall body of knowledge (Levy & Ellis, 2006). An extensive search of the literature using interdisciplinary fields was performed to ensure breadth, depth, rigor, consistency, clarity, brevity, as well as useful analysis and synthesis (Hart, 1998). The literature review provides the discovery of existing knowledge, approaches, and a theoretical foundation for the design, development, and testing criteria that enable the validation of a Cybersecurity Threats Classification and Communication standard.

Threat Classifications

Classifying threats allows individuals to detect, measure, and evaluate significant threats and further study the occurrence and development from its technical nature (Tang,

Wang, Ming, & Li, 2012). A threat classification aims to contribute to understanding the nature of the threats, which is the first step in effective threat mitigation (Alhabeeb et al., 2010).

The classification of threats assists individuals by providing a logical organization of the identified threats which ease the tasks of assessment and evaluation of the impacts, as well as develop countermeasures that prevent or mitigate the threat (Alhabeeb et al., 2010; Almutairi & Riddle, 2017; Farahmand, Navathe, Sharp, & Enslow, 2005; Tang et al., 2012). Classifying threats creates a segmentation of all possible threats to each of its dimension, where the dimension is defined as an elementary aspect or extent of all threats, e.g., special segmentation, temporal segmentation, or spatiotemporal segmentation (Alhabeeb et al., 2010; Baldwin et al., 2011; Bompard, Huang, Wu, & Cremenescu, 2013; Lindqvist & Jonsson, 1997; NIST, 2012; Ruf et al., 2006; Tang et al., 2012). The domain of threats can have several dimensions or criteria. Some of these dimensions or criteria can shed light on the understanding of risks exposed to a system. Literature has identified several criteria used, e.g., source, agent, motivation, and impact, as criteria for classifying threats (Farahmand et al., 2005; Geric & Hutinski, 2007; Ruf et al., 2006).

Previous classifications have attempted to understand the characteristics and nature of known threats to support the prediction of threats in new systems (e.g., Mitrokotsa, Rieback, & Tanenbaum, 2010); for example, the kinds of vulnerabilities in an Android OS might be similar to the kinds of vulnerabilities in a Symbian OS because of both OS's exhibit similar basic functionality (Igre & Williams, 2008). The development and testing of threat classifications have been performed for IoT devices (Ferrando & Stacey,

2017), information systems (Jouini & Rabai, 2016a), network security (Tang et al., 2012), blockchains (Mosakheil & Hayat, 2018), cloud computing (Masetic et al., 2017), smart homes (Anwar, Nazir, & Mustafa, 2017), power systems (Bompard et al., 2013), RFID (Mitrokotsa et al., 2010), and other fields such as chemical, pharmaceutical, and healthcare. Additionally, literature relating specifically to information systems purports six principles as best practices for classification development. These principles are: 1) mutually exclusive, 2) exhaustive, 3) unambiguous, 4) repeatable, 5) accepted, 6) useful. The full support of the classification principles is not present in current threat classifications (Alhabeeb et al., 2010), but it is important to note that all the threat classification principles are useful, but not all are necessary. For example, not all classifications strive to be mutually exclusive.

In this section, a review of the literature is presented to provide an overview of the different approaches to threat classifications used in literature and practice. The literature review categorizes threat classifications into attack techniques and threat impacts. See Tables 1 and 2 for a summary of classification categories.

Attack Techniques

Several known attack threat classifications proposed from literature, based on the attack technique, consider the methods employed by attackers to exploit vulnerabilities and the attacker's perspective of tools, motivations, and objectives. (Alhabeeb et al., 2010; Alhakami, Mansour, & Ghazanfar, 2014; Bompard et al., 2013; Jouini et al., 2014). There have been several attempts to classify threats in the literature based on the intended effects of the attack, i.e., DOS and DDOS (Avizienis, Laprie, Randell, & Landwehr, 2004; Mitrokotsa et al., 2010; Tang et al., 2012). Avizienis et al. (2004) identified the

increasing development and procurement of systems whose services are much trusted by organizations, governments, and individuals. Avizienis et al. (2004) classified threats to vital system services into faults, errors, and failure, e.g., EMV2 Error library. Trivedi, Kim, Roy, & Medhi (2009) extended the classifications on computer system services by Avizienis et al. (2004) and included accidents as a threat category. Both studies provide an analysis of the threats to both dependability and their attributes that arise from faults during systems engineering and use (Avizienis et al., 2004; Trivedi et al., 2009). Other studies have classified threats based on the type of asset that each attack is taking place (Chidambaram, 2004; Mitrokotsa et al., 2010). Chidambaram (2004) classified threats to enterprise architectures into network threats, server or host threats, and application threats while Mitrokotsa et al. (2010) distinguished attacks in the physical, the network transport layer, application layer, strategic layer, and multilayer. Additionally, classifications have been based on a different dimension that the system interacts with such the case with Bompard et al. (2013) that classified threats to power systems into four categories: natural, accidental, malicious, and emerging.

Literature has also identified threat classifications that take into account the techniques used by attackers, i.e., bypassing authentication (Applegate & Angelos, 2013; Feng, Wang, & Lia, 2014; Tang et al., 2012). Geric & Hutinski (2007) and Alhabeeb et al. (2010) developed threat classifications that sought to differentiate threats and represent different areas of information systems with threats. Geric & Hutinski's (2007) classification possessed four main categories: security threat frequency, area of security threat activity, and security threat force. Building on Geric & Hutinski (2007) classification, Alhabeeb et al. (2010) classified threats into the attacker's prior

knowledge, the criticality of the area, and loss. The classifications are dynamic because they link threats to the potentially affected area and the threats' source. Several other studies have device/technology specific threat classifications (AB, 2012; Alhakami et al., 2014), network threats classification (Demchenko, Gommans, de Laat, & Oudenaarde, 2005; Rufi, 2008), and information systems threats classification (Alhabeeb et al., 2010; Geric & Hutinski, 2007; Kjaerland, 2006). Although, the literature on threats classifications based on attack techniques does not consider the impact of the identified threats, which allow to quickly identify what needs to be protected and how to protect. The classifications based on attack techniques are not appropriate for this study due to threats arising from different agents such as mobile providers, user failure to protect their device, and external attackers.

Table 1

Summary of Classifications Based on Attack Techniques

Study	Methodology	Sample	Instrument/ Construct	Main finding or contribution
AB, 2012	Developmental	Authentication systems	Yubikey	This study classified threats to user authentication systems. Threats were classified into six classes: server attacks, protocol attacks, host attacks, device attacks, user attacks, other attacks.
Alhabeeb et al., 2010	Literature review and synthesis	Seven classifications developed by governments, institutions, scientists, and information systems security professionals	Threats classification pyramid	Classified deliberate threats to information system security based on the attacker's prior knowledge, the criticality of the area, and loss.

Table 1

Summary of classifications based on attack techniques (Cont.)

Study	Methodology	Sample	Instrument/ Construct	Main finding or contribution
Alhakami et al., 2014	Literature review and synthesis	Security challenges in CR networks	Spectrum sharing classification, Protection, and detection techniques	Classified threats in cognitive network systems (CRNs) in two categories: Threats in conventional wireless/CR networks and Security threats specific to CRN users.
Almutairi & Riddle, 2017	Literature review and synthesis	Four previously developed threat classifications	Outsourcing threats classification	Developed a hybrid threat classification approach for outsourced IT services.
Almutairi & Riddle, 2018	Focus group, Questionnaire	30 government IT agents in the Middle East	Outsourcing threats classification	Evaluated a previously developed classification for outsourced IT services.
Applegate & Stavrou, 2013	Empirical study via prototyping	Real-world cyber conflict-related events and the individuals, organizations or states that participated in those events	Cyber conflict taxonomy	Developed a classification for security incidents to give users the ability to classify events and expose logical connections and links between actors, types of attacks, and vectors, as well as types of impacts associated with events.
Avizienis et al., 2004	Literature review	Eight previously developed taxonomies	The fault-error-failure model	Avizienis et al. (2004) presented a taxonomy of threats that may affect a system during its entire life. This study classified threats to service failures into three main classes: faults, errors, and failures.

Table 1

Summary of classifications based on attack techniques (Cont.)

Study	Methodology	Sample	Instrument/C onstruct	Main finding or contribution
Anwar et al., 2017	Literature review and synthesis	28 threats to smart homes identified in the literature.	Taxonomy for domain-specific threats in smart homes	Developed a classification of threats for smart homes. Three broad threat categories were identified: intentional threats, unintentional threats, malfunction.
Bompard et al., 2013	Survey	100 representative historical blackouts	Quantitative trend analysis	Bompard et al. (2013) classified threats to power systems into four categories: natural threat, accidental threat, malicious threat, and emerging threat.
Chidambaram, 2004	Literature review and synthesis	17 threats	Threat modeling system	Developed the Step-by-step method which reviewed and organized threats in three categories: network threats, server/host threats, application threats
Demchenko et al., 2005	Literature review and synthesis	27 known vulnerabilities in grid middleware implementation.	Classification model for potential Grid and Web Services attacks and vulnerabilities	Classified Web service threats into Web Services Interface Probing, XML Parsing System, Malicious XML Content, External Reference Attacks, SOAP XML Protocol Attacks, XML Security Credentials Tampering, Secure Key/Session Negotiation Tampering

Table 1

Summary of classifications based on attack techniques (Cont.)

Study	Methodology	Sample	Instrument/C onstruct	Main finding or contribution
Geric & Hutinski, 2007	Literature review and synthesis	Previously developed classification criteria	Information system security risks (threats) classification	Developed a hybrid model for the classification of information system security threats. They considered three main criteria: security threat frequency, area/focus domain of security threat activity, and security threat source.
Guttman & Roback, 1995	Literature review	Information security system threats significance criteria.	NIST classification	This study provided a classification of threats to information systems. Threats were classified into errors and omissions, fraud and theft, and employee sabotage, loss of infrastructure, malicious hackers, malicious code, viruses, trojan horses, worms, and threats to personal privacy
Jian et al., 2012	Literature review	Previously developed classifications for network security threats.	Multi-dimension architecture on network security threats	This study classified threats into the source, which are further subcategorized into incidental and intentional, target subcategorized into target type and effect, and feature subcategorized into platform dependencies, vulnerability relevance, and spreadability.

Table 1

Summary of classifications based on attack techniques (Cont.)

Study	Methodology	Sample	Instrument/C onstruct	Main finding or contribution
Jouini et al., 2014	Literature review and synthesis	Five previously developed threat classification models	Hybrid threat classification model for information system security	This study developed a hybrid threat classification model for information systems. Threats are classified into the source, agent, motivation, intention, and impact.
Jouini & Rabi, 2016a	Literature review and synthesis	Previous threat classification models	The multi-dimensional Threats classification model	Categorized different threat classifications into classifications based on attack techniques and threat impacts.
Jouini & Rabi, 2016b	Literature review and synthesis	Previous threat classification models	The multi-dimensional Threats classification model	Developed a threat classification that classified threat models into dimensions and perspectives.
Kjaerland, 2006	Exploratory study via Multidimensional scaling (MDS)	1397 cases of cyber-attacks towards commercial and government sectors.	Taxonomy based on cyber incidents	Examined the relationship between targets, and the impact of attacks and categorized cyber intrusions into the method of operation, the impact of the intrusion, the source of the intrusion, and target.
Mitrokotsa et al., 2010	Literature review and synthesis	Previous literature on RFID classifications	Classification of RFID attacks	Classified threats associated with Radio Frequency Identification systems. They distinguished attacks in the physical layer, network transport layer, application layer, strategic layer, and multilayer.

Table 1

Summary of classifications based on attack techniques (Cont.)

Study	Methodology	Sample	Instrument/C onstruct	Main finding or contribution
Ruf et al., 2008	Literature review and synthesis	Seven threats	Orthogonal classification schema	The article proposed a model that classifies the threat space into three orthogonal dimensions: motivation, localization, and agent.
Tang et al., 2012	Theoretical	21 threats	Multi- dimension network security threats classification architecture	Classified network security threats into the source of threats, the target of threats, the effect of threats, platform dependencies, vulnerability relevance, and spreadability, in order to detect and evaluate network security threats and suggest countermeasures.
Trivedi et al., 2009	Case study	22 threats	Classification of dependability and security models	Proposed to classify threats into four categories: faults/attacks, errors, failures, and accidents.

Threat Impacts

Threat classification approaches, based on the impact of a threat, consider the goal of the threat to classify threats. The threat impact approach takes into account only the threat impact when developing a classification. Microsoft's STRIDE (Swiderski & Snyder, 2004) and the ISO 7498-2 model (ISO, 1989) are examples of this approach. Swiderski and Snyder (2004) originally introduced the spoofing identity, tampering with data, repudiation, information disclosure, denial of service, and elevation of privilege

(STRIDE) threat modeling approach as a classification for potential threats. STRIDE is considered an excellent approach to classifying threats because of the goal-oriented approach (Sangchoolie, Folkesson, & Vinter, 2018). This approach, in its origins, involves element-based threat elicitation. More recently, it evolved to an interactive-based threat elicitation and tool support both within Microsoft and outside the organization (Dhillon, 2011; Microsoft Corporation, 2016; Shostack, 2014; Shostack, 2008). The STRIDE model is a favorite and straightforward threat model that highlights many top threats (Bertino et al., 2004; Farahmand et al., 2005; Sangchoolie et al., 2018), although the STRIDE model does not cover all threats and threat consequences and only provides an ambiguous approach to understanding the nature of threats.

The ISO standard (ISO 7498-2) has classified threats into five categories of threat impacts and services: Destruction of information and other resources, corruption or modification of information, theft, removal or loss of information and other resources, disclosure of information, and interruption of services. Similarly, the NIST threats classification based on information systems significance criteria, classified threats into one of the following groups: errors and omissions, fraud and theft, employee sabotage, loss of physical and infrastructure support, malicious hackers, industrial espionage, malicious code, foreign government espionage, and threats to personal privacy. Both ISO 7498-2 and NIST's threats classification included exhaustive classifications of threats that provided organized and flexible structures.

Table 2

Summary of classifications based on impact

Study	Methodology	Sample	Instrument/C onstruct	Main finding or contribution
Abrams, 1998	Theoretical		National Airspace System Infrastructure Management System (NIMS)	Developed a model that organizes Infrastructure Management System threats by their consequences.
Farahmand et al., 2005	Literature review and synthesis	Single e- commerce organization	The probabilistic evaluation of the impact of security threats	Considered threats to a network system using two points of view: the threat agent and penetration technique.
ISO, 1989			Framework for the development of existing and future Standards	Identified five security threats and services as a reference model. 1. Destruction of information or other resources, 2. Corruption or modification of information, 3. Theft, removal, or a loss of information or other resources, 4. Disclosure of information; and 5. Interruption of services The classification covers all types of threats in an organized and flexible structure.
NIST, 2012	Review of literature	Information security system threats significance criteria	NIST threat classification	Classified threats to information systems based on significance criteria and distinguished nine types of security threats.

Table 2

Summary of classifications based on impact (Cont.)

Study	Methodology	Sample	Instrument/Construct	Main finding or contribution
Swiderski & Snyder, 2004	Developmental		Data Flow Diagram	Developed the STRIDE method for classifying computer security threats countermeasures that relate to the network, host, and application layers. The classification was based on the motivation of the threat.
Web Application Security Consortium, 2010	Subject Matter Experts	30 participants	WASC Threat Classification	Classified threats to the security of a website into six categories.

Hazard Communication

The diverse literature on hazard communication has recognized the dependence on clear and specific information through pictograms, labels, and Safety Data Sheets (SDS) (Monterio et al., 2018; Vaillancourt et al., 2018; Van den Berg et al., 2016). Hazard communication has been studied and used in several fields (i.e., medical, pharmaceutical, agriculture, chemical, engineering, information technology, and crisis communication), which inquire into either the comprehension or development of hazard communication tools (e.g., Boelhouwer et al., 2013). The Globally Harmonized System (GHS) of Classification and Labelling of Chemicals, which was adopted by the United States Occupational Safety and Health Administration (OSHA) under the Hazard Communication Standard (HCS) in June 2016 recognized the use of pictograms, labels, and SDS as a way of recognizing hazards in the workplace (OSHA, 2012; Pratt, 2002;

United Nations, 2013; U.S Department of Labor; Winder, Azzi, & Wagner, 2005).

Pictograms, labels, and SDS, in the chemical industry, for example, are required when a hazard or threat is not evident because of the inherent warning of danger or when a users ability to detect and respond to a threat is limited. Hazard communication has a broad application around chemicals with standardized rules in place, i.e., OSHA, DOT, HazMat, SARA that require communication of hazards within workplaces and for the public. This section will explore literature into the potential of safety data sheets, labels, and pictograms.

Safety Data Sheets

Sadhra, Petts, McAlpine, Pattison, and MacRae (2002), as well as Niewohner, Cox, Gerrard, and Pidgeon (2004) demonstrated that users relate to chemical hazards through particular work practices and exposures performed during the workday which help in shaping attitudes towards threats within the workplace. Sadhra et al. (2002) investigated worker comprehension of SDSs in the electroplating industry and found that through following standard work practices, participants learned from fellow workers, and their understanding of acute risks of chemicals increased. Niewohner et al. (2004) used surveys, semi-structured interviews, and focus groups to investigate SDS comprehension in small businesses in the United Kingdom. Workers were found to shape their attitudes towards hazards through their everyday work and exposure to hazards in the work environment (Niewohner et al., 2004). Niewohner et al.'s (2004) finding supports Sadhra et al. (2002). Equally important to note is that general information on SDSs was of little relevance to most participants; 92% of workers thought SDSs were too complicated (Sadhra et al., 2002). Furthermore, Niewohner et al. (2004) and Sadhra et al. (2002)

reported that even with SDSs, there is a lack of understanding of potential long-term effects of chemicals used in the everyday work environment.

Other studies evaluated the information presented in SDS or evaluated the order of presented information in SDSs. Seki et al. (2001) sent surveys to 422 organizations that used chemicals in the workplace to assess the comprehension of eight terms commonly used on SDS. Responses were organized based on the size of each organization. Seki et al. (2001) found that 52%, 50.8%, and 25% for small, medium, and large organizations, respectively, considered the SDS unsatisfactory (Seki et al., 2001). Smith-Jackson and Wogalter (1998) investigated the SDS sections' order and further extended their 1998 study in Smith-Jackson and Wogalter (2007), which used a mental model approach to look at naïve users, homemakers, and firefighters to determine an optimal order for SDS sections for these groups. Participants in the Smith-Jackson and Wogalter (2007) study exhibited a higher preference for certain sections over others, i.e., health effect data as the highest priority.

Table 3

Summary of safety data sheet studies

Study	Methodology	Sample	Instrument/ Construct	Main finding or contribution
Niewohner et al., 2004	Questionnaire, semi structured verbal protocols, and user discussion groups	90 participants	Multimethod evaluation strategy	The article reported SDSs to be inadequate as a means of informing chemical protection. Additionally, general chemical information was reported to be of little relevance to most users, and instead, chemical hazards are learned through everyday work and exposure to the chemicals.

Table 3

Summary of safety data sheet studies (Cont.)

Study	Methodology	Sample	Instrument/ Construct	Main finding or contribution
Sadhra et al., 2002	Interviews and Questionnaires	21 participants in face-to-face interviews, 84 participants for the questionnaires	Chrome plating chemicals	Reported an incomplete understanding of the long term or chronic effects of chemicals. The experience with the use of a chemical was found to affect an individual's knowledge. SDSs were found to be of little effect.
Seki et al., 2001	Questionnaire	422 organizations	Safety Data Sheets	Reported the lack or misuse of safety data sheets due to a lack of knowledge and understanding. Additionally, safety data sheets were found to be difficult to understand.
Smith-Jackson & Wogalter, 1998	Survey	60 participants	Safety Data Sheets	The article reported that participants favored the use of a sorting method based on the priority of communicating information related to hazard. Additionally, 57% of participants reported difficulty in understanding the safety data sheets.
Smith-Jackson & Wogalter, 2007	Experiment	90 participants	Safety Data Sheets	The article provided support for preferred orders of SDS information among users. The particular orders indicated patterns reflecting schemas that centered on survival or health. User preferred the use of color and pictorials/symbols in MSDSs.

Labels

Previous research on safety labels suggested that warnings must be understood to be effective (Dorris & Purswell, 1978; O’Conner & Lirtzman, 1984). O’Conner and Lirtzman (1984) suggested that too many hazard statements on a label increase the amount of time that the participant needs to respond to a question about a particular item on a label. Rhoades, Frantz, and Miller (1990) supported the amount of hazard statements on labels, which found that overly detailed warnings overloaded the participant. Moreover, literature suggested that pictograms’ addition to the label may prove to be easily recognizable and have a more intrinsic interest than written labels only (Dorris & Purswell, 1978; Robinett & Hughes, 1984). Young and Wogalter (1990) found the pairing of pictograms with written labels associated both in memory, which in turn cues the warning message and facilitates the retrieval of hazard information from written warnings on re-exposure to a pictogram. Although previous literature identified the benefits of pairing labels with pictograms Robinett and Hughes (1984) suggested that the use of pictograms without text may be preferable.

Table 4

Summary of labels studies

Study	Methodology	Sample	Instrument/ Construct	Main finding or contribution
Rhoades et al., 1990	Case study	Three case studies	Semantic features analysis, and script analysis	The article reported that overly detailed warning labels might overload an individual. Furthermore, the authors suggested the use of pictograms with warning labels, and product development should consider user knowledge and patterns of behavior.

Table 4

Summary of labels studies (Cont.)

Study	Methodology	Sample	Instrument/ Construct	Main finding or contribution
Robinett & Hughes, 1984	Design case study	30 participants		The results indicate that pictograms without text are a preferred communication method.
Young & Wogalter, 1990	Experiment	64 undergraduate students	Comprehension and memory performance	Paired pictograms with written warnings as to associate the two in memory; this will cue the warning message and facilitate retrieval of information.

Pictograms

Pictograms include symbols and short, clear messages used as graphic signs which convey safety information that warn of the dangers and identify correct behaviors and attitudes (Chafarro & Cavallo, 2015). Pictograms have been used in hazard/threat communications to convey hazards/threats, and increase the comprehension of labels. Pictograms provide several benefits such as the quick recall of instructions and concepts, providing the reading impaired or individuals unfamiliar with the local language and understanding of the information provided (Lesch, 2003; Wogalter, Conzola, & Smith-Jackson, 2002; Wogalter & Laughery, 1996; Wogalter, Silver, Leonard, & Zaikina, 2006; Wogalter, Sojourner, & Brelsford, 1997; Young & Wogalter, 2000), and the visual impact for the public domain to condense and communicate hazard/threat information (Chafarro & Cavallo, 2015; Duarte, Rebelo, Teles, & Wogalter, 2014; Lui & Hoelscher, 2006). This section will review the literature on pictograms' effects on labels and SDSs,

internal and external characteristics that affect pictogram comprehension, and pictogram development.

Effects of Pictograms on labels and SDS

Pictograms are increasingly being used in conjunction with labels and SDS to increase comprehension of threats in the workplace and the public domain (Boelhouwer et al., 2013; Kalsher, Wogalter, & Racicot, 1996). Several researchers have demonstrated improved communication effects, understanding, and adherence to safety rules when labels and safety data sheets are supplemented with pictograms (Boelhouwer et al., 2013; Dowse & Ehlers, 2005, Kalsher et al., 1996). Boelhouwer et al. (2013) and Dowse and Ehlers (2005) indicate a significant positive influence on comprehension, understanding, and adherence when pictograms are present. Boelhouwer et al. (2013) performed two experiments that evaluated the difference in comprehension of the information presented in SDSs and labels accompanied by pictograms. Specifically, Boelhouwer et al. (2013) sought to observe how the addition of hazard and precautionary pictograms to SDSs and labels improved the transfer of information to individuals. Similarly, Dowse and Ehlers's (2005) experiment compared text-only labels with text-labels accompanied with pictograms to assess the comprehension, understanding, and adherence of individuals with limited reading skills. Both studies found the addition of pictograms to positively influence the communication of hazard/threat information (Boelhouwer et al., 2013; Dowse & Ehlers, 2005). Additionally, pictograms were found to positively influence the communication of information for both individuals considered naïve and expert users (Boelhouwer et al., 2013), and the addition of pictograms positively influenced the understanding and adherence of safety rules on medicine labels (Dowse & Ehlers, 2005).

Contrary to the improved comprehension, understanding, and adherence of SDS and labels with an accompanying pictogram, several studies have reported the poor understanding of pictograms (Chan & Ng, 2010a; Dowse & Ehlers, 2001; Duarte & Rebelo, 2005; Liu, Zhong, & Xing, 2005; Rother, 2008). Specifically, several researchers investigated pharmaceutical (Dowse & Ehlers, 2001), industrial safety (Chan & Ng, 2010a), and pesticide (Rother, 2008) pictograms for their effectiveness in communicating to individuals and identified low comprehension and understanding of the pictograms (Dowse & Ehlers, 2001; Rother, 2008). Thus, there appear to be differing conclusions found in the ability of pictograms to enhance SDSs and labels. Table 5 provides a summary of research studies regarding the addition of pictograms to SDS and labels.

Table 5

Summary of studies on pictogram interaction with safety data sheets (SDS) and labels

Study	Methodology	Sample	Instrument/ Construct	Main finding or contribution
Boelhouwer et al., 2013	Experiment	90 undergraduate students and 45 professionals	Pictograms, SDSs, and labels	Reported that including pictograms to SDSs decreased response time to questions in both naïve and expert users
Chan & Ng, 2010a	Experiment and questionnaire	60 participants randomly assigned to control, paired-associate learning, recall training, and recognition training	Training evaluation questionnaire	Participants showed improvements in comprehension, indicating training improved comprehension of safety signs. Sign characteristic had no significant influence on training effectiveness.
Dowse & Ehlers, 2005	Experiment	87 participants	Pictogram comprehension	Significant increase in comprehension and adherence to medicine labels.

Table 5

Summary of studies on pictogram interaction with safety data sheets (SDS) and labels

(Cont.)

Study	Methodology	Sample	Instrument/ Construct	Main finding or contribution
Dowse & Ehlers, 2001	Interview	46 participants		The findings from the article indicate a low comprehension level of pesticide labels and pictograms. Further, training led to a significant increase in comprehension over time.
Duarte & Rebelo, 2005	Survey study	60 participants	Comprehension of Safety Signs	The results of the article found that pictorial symbol, color, and shape are significant factors affecting people to understand a symbol. Additionally, comprehension levels of safety signs do not adhere to ANSI or ISO comprehension criteria.
Kalsher, Wogalter, & Racicot, 1996	Experiment	84 undergraduates in Experiment 1, 58 older adults in experiment 2	Tag and fold-out designs	The article reported that both undergraduates and older adults preferred labels with pictograms. Further, undergraduates and older adults preferred alternative labels, especially the tag labels, and labels with pictorials
Rother, 2008	Questionnaire	115 farm workers	Gender	The article reported finding only one out of the ten pictograms provided correct responses. Male participants had more correct responses compared to females.

Extrinsic/Intrinsic Characteristics

Pictograms lack lucidity, causing different interpretations of the intended message that favor improper actions, attitudes, and the increased possibility of accidents (Monteiro, Ispolnov, & Heleno, 2018). Literature has identified several characteristics that have been proven to affect an individual's comprehension of pictograms (Davies, Haines, Norris, & Wilson, 1998; Lui & Hoelscher, 2006). External and internal characteristics have been identified by researchers that affect an individual's comprehension of a pictogram (Davies et al., 1998; Lui & Hoelscher, 2006). Extrinsic characteristics identified from the literature as significant predictors of pictogram comprehension are education, gender, age (Chafarro & Cavallo, 2015; Davies et al., 1998; Monterio et al., 2016), professional experience, cultural background (Blees & Mak, 2012), and training. Apatsidou et al. (2018) and Walters, Lawrence, and Jalsa (2017) expressed the need for education and professional experience to improve pictograms comprehension. Walters et al. (2017) articulated the need to incorporate hazard communication training and education within educational curricula, which were supported by Apatsidou et al. (2018). Apatsidou et al. (2018) assessed the comprehension level of hazard communication and awareness through a closed-ended questionnaire. Comprehension was found to depend on education ($P=0.022$) and professional experience ($P=0.014$) statistically, which in turn enhanced pictogram comprehension and understanding. Similarly, Ng and Chan (2008) and Ta et al. (2010) identified education to affect pictogram comprehension significantly. However, studies have reported no significant effects of education on pictogram comprehension (Rubbiani, 2010).

Training has also been identified by literature to be significant in facilitating the understanding of pictograms (Hara et al., 2007; Rubbiani, 2010; Ta et al., 2010). Several studies have shown that training has led to significant improvements in pictogram comprehension as well as improved speed and reliability (Lesch, 2003; Lesch, 2008). Conversely, empirical studies have reported inconsistent results on training effects (Brahm & Singer, 2013). Several studies reported no significant effects of training on comprehension or reported a decline of comprehension in the post-training phase, although reports identified recall training to be the only effective training type (Caffaro & Cavallo, 2015; Chan & Ng, 2010b; Joshi & Kothiyal, 2011; Wang & Chi, 2003).

Pictogram comprehension based on individual age and gender reports a disparity in literature. Age is identified as a significant predictor of an individual's ability to comprehend pictograms (Blees & Mak, 2012; Ng & Chan, 2007; Rother, 2008; Smith-Jackson & Essuman-Johnson, 2002; Smith-Jackson, Wogalter, & Quintela, 2010) and positively impact performance and cognitive processes of an individual's comprehension (Beaufils et al., 2014). Younger individuals can better comprehend pictograms (Blees & Mak, 2012; Hancock, Fisk, & Rogers, 2005; Lesch, 2003). However, gender and age characteristics have also been reported to have no significant difference in pictogram comprehension (Caffaro & Cavallo, 2015; Hara et al., 2007; Rubbiani, 2010; Ta et al., 2010).

The familiarity of a pictogram varies according to the cultural background because the meaning of a pictogram and its relation to the depiction based on conventions differ across cultures (Blees & Mak, 2012; Ng & Chan, 2007). Literature has shown cultural background to affect the comprehension of pictograms. The article by Blees and Mak

(2012) compared comprehension levels of Dutch and Chinese individuals through a web survey and reported a significant effect on individuals' comprehension.

Intrinsic characteristics of pictograms such as familiarity (Liu & Ho, 2012; Wang & Chi, 2003), visibility (Davies et al., 1998; Ng & Chan, 2013), concreteness (Liu & Ho, 2012), simplicity and accuracy (Lesch, 2003; Lesch, 2008; Liu & Ho, 2012; Wang & Chi, 2003) are reported to relate to pictograms. Literature has used familiarity, visibility, concreteness, simplicity, and accuracy to investigate the comprehension of traffic pictograms (Ng & Chan, 2007). These characteristics have become important concerns in research on pictograms (Chan & Ng, 2010; Ng & Chan, 2008; Ng & Chan, 2009). The literature on familiarity (i.e., previous experience with a warning) has reported significant effects of familiarity on pictogram comprehension (Chan & Ng, 2010a; Hancock, Rogers, Schroeder, & Fisk, 2004; Ng & Chan, 2007, 2008). Liu and Ho (2012) reported a high correlation of familiarity with pictogram comprehension; similar reports found the high correlation of familiarity (e.g., Ben-Bassat & Shinar, 2006; Rosson, 2002), thus implying that pictogram design should be familiar to the individual, this would assist in comprehending pictograms. Conversely, literature has also reported no effect of familiarity with a pictogram on the likelihood of comprehending its meaning (Chan & Ng, 2010b; Ng & Chan, 2011).

Other characteristics that affect comprehension are visibility, concreteness, accuracy, simple. Low visibility of pictograms can cause a failure in information transfer (Davies et al., 1998; Ng & Chan, 2013). Concreteness indicates the degree to which something is material and genuine (Liu & Ho, 2012). Pictograms are concrete if they depict real objects, materials, or people. Pictograms with concrete designs are easily understood

compared to ambiguous designs that can potentially confuse an individual's understanding (Foster & Afzainia, 2005; Passini et al., 2008; Rousek & Hallbeck, 2011; Wolff & Wogalter, 1993). Further, the accuracy of semantic depiction is an indication of how close, accurate, and comprehensive the pictogram design is to what the pictogram is meant to signify (Liu & Ho, 2012). Young and Wogalter (1990) indicated that improved identification of a symbol precisely communicated a pictogram semantic meaning. Finally, intricate and in-depth details in a pictogram make the pictogram complex but simple when only a few elements or details are present (Dewar, 1999; Huang et al., 2002; Lin, 1992).

Table 6

Summary of studies on pictogram characteristics

Study	Methodology	Sample	Instrument /Construct	Main finding or contribution
Apatsidou et al., 2018	Questionnaire	200 healthcare professionals and 150 healthcare specialists		50-60% of professional users perceived pictograms adequately. Participants were aware of hazardous products during their everyday life, but perception of hazard and the severity varied significantly between the two groups and depended on educational and professional levels. Study reported limited use of SDSs, which was observed in 18% of professional users and 23% of health care specialists.
Ben-Bassat & Shinar, 2006	Experiment	40 participants	Comprehension level	The article reported that following sound ergonomic principles of good design significantly increases comprehension by individuals from different backgrounds.

Table 6

Summary of studies on pictogram characteristics (Cont.)

Study	Methodology	Sample	Instrument/Construct	Main finding or contribution
Brahm & Singer, 2013	Subject Matter Experts	2787 organizational participants	Hazard training	Engaging training methods are more effective than non-engaging methods for improving user comprehension.
Blees & Mak, 2012	Survey	85 Dutch and 50 Chinese participants	Cross-cultural pictogram comprehension	Dutch subjects had a better comprehension score and a lower response time than Chinese. A strong correlation between comprehension levels of Dutch and Chinese, thus the same pictorials were easier or harder to understand for both cultural groups.
Caffaro & Cavallo, 2015	Questionnaire	281 owners or users of agricultural machinery	ISO standard for safety signs (ISO 7010:2011) and the ANSI Z535.3-2011	Users comprehended the safety pictograms to some extent, with high variability, but none have complete and exhaustive knowledge of them. Age, education, and occupation did not have any effect on safety pictogram comprehension
Chan & Ng, 2010a	Experiment and questionnaire	60 participants randomly assigned into four equal-sized groups of control, paired-associate learning, recall training, and recognition training	Training evaluation questionnaire	Reported a significant improvement in comprehension, indicating training improved comprehension of safety signs. Recall training improved post-training tests. The recall task-evoked an indebt level of learning compared to the recognition task. Sign characteristics had no significant influence on training effectiveness.

Table 6

Summary of studies on pictogram characteristics (Cont.)

Study	Methodology	Sample	Instrument/ Construct	Main finding or contribution
Chan & Ng, 2010b	Experiment	60 participants	Prospective user factors and cognitive sign features	Prospective user factors and sign features were significantly involved in effectively communicating sign messages.
Duarte et al., 2014	Questionnaire	Adult workers, college students, and persons who have cerebral palsy.	Open comprehensi on testing from ISO 9186 criteria	Participants poorly understood most of the safety signs evaluated. Regardless of each participant's grouping, many of them were unfamiliar with most of the signs and did not understand the meaning of the pictograms or shape- color components.
Davies et al., 1998	Two-part experiment	13 product- related pictograms	Pictogram comprehensi on survey	Reported poor understanding of pictograms, particularly those that are abstract.
Hancock et al., 2005	Experiment	52 young adults (18-23 years) and 47 elderly (65-75 years) participants	Comprehensi on of explicit and implied warnings by the young and elderly	Memory, inferencing ability, and knowledge are important factors in warning comprehension.
Hara et al., 2007	Survey	81 students, 56 company workers, 9 researchers, 47 others (retired employees, homemakers, and doctors)	Recognition tests on labels, pictograms, and SDS	Most subjects who are uninformed on pictograms, responded correctly, implying that pictograms are easy to understand, and using the appropriate pictogram is effective at encouraging proper behaviors. However, the subjects found it difficult to recognize the meanings of labels.

Table 6

Summary of studies on pictogram characteristics (Cont.)

Study	Methodology	Sample	Instrument/ Construct	Main finding or contribution
Hancock et al., 2004	Experiment	104 participants	Phrase generation procedure	Comprehension rates of safety symbols were below 85%, which is recommended by the American National Standards Institute. Individually, older adults scored lower than younger adults. Critical safety information depicted on signs and household products may be misunderstood if it is only presented in pictorial form.
Joshi & Kothiyal, 2011	Empirical study	200 participants	Medication pictograms	Participants did not understand the meaning of pictograms before an explanation, but after an explanation of the pictograms, interpretation of pictograms improved.
Lesch, 2003	Experiment	92 participants recruited through a local newspaper.	Comprehension, age	Significant improvements with comprehension among participants aged between 18 and 35 years.
Lesch, 2008	Experiment	43 participants recruited through a local newspaper.	Comprehension, training	Verbal training improved pictogram comprehension by 30%, and accident scenario training improved comprehension by 36%.
Lui & Hoelscher, 2006	Analytical, descriptive study	166 participants	Graphical symbols - Test methods for judged comprehensibility and comprehension.	Safety signs without a supplementary text have an advantage over safety signs that do, such as high visual effect for influential information transfer, concise informing, and language independence.

Table 6

Summary of studies on pictogram characteristics (Cont.)

Study	Methodology	Sample	Instrument/ Construct	Main finding or contribution
Liu & Ho, 2012	Experiment	30 young participants and 30 elderly participants.	Cluster analysis method	Results indicated that 33.33% of directional symbols in central railway hubs were difficult to comprehend or easy to misunderstand for both older and younger adults. Easily misunderstood symbols increased the time required to follow routes and number of errors. Familiarity had the highest correlation with symbol comprehension performance
Monteiro et al., 2018	Open-ended tests	299 participants	Visual perception of chemical hazard pictograms	Reported inadequate knowledge of hazard pictograms by future engineers.
Ng & Chan, 2007	Experiment	41 participants	Sign design feature guessability	Previous experiences were found to be a significant predictor of guessing performance. Subjects who claimed to pay attention to traffic signs performed better at sign guessing than those who did not. Traffic incident experience did not affect awareness of, or knowledge about, traffic signs. Sign guessability varied with the five design features.
Ng & Chan, 2008	Survey	109 full driver's license holders	Factors and features of sign design	Education is essential to sign comprehension. Concreteness, simplicity, meaningfulness are not the major sign design features.

Table 6

Summary of studies on pictogram characteristics (Cont.)

Study	Methodology	Sample	Instrument/ Construct	Main finding or contribution
Ng & Chan, 2011	Experiment	36 participants	Sign comprehension	Type of training method significantly improved comprehension of sign meaning. Recall training participants performed better in a post-training test than those from paired-associate learning and recognition training. Semantic closeness had a long-lasting effect, in terms of the timescale on traffic sign comprehension, making traffic signs more meaningful after their intended meanings were studied.
Rubbiani, 2010	Survey method	100 participants	Agricultural SDS and labels for risk information	Pictograms were poorly understood. Age and education had no significant effects on comprehension. Although, understanding of pictograms is facilitated by training.
Rother, 2008	Questionnaire	115 farm workers	Comprehension, gender	One out of the ten pictograms provided correct responses. Male participants had more correct responses compared to females.
Smith- Jackson & Essuman- Johnson, 2002	Field survey	31 trade and industry workers	Comprehension	Two out of the six pictograms resulted in more than 50% of correct responses

Table 6

Summary of studies on pictogram characteristics (Cont.)

Study	Methodology	Sample	Instrument/ Construct	Main finding or contribution
Ta et al., 2010	Questionnaire	150 industrial workers	Hazard communication comprehensibility testing tool	Education level and professional experience improved comprehension of pictograms. Although gender and age did not contribute to an individual's comprehension.
Wogalter, Conzola, & Smith-Jackson, 2002	Literature review		Holistic development framework	The article reported guidelines and evaluation approaches of warnings based on literature.
Wogalter et al., 1997	Two-part Experiment	60 undergraduate students	Comprehensibility of Safety Pictorials	Training significantly increased pictogram comprehension. Easy pictograms were comprehended (both initially and following training) better than difficult pictograms. Pictogram comprehension post-training was found to be stable over time.
Walters et al., 2017	Survey	226 participants	Knowledge, Attitude, and Practices (KAP), and safety awareness questionnaire	A high level of awareness among the participants relating to hazard identification and emergency response. High familiarity with pictograms was observed.
Young & Wogalter, 2000	Questionnaire	50 participants	Open-ended comprehension testing	

Table 6

Summary of studies on pictogram characteristics (Cont.)

Study	Methodology	Sample	Instrument/ Construct	Main finding or contribution
Wang & Chi, 2003	Experiment	60 participants	Topcon Screenscope SS-3, Standard pseudo- isochromatic charts, Hazard symbols	Hazardous material pictograms, labels, and training were significant factors of comprehension. Pictogram comprehension among the three educational specializations also showed a significant difference. Comprehension of hazard pictograms and labels increased after receiving training.
Young & Wogalter, 1990	Experiment	64 undergradu ate students	Comprehensi on and memory performance	Pairing pictograms with written warnings may associate the two in memory; this will cue the warning message and facilitate retrieval of information.

Pictogram development

The development of pictograms involves the connection of existing knowledge of individuals, gaining their attention and holding the individual's interest, and presenting the information in a way that promotes recall (Mansoor & Dowse, 2004). Pictograms are composed of two elements: the graphic representation or symbol and the intended meaning or referent (Choi, 2011; Montagne, 2013; Spinillo, 2012). The referent reflects the design and implementation of pictograms (Dowse & Ehlers, 2001); therefore, the referent is dependent on context and culture. Literature reports the use of the stepwise approach in developing and testing pictograms (ISO 9186-1:2014; Montagne, 2013). Firstly, pictogram development begins with indentifying information needs or behavior

changes necessary for the target individual (Montagne, 2013). Secondly, once the intended message is identified, pictograms generated and tested determine whether the proposed pictogram conveys the intended message (Montagne, 2013). Finally, the validation and redesign of the pictograms, as indicated (Montagne, 2013).

Vaillancourt et al. (2018a) and Montagne (2013) developed a comprehensive and iterative pictogram design process for healthcare professionals. Montagne (2013) proposed a pharmaceutical development model and testing for an individual's comprehension and use. The development process followed the stepwise approach for scale development by Devellis (2012). Similarly, Vaillancourt et al. (2018a) took Montagne's (2013) lead and developed a design process for medication safety pictograms that depicted safety issues and high alert drug classes that represented healthcare professionals' risks. Pictograms were developed following an iterative design process to represent medical safety issues previously identified. Furthermore, a Delphi technique survey was conducted with self-identified experts and ended up with nine pharmaceutical pictograms that improved medication safety. Vaillancourt et al. (2018b) followed up with a study that sought to validate the nine previously developed pictograms. The validation process involved a comprehension assessment and recall assessment (Vaillancourt et al., 2018b). Vaillancourt et al. (2018b) reported that participants in the comprehension assessment correctly guessed four of the nine pictograms developed for medication safety; further, during recall assessment, 67% of participants correctly recalled the meanings of seven of the nine developed pictograms.

Table 7

Summary of studies on pictogram development

Study	Methodology	Sample	Instrument/ Construct	Main finding or contribution
Choi, 2011	Literature review	44 articles		Various forms of visual aids, pictograms that use simple line drawings combined with simplified labels are the most efficient and practical tools to improve discharge education.
Dowse & Ehlers, 2001	Interview	46 participants		Low comprehension level of pesticide labels and pictograms. Further, training led to a significant increase in comprehension over time.
Mansoor & Dowse, 2004	Questionnaire	50 total participants (30 – phase 1, 20 – phase 2)	Pictogram sequence	Pictograms were correctly interpreted by 66.7% of participants in phase one and 85% in phase 2. The developed pictograms were considered acceptable based on ANSI and ISO criterion.
Montagne, 2013	Literature review and synthesis	Previous literature in the development of pictograms in several fields.	Pharmaceutical pictograms model for development and testing	Pictograms are essential in redesigning medical information to improve comprehension and recall. Prior training on a pictogram's intended meaning and the use of pictograms increased effectiveness.
Spinillo, 2012	Literature review		Graphic and cultural aspects of pictograms	Culture had a decisive role in the interpretation of pictograms. Pictograms should be developed with the cultural background of individuals in mind.

Table 7

Summary of studies on pictogram development (Cont.)

Study	Methodology	Sample	Instrument/ Construct	Main finding or contribution
Vaillancourt et al., 2018a	Delphi survey	58 participants (32 clinical pharmacists, 20 pharmacy managers, 6 other healthcare professions)	Comprehensive and iterative design process for pictograms	The article developed pictograms to represent each of the previously identified safety issues and underwent an iterative design process. A Delphi survey with self-declared experts from the FIP was conducted to identify international preferences for the pictograms to represent these nine key medication safety issues
Vaillancourt et al., 2018b	Empirical study	101 pharmacy students in phase 1 and 67 in phase 2	Comprehension and recall of safe handling for medications	In phase 1, participants could only guess the meaning of 4 out of the 9 developed pictograms. During phase 2, four weeks later, 67% of participants correctly recalled the meaning of 7 out of the 9 pictograms. Thus showed that training on the meaning of pictograms could increase comprehension of complex information

IS Effectiveness

Scholars have acknowledged the challenges faced with defining and accurately measuring IS effectiveness (Bailey & Pearson, 1983; Doll, Xia, & Torkzadeh, 1994; Lee, Kim, & Lee, 1995). IS effectiveness has been defined as “belief about the level of importance that users hold for IS characteristics” (Levy, Murphy, & Zanakis, 2009, p. 94). Levy (2006) indicates that to measure IS effectiveness entirely, measurements must include the causal factors or values, as well as the resulting construct or user satisfaction

(p. 60). Levy et al. (2009) focused on the importance of the value construct in IS research. Literature indicates that User Satisfaction theory and Value Theory suggests that values influence attitudes that influence behaviors and, influence satisfaction (Levy, 2006, p. 6). Thus, this study addresses perceived effectiveness as a measure of satisfaction and value.

User satisfaction with IS is the extent to which users perceive that the IS available to them meets their user information requirements at the appropriate time (Bailey & Pearson, 1983; Doll & Torkzadeh, 1991; Ives, Olson, & Baroudi, 1983; Kim, 1989; Dooley, 2015). Levy (2006) proposed that satisfaction should be a surrogate measurement of IS effectiveness (p. 42). Researchers have found that user involvement in the development process leads to higher levels of user satisfaction (Bano, Zowghi, & Rimini, 2017). Accordingly, researchers have identified user satisfaction as a strong determinant of effectiveness (Kurucay & Inan, 2017). User satisfaction is an important theoretical issue in IS. However, studies have argued the dimensionality of the construct. Doll et al. (1994) argued for user satisfaction as a one-dimension construct; this is different from Bailey and Pearson (1983), who argued for satisfaction as a bi-dimensional attitude. Thus, the intensity of a users reaction relative to the information requirements must be measured. Bano et al. (2017) confirmed the bi-dimensional construct due to user satisfaction with the involvement process and satisfaction with the delivered product.

Based on the cognitive value theory, “value” refers to the individual’s perceived level of importance (Rokeach, 1969). Rokeach (1973) noted that value is “an enduring belief that a specific mode of conduct or end-state of existence is personally or socially preferable to an opposite or converse mode of conduct or end-state of existence” (p. 5).

The expectancy-value theory describes motivation as a combination of user needs and the value of the goals in the system (Sigaard & Skov, 2015). According to Sedera, Lokuge, Grover, Sarker, and Sarker (2016), the increased value will allow for innovation. For this study, the developed CTC&CS will be considered effective when mobile device users perceive the CTC&CS as highly important, and users are satisfied with the communication methods (Levy, 2006). Levy (2006) utilized a 6-point Likert scale for assessing value; the scale ranged from 'Not important' to 'Extremely important.' Sedera et al. (2016) used a 7-point Likert scale to evaluate enterprise systems and digital platforms' value. Kurucay and Inan (2017) used a 5-point Likert scale to gauge an online course's effectiveness. This study evaluated student satisfaction with e-learning. Thus, this study will utilize a 7-point Likert scale for user satisfaction and value assessment.

Table 8

Summary of studies on Effectiveness

Study	Methodology	Sample	Instrument/C onstruct	Main finding or contribution
Bailey & Pearson, 1983	Survey study	29 questionnaires and 32 manager interviews	7-point scale of satisfaction	IS user satisfaction measurement.
Bano, Zowghi, & Rimini, 2017	Empirical study	Secondary data collected from two case studies and 12 subjects	3-point scale of satisfaction	User satisfaction contributes to system success.
Doll, Xia, & Torkzadeh, 1994	Empirical study	409 participants	End user computing satisfaction (EUCS)	Validation of the EUCS instrument in measuring user satisfaction.

Table 8

Summary of studies on Effectiveness (Cont.)

Study	Methodology	Sample	Instrument/Construct	Main finding or contribution
Doskey, Mazzuchi, & Sarkani, 2015	Experiment	27 competencies	Effectiveness , Bayesian belief network, SE REI	System engineering relative effective index model can be used to measure system engineering performance.
Harrati, Bouchrika, Tari, & Ladjailia, 2016	Experiment	50 lecturers in Computer Science and Electrical Engineering at different universities	System Usability Scale (SUS)	System Usability Scale is not an adequate measure for expressing the true acceptance and satisfaction.
Kurucay & Inan, 2017	Experiment	77 students	24 items using a five-point Likert-scale	The interaction between learners enrolled in online course lead to higher satisfaction.
Lee, Kim, & Lee, 1995	Case study and survey	236 participants from 11 different companies	Satisfaction (EUCS)	The strong positive relationship between end-user IS acceptance, IS satisfaction, and job satisfaction.
Levy, 2006	Experiment	192 student participants	IS effectiveness, LeVIS index, EUCS	Identified and defined the relationship between value and satisfaction to indicate IS effectiveness.
Sigaard & Skov, 2015	Experiment	7 participants	Expectancy value theory	The theory of expectancy-value more directly measures the effect of subjectively perceived value and perception of their capability on information-seeking behavior.
Sedera, Lokuge, Grover, Sarker, & Sarker, 2016	Experiment	189 participating organizations	Effectiveness , 7-point Likert scale	The innovation of digital platforms is possible through the moderation of enterprise system platforms.

Summary what is Known and Unknown

A review was conducted of various aspects of threat classifications, safety data sheets, labels, and pictograms to provide the foundation for this study. This review describes the known and unknown of this study. Through this review of the literature, various classifications and communication methods are reviewed in this section as they relate to cybersecurity for mobile devices.

The classifications identified from literature had shown to either classify threats based on the techniques used by an attacker (Alhabeeb et al., 2010; Alhakami et al., 2014; Bompard et al., 2013; Jouini et al., 2014) or based on the impact of a threat (ISO 7498-2; NIST, 2012; Swiderski & Snyder, 2004). The attack technique approach to threat classification does not consider the impact of the identified threat. The approach based on attack techniques is not appropriate for this study where threats can arise from different agents, i.e., mobile providers, work/personal use environments, environmental and physical threats. Additionally, most threat classifications identified from literature are limited to the use of one or two criteria, provide a non-exhaustive list of threats, and categories that are not mutually exclusive. These limitations would not be enough in environments that are continually changing, such as the use of mobile devices. Additionally, threat classifications have identified threats for several areas: networks, computer systems, information systems, RFID, cryptocurrency, and IoT but are limited to threats classification specifically for mobile devices.

Hazard communications have been developed and tested in several different industries, such as pharmaceuticals, agriculture, chemical, information technology, and crisis communication (Caffaro et al., 2017; Dowse & Ehlers, 2001; Kay & Terry, 2010).

Comprehension testing of safety data sheets, labels, and pictograms have reported mixed results. Safety data sheets and labels have resulted in low or poor comprehension by individuals (Caffaro & Cavallo, 2015; Hara et al., 2007; Rubbiani, 2010; Ta et al., 2010), although the addition of pictograms to safety data sheets and labels have been reported in some studies to improve comprehension levels by individuals (Ng & Chan, 2008; Ta et al., 2010; Walters et al., 2017) while others reported no effects with the addition of pictograms (Chan & Ng, 2010a; Dowse & Ehlers, 2001; Duarte & Rebelo, 2005; Liu, Zhong, & Xing, 2005; Rother, 2008).

Literature has also reported on intrinsic and extrinsic characteristics of pictograms that affect individuals' comprehension (Monteiro et al., 2018). Extrinsic characteristics such as education, age, gender, professional experience, and training reported varying results on each characteristic's significance on comprehension of pictograms. Simultaneously, individuals' cultural background was the only reported characteristic to affect comprehension of pictograms by individuals significantly (Blees & Mak, 2012). Identified from literature are intrinsic characteristics such as familiarity, visibility, concreteness, simplicity, and accuracy. The characteristics of familiarity, visibility, concreteness, simplicity, and accuracy of pictograms were reported to significantly affect comprehension, although familiarity has also been found not to affect pictogram comprehension.

Several industries such as healthcare, pharmaceuticals, chemical, and agriculture have developed pictograms, labels, and SDSs using an iterative design process (Vaillancourt et al., 2018a) and further empirically tested the comprehension of the SDS, labels, and pictograms and the recall ability (Vaillancourt et al., 2018b). Thus, given the use of

pictograms, labels, and safety data sheets in several industries and the related perspective within cybersecurity to inform and protect mobile users from cybersecurity threats, this study will develop pictograms, labels, and safety data sheets within the context of mobile devices and cybersecurity threats.

Chapter 3

Methodology

Overview of Research Design

This study was classified as a developmental research design. The developmental research attempts to answer how the construction of the “thing” addresses a problem (Ellis & Levy, 2009). Developmental research is a way to “create knowledge grounded in data systematically derived from practice” (Richey & Klein, 2007, p. 1). Ellis and Levy (2009) identified three major elements in developmental research: 1) product criteria are established and validated; 2) process for product development is accepted and formalized; as well as 3) determining the product criteria is met through a formalized, accepted process. This approach is appropriate, as seen in its use in the chemical transportation industry (OSHA, 2016). Employers and their workers have seen benefits to the development of hazard communications standards. Such benefits include an increase in quality and consistency of information, improved understanding of chemical hazards as well as better health and safety of workers. Additionally, workers exposed to chemical hazards have access and understand hazard information more efficiently.

Figure 1 illustrates the research design this study followed. Phase 1 utilized an expert-review process following the Delphi technique to validate the initial criteria for the mobile device cybersecurity classification (Ramim & Lichvar, 2014). Experts were recruited from industry, government, and academia that specialize in cybersecurity.

SMEs' expertise was surveyed to identify their experience and job function within their current roles based on the number of years they have worked within their current organizations. Phase 2 operationalized the previously elicited and validated criteria for the mobile device cybersecurity classification into pictograms, labels, and safety data sheets used to assess users' ability to identify and take precautions against cybersecurity threats. Finally, Phase 3 used the previously developed and validated pictograms, labels, as well as safety data sheets to conduct a quantitative study. This research evaluated mobile device users' perceived effectiveness by collecting user satisfaction and value ratings of the pictograms, labels, and safety data sheets.

The main research question of this study was: What is the perceived effectiveness of validated pictograms, labels, and safety data sheets of the most common cybersecurity threats in warning mobile device user's against cybersecurity threats? Mobile device users were evaluated on their satisfaction and value ratings with the developed communication standards to identify the users' perceived effectiveness.

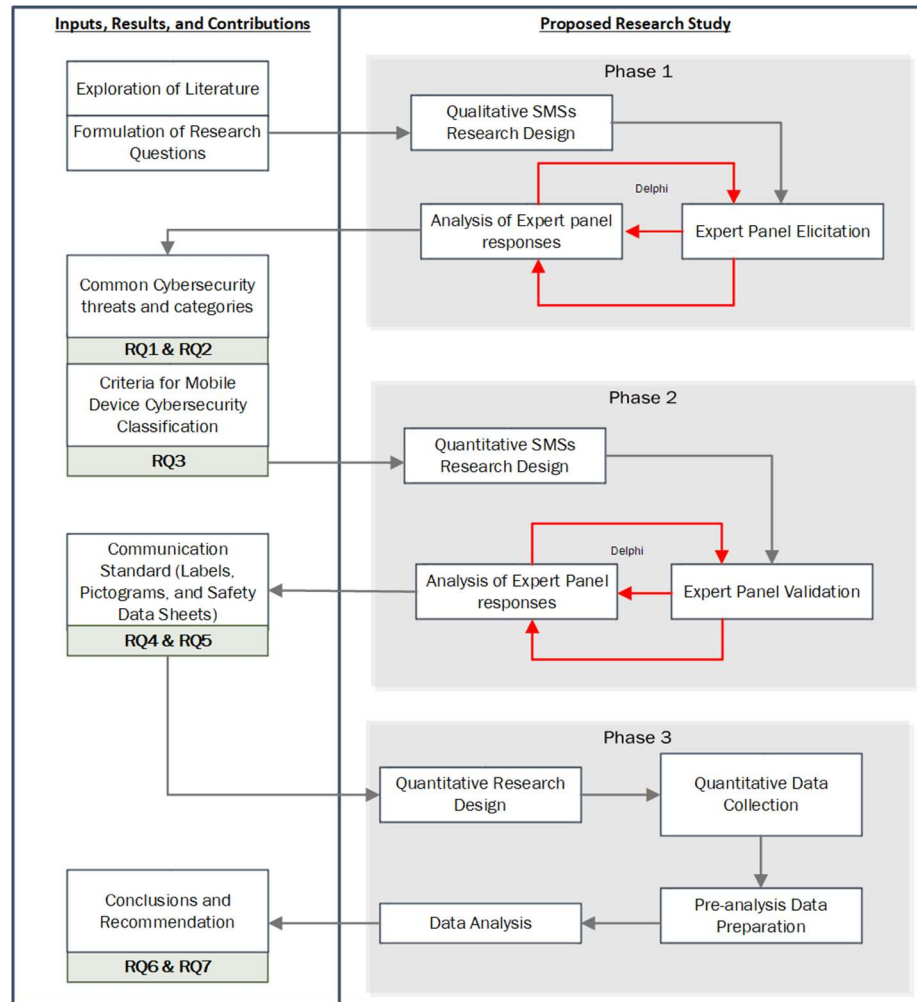


Figure 1. Overview of the Research Design Process

Instrument Development

Expert Panel

Content validity is established with literature reviews, pre-testing, and expert panels (Straub, 1989). An expert Subject Matter Expert (SME) possesses skills (i.e., knowledge, experiences, & abilities) in a field or domain (Lichvar, 2011). Further, expert panels can attest to the viability of measures to include an adequate and fully representative set of items that tap a concept (Sekaran & Bougie, 2013, p. 226). Using the Delphi technique provides a consensus-building method without confrontations among the experts (Dalkey

& Helmer, 1963). The Delphi technique is a group-based iterative communication process that allows experts to address complex issues effectively and efficiently (Okoli & Pawlowski, 2004; Ramim & Lichvar, 2014; Scheele, 1975). Brancheau and Wetherbe (1987), as well as Schmidt, Lyytinen, Keil, and Cule (2001), used the Delphi technique for forecasting, identification of issues, and concept/framework development.

Additionally, the Delphi technique ensures reliability and validity with the exposure of differing and contradictory opinions while seeking convergence through SMEs feedback (Schmidt et al., 2001). This study followed the Delphi technique to ascertain expert opinion on a list of common threats, categories of threats, and classification criteria obtained from literature while also validating the criteria and communication standard (Ramim & Lichvar, 2014).

Anonymity, iteration, controlled feedback, and statistically clustering responses are key features of the Delphi technique (Rowe & Wright, 1999). Maintaining anonymity in this study was done with the set of Web-based survey instruments. Each iteration incorporated feedback from the SMEs responses into the next iteration of the Delphi technique data collection; the Delphi technique will usually iterate through one to six rounds (Worrell, Di Gangi, & Bush, 2013). Once the common cybersecurity threats and categories for mobile devices were identified, classification criteria were developed based on SMEs responses, which will make up the threats classification. Before data collection, the threats, categories, and classification criteria utilized to develop the pictograms, labels, and safety data sheets, were presented to 48 experts in the cybersecurity field for review and validation. Experts for phase one were recruited from academia, industry, and government agencies with deep expertise in cybersecurity threats having academic of

professional experience in cybersecurity. Experts in phase two were recruited from academia and industry with expertise in design. The expert recruitment email notice is available in Appendix B. Changes suggested by the panel were addressed and incorporated. The pictograms, labels, and safety data sheets were presented to the panel as an iteration of the Delphi technique. Carlton and Levy (2015) identified critical cybersecurity threats posed to organizations by non-IT professionals while Brown, Dog, Franklin, McNab, Voss-Northrop, Peck, and Stidham (2016) provided a mobile threat catalog that describes, identifies and structures threats posed to mobile devices. The list identified in Table 9 will be used as a starting point for a list of cybersecurity threats.

Table 9

Cybersecurity Threat Categories

Research	Threat categories
Carlton & Levy, 2015	Work Information Systems (WIS), Malware, Personally Identifiable Information (PII)
Brown et al., 2016	Vulnerable application, Malicious/Privacy-invasive application, Operating System, Mobile Boot firmware, Subscriber Identity Module (SIM) / Universal Subscriber Identity Module (USIM) / Universal Integrated Circuit card (UICC), Device drivers, Isolated Execution Environments, Baseband firmware security, Network Threats, Authentication, Supply Chain, Physical Access, Mobile Ecosystem, Global Positioning System (GPS), Enterprise Mobility Management, Private Mobile Application Stores, Mobile Payment, Cellular infrastructure

Table 10

Proposed mobile cybersecurity threats for CTC&CS

Type of threat	Threats
Physical access threats	<ul style="list-style-type: none"> - Loss or theft of a device. - Malicious charging station. - Unauthorized access to device data. - Data loss through temporary access to an unattended and unlocked mobile device. - Battery damaged from overheating. - Physically swapping a user's SIM with a compromised SIM to run malicious applets. - Theft of SIM card to perform illegal activities such as identity fraud and theft of services.
Threats to software and operating systems	<ul style="list-style-type: none"> - The exploitation of operating system software vulnerabilities to gain escalated privileges. - Deliberate rooting of a device through inherent weaknesses in hardware. - The unintentional installation of malicious apps via USB or an infected computer without the user's knowledge. - The installation of a malicious device management profile. - Use of mobile services that force the device user to place the device into an insecure configuration to use them. - Deliberately unlocking the bootloader through the device user/owner who installs custom operating systems, which then enables the use of the bootloader to install malware. - Exploiting the boot firmware software vulnerability. - Downgrading operating system to an exploitable version. - The exploitation of remote code execution vulnerability, for example, to install unauthorized firmware that enables eavesdropping. - The exploitation of mobile device backups stored on a compromised PC. - Mobile device backups stored on a device or vendor cloud service operating system with unauthorized access. - The exploitation of cloud backups or other cloud file storage performed by individual mobile applications. - A malicious app distributed through a third-party app store. - Installing malicious third-party apps with insufficient security procedures for the checking of application integrity. - The exploitation of app store remote installation capabilities to install malicious apps onto mobile devices.

Table 10

Proposed mobile cybersecurity threats for CTC&CS (Cont.)

Type of threat	Threats
Threats to software and operating systems (Cont.)	<ul style="list-style-type: none"> - Track, locate, or wipe device without consent due to the exploitation of infrastructure or cloud services, e.g., Google's Android Device Manager or Apple's Find my iPhone. - Applications removed from the app store due to security vulnerabilities or dangerous behaviors observed but still present on the mobile device, i.e., zombie apps. - Laws and regulations on the mobile data and device from foreign nations, i.e., lawful intercept, IP, data privacy. - Third-party app store distributing malicious apps. - Unauthorized or unintentional wiping of personal user data from devices. - Achieving code execution by exploiting vulnerabilities in SD cards. - The unauthorized disclosure of data stored on an attached SD card. - Malicious app on the device uses SD card to deliver malicious files to a USB-connected computer.
Authentication threats	<ul style="list-style-type: none"> - Unauthorized disclosure of sensitive data displayed on the device lock screen. - PIN/password brute force. - Computer vision attacks inferring the PIN/password from video recordings. - Inferring the PIN/password from screen smudges. - Inferring PIN through device sensor information. - Android: Spoofing of NFC token or Bluetooth devices that automatically unlock the mobile device, or keeps a mobile device unlocked (e.g., Android Smartlock). - Biometric spoofing. - Theft (Use of authorized credentials). - A malicious application that captures credentials. - Man-in-the-middle network attacker substitutes malicious web site that captures credentials. - Phishing attack via e-mails that link to malicious applications or websites that captures credentials.

Table 10

Proposed mobile cybersecurity threats for CTC&CS (Cont.)

Type of threat	Threats
Application-based threats	<ul style="list-style-type: none"> - Software vulnerabilities in a bank payment application. - Accidental purchase of in-app content. - Host card emulation mobile payment application-level attacks. - Compromise leads to the distribution of rogue / malicious applications. - Links in the app store pointing to fake or malicious versions of an app. - MITM attack providing illegitimate apps when users request legitimate apps. - Use of links or NFC tags, QR codes, or other distribution channels (e.g., SMS, email) to point to malicious apps. - Passive eavesdropping of unencrypted app traffic. - The app exposes sensitive information to untrusted apps. - Malicious code downloaded by visiting a malicious URL. - WebView app vulnerable to browser-based attacks. - Trojan app impersonates a legitimate app, Sending premium SMS messages without user authorization. - The app conducts audio or video surveillance. - App silently intercepts SMS messages. - App evades vetting by loading malicious code at runtime. - App vetting fails to detect malicious app code. - App abuses Device Administrator permission to avoid uninstallation. - Surreptitiously reporting device location. - Malicious app abuses existing root access. - Exploits OS or lower-level vulnerability to achieve privilege escalation. - The app encrypts/encodes and ransoms files. - Malicious app impersonates a legitimate app. - The malicious app exploits device access to enterprise resources. - App provides remote control over the device. - Privacy-invasive behaviors by pre-installed apps. - App entices the user to perform hidden actions in another app. - Consuming device resources to perform computations for the attacker. - Malware uses a device to conduct DDoS attacks. - A malicious app captures the raw screen buffer. - The app records audio by stealthily placing or answering phone calls. - Malware avoids detection by uninstalling itself.

Table 10

Proposed mobile cybersecurity threats for CTC&CS (Cont.)

Type of threat	Threats
Cellular-based threats	<ul style="list-style-type: none"> - Air Interface Eavesdropping. - Rogue base station that can track devices. - Downgrade Attacks via Rogue Base station. - Jamming Device Radio Interface. - Jamming Base Station Radio Interface. - Voicemail hacking using default PINs. - Lack of caller ID information authentication. - DoS caused by text messages sent to the device or an application. - Eavesdropping on unencrypted message content. - Device enumeration and fingerprinting via silent SMS. - DoS via sending thousands of silent messages.
GPS based threats	<ul style="list-style-type: none"> - Device jamming that prevents proper use of location services. - Spoofing, which may allow an attacker to confuse or control the location at which a mobile device calculates its position.
Network-based threats	<ul style="list-style-type: none"> - NFC Payment replay attacks. - Compromised mobile payment terminal. - Enrollment of credit/debit card without cardholder authorization. - Rogue access points. - Wi-Fi SSID Tracking. - Eavesdropping. - Hotspot hijacking. - Client MAC address tracking. - Signal jamming. - Bluebugging. - Sending unsolicited messages to a mobile device through Bluetooth (Bluejacking). - Secure Simple Pairing attacks. - Pairing eavesdropping attacks. - Blueprinting - remotely fingerprint Bluetooth-enabled devices. - BlueStumbling discovers, locate, and identify users based on their Bluetooth device addresses. - Bluesnarfing - gives an attacker full access to calendar, contacts, e-mail, and text messages. - Man-in-the-middle by relaying NFC packets. - Malicious NFC tags. - Use of ultrasonic beacons to track device location and/or user behavior.

CTC&CS development

The CTC&CS includes the developed communication standards in the form of pictograms, labels, and safety data sheets to provide mobile users with warnings of cybersecurity threats. The purpose of the CTC&CS is to systematically identify cybersecurity threats, draw the user's attention to those threats, and enable them to take protective actions as appropriate. The development of cybersecurity threat communication tools has several significant issues, the most crucial being comprehensibility of the information provided. The literature review provides some guiding aspects of developing communication tools. Firstly, the information should be conveyed in more than one way. Secondly, the comprehensibility of the system's components should take account of existing studies and literature, as well as any evidence gained from testing (United Nations, 2011). Lastly, the phrases used to indicate the degree (severity) of threat should be consistent across the categories of threats (UNCE, 2009). The chemical industry has standardized its label elements that are directly related to the endpoints of the hazard level of chemicals. The chemical industry's standard label elements include symbols (pictograms), signal words, and hazard statements.

The researcher developed the pictograms, labels, and safety data sheets specific to mobile threat categories and threats, as appropriate. This standard makes it easier for users of different knowledge backgrounds to implement the system. Pictograms include threat symbols plus other graphic elements, such as borders, background patterns, or colors, which are used for the intention to convey specific information (UNCE, 2009).

Signal words indicate the degree of severity of a threat. Signal words used in chemical labeling are "Danger," which denoted more severe threats, and "Warning" for less severe

threats. Signal words will be standardized and assigned to hazard categories. Threat statements are standardized then further assigned phrases that describe the threat(s) as determined by the classification. Other elements in labels include precautionary statements as well as pictograms, product identifiers, supplier identification, and supplemental information. Where cybersecurity threats present more than one classified threat, a precedence scheme for pictograms and signal words will be followed, i.e., if the signal word “Danger” applies, the signal word “Warning” should not appear. All assigned threat statements will appear on the label with the specified order on how they appear. Cybersecurity threat pictograms, signal words, and hazard statements will be located together on the label. See Figure 2.

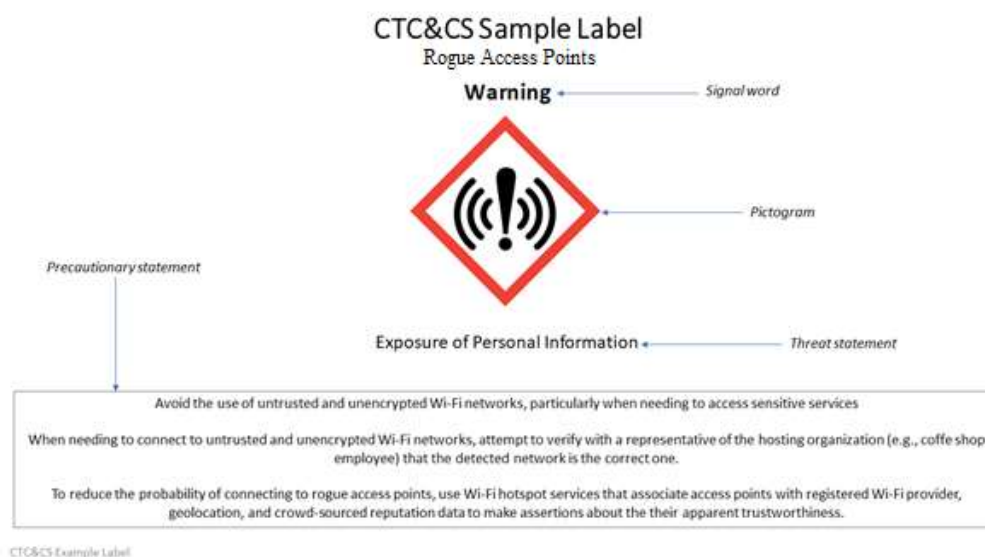


Figure 2. Sample Label (Wifi warning)

Safety Data Sheets (SDS) provides comprehensive information about the use of chemicals (UNCE, 2009). They are a vital source of information for employers and workers on threats. The SDS provides a source of information about threats and obtains advice on safety precautions. Furthermore, SDS gives organizations the ability to develop

working protection measures and training that are specific for their organization and consider measures necessary for protection. The SDS should provide a clear description of the data used to identify the threats. The SDS would follow the minimum information needed on an SDS from the chemical industry. All threat communication systems should specify a means of responding in an appropriate and timely manner to new information, as well as updating labels and SDS information accordingly. See Appendix A for a sample SDS. Initially, use of SDSs only covered the manufacturing industries, but over time, its use has extended to cover other work environments (Ahmed, Naji, & Tseng, 2020). Furthermore, the use of SDSs has not only been implemented in the USA but also in Europe and Canada (Ahmed, Naji, & Tseng, 2020).

The development of pictograms, labels, and SDS went through an iterative process and designed between three to five pictograms for each of the main validated categories and threats from phase one of this study. Graphic designers were employed to design the communication standard. General ideas for the initial designs of the communication standards were provided to the graphic designers. Upon completion, an online survey was sent to a panel of 43 graphic designers to solicit feedback on the pictograms, labels, and safety data sheets.

User-perceived effectiveness of CTC&CS

Once the CTC&CS pictograms, labels, and safety data sheets were developed based on SME agreement on pictograms, labels, and safety data sheets, the perceived effectiveness of the developed communication methods was tested. Identifying the perceived effectiveness of the developed pictograms, labels, and safety data sheets were performed with non-IT professional. Hong, Tai, Hwang, Kuo, and Chen (2017) utilized

determinants of satisfaction and utility value within 150 questionnaires to determine the effectiveness of using government e-learning systems. IS effectiveness has been difficult to evaluate. By examining the satisfaction and value of specific cybersecurity threat communication standards, the pictograms' perceived effectiveness, labels, and safety data sheets can be determined (Doll, Xai, & Torkzadeh, 1994; Levy et al., 2009). For this study, effectiveness was measured by obtaining users' perceived value and satisfaction (Levy, 2006; Levy et al., 2009). The survey in Appendix E was administered to mobile device users to obtain ratings for the satisfaction and value of the developed communication standards. The survey consisted of a 7-point Likert scale assessing each communication standard. The survey was administered using the online tool, Google forms.

Reliability and Validity

Reliability

The CTC&CS was developed to provide mobile users with warnings and steps to remedy cybersecurity threats incorporated into pictograms, labels, and safety data sheets. A cybersecurity security classification should respect the following principles: Mutual exclusivity; every threat is classified in one category and excludes all others, exhaustiveness; all possibilities must be included in each category, unambiguous; all categories must be clear and precise so that classification is specific (Alhabeeb et al., 2010). Categories should be based on unambiguous classification criteria that define what threats to be placed in that category. Repeatable, so that repeated applications result in the same classification, regardless of who is classifying. Accepted, which makes specific categories logical, intuitive and practices easy to be accepted by the majority, and useful,

so that insight into the field of inquiry can be gained and adapted to different application needs (Jouini, Rabai, & Aissa, 2014). These principles will be used to evaluate the cybersecurity threat classification. A proper classification should support the most presented principles (Amoroso, 1994; Farahmand et al., 2005; Gordon, Loeb, Lucyshyn, & Richardson, 2005; Howard, 1997). The threats, categories, and classification criteria were tested for reliability through an expert panel using the Delphi technique. Upon developing the communication standards, each pictogram, label, and safety data sheet were validated through an expert panel using the Delphi technique and increasing reliability.

Validity

Internal validity, according to Straub (1989), stated: “whether the observed effects could have been caused by or correlated with a set of non-hypothesized or unmeasured variables” (p. 151). Straub (1989) suggested that “internal validity in Management Information Systems (MIS) research can be maximized by an investigation of all the appropriate constructs and variables related to the studied phenomenon” (p. 151). In establishing internal validity, the research attempts to rule out alternative explanations (Straub, Boudreau, & Gafen, 2004). This study gathered data from an expert panel before the development of a final survey instrument to minimize internal validity threats.

External validity concerns the generalized nature of study findings to other populations (Sekaran, 2003). Researchers have suggested that studies’ results can be generalized to specific persons, groups, and times (Cook & Campbell, 1979; Jouini et al., 2014). Results can also be generalized across targeted groupings. This research focused on efficiently communicating cybersecurity threats to mobile users. The researcher

developed an instrument to standardize cybersecurity threat communications that can be generalized to represent end-users in general.

Instrument validity examines the validity of the content and constructs (Levy, 2006). According to Straub (1989), an instrument is considered valid or invalid based on the content of the items being measured and whether they comprehensively represent the construct. Additionally, Straub (1989) argued that research findings might be better substantiated with instrument validation. Straub (1989) recommended that qualitative and quantitative research methods be used to validate instruments to ensure the instrument is not obstructing accurate data collection. Content validity was facilitated through a review of existing literature and iterative feedback from a panel drawn from a representative sample of cybersecurity and graphic design experts.

Perceived Effectiveness

Once the communication methods in the forms of pictograms, labels, and safety data sheets were developed, the effectiveness was determined. Mobile users' satisfaction and value of the pictograms, labels, and safety data sheets were measured. Rating the value measure is beneficial compared to ranking characteristics; this allows participants to denote equal value characteristics if one did not outweigh the other (Levy, 2004). The perceived effectiveness of the CTC&CS was determined using the combination of users' perceived value and satisfaction to indicate the level of the CTC&CS effectiveness (Levy, 2006; Dooley, Levy, Hackney, & Parrish, 2017). By presenting the communication methods to mobile device users, the perceived effectiveness can be evaluated.

Population and Sample

This study evaluated the perceived effectiveness of 208 non-IT professionals using the CTC&CS. Non-IT professionals included any person who performs personal or work-related functions using a mobile device that does not work in an IT-related field. These non-IT professionals included but were not limited to office assistants or managers. IT or technical service professionals are excluded as the focus of this study was on the general population. With the use of demographic data, the sample was tested to view a representation of the collected data to the generalized study population (Sekaran & Bougie, 2016). Further, categorical demographic data were collected to assist in identifying the characteristics of the participants (Terrell, 2012). Therefore, demographic data, such as age, gender, cultural background, and job function, were collected as part of this study.

Data Collection

With the use of the developed and validated pictograms, labels, and safety data sheets, mobile device users were evaluated on their perceived effectiveness with the communication methods. Pictograms, labels, and safety data sheets were presented as part of the survey, and the participants rated the level of satisfaction for each communication method on a 7-point Likert scale from “Extremely unsatisfied” to “Extremely satisfied.” Likewise, participants rated each communication’s method’s level of importance on a 7-point Likert scale from “Not important” to “Extremely important.”

Pre-analysis Data Screening

Pre-analysis data screening involves the process of detecting and dealing with irregularities or problems with collected data (Levy, 2006) and may also be an indicator

that the developed tool is not performing as expected. According to Mertler and Vannatta (2010), data must be checked for accuracy and consistency. Rigorous data examination must be completed before the final data analysis as missing data may create substantial effects (Alias, 2015; Hair, Black, Babin, & Anderson, 2010). Missing data were evaluated before and during the final analysis of data to ensure a consistent, valid, and reliable tool (Levy, 2006; Onwuegbuzie et al., 2010).

Data Analysis

Findings of the data collected from the literature review, expert panel, and the tests of the CTC&CS user-perceived effectiveness was used to develop a valid and reliable assessment of the use of the CTC&CS in warning users. Furthermore, an empirical investigation using the CTC&CS was conducted to evaluate the user-perceived effectiveness of the CTC&CS. The iterative processes lead to increased instrument fidelity as well as reliability and validity (Alais, 2015; Onwuegbuzie et al., 2010). Using the literature and expert panel, the identification of common threats, categories of threats, and criteria for classification, this study addressed RQ1, RQ2, and RQ3. RQ4 and RQ5 were addressed by using literature review and an expert panel for establishing pictograms, labels, and safety data sheets for each category identified. To address RQ6, quantitative data analysis was performed to obtain mobile users rated effectiveness based on quantified research analysis. Finally, RQ7 was addressed by quantitatively evaluating for the perceived effectiveness based on (a) age, (b) gender, (c) years of education, (d) years of work experience, and (e) years of mobile device use.

Resources

IRB approval was obtained to work with human subjects (see Appendix F). Access to cybersecurity experts was required to follow the Delhi method expert panel process. An online survey tool, Google form that is accessible via the Internet, was used to collect participant data. This study followed IRB standards of data collection. The participants were informed that their participation is voluntary; their anonymity is protected; the survey's completion is not required and can stop at any time. Additionally, there were no requests for personal or sensitive information. Following data collection, SPSS was used to analyze the data.

Summary

Chapter three included an overview of the research design and methodology. This study was classified as a developmental study and used a sequential exploratory approach to validate the CTC&CS. The threats classification and communication methods were developed using a literature review, in addition to feedback by an expert panel. Feedback from SMEs was used to revise the CTC&CS until a consensus is reached using the Delphi technique. Finally, chapter three concludes with the resources used to carry out the research.

Chapter 4

Results

Overview

This chapter presents the results of the data collection and data analysis performed in the study. The main goal of the study was to design, develop, and empirically test a set of criteria, which enables the validation of a Cybersecurity Threats Classification and Communication Standard (CTC&CS) for mobile devices. The study used a three-phased approach to address the set of research questions. Data collection and analysis for Phase one used SMEs through the Delphi technique, identified, as well as validated mobile device cybersecurity threats and cybersecurity threat categories. Data collection and analysis for Phase two operationalized the identified cybersecurity threats as well as threat categories and validated the designed with SME using the Delphi technique. Phase three involved the main data collection and analysis that included the response rate, pre-analysis data screening, description of this study participants, results of the calculated perceived effectiveness, system usability scale, and ANCOVA. This chapter concludes with an overall summary of the results of this study.

Expert Panel – Phase One (RQ1, RQ2, & RQ3)

This study employed the Delphi technique to identify the expert opinion of cybersecurity threats, common threat categories, as well as produce a classification based on cybersecurity threats and categories. The Delphi technique is an iterative group communication process that allows experts to address complex problems effectively and

without confrontation (Dalkey & Helmer, 1963; Okoli & Pawlowski, 2004; Ramim & Lichvar, 2014). Anonymity was maintained in this phase of the study through the use of a Web-based survey (Rowe & Wright, 1999). Between each inquiry, SME responses were incorporated into the following survey to control the feedback. The survey instruments were designed electronically using Google forms.

The first round of the Delphi technique consisted of 11 cybersecurity threat categories and 104 cybersecurity threats obtained from a survey of the existing body of knowledge. These threat categories and cybersecurity threats were identified and presented to SMEs; each cybersecurity threat was matched to one of the 11 categories. The 11 categories and 104 cybersecurity threats were presented to SMEs in a Web-based survey using a 7-point Likert scale. Based on a score of '1' for strongly disagree and '7' for strongly agree, each threat category and cybersecurity threat were evaluated to determine its validity to be included in the core set of categories and cybersecurity threats. Based on SME feedback, the list of 11 threat categories and 104 cybersecurity threats were narrowed to six threat categories and 85 cybersecurity threats. In the second Delphi technique round, the six threat categories and 85 cybersecurity threats identified as significant in the first round of the Delphi technique were then presented to SMEs using the same 7-point Likert scale survey. Each threat category and cybersecurity threat were evaluated to determine if they were valid to be included in a cybersecurity threats classification if the categories and threats are valid or not. To answer RQ1, RQ2, and RQ3, the survey was sent to 39 SMEs in each round of the Delphi technique. Responses were obtained from 26 SMEs in round one, and 22 responses in round two were received for a response rate of 66.7% and 56.4%, respectively.

Pre-analysis Data Screening

Pre-analysis data preparation did not identify any SME responses that needed to be removed. No incomplete data sets were submitted, as designed due to all survey items being set as required during the instrument's development.

Demographic data analysis

Upon completing the pre-analysis data preparation, a demographic analysis was conducted on the collected data to assess the sample. Phase one accomplished the goal of ensuring the expertise of respondents. A summary of the demographic data is shown in Table 11.

Table 11

Summary of Phase One Demographics of the SMEs (N=48)

Item	Round One		Round Two	
	Frequency	%	Frequency	%
Age				
21 - 30	1	3.8%	0	0.0%
31 – 40	9	34.6%	11	50.0%
41 – 50	14	53.8%	9	40.9%
51 - 60	2	7.7%	2	9.1%
Gender				
Female	7	26.9%	5	22.7%
Male	19	73.1%	17	77.3%
Education Level				
Masters	13	50%	7	31.8%
Doctorate	13	50%	15	68.2%

Table 11

Summary of Phase One Demographics (N=48) (Cont.)

Item	Round One		Round Two	
	Frequency	%	Frequency	%
Position at the Organization				
Supervisor	2	7.70%	1	4.50%
Manager	11	42.30%	5	22.70%
Director/VP	2	7.70%	4	18.20%
C-level	3	11.50%	4	18.20%
Academic	8	30.8%	8	36.4%
Work Sector				
Federal government	2	7.70%	2	9.10%
Academia	10	38.50%	14	63.60%
Private/Industry	14	53.80%	6	27.30%
Years of Experience				
5 – 10	1	3.80%	1	4.50%
11 – 15	3	11.50%	7	31.80%
16 – 20	12	46.20%	12	54.50%
21 and greater	10	38.5%	2	9.1%

Data Analysis

The consensus of SMEs' opinion emerged with six categories (Application, Authentication, Cellular, LAN & PAN, Payment, Physical access) and 62 cybersecurity threats. The average rating of the SMEs' responses for each category was calculated so that categories with less than 70% agreement or a rating of less than five were removed while a rating of 70% or higher or five or more was retained. The level of 70 of each category was computed using the average rating given by the SMEs. Payment threats were identified as the most severe receiving an average of 6.92, while cellular threats

averaged the lowest with a rating of five. The table below displays the collective results of both Delphi rounds identifying the agreed upon threat categories, which are arranged by level of severity with Payment threats being the most severe. Appendix G displays the consolidated results identifying the agreed upon threats arranged within the respective categories of threats.

Table 12

Summary of Threat categories

Threat Categories	Rated 5 or higher	Average
Payment threats	100%	6.92
Application threats	100%	6.88
Authentication threats	100%	6.65
LAN & PAN threats	100%	6.46
Physical access threats	84.6%	5.46
Cellular threats	78%	5

Expert Panel – Phase Two (RQ4 & RQ5)

The classification and validation of a cybersecurity threats classification for mobile devices was a positive step for this study. At the beginning of phase two and using the results of phase one as a foundation, operationalization of the six categories and their cybersecurity threats into pictograms, labels, and safety data sheets was made. Each communication standard was designed in this study to include two to three cybersecurity threats from each of the categories identified in phase one.

Students studying graphic design or a similar course were employed to design the communication standard. In order to ascertain general ideas for the initial designs of the communication standards, the graphic designers were provided with firstly, standardized design rules from OSHA and ISO, secondly, the categories and threats from phase one

and finally, the commonly used graphic elements that depict or could depict each of the identified cybersecurity threat categories from phase one. The graphic designers developed two to three pictograms for each of the identified categories and one label and safety data sheet for each category.

Upon completing developing the pictograms, labels, and safety data sheets, a survey was sent to a panel through Google surveys to solicit feedback on the pictograms, labels, and safety data sheets. Recommendations of the SMEs' were incorporated into the communication standards before the second round of the Delphi technique. The SMEs were asked to review the communication standards again after revisions, at which time the original feedback and adjustments were validated. After round two of the Delphi technique, a consensus of SMEs' opinion was reached regarding the design and presentation of pictograms, labels, and safety data sheets. Thus, no additional iterations with the panel were required. The Delphi technique reinforced the validity of the communication standards. Out of the 40 invitations to participate, 24 responded, generating a 60% response rate. Thus, RQ3 and RQ4 were addressed with the operationalization of the classification categories and cybersecurity threats with the developments of the pictograms, labels, safety data sheets, and the validation through the Delphi technique.

Pre-analysis Data Screening

Pre-analysis data screening of phase two did not identify any SME responses that needed to be removed. Survey submission was complete as designed due to survey items being required during the development of the instrument.

Demographic Data Analysis

Pre-analysis data preparation and a demographic analysis were conducted on the collected data to assess the sample. A summary of the demographic data is shown in Table 13.

Table 13

Summary of Phase Two Demographics (N = 43)

Item	Round One		Round Two	
	Frequency	%	Frequency	%
Age				
21 - 30	17	70.8%	15	78.9%
31 – 40	5	20.8%	4	21.1%
41 – 50	2	8.3%		
Gender				
Female	14	58.3%	11	57.9%
Male	10	41.7%	8	42.1%
Education Level				
Masters	7	29.2%	16	84.2%
Bachelors	17	70.8%	3	15.8%
Position at the Organization				
Student	3	12.5%	0	0.0%
Entry level	5	20.8%	3	15.8%
Supervisor	12	50.0%	9	47.4%
Manager	2	8.3%	5	26.3%
Academic	2	8.3%	2	10.5%
Work Sector				
Academia	5	20.8%	2	10.5%
Private/Industry	19	79.2%	17	89.5%

Table 13

Summary of Phase Two Demographics (Cont.)

Item	Round One		Round Two	
	Frequency	%	Frequency	%
Work Sector				
Academia	5	20.8%	2	10.5%
Private/Industry	19	79.2%	17	89.5%
Years of Experience				
1 – 4	7	29.2%	2	10.5%
5 – 10	12	50.0%	13	68.4%
11 – 15	5	20.8%	4	21.1%

Data Analysis

The feedback received in phase two of this study included minor changes to colors used in pictograms and sections' visual arrangement within a label and the safety data sheet. To attest to the development of the communication tools, an SME comments elaborated on the creativity and design. Based on the feedback, minor changes to the pictograms, labels, and safety data sheets were performed, leading to the final version of the survey instrument for distribution in this study. Thus, phase two's feedback indicated that the pictograms, labels, and safety data sheets, evaluated by the phase two participants, met the acceptance criteria of having achieved a rating of five or higher by 70% of the participants. No additional iterations with the expert panel were required. The Delphi technique reinforced the validity of the developed pictograms, labels, and safety data sheets and answered research questions four and five.

Main Data Collection – Phase Three (RQ6 & RQ7)

Phase one of this study collected data from information security professionals; data was collected from graphic design professionals during phase two. For Phase three of this study, data collection was conducted mid-April 2020 to early May 2020. The following sections detail the data collection process for Phase three.

Pre-Analysis Data Screening

In Phase three, participants were recruited through a participation invitation sent through email and LinkedIn. The targeted population was non-IT professionals. Non-IT professionals included any person who performs personal or work-related functions using a mobile device and does not work in an IT-related field. The final survey instrument was sent to 683 participants. Responses from 208 were received, constituting a response rate of 30%.

Before data analysis, pre-analysis data screening was performed on the data collected from the participants. Participant responses were collected with the use of Google Forms[®], a web-based tool. This tool allowed for technical restrictions to form submissions without completing all questions. This ensured completeness during the data collection, thus, impeding partial submissions. Elimination of cases, verification of missing data, and addressing extreme cases or outliers was performed in the pre-analysis data screening to ensure the accuracy of the data collected (Levy, 2006).

Data accuracy was not a matter of concern as the survey was designed to receive a single valid answer for each question. Once collected, completed responses were downloaded and imported into SPSS for further pre-analysis data screening. The data was analyzed for any response set issues; no response-set cases appeared. Respondents were

required to select from a fixed set of answers and were unable to leave any items unanswered. However, to ensure the data's accuracy, descriptive statistics identified the minimum and maximum values for the responses to determine if responses were within the expected value range and were not accidentally corrupted during the transfer of data between Google forms and SPSS. All responses were within the expected ranges, and none were removed. Thus generating 208 responses constituting a 30% response rate for analysis.

Demographic Analysis

After completing the pre-analysis data screening, 208 responses remained for analysis, with demographics that represent a likeness to that of the general sample targeted. Of these, 89 or 42.8% were females, and males completed 119 or 57.2%. Overall, 190 or 91.3% had five or more years of work experience, and 138 or 66.3% use their mobile device for work-related activities. An analysis of the participants' education level revealed that 28 or 13.5% had a high school degree, 16 or 7.7% had an associate degree, 110 or 52.9% achieved a bachelor degree, 52 or 25% received a master degree, and 2 or 1% received a doctorate. Moreover, 168 or 80.8% of the participants indicated having 1 to 3 years of experience with cybersecurity while 21 or 10.1% indicated having 4 – 6 years of experience, and 19 or 9.1% indicated no experience with cybersecurity. Table 14 displays the details of the demographics of the population.

Table 14

Summary of Phase Three Demographics (N= 208)

Item	Frequency	%
Age		
19 - 24	10	4.8
25 - 29	52	25.0
30 - 34	34	16.3
35 - 39	36	17.3
40 - 44	34	16.3
45 - 54	26	12.5
55 - 59	16	7.7
Gender		
Female	89	42.8
Male	119	57.2
Education		
High School	28	13.5
Associates	16	7.7
Bachelors	110	52.9
Masters	52	25.0
Doctorate	2	1.0
Work Experience		
Under 1	11	5.3
1 - 4	7	3.4
5 - 10	97	46.6
11 - 15	42	20.2
21 and greater	51	24.5
Years of device use		
Under 1	2	1.0
1 - 3	16	7.7
4 - 6	48	23.1
7 - 9	45	21.6
10 and more	97	46.6
Cybersecurity experience		
1 - 3	32	15.4
4 - 6	138	66.3
7 - 9	1	0.5
None	37	17.8

Data Analysis

After the pre-analysis data screening and the demographic analysis were completed, the perceived effectiveness ratings and analysis of covariance (ANCOVA) were used to assess RQ6 and RQ7, respectively. The data for the level of satisfaction and the value/importance was analyzed to determine the respective perceived effectiveness. To address RQ6, what is the users' perceived effectiveness (i.e., satisfaction & value/importance) of pictograms, labels, and safety data sheets in warning mobile device users against cybersecurity threats? After viewing the developed pictograms, labels, and safety data sheets, participants were presented with a 7-point Likert rating scale for satisfaction and value/importance to assess each of the items. Each item's satisfaction and value/importance were calculated to determine the users' perceived effectiveness (Levy, 2006). Perceived effectiveness was determined using the geometric mean and the formula below. The value of 49 is used to normalize the effectiveness output. This is based on the multiplication of the maximum ratings of satisfaction and value/importance scales. See Figure 3 for the formula used. Figures 4, 5, and 6 summarize the ratings of satisfaction, value/importance, and effectiveness, respectively.

$$\left(\frac{1}{n}\right) \cdot V_o \cdot S_o \Rightarrow \left(\frac{1}{49}\right) \cdot V_o \cdot S_o$$

Figure 3. Effectiveness Formula



Figure 4. Final list of pictograms

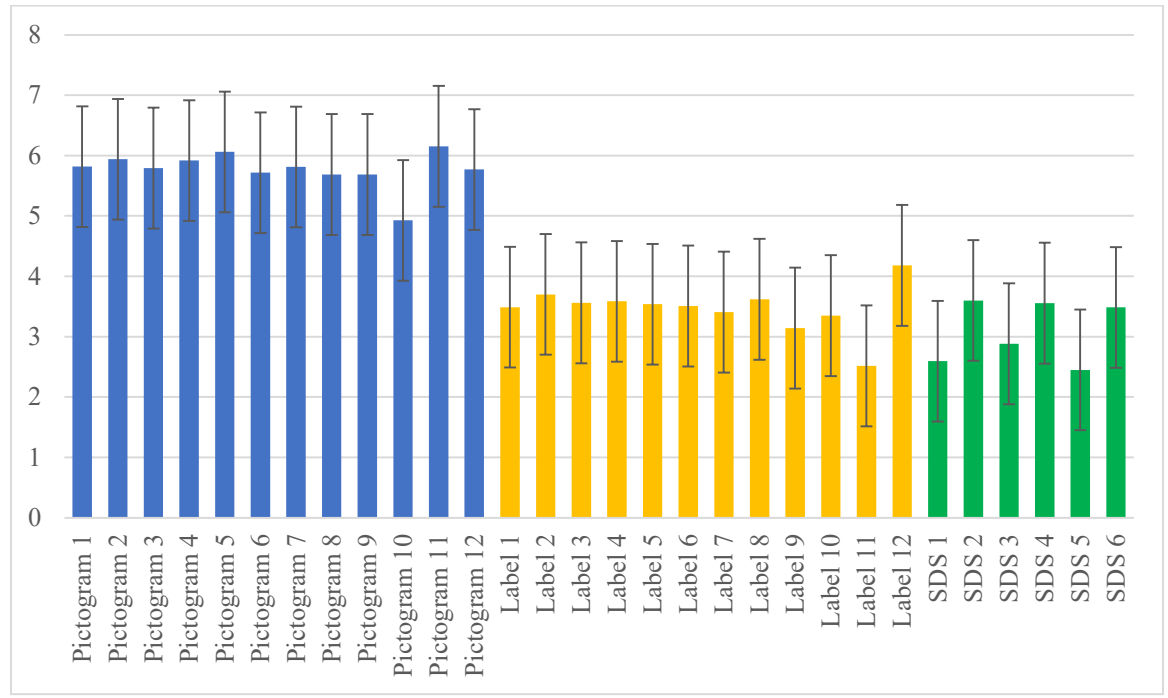


Figure 5. Satisfaction means (N= 208)

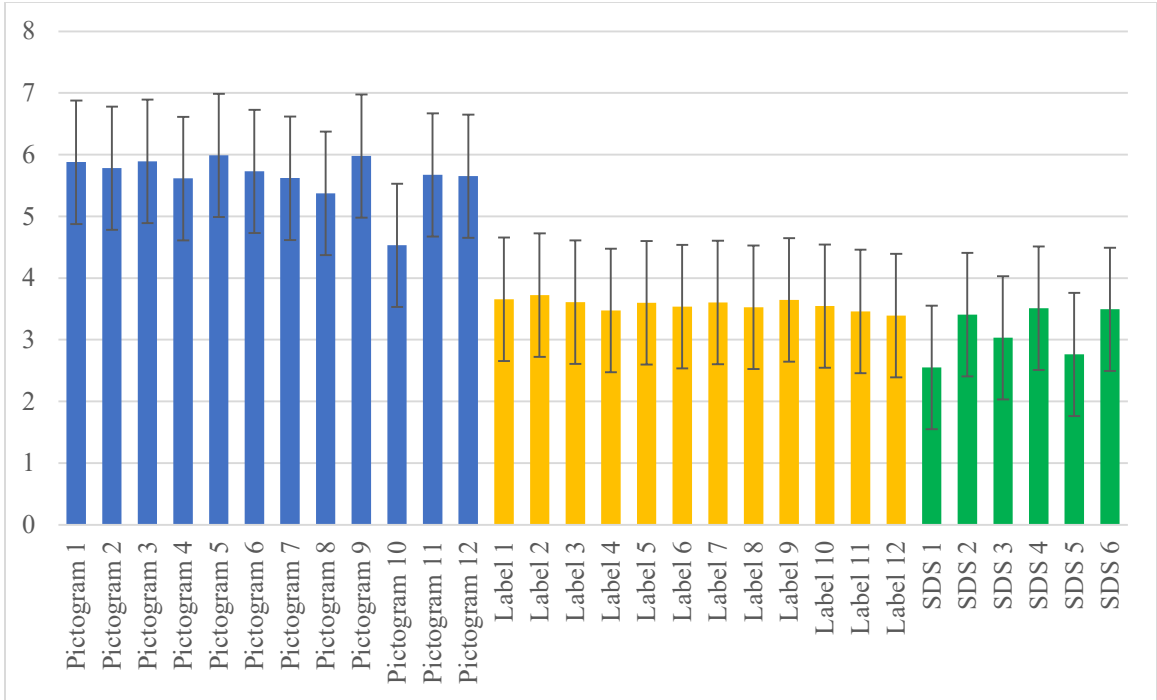


Figure 6. Value means (N= 208)

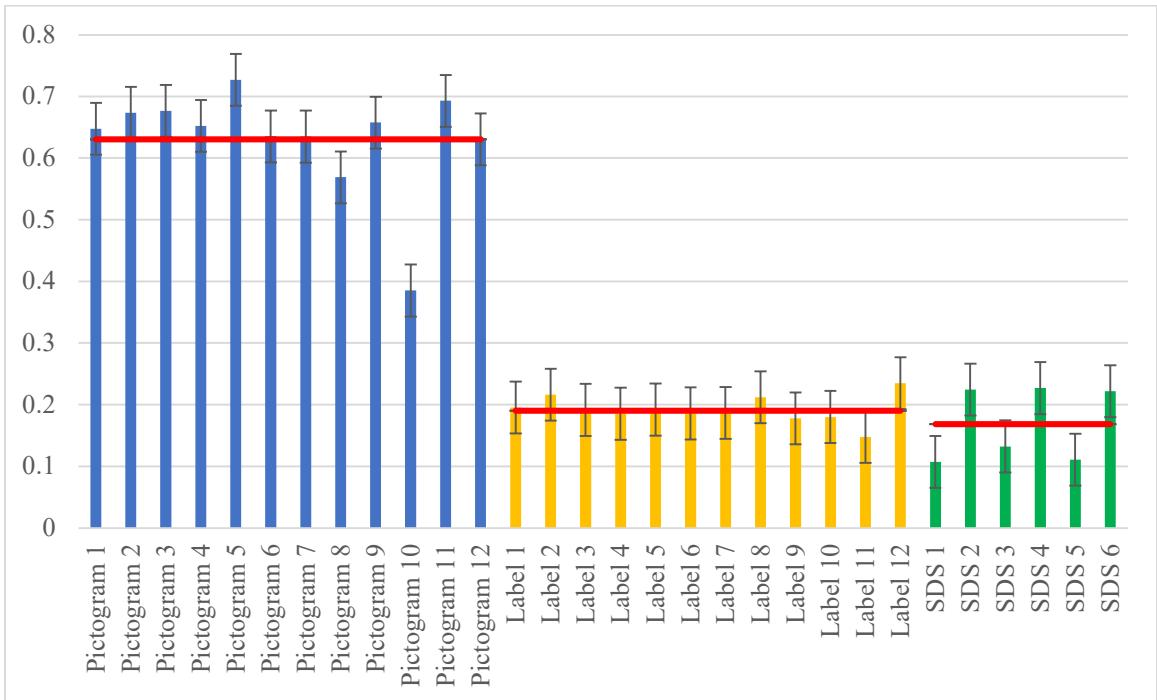


Figure 7. Effectiveness means (N= 208)

Furthermore, the modified System Usability Scale (SUS) statements were extracted for analysis (Bangor, Kortum, & Miller, 2008) to provide an adjective rating that correlates an acceptable SUS score of 68 or above. The statements alternate between positive and negative statements. Therefore, the raw SUS score was calculated based solely on the 10 SUS statements within the main survey instrument. The odd-numbered questions from the SUS express positive attitudes while even ones negative. The SUS score was calculated by subtracting one from the user responses to odd statements and subtracting corresponding values from five from even-numbered statements. Then adding all the participants' responses and further multiplying the total by 2.5 will provide a range from 0 – 100. Appendix H represents the SUS score for the 10 items based on participant responses. Appendix I represents the inflated score between 0 and 100 and the corresponding adjective rating based on participant responses. Table 15 and figure 8 produce a summary of the SUS results.

Table 15

Summary of SUS scores (N= 208)

# of respondents	SUS Score	Percentile range	Adjective
7	84.1 - 100	96 - 100	Best Imaginable
11	80.8 - 84.0	90 - 95	Excellent
8	78.9 - 80.7	85-89	Excellent
5	77.2 - 78.8	80-84	Excellent
14	74.1 – 77.1	70 – 79	Excellent
0	72.6 – 74.0	65 – 69	Excellent
15	71.1 – 72.5	60 – 64	Good
64	65.0 – 71.0	41 – 59	Good
0	62.7 – 64.9	35 – 40	Good
73	51.7 – 62.6	15 – 34	OK
11	25.1 – 51.6	2– 14	Poor
0	0-25	0-1.9	Worst Imaginable

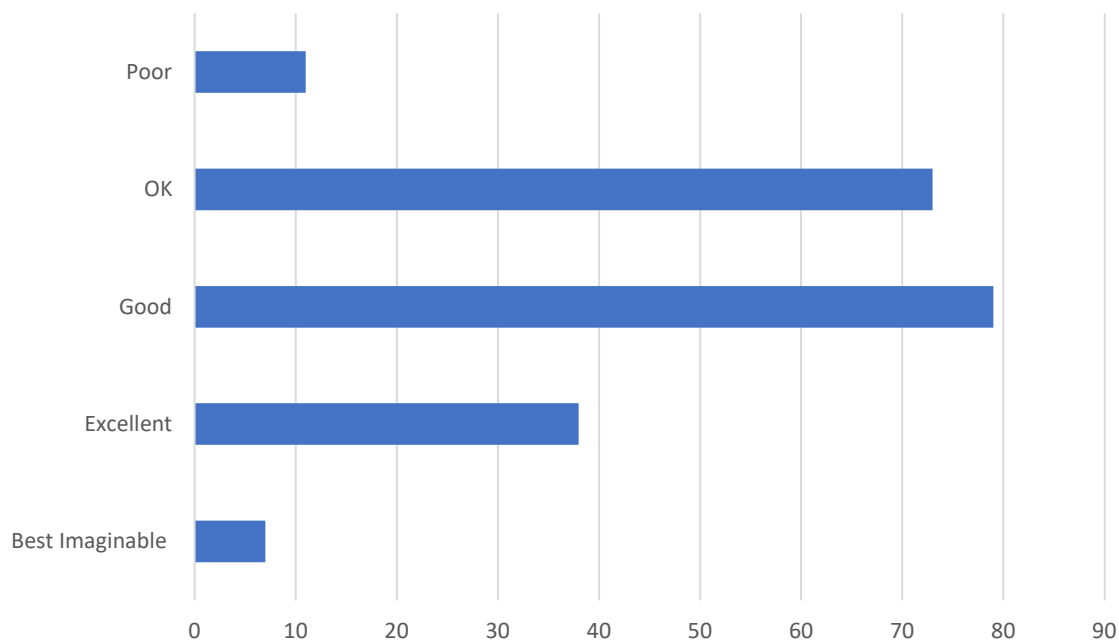


Figure 8: Number of respondents for each corresponding SUS adjective (N= 208)

To address RQ7, ANCOVA was performed utilizing SPSS[®] version 25, analyzing for significant mean differences for effectiveness when controlled for demographic indicators: age, gender, years of education, years of work experience, and years of mobile device use. The results of the ANCOVA indicated no significant differences for effectiveness with pictograms, labels, and SDSs when controlled for demographics, aside from SDSs, when controlled for education and labels when controlled for years of device use. The effectiveness with SDSs when controlled for education, indicate significant difference, $F(1,202) = 4.060, p = 0.045$. For effectiveness with labels when controlled for years of device use, indicate a significance level that borders the $p < 0.05$ level, $F(1,202) = 3.471, p = 0.064$. Tables 15, 16, and 17 presents the ANCOVA results for effectiveness with pictograms, labels, and SDSs when controlled for demographic indicators.

Table 16

ANCOVA Summary Table – Pictograms (N= 208)

Variable	SS	df	MS	F	p	η_p^2
Age	0.002	1	0.002	0.410	0.523	0.002
Gender	0.001	1	0.001	0.292	0.590	0.001
Education	0.002	1	0.002	0.453	0.502	0.002
Years of work experience	0.001	1	0.001	0.221	0.638	0.001
Years of device use	<0.0005	1	<0.0005	0.043	0.837	<0.0005

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 17

ANCOVA Summary Table – Labels (N= 208)

Variable	SS	df	MS	F	p	η_p^2
Age	0.004	1	0.004	1.901	0.170	0.009
Gender	<0.0005	1	<0.0005	0.006	0.938	<0.0005
Education	<0.0005	1	<0.0005	0.002	0.966	<0.0005
Years of work experience	<0.0005	1	<0.0005	0.076	0.784	<0.0005
Years of device use	0.008	1	0.008	3.471	0.064	0.017

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 18

ANCOVA Summary Table – SDS (N= 208)

Variable	SS	df	MS	F	p	η_p^2
Age	0.001	1	0.001	0.589	0.445	0.003
Gender	<0.0005	1	<0.0005	0.043	0.835	<0.0005
Education	0.009	1	0.009	4.060	0.045 *	0.020
Years of work experience	0.001	1	0.001	0.371	0.543	0.002
Years of device use	0.001	1	0.001	0.292	0.590	0.001

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Summary

In this chapter, the results of the study were presented in the sequence of steps performed. There were three phases as part of this research design that was utilized to address the seven research questions. First, the chapter began with Phase one of this research study, which used the Delphi technique to identify the expert opinion of cybersecurity threats, common threat categories, and produce a classification based on cybersecurity threats and categories. The results of the surveys using the Delphi technique were discussed. Furthermore, the discussion included the expert panel's elicitation to confirm cybersecurity threats and categories of threats for mobile devices. Next, Phase two of this study was discussed, which involved operationalizing the SMEs' identified cybersecurity threats and categories of threats to mobile devices in pictograms, labels, and safety data sheets. This study encompassed the expert panel's engagement in developing and validating the operationalized cybersecurity threats and threat categories using the Delphi technique. The chapter concluded with Phase three that collected and analyzed the results of the developed communication standards with non-IT professionals.

In Phase one of this study, an expert consensus emerged with six categories (Application, Authentication, Cellular, LAN & PAN, Payment, Physical access) and 62 cybersecurity threats. The average rating of responses with 70% or high in expert panel agreement was retained. The level of severity of each category was computed using the average rating given by the SMEs. Payment threats were identified as the most severe receiving an average of 6.92, while cellular threats averaged the lowest with a rating of five.

In Phase two of this study, phase one's results were operationalized into pictograms, labels, and safety data sheets. Each communication standard was designed in this study to include two to three cybersecurity threats from each of the categories identified in phase one. Upon completing developing the pictograms, labels, and safety data sheets, a survey was sent to solicit feedback. Recommendations from respondents were incorporated before the next round of Delphi. The Delphi technique reinforced the validity of the communication standards.

In Phase three of this study, the perceived effectiveness for the pictograms, labels, and safety data sheets was determined, and ANCOVA was performed to address RQ6 and RQ7, respectively. Additionally, the usability of the pictograms was determined with the SUS.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusions

This study addressed the research problem of the lacking cybersecurity threat classifications and communication standards criteria for mobile device users, while mobile device compromises are on the rise (Hovav & Gray, 2014; Peha, 2013). The increasing use of mobile devices allows users to be connected continuously and has become an essential part of everyday life (Cheng & Wang, 2019). Nevertheless, the increased connectivity does not come without its risks as well as potential harm. Mobile devices continue to be increasingly targeted by malicious actors and cause substantial damage to individuals (Narwal, 2019). However, when it comes to self-protection, individuals are unaware of the cybersecurity threats to mobile devices (Butler, 2020). The results of the study facilitated an increase in the body of knowledge regarding the classification and communication of threats to mobile devices. Moreover, the study addressed a valid problem with practical significance (Terrell, 2015).

The main goal of this study was to design, develop, and empirically test a set of criteria, which enables the validation of a Cybersecurity Threats Classification and Communication Standard (CTC&CS) for mobile devices. Building on the work of Alhabeeb et al. (2010), Davinson and Sillence (2010), as well as Shillair et al. (2015), this

work was classified as developmental research. Thus, the study developed a classification and communication standard in the form of pictograms, labels, and safety data sheets and tested the effectiveness of the communication methods on non-IT professionals.

Furthermore, the study sought to determine any significant differences in the effectiveness of pictograms, labels, and safety data sheets when controlled for age, gender, years of education, years of work experience, and years of mobile device use. Therefore, a three-phased approach was used to meet the goals and answer seven research questions.

In Phase One, this study recruited a group of 26 and 22 SMEs from academic and industry sectors to address the first three research questions:

RQ1. What are the specific Subject Matter Experts' (SMEs) identified most common cybersecurity threats to mobile devices?

RQ2. What are the specific SMEs' identified most common categories of cybersecurity threats to mobile devices?

RQ3. How can the SMEs' identified most common cybersecurity threats be classified and to what degree of severity?

This study reviewed the literature to identify cybersecurity threats and threats categories for cybersecurity threats to mobile devices. Then using an anonymous online survey to collect quantitative data, two rounds of the Delphi technique were conducted with 26 and 22 SMEs respectively to validate cybersecurity threats and threats categories to mobile devices for a cybersecurity threats classification for mobile devices. The SMEs' feedback was used to modify the list of cybersecurity threats and threats categories, which resulted in a consensus to accept the cybersecurity threats and threats

categories, thus addressing RQ1 and RQ2. Furthermore, the final list of cybersecurity threats was arranged into each of the final six categories identified by SMEs. Average SMEs category ratings were calculated, ratings of 70% or higher were kept. The level of severity of each category was computed using the average rating given by the SMEs, thus, addressing RQ3.

In Phase Two, the researcher recruited a group of 24 and 19 SMEs from academic and industry sectors to address:

RQ4. What pictograms, labels, and safety data sheets can be assigned to represent the previously validated, classified most common cybersecurity threats?

RQ5. What are the SMEs' validated pictograms, labels, and safety data sheets?

Using the results of phase one as a foundation, pictograms, labels, and safety data sheets were developed. Students studying graphic design or a similar course were employed to design the communication standard. To ascertain general ideas for the initial designs of the communication standards, the graphic designers were provided with firstly, standardized design rules from OSHA (OSHA 1910.1200) and ISO (ISO/IEC Guide 74:2004), secondly, the categories and threats from phase one and finally, the commonly used graphic elements that depict or could depict each of the identified cybersecurity threat categories from Phase one. The graphic designers developed two to three pictograms for each of the identified categories and one label and safety data sheet for each category. Using an anonymous online survey, quantitative data were collected and analyzed, resulting in only minor changes. After round two of the Delphi technique, a consensus of SMEs' opinion was reached regarding the design and presentation of pictograms, labels, and safety data sheets, thus, addressing RQ4 and RQ5.

In Phase Three, the effectiveness of the pictograms, labels, and safety data sheets were computed, and ANCOVA was performed to address RQ6 and RQ7:

RQ6. What is the perceived effectiveness of pictograms, labels, and safety data sheets in warning mobile device user's against cybersecurity threats?

RQ7. What are the perceived effectiveness of pictograms, labels, and safety data sheets in warning mobile device user's against cybersecurity threats when controlled for (a) age, (b) gender, (c) years of education, (d) years of work experience, and (e) years of mobile device use?

The results of RQ6 showed that the perceived effectiveness with pictograms was overall high effectiveness ($n = 208$, $m = 0.6791$, $SD = 0.06529$) while perceived effectiveness with the labels ($n = 208$, $m = 0.2535$, $SD = 0.04895$) and safety data sheets ($n = 208$, $m = 0.1992$, $SD = 0.04761$) were low effectiveness. The participants found pictograms to be highly effective; this means that the participants were more satisfied with the pictogram characteristics, i.e., color, shapes, visual complexity, and found these characteristics important. On the other hand, labels and SDS low effectiveness identified that participants were not satisfied or lacked to identify importance with characteristics of labels and SDS. This could be due to the labels and SDSs being not user-centered for several reasons, such as the scarce completeness of information in the SDS, the poor quality of the information contained in the SDS (Caffaro et al., 2018; Rubbiani, 2010). Additionally, difficulties should be taken into account for user interpretations, understanding and recalling the information contained in the label and the SDS, due to the difficult wording and limited training by the participants (Caffaro et al., 2018).

For RQ7, the ANCOVA results indicated significant differences in perceived effectiveness with SDSs when controlled for education. Additionally, the significance level of years of mobile device use bordered the $p < 0.05$ level. Also, users correctly identified the type of threat shown in the pictograms when provided with a multiple-choice list of cybersecurity threats. The majority of participants were able to correctly identify the threats in the pictogram from a multiple-choice list.

Results from the 10 items analyzed to determine the SUS scores, 78 participants had a SUS score above 70, which is deemed an acceptable score. The sample average SUS score was 65.6%. Thus, the pictograms' overall perceived usability can be deemed usable based on the SUS score, adjective rating, and acceptability (Bangor, Kortum, & Miller, 2008).

Discussions

The first result of this study was the development of a validated cybersecurity threats classification and communication standard, which adds significant value to the body of knowledge, as there is limited research specific to the classification of cybersecurity threats to mobile devices. Previous literature on cybersecurity threats classifications has classified threats to IoT devices, information systems, network security, blockchains, cloud computing, smart homes, and several other technologies (Ferrando & Stacey, 2017; Jouini & Rabai, 2016a; Masetic et al., 2017; Mosakheil & Hayat, 2018) but nonspecific for mobile devices, which is a growingly used device. The second result indicates that overall, pictograms appeared to be highly effective. 11 of the 12 pictograms were identified as effective by the participants. This result is consistent with previous literature that found pictograms effective in positively influencing comprehension, understanding,

and adherence by users to hazard/threat information whether the user was considered a naïve or expert user (Boelhouwer et al., 2013; Dowse & Ehlers, 2005). Contrary to these findings, studies have also found pictograms ineffective in conveying the intended message (Chan & Ng, 2010a). However, these studies were limited to university students aged 19 to 25, so care should be taken in generalizing the results to other age groups. The third result indicates that the effectiveness of all the labels is generally low. The labels' satisfaction and value rating compared to the pictograms were significantly lower, which could indicate the extra work required to understand the label. Users are lazy and do not have the time or put in the effort to read even when presented with important warning labels. Furthermore, the layout and design characteristics of labels were complex which decreased the satisfaction and values, thus decreasing effectiveness. This result is consistent with Rhoades et al. (1990), which reported that overly detailed labels could overload users, which increases the amount of time a user will take to understand a label. This increased complexity and time needed to understand the label turn the user away from further processing it. The fourth result indicates that effectiveness with SDSs was overall very low. Although all SDSs resulted in low effectiveness, half of the SDSs presented resulted in even lower effectiveness compared to the other half of the SDSs presented. Again, this is caused by users being lazy to read and the increased complexity in the SDSs; half of the SDSs presented more information to process compared to the other half of SDSs. Overwhelmingly, the results are consistent with previous studies that found SDSs unsatisfactory as a means of informing on protection measures as well as the complexity found by users in using SDSs (Sadhra et al., 2002; Seki et al., 2001). The fifth result indicated no significant difference found for perceived effectiveness with

pictograms when controlled for demographics. The sixth results, while indicated that there were no significant differences overall for perceived effectiveness with pictograms, the perceived effectiveness of SDSs when controlled for education was a significant difference. Additionally, for labels, the years of device use boarded the cut-off level of significance for effectiveness. This result is consistent with previous findings, which found significant differences with SDSs based on education (Ng & Chan, 2008), where more highly educated people had a better understanding of SDSs.

Implications

There are implications of this study concerning the existing body of knowledge in IS and InfoSec. This research developed and tested a mobile device threats classification and communication methods for mobile device users to identify cybersecurity threats posed to their devices. Many cybersecurity tools presenting visualizations are rarely developed and evaluated for their effectiveness and do not take account of the needs of the user (Adams & Snider, 2018; ISO 9241-210:2019; Sethi et al., 2016). This study identified SME validated cybersecurity threats and threat categories, designs for pictograms, labels, and safety data sheets, and further surveyed non-IT professional participants on the effectiveness of the designed pictograms, labels, and safety data sheets. With the popularity of mobile devices, coupled with the valuable and private information that mobile devices hold, make users and their devices vulnerable to new threats to cybersecurity (Bertino, 2016; Bitton et al., 2018; Patten & Harris, 2013); it is vital to ensure mobile device users are enabled to identify and mitigate potentially malicious mobile cybersecurity threats (Alhabeeb et al., 2010; Almutairi & Riddle, 2017).

In this study, the data collection occurred over twelve weeks—this period allowed SME participants to respond and, if needed, follow-ups, as well as the main data collection. Using an expert panel required regular follow-ups, which resulted in delays. Though follow-ups were found to be a way for reducing non-response within the Delphi process, a drawback to the Delphi process is that the survey method may slow data collection (Chang et al. 2018).

This study provides mobile device users with pictograms that are perceived as effective when identifying potential cybersecurity threats to mobile devices. These cybersecurity threats pictograms could assist with identifying and mitigating mobile device cybersecurity threats (Kido, Shimojo, & Yanai, 2020). Figure 7 provides the final list of pictograms identified as effective.

Recommendations and Future Research

This study was developmental research and outlined the approach to design and test pictograms, labels, and safety data sheets for cybersecurity threats to mobile devices. The cybersecurity threats, threats categories, as well as the pictograms, labels, and safety data sheets, were developed and validated using the Delphi technique. Followed by the data collection from non-IT professionals, which collected ratings for satisfaction and value/importance, which was used to calculate user effectiveness with the pictograms, labels, and safety data sheets. The findings and results of the statistical analysis were reported.

There are areas for future research that were identified based on the results of this developmental study. Future research should first recruit participants, assess their education and reading levels, and segregate them in comparison groups. This will allow

future research to observe discrepancies of pictogram effectiveness between different educational levels and reading levels. Second, future research should focus on identifying the most effective designs for pictograms within the cybersecurity context. Third, longitudinal studies should be performed to understand the aspects that affect the effectiveness of pictograms. This will make it possible to test the pictograms in the same population, and the least understandable pictograms can be redesigned and tested again until an acceptable result is achieved. Thus, it is possible to gain a deeper understanding of relationships among the factors observed, e.g., between educational and cultural aspects with the understanding of pictograms.

Summary

This chapter presents the conclusions and implications drawn from this research's results with respect to the research problem and the main goal. Furthermore, recommendations for future research are provided. Finally, this chapter concludes with an overall summary of this research study.

This study attempted to address cybersecurity threat classifications, and communication standards criteria are lacking for mobile device users, while mobile device compromises are on the rise (Hovav & Gray, 2014; Peha, 2013). This process was conducted by developing a cybersecurity threats classification, and communication standard using SME validated threats, threats categories, and the communication standards in the form of pictograms, labels, and safety data sheets. This study achieved the goal of this study by using a three-phased approach. First, using the Delphi technique, SMEs identified cybersecurity threats and threats categories for mobile devices that should be included in a mobile device cybersecurity threats classification. Next,

pictograms, labels, and safety data sheets were operationalized, and using the Delphi technique, SMEs validated the communication standards. Finally, the perceived effectiveness ratings of the pictograms, labels, and safety data sheets were collected and analyzed.

Appendix A

SAFETY DATA SHEET 1

Section 1: Threat Identification

Threat Category: Application

Threat: Malware uses a device to conduct DDoS attacks

Threat Origin: Android.Tascudap

CVE Examples (if any):

CVE-2017-6982

CVE-2017-2495

CVE-2017-0599

CVE-2017-0600

CVE-2017-0603

Signal Word: Warning

Threat Statement: May prevent access to mobile services such as email, websites, online accounts (i.e., banking) or others that rely on the mobile device.

Threat Description:

Distributed Denial of Service (DDoS) is a cyber attack on your devices with the intended purpose of disrupting normal operation. This is done by flooding the target with a constant flood of traffic which will overwhelm your device causing a disruption or denial of service.

Section 2: Countermeasures

Mobile Users: 1) Reduce the risk of installing apps with trojan functionality by only downloading apps from official app stores i.e., Google store, Apple Store.
2) Use malware detection apps.

Organizations:

Pictograms:

**Section 3: Regulatory Information**

National and/or regional regulatory information:

NIST Special Publication 800-163

Section 4: Other Information

SDS date of preparation/update: May 19, 2020

Where changes have been made to previous version:

Other useful information: N/A

Section 5: References

Ogata, M. A., Franklin, J., Voas, J. M., Sritapan, V., & Quiroigico, S. (2019). *Vetting the Security of Mobile Applications* (No. Special Publication (NIST SP)-800-163 Rev. 1).

SAFETY DATA SHEET 2

Section 1: Threat Identification

Threat Category: Physical Access

Threat: Malicious Charging Station

Threat Origin: MACTANS: Injecting Malware Into iOS Devices Via Malicious Chargers

CVE Examples (if any):

Signal Word: Warning

Threat Statement(s):

1. May expose device to malware.
2. May cause loss of confidentiality, integrity, and availability of device data.

Threat Description:

A malicious charging station threat aka 'juice jacking' uses public mobile charging stations to provide unauthorized access to attackers during the charging process; leveraging illegitimate access to get your personal information. This type of threat originates from USB charging ports installed in public locations such as airports, cafes, etc. Once a device is plugged-in and a connection established, malware can be installed on your device and/or personal information taken from your mobile device.

Section 2: Countermeasures

Mobile Users:

- 1) Avoid use of public charging stations, which may house malicious chargers.
- 2) Ensure Android USB debugging is disabled unless explicitly needed (e.g. by app developers).
- 3) Do not accept any prompt to trust an untrusted or public USB charger.

Organizations:

Pictograms:



Section 3: Regulatory Information

National and/or regional regulatory information: N/A
Section 4: Other Information
SDS date of preparation/update: May 19, 2020 Where changes have been made to previous version: Other useful information: N/A
Section 5: References

SAFETY DATA SHEET 3

Section 1: Threat Identification
Threat Category: Authentication Threat: Phishing attack Threat Origin: CVE Examples (if any): Signal Word: Warning Threat Statement(s): <ol style="list-style-type: none"> 1. May cause identity and data theft from device. 2. Causes unauthorized use of personal information i.e., username, credit card information. Threat Description: Phishing is a method of trying to gather personal information using deceptive emails, SMS, MMS, applications, and websites. The objective of the attacker is to trick the user into thinking and email, SMS, websites etc. are legitimate such as a message from your bank.
Section 2: Countermeasures

Mobile Users:

1. Always double-check and make sure the address is correct.
2. Scrutinize urgent emails to make sure it is legitimate.
3. Check for generic greetings and whether the email has been personalized to you.
4. **Do not** click on random links received from an incorrect "From" Address.

Organizations:**Pictograms:****Section 3: Regulatory Information****National and/or regional regulatory information:**

N/A

Section 4: Other Information**SDS date of preparation/update:** May 19, 2020**Where changes have been made to previous version:****Other useful information:** N/A**Section 5: References**

SAFETY DATA SHEET 4

Section 1: Threat Identification**Threat Category:** Cellular**Threat:** Eavesdropping**Threat Origin:****CVE Examples (if any):****Signal Word:** Warning**Threat Statement(s):**

1. May cause a loss of privacy, identity theft, and/or financial loss.

Threat Description:

Section 2: Countermeasures

Mobile Users:

1. Avoid public wi-fi network.
2. Install and keep updated antivirus software.
3. Use strong passwords.

Organizations:
Pictograms:


Section 3: Regulatory Information

National and/or regional regulatory information:

N/A

Section 4: Other Information

SDS date of preparation/update: May 19, 2020

Where changes have been made to previous version:

Other useful information: N/A

Section 5: References

SAFETY DATA SHEET 5

Section 1: Threat Identification

Threat Category: LAN & PAN

Threat: Rogue access points

Threat Origin: Guidelines for Securing Wireless Local Area Networks (WLANs) (SP 800-163)

CVE Examples (if any):

Signal Word: Warning

Threat Statement(s):

1. May cause identity and data theft from device.
2. Causes unauthorized use of personal information i.e., username, credit card information.

Threat Description:

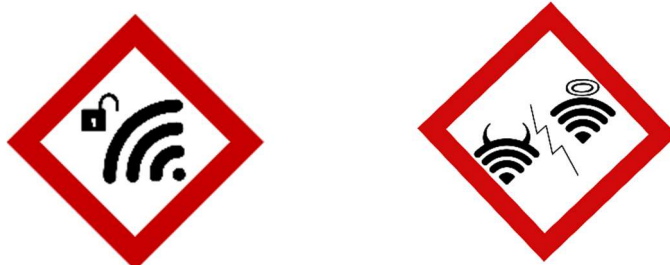
Rogue Access Points pose threats to private mobile devices through the use of unsecured or free public Wi-Fi. This threat provides a wireless backdoor into your network communications and eventually access to your device data.

Section 2: Countermeasures**Mobile Users:**

1. Avoid the use of untrusted and unencrypted Wi-Fi networks, particularly when needing to access sensitive services.
2. When needing to connect to untrusted and unencrypted Wi-Fi networks, attempt to verify with a representative of the hosting organization (e.g., coffee shop employee) that the detected network is the correct one.
3. To reduce the probability of connecting to rogue access points, use Wi-Fi hotspot services that associate access points with registered Wi-Fi provider, geolocation, and crowd-sourced reputation data to make assertions about their apparent trustworthiness.

Organizations:

1. To reduce the probability of connecting to rogue access points, use Wi-Fi hotspot services that associate access points with registered Wi-Fi provider, geolocation, and crowd-sourced reputation data to make assertions about their apparent trustworthiness.
2. To avoid this threat, only allow mobile devices to connect to authorized Wi-Fi networks that use WPA2 encryption.

Pictograms:**Section 3: Regulatory Information****National and/or regional regulatory information:**

N/A

Section 4: Other Information

SDS date of preparation/update: May 19, 2020

Where changes have been made to previous version:

Other useful information: N/A

Section 5: References

SAFETY DATA SHEET 6

Section 1: Threat Identification

Threat Category: Payment

Threat: NFC Payment Attack

Threat Origin: Apple iOS version 9.3 and further

CVE Examples (if any):

CVE-2017-17225

CVE-2017-15322

CVE-2008-5826

Signal Word: Warning

Threat Statement(s):

1. May cause a loss in confidentiality, integrity, and availability of payment data.

Threat Description:

Near Field Communication (NFC) is a short-range wireless connectivity standard that uses magnetic field induction to enable communication between devices that are touched together or brought within a few centimeters of each other. An NFC payment attack allows an attacker to extract data from a mobile device using a mobile payments system and a Point of Sale System (PoS).

Section 2: Countermeasures

Mobile Users:

1. Disable NFC when not in use to reduce opportunity for an attack.
2. Avoid activating; or if already activated, deactivate mobile payment features i.e., Apple Pay, Google pay.
3. Ensure payment services such as Google pay, and Apple pay are configured to require password, pattern, or biometrics authentication to complete any contactless payment transactions.

Organizations:

Pictograms:

**Section 3: Regulatory Information**

National and/or regional regulatory information:

N/A

Section 4: Other Information

SDS date of preparation/update: May 19, 2020

Where changes have been made to previous version:

Other useful information: N/A

Section 5: References

112. Consuming device resources to perform computations for the attacker*Mark only one oval.*

	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

113. Malware uses device to conduct DDoS attacks*Mark only one oval.*

	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

114. A malicious app captures the raw screen buffer*Mark only one oval.*

	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

115. App records audio by stealthily placing or answering phone calls*Mark only one oval.*

	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

116. Malware avoids detection by uninstalling itself*Mark only one oval.*

	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

Please tell us about yourself**117. 1. What is your age group***Mark only one oval.*

- 21 - 30
- 31 - 40
- 41 - 50
- 51 - 60
- 61 - 70
- 71 and above

118. **2. What is your gender**

Mark only one oval.

- Male
 Female

119. **3. What is your education level?**

Mark only one oval.

- High school
 Associates
 Bachelors
 Masters
 Doctorate

120. **4. Position at your organization**

Mark only one oval.

- Entry level
 Supervisor
 Manager
 Director/VP
 C-level
 Academic
 Other: _____

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

Mark only one oval.

- < 1
 1 - 4
 5 - 10
 11 - 15
 16 - 20
 21 and greater

122. **6. What sector do you work in?**

Mark only one oval.

- Federal government
 State government
 Academia
 Private
-

15. Possible countermeasures for organization*Mark only one oval.*

	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

16. Possible countermeasures for developer*Mark only one oval.*

	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

17. Other information*Mark only one oval.*

	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

18. Date of preparation*Mark only one oval.*

	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

19. Date of last revision*Mark only one oval.*

	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

20. Possible causes of threat*Mark only one oval.*

	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

21. Please enter any suggestions on how to improve mobile device threat safety data sheets?

Pictograms

As an Information Security SME, please rate the level of agreement

22. Pictogram shall be in the shape of a square set at a point and shall include a black threat symbol on a white background with a red frame sufficiently wide to be clearly visible. Please see the attached sample



Mark only one oval.

1 2 3 4 5 6 7

Strongly disagree Strongly agree

23. Pictogram shall be in the shape of a square set at a point and shall include a black threat symbol on a yellow background with a black frame sufficiently wide to be clearly visible. Please see the attached sample



Mark only one oval.

1 2 3 4 5 6 7

Strongly disagree Strongly agree

24. Please enter any suggestions on how to improve mobile device threat pictograms?

Appendix D

Study Participants' Recruitment Announcement

Dear Participant,

I am a Doctoral candidate at Nova Southeastern University working on a dissertation that seeks to design a mobile device threats classification, develop a communication standard for the main categories of cybersecurity threats to mobile devices, and test the use of the developed communication standard. The results of this study will provide researchers and practitioners insight on the cybersecurity threats to mobile devices and the applicability of incorporating pictograms, labels, and safety data sheets as a communication tool for mobile device cybersecurity threats.

I would appreciate your time in participating in this developmental study. All information gathered during this study will be protected and will not be distributed for any other use than academic research. Moreover, this study will not collect any personally identifiable information and is completely anonymous.

If you are willing to participate in this research, please select the link below to complete this brief survey. Completion of this survey indicates your voluntary participation in this study.

[Click Here for Survey](#)

Should you have any questions, please email me at ej459@mynsu.nova.edu.

Best Regards,

Emmanuel Jigo

College of Engineering & Computing
Nova Southeastern University

Appendix E

Initial Draft Study Participants' Survey Instrument

Mobile Device Threats Communications (Draft)

Dear Participants,

My name is Emmanuel Jigo. I am a PhD student at Nova Southeastern University. I am conducting a research study that focuses on developing a mobile device threats communication standard for my dissertation work. The results of this research study will provide researchers and practitioners additional insight into mobile device threats and approaches to communicate these threats.

I would appreciate your time in participating in this research study. This study will be administered through an online survey. As a participant, you will be presented with SDSs, labels, and pictograms then answer questions that relate to SDSs, labels, and pictograms.

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 survey do not collect personally identifiable information and is fully anonymous. You may stop your participation at any time. If you agree to participate.

Thank you,
Emmanuel Jigo
Ph.D. candidate in Information Systems
Nova Southeastern University

CTC&CS effectiveness (Satisfaction)

The following lists are related to the cybersecurity threats communication methods from the CTC&CS. Please go through each item and rate your level of satisfaction you attribute to each item when identifying cybersecurity threats on mobile devices. Rate the level of satisfaction from: "Extremely unsatisfied" to "Extremely satisfied" using the following scale:

- 1 - Extremely unsatisfied
- 2 - Very unsatisfied
- 3 - Unsatisfied
- 4 - Neutral
- 5 - Satisfied
- 6 - Very satisfied
- 7 - Extremely satisfied

1. Pictogram 1

Mark only one oval.

	1	2	3	4	5	6	7	
Extremely unsatisfied	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Extremely satisfied

2. Pictogram 2

Mark only one oval.

	1	2	3	4	5	6	7	
Extremely unsatisfied	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Extremely satisfied

10. Label + Pictogram 5*Mark only one oval.*

	1	2	3	4	5	6	7	
Extremely unsatisfied	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Extremely satisfied

11. Safety Data Sheet 1*Mark only one oval.*

	1	2	3	4	5	6	7	
Extremely unsatisfied	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Extremely satisfied

12. Safety Data Sheet 2*Mark only one oval.*

	1	2	3	4	5	6	7	
Extremely unsatisfied	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Extremely satisfied

13. Safety Data Sheet 3*Mark only one oval.*

	1	2	3	4	5	6	7	
Extremely unsatisfied	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Extremely satisfied

14. Safety Data Sheet 4*Mark only one oval.*

	1	2	3	4	5	6	7	
Extremely unsatisfied	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Extremely satisfied

15. Safety Data Sheet 5*Mark only one oval.*

	1	2	3	4	5	6	7	
Extremely unsatisfied	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Extremely satisfied

CTC&CS effectiveness (Importance)

The following lists are related to the cybersecurity threats communication methods from the CTC&CS. Please go through each item and rate your level of importance you attribute to each item when identifying cybersecurity threats on mobile devices. Rate the level of importance from: "Not important" to "Extremely important" using the following scale:

- 1 - Not important
- 2 - Not so important

22. Label + Pictogram 2*Mark only one oval.*

	1	2	3	4	5	6	7	
Not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Extremely important

23. Label + Pictogram 3*Mark only one oval.*

	1	2	3	4	5	6	7	
Not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Extremely important

24. Label + Pictogram 4*Mark only one oval.*

	1	2	3	4	5	6	7	
Not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Extremely important

25. Label + Pictogram 5*Mark only one oval.*

	1	2	3	4	5	6	7	
Not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Extremely important

26. Safety Data Sheet 1*Mark only one oval.*

	1	2	3	4	5	6	7	
Not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Extremely important

27. Safety Data Sheet 2*Mark only one oval.*

	1	2	3	4	5	6	7	
Not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Extremely important

28. Safety Data Sheet 3*Mark only one oval.*

	1	2	3	4	5	6	7	
Not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Extremely important

29. Safety Data Sheet 4*Mark only one oval.*

	1	2	3	4	5	6	7	
Not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Extremely important

30. Safety Data Sheet 5*Mark only one oval.*

	1	2	3	4	5	6	7	
Not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Extremely important

Participants Demographics**31. What is your age group?***Mark only one oval.*

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

32. What is your gender?*Mark only one oval.*

- Male
- Female

33. How many years have you been using a mobile device?*Mark only one oval.*

- Under 1
- 1 - 3
- 4 - 6
- 7 - 9
- 10 and more

34. **Do you use your mobile device both for work and personal use?**

Mark only one oval.

- Yes
 No

35. **How many years have you been using a mobile device for work-related activities?**

Mark only one oval.

- Under 1
 1 - 3
 4 - 6
 7 - 9
 10 and more
 Never

36. **How many years of experience do you have with cybersecurity threats?**

Mark only one oval.

- Under 1
 1 - 3
 4 - 6
 7 - 9
 10 and more
 None

37. **Which mobile device manufacturer(s) & device model(s) do you use for work (e.g. Apple iPhone, Samsung Galaxy etc.)**

Appendix F

IRB Approval Letter



MEMORANDUM

To: **Emmanuel Jigo, Masters**

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

Date: **September 5, 2019**

Re: **IRB #: 2019-450; Title, "Development of Criteria for Mobile Device Cybersecurity Threat Classification and Communication Standards (CTC&CS)"**

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.

Appendix G

SME Identified Categories and Threats

Category	Threat	Rated 6 or Higher	Average Rating
Application Threats		100%	6.88
	App encrypts/encodes and ransoms files	96.1%	6.88
	App silently intercepts SMS messages	96.2%	6.85
	Malicious app impersonates a legitimate app	92.3%	6.85
	Malware uses a device to conduct DDoS attacks	92.3%	6.85
	Malware avoids detection by uninstalling itself	96.1%	6.81
	A malicious app captures the raw screen buffer	88.4%	6.73
	The app records audio by stealthily placing or answering phone calls	100%	6.73
	Malicious code downloaded by visiting a malicious URL	100%	6.69
	The malicious app exploits device access to enterprise resources	96.2%	6.65
	Exploits OS or lower-level vulnerability to achieve privilege escalation	96.2%	6.62
	Passive eavesdropping of unencrypted app traffic	88.4%	6.58
	Surreptitiously reporting device location	96.1%	6.58
	App provides remote control over the device	96.2%	6.46
	The app conducts audio or video surveillance	96.2%	6.27
	Trojan app impersonates a legitimate app	96.1%	6.23
	Malicious app abuses existing root access	96.1%	6.23
	App abuses Device Administrator permission to avoid uninstallation	76.9%	6.19

Category	Threat	Rated 6 or Higher	Average Rating
Authentication Threats	The app exposes sensitive information to untrusted apps	80.8%	6.12
	Consuming device resources to perform computations for the attacker	92.3%	6.08
	App entices the user to perform hidden actions in another app	76.9%	6.04
	WebView app vulnerable to browser-based attacks	80.1%	5.92
	Privacy invasive behaviors by pre-installed apps	76.9%	5.92
		100%	6.65
	Phishing attack via e-mails that link to malicious applications or websites that captures credentials	100%	6.96
	Biometric spoofing	96.1%	6.73
	A malicious application that captures credentials	100%	6.73
	Theft (Use of authorized credentials)	100%	6.69
Cellular Threats	PIN/password brute force	76.9%	6.46
	Man-in-the-middle network attacker substitutes malicious web site that captures credentials	75.4%	6.00
	Android: Spoofing NFC tokens or Bluetooth enabled devices which auto-unlock the mobile device or keeps a mobile device unlocked (i.e., Smartlock)	78.4%	5.65
		78%	5.00
	Eavesdropping on unencrypted message content	100%	6.88
	DoS via sending thousands of silent messages	96.1%	6.73
	No validation or authentication of caller ID information	96.2%	6.69

Category	Threat	Rated 6 or Higher	Average Rating
LAN & PAN Threats	Preventing Emergency Calls via Rogue Base station	96.1%	6.42
	Air Interface Eavesdropping	88.5%	6.31
	Device enumeration and fingerprinting via silent SMS	78.4%	5.46
	Jamming Device Radio Interface	74.6%	5.42
	Device and Identity Tracking via Rogue Base station	70.7%	5.15
		100%	6.46
	Bluebugging - Attacker can make and take calls, listen to phone conversations, read contacts and calendars	96.2%	6.65
	Hotspot hijacking - Malicious Wi-Fi networks masquerading as legitimate Wi-Fi networks	92.3%	6.62
	Rogue access points	84.6%	6.50
	Bluejacking - unsolicited messages send to Bluetooth-enabled mobile device	96.1%	6.50
	Eavesdropping over unencrypted/insufficiently encrypted wifi network	100%	6.42
	Man-in-the-middle by relaying NFC packets	76.2%	6.38
	Bluesnarfing - give the attacker full access to calendar, contacts, e-mail and text messages	96.1%	6.31
	Malicious NFC tags	92.4%	6.27
	Wi-Fi SSID Tracking	76.9%	6.19
	Blueprinting - remotely fingerprint Bluetooth-enabled devices	77.0%	5.81
	Denial of service attack through Bluetooth connection	75.4%	5.65
Pairing eavesdropping attacks	77.7%	5.58	

Category	Threat	Rated 6 or Higher	Average Rating
Payment Threats	Client MAC address tracking	76.1%	5.54
	BlueStumbling - discover, locate, and identify users based on their Bluetooth device addresses	78.5%	5.38
		100%	6.92
	Compromised mobile payment terminal	96.1%	6.65
	Near Field Communication (NFC) Payment replay attacks	96.2%	6.12
	Software vulnerabilities in the bank payment application	84.7%	5.92
	Accidental purchase of in-app content	71.6%	5.77
Physical Access Threats	Credit or debit card enrolled into mobile payment without cardholder authorization	73.8%	5.69
		84.6%	5.46
	Unauthorized access to device data	100%	6.92
	Device loss or theft	100%	6.88
	Malicious charging station	79.2%	6.31
		71.5%	5.92
	Data loss via third party temporary access to unattended and unlocked mobile device		

Appendix H

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Raw SUS Sum Score	Raw SUS mean score
4	-1	5	2	3	0	5	-1	3	2	22	2.2
6	1	5	0	4	0	6	1	2	2	27	2.7
6	0	5	3	5	1	4	4	2	0	30	3
5	0	5	3	3	0	5	2	3	3	29	2.9
6	-1	5	2	5	-1	4	4	6	3	33	3.3
5	-2	6	0	3	2	5	0	5	3	27	2.7
4	-2	4	2	3	2	4	3	6	-1	25	2.5
6	-1	5	3	3	-1	6	-2	4	3	26	2.6
6	-1	6	0	4	0	5	-2	5	4	27	2.7
5	1	5	1	3	2	6	4	4	3	34	3.4
5	0	5	2	5	-1	6	1	2	4	29	2.9
6	-2	4	3	3	1	5	1	4	0	25	2.5
4	-1	4	2	4	2	5	2	5	3	30	3
5	-1	4	3	5	1	5	2	4	4	32	3.2
6	0	4	1	5	2	4	4	2	2	30	3
5	-1	6	2	4	1	6	3	3	0	29	2.9
5	-2	5	1	4	1	4	0	6	-1	23	2.3
4	-1	6	3	3	0	5	1	3	-1	23	2.3
4	-1	6	3	5	1	6	0	3	4	31	3.1
4	0	4	2	4	1	5	3	3	1	27	2.7
4	1	4	3	3	-1	5	0	3	2	24	2.4
6	0	4	2	5	0	6	0	6	3	32	3.2
4	0	5	3	5	1	5	3	6	0	32	3.2
6	-1	4	0	4	0	5	-1	5	-1	21	2.1
4	-2	5	2	5	1	4	2	2	2	25	2.5
6	-1	6	3	3	0	5	3	2	3	30	3
4	-1	4	1	5	-1	5	3	5	3	28	2.8
5	0	5	2	4	-1	4	4	6	-1	28	2.8
5	0	6	3	4	2	4	3	6	1	34	3.4
6	-2	6	3	4	-1	6	3	3	-1	27	2.7
5	-2	6	1	3	1	5	2	2	4	27	2.7
4	0	5	0	4	2	4	-2	4	1	22	2.2
6	1	5	0	5	-1	4	3	6	4	33	3.3
6	1	5	1	5	-1	4	0	6	1	28	2.8
4	1	6	0	4	2	5	0	5	1	28	2.8
4	-2	5	2	3	-1	6	-2	6	0	21	2.1
5	0	5	0	3	2	4	2	4	-1	24	2.4
4	1	4	1	4	1	5	-2	2	4	24	2.4
4	0	6	1	3	-1	5	2	4	3	27	2.7

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Raw SUS Sum Score	Raw SUS mean score
6	-2	4	2	3	0	6	2	5	-1	25	2.5
5	-2	5	0	3	1	4	-1	3	-1	17	1.7
5	1	5	1	4	1	4	0	2	-1	22	2.2
4	-1	6	1	3	-1	6	3	6	1	28	2.8
4	-1	6	1	5	1	4	0	4	1	25	2.5
5	-2	5	0	3	2	5	-2	5	-1	20	2
4	1	6	1	3	1	5	3	2	1	27	2.7
6	-2	6	0	4	0	5	-2	3	3	23	2.3
6	-2	6	0	4	0	5	-2	3	3	23	2.3
6	1	6	1	5	2	6	-2	5	0	30	3
4	-1	6	2	3	1	5	-2	3	-1	20	2
4	-2	6	1	4	1	6	-1	2	1	22	2.2
6	-1	6	1	3	2	4	4	5	0	30	3
4	-2	5	2	4	-1	5	3	6	-1	25	2.5
5	0	4	0	4	0	4	4	6	1	28	2.8
5	0	5	2	5	1	4	3	6	2	33	3.3
4	-2	6	2	4	2	5	-2	6	1	26	2.6
4	-2	4	1	3	1	4	-2	3	1	17	1.7
4	-1	4	2	4	-1	6	-1	4	2	23	2.3
4	0	4	2	4	1	4	-2	3	2	22	2.2
4	-2	6	0	5	1	6	3	3	0	26	2.6
6	-2	6	3	3	0	4	-1	3	3	25	2.5
5	-1	4	3	5	2	4	-1	6	0	27	2.7
6	1	5	2	4	-1	5	-2	5	-1	24	2.4
4	-2	4	1	3	-1	6	-2	2	1	16	1.6
4	0	5	2	4	-1	5	-1	5	2	25	2.5
4	0	4	1	3	1	4	-2	4	3	22	2.2
5	-1	5	1	4	0	5	1	4	-1	23	2.3
6	-1	4	1	4	2	6	-2	2	-1	21	2.1
5	0	6	0	3	1	6	-1	2	1	23	2.3
4	-1	6	0	3	2	6	-1	5	3	27	2.7
4	-2	4	3	4	0	4	-2	5	0	20	2
6	-1	4	1	5	1	5	-2	6	1	26	2.6
6	1	5	0	4	1	4	-2	3	-1	21	2.1
4	-2	4	2	3	0	5	4	4	1	25	2.5
6	-1	4	0	3	-1	6	1	2	4	24	2.4
6	0	6	3	5	0	6	1	2	-1	28	2.8
4	-2	4	3	5	2	5	-2	5	4	28	2.8
6	0	6	2	4	-1	6	4	6	0	33	3.3
5	1	6	0	3	-1	5	-1	4	4	26	2.6
6	-2	4	0	5	-1	5	2	3	4	26	2.6

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Raw SUS Sum Score	Raw SUS mean score
6	-2	5	3	3	0	6	-2	4	3	26	2.6
6	-1	6	3	5	-1	5	3	4	4	34	3.4
4	-1	5	0	4	2	4	4	5	2	29	2.9
5	0	6	2	5	-1	6	0	2	2	27	2.7
6	-2	5	2	3	-1	6	4	4	-1	26	2.6
5	-1	6	1	4	0	6	-1	6	3	29	2.9
5	-1	5	1	3	0	4	4	6	4	31	3.1
5	-1	4	3	5	-1	6	3	2	-1	25	2.5
4	-2	4	1	5	2	5	-2	4	0	21	2.1
5	-2	6	1	5	0	4	3	4	1	27	2.7
4	0	4	3	3	0	4	-2	2	4	22	2.2
4	0	6	3	4	-1	4	-1	2	4	25	2.5
6	1	6	3	5	0	6	1	2	0	30	3
5	-2	6	0	5	2	5	-2	4	-1	22	2.2
4	0	4	3	3	0	5	-1	3	4	25	2.5
5	1	5	2	4	-1	5	0	3	-1	23	2.3
5	-1	5	1	3	0	6	0	6	1	26	2.6
5	0	4	2	5	-1	4	-1	2	0	20	2
5	-2	6	2	5	-1	4	-2	6	2	25	2.5
4	0	6	0	4	2	6	-2	6	4	30	3
6	-2	5	1	3	1	6	2	2	1	25	2.5
6	-1	5	2	4	0	6	1	4	3	30	3
5	0	4	2	4	1	4	2	6	-1	27	2.7
4	1	6	1	4	1	5	-1	3	-1	23	2.3
5	0	4	2	3	2	6	-2	3	-1	22	2.2
6	1	5	1	3	-1	5	-1	3	1	23	2.3
5	-2	4	0	4	2	4	-2	6	4	25	2.5
4	0	5	3	5	0	4	-2	6	1	26	2.6
5	1	4	0	4	0	5	4	6	4	33	3.3
6	-1	4	3	5	2	6	1	3	-1	28	2.8
6	1	6	3	3	2	5	-1	2	-1	26	2.6
4	1	5	1	5	0	6	3	6	1	32	3.2
4	-1	5	1	4	2	5	4	3	-1	26	2.6
4	-1	4	3	3	-1	4	-1	6	2	23	2.3
5	0	6	3	3	0	5	0	3	1	26	2.6
6	0	4	3	3	0	4	3	6	4	33	3.3
4	-2	6	1	4	0	4	1	2	0	20	2
6	1	6	3	4	1	5	-2	2	3	29	2.9
6	-2	6	0	5	-1	4	4	6	0	28	2.8
6	-2	5	0	5	-1	4	0	6	0	23	2.3
4	-2	5	0	4	0	5	3	6	3	28	2.8

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Raw SUS Sum Score	Raw SUS mean score
6	0	4	2	4	0	5	-2	6	-1	24	2.4
5	1	6	1	3	1	4	3	3	2	29	2.9
4	0	6	2	5	0	4	-1	6	-1	25	2.5
4	-2	5	3	4	1	4	1	6	2	28	2.8
6	1	6	3	5	2	4	-1	6	4	36	3.6
5	-1	5	1	3	-1	5	2	5	4	28	2.8
5	0	6	3	5	0	4	3	5	3	34	3.4
6	0	4	0	5	2	4	-2	5	4	28	2.8
5	-1	6	1	5	2	4	-2	6	1	27	2.7
5	0	5	0	5	-1	6	0	3	0	23	2.3
4	0	5	2	5	-1	4	4	4	2	29	2.9
5	1	4	0	4	-1	5	2	6	1	27	2.7
6	-1	4	0	5	2	4	0	2	4	26	2.6
5	-2	4	0	4	1	4	0	5	3	24	2.4
5	0	5	3	4	-1	6	3	3	3	31	3.1
5	-1	6	3	5	1	5	1	5	4	34	3.4
4	-2	4	2	4	-1	5	3	4	-1	22	2.2
6	-1	4	0	4	-1	4	2	6	0	24	2.4
5	-2	5	1	3	-1	6	-2	3	2	20	2
6	-1	6	0	3	2	4	0	4	0	24	2.4
6	0	5	1	4	-1	4	0	4	3	26	2.6
5	-2	4	0	5	2	4	2	6	2	28	2.8
4	1	4	0	5	-1	4	3	6	0	26	2.6
6	0	4	1	4	0	6	-1	6	3	29	2.9
5	0	5	2	4	1	4	-1	4	-1	23	2.3
6	1	6	3	3	1	6	3	3	-1	31	3.1
6	1	6	1	5	1	6	-1	5	2	32	3.2
5	0	4	1	5	2	5	-2	5	1	26	2.6
6	-1	6	3	5	-1	5	1	3	-1	26	2.6
4	-1	5	0	4	2	5	1	6	-1	25	2.5
5	1	5	1	5	2	4	0	2	4	29	2.9
4	-2	4	1	4	-1	6	-1	3	2	20	2
4	0	4	0	5	1	5	3	3	2	27	2.7
6	1	5	1	4	0	4	-2	5	-1	23	2.3
4	-1	4	3	4	-1	6	-1	6	-1	23	2.3
5	-1	4	3	4	2	4	-2	5	1	25	2.5
5	1	6	0	5	-1	6	-2	6	-1	25	2.5
6	0	4	1	5	2	4	1	6	4	33	3.3
6	-1	5	1	4	1	5	4	3	4	32	3.2
4	-1	6	1	5	-1	4	1	5	1	25	2.5
5	-1	4	3	5	2	6	1	5	3	33	3.3

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Raw SUS Sum Score	Raw SUS mean score
5	-1	4	3	4	-1	4	-1	5	-1	21	2.1
5	0	6	1	4	1	6	3	4	3	33	3.3
4	1	6	3	3	0	4	2	5	1	29	2.9
6	0	4	0	5	-1	5	1	5	2	27	2.7
5	-1	4	1	5	2	5	-1	5	3	28	2.8
6	1	6	1	5	0	5	-1	4	0	27	2.7
5	-1	4	1	3	2	6	2	2	2	26	2.6
4	1	5	3	3	2	4	3	4	1	30	3
5	-1	6	3	5	-1	4	1	4	3	29	2.9
5	0	4	1	3	2	6	2	3	1	27	2.7
5	-1	6	2	3	-1	5	4	2	1	26	2.6
6	-1	6	3	5	1	4	-2	4	2	28	2.8
4	0	4	3	3	-1	4	1	6	-1	23	2.3
5	1	5	3	3	2	6	0	3	4	32	3.2
4	0	6	0	5	1	6	1	6	4	33	3.3
4	0	6	2	4	2	6	3	2	1	30	3
5	-2	5	0	5	2	6	2	5	4	32	3.2
5	-1	6	1	5	2	4	0	2	2	26	2.6
6	-1	4	2	5	2	5	4	2	0	29	2.9
6	-1	6	2	4	1	4	3	2	2	29	2.9
5	-1	4	0	5	0	6	-2	6	1	24	2.4
5	1	6	2	5	0	6	4	2	4	35	3.5
4	0	6	0	3	2	4	-1	4	1	23	2.3
4	-1	4	2	5	1	6	3	5	4	33	3.3
4	-1	4	2	3	-1	6	-1	6	2	24	2.4
4	-1	6	0	3	0	6	1	2	4	25	2.5
5	1	5	3	3	-1	5	4	5	0	30	3
6	-2	5	1	4	0	4	-2	5	3	24	2.4
5	-2	6	3	3	2	4	1	5	-1	26	2.6
5	0	5	0	4	2	4	0	2	2	24	2.4
5	0	6	1	4	0	4	2	4	1	27	2.7
4	-2	4	3	5	0	5	-1	4	1	23	2.3
5	1	6	3	3	0	4	-2	5	2	27	2.7
6	1	6	1	3	0	6	4	2	1	30	3
6	-2	4	1	3	0	4	-2	2	4	20	2
4	0	5	3	3	-1	6	4	5	2	31	3.1
4	0	5	0	4	2	4	-2	4	1	22	2.2
4	-2	5	2	4	-1	5	3	6	-1	25	2.5
5	1	6	0	3	-1	5	-1	4	4	26	2.6
6	-1	5	2	4	0	6	1	4	3	30	3
5	-2	4	0	4	2	4	-2	6	4	25	2.5

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Raw SUS Sum Score	Raw SUS mean score
4	-2	5	3	4	1	4	1	6	2	28	2.8
5	-1	6	1	5	2	4	-2	6	1	27	2.7
5	0	5	2	4	1	4	-1	4	-1	23	2.3
5	1	5	1	5	2	4	0	2	4	29	2.9
5	-1	6	2	3	-1	5	4	2	1	26	2.6

Appendix I

Participant	Inflated Score (adjusted to a range of 0 - 100)	Adjective Rating
p1	55	Good
p2	67.5	Good
p3	75	Excellent
p4	72.5	Good
p5	82.5	Excellent
p6	67.5	Good
p7	62.5	Good
p8	65	Good
p9	67.5	Good
p10	85	Excellent
p11	72.5	Good
p12	62.5	Good
p13	75	Excellent
p14	80	Excellent
p15	75	Excellent
p16	72.5	Good
p17	57.5	Good
p18	57.5	Good
p19	77.5	Excellent
p20	67.5	Good
p21	60	Good
p22	80	Excellent
p23	80	Excellent
p24	52.5	Good
p25	62.5	Good
p26	75	Excellent
p27	70	Good
p28	70	Good
p29	85	Excellent
p30	67.5	Good
p31	67.5	Good
p32	55	Good
p33	82.5	Excellent
p34	70	Good
p35	70	Good
p36	52.5	Good
p37	60	Good
p38	60	Good
p39	67.5	Good

Participant	Inflated Score (adjusted to a range of 0 - 100)	Adjective Rating
p40	62.5	Good
p41	42.5	Ok
p42	55	Good
p43	70	Good
p44	62.5	Good
p45	50	Ok
p46	67.5	Good
p47	57.5	Good
p48	57.5	Good
p49	75	Excellent
p50	50	Ok
p51	55	Good
p52	75	Excellent
p53	62.5	Good
p54	70	Good
p55	82.5	Excellent
p56	65	Good
p57	42.5	Ok
p58	57.5	Good
p59	55	Good
p60	65	Good
p61	62.5	Good
p62	67.5	Good
p63	60	Good
p64	40	Ok
p65	62.5	Good
p66	55	Good
p67	57.5	Good
p68	52.5	Good
p69	57.5	Good
p70	67.5	Good
p71	50	Ok
p72	65	Good
p73	52.5	Good
p74	62.5	Good
p75	60	Good
p76	70	Good
p77	70	Good
p78	82.5	Excellent
p79	65	Good
p80	65	Good

Participant	Inflated Score (adjusted to a range of 0 - 100)	Adjective Rating
p81	65	Good
p82	85	Excellent
p83	72.5	Good
p84	67.5	Good
p85	65	Good
p86	72.5	Good
p87	77.5	Excellent
p88	62.5	Good
p89	52.5	Good
p90	67.5	Good
p91	55	Good
p92	62.5	Good
p93	75	Excellent
p94	55	Good
p95	62.5	Good
p96	57.5	Good
p97	65	Good
p98	50	Ok
p99	62.5	Good
p100	75	Excellent
p101	62.5	Good
p102	75	Excellent
p103	67.5	Good
p104	57.5	Good
p105	55	Good
p106	57.5	Good
p107	62.5	Good
p108	65	Good
p109	82.5	Excellent
p110	70	Good
p111	65	Good
p112	80	Excellent
p113	65	Good
p114	57.5	Good
p115	65	Good
p116	82.5	Excellent
p117	50	Ok
p118	72.5	Good
p119	70	Good
p120	57.5	Good
p121	70	Good

Participant	Inflated Score (adjusted to a range of 0 - 100)	Adjective Rating
p122	60	Good
p123	72.5	Good
p124	62.5	Good
p125	70	Good Best
p126	90	Imaginable
p127	70	Good
p128	85	Excellent
p129	70	Good
p130	67.5	Good
p131	57.5	Good
p132	72.5	Good
p133	67.5	Good
p134	65	Good
p135	60	Good
p136	77.5	Excellent
p137	85	Excellent
p138	55	Good
p139	60	Good
p140	50	Ok
p141	60	Good
p142	65	Good
p143	70	Good
p144	65	Good
p145	72.5	Good
p146	57.5	Good
p147	77.5	Excellent
p148	80	Excellent
p149	65	Good
p150	65	Good
p151	62.5	Good
p152	72.5	Good
p153	50	Ok
p154	67.5	Good
p155	57.5	Good
p156	57.5	Good
p157	62.5	Good
p158	62.5	Good
p159	82.5	Excellent
p160	80	Excellent
p161	62.5	Good
p162	82.5	Excellent

Participant	Inflated Score (adjusted to a range of 0 - 100)	Adjective Rating
p163	52.5	Good
p164	82.5	Excellent
p165	72.5	Good
p166	67.5	Good
p167	70	Good
p168	67.5	Good
p169	65	Good
p170	75	Excellent
p171	72.5	Good
p172	67.5	Good
p173	65	Good
p174	70	Good
p175	57.5	Good
p176	80	Excellent
p177	82.5	Excellent
p178	75	Excellent
p179	80	Excellent
p180	65	Good
p181	72.5	Good
p182	72.5	Good
p183	60	Good Best
p184	87.5	Imaginable
p185	57.5	Good
p186	82.5	Excellent
p187	60	Good
p188	62.5	Good
p189	75	Excellent
p190	60	Good
p191	65	Good
p192	60	Good
p193	67.5	Good
p194	57.5	Good
p195	67.5	Good
p196	75	Excellent
p197	50	Ok
p198	77.5	Excellent
p199	55	Good
p200	62.5	Good
p201	65	Good
p202	75	Excellent
p203	62.5	Good

Participant	Inflated Score (adjusted to a range of 0 - 100)	Adjective Rating
p204	70	Good
p205	67.5	Good
p206	57.5	Good
p207	72.5	Good
p208	65	Good

Appendix J

<p>Physical Access Data Loss</p>  <p>Warning Will cause loss of data May cause unauthorized use of personal information i.e., username, credit card information</p> <p>Ways of Identification:</p> <ol style="list-style-type: none"> 1. Please refer to countermeasures to protect yourself. <p>Countermeasures:</p> <ol style="list-style-type: none"> 1. Backup device regularly. 2. Make sure two-factor authentication is enabled. 3. Set up remote deletion of device data. <p>Refer to SDS for more information.</p>	<p>Physical Access Malicious Charging Station</p>  <p>Warning May expose device to malware. May cause loss of confidentiality, integrity, and availability of device data</p> <p>Ways of Identification:</p> <ol style="list-style-type: none"> 1. Please refer to countermeasures to protect yourself. <p>Countermeasures:</p> <ol style="list-style-type: none"> 1. Avoid using public USB ports to charge your device. 2. Use device AC charging adaptor and your own cables. 3. Carry a certified mobile battery to avoid reliance of public power sources of opportunity. 4. Don't use someone else's PC/laptop for charging your device. 5. Monitor device for unusual activity 6. Delete suspicious apps you don't recall installing. 7. Restore device to factory setting. 8. Install anti-virus on device. 9. Keep device UpToDate. <p>Refer to SDS for more information.</p>	<p>Authentication Biometric Spoofing</p>   <p>Warning May allow attacker to impersonate user and gain access to device.</p> <p>Ways of Identification:</p> <ol style="list-style-type: none"> 1. ***Please refer to countermeasures to prevent this threat.*** <p>Countermeasures:</p> <ol style="list-style-type: none"> 1. Ensure that the mobile apps and operating system is UpToDate. <p>Refer to SDS for more information.</p>
<p>Application Ransomware</p>  <p>Warning May lock or steal device data before demanding payment to return data or unlock device.</p> <p>Ways of Identification:</p> <ol style="list-style-type: none"> 1. Fake links 2. Apps not downloaded from legitimate app stores i.e., Google play <p>Countermeasures:</p> <ol style="list-style-type: none"> 1. Ensure that the mobile apps and operating system is UpToDate. 2. Make sure all apps are downloaded from either the App Store or Google Play. 3. Back-up files of the mobile device. 4. Use and run regular scans using a comprehensive security solution i.e., Norton Mobile Security, Malwarebytes. 5. Don't share personal information. 6. Don't save passwords on device. <p>Refer to SDS for more information.</p>	<p>Application DDoS</p>    <p>Warning May prevent access to mobile services such as email, websites, online accounts (i.e., banking) or others that rely on the mobile device.</p> <p>Ways of Identification:</p> <ol style="list-style-type: none"> 1. Unusually slow network performance i.e., opening files/apps or accessing websites. 2. Unavailability of particular websites. 3. Inability to access any apps or websites. <p>Countermeasures:</p> <ol style="list-style-type: none"> 1. Install and maintain antivirus on mobile device. 2. Only download trustworthy apps. 3. Check ratings and reviews of apps before installing. <p>Refer to SDS for more information.</p>	<p>Cellular Eavesdropping</p>  <p>Warning May cause a loss of privacy, identity theft, and/or financial loss.</p> <p>Countermeasures:</p> <ol style="list-style-type: none"> 1. Avoid public wi-fi network. 2. Install and keep updated antivirus software. 3. Use strong passwords. <p>Refer to SDS for more information.</p>
<p>Application Mobile Malware</p>  <p>Warning May steal personal and business information without users knowledge</p> <p>Ways of Identification:</p> <ol style="list-style-type: none"> 1. Unexplained increase in mobile data usage. 2. Battery is draining faster than usual. 3. Device starts to overheat. 4. Unfamiliar apps start to show up on device. 5. Wi-Fi and mobile data turn on automatically. 6. Sudden appearance of pop-up ads. <p>Countermeasures:</p> <ol style="list-style-type: none"> 1. Ensure that the mobile apps and operating system is UpToDate. 2. Make sure all apps are downloaded from either the App Store or Google Play. 3. Do not jailbreak mobile device. <p>Refer to SDS for more information.</p>	<p>Authentication Email Phishing attack</p>   <p>Warning May cause identity and data theft from device. Causes unauthorized use of personal information i.e., username, credit card information</p> <p>Ways of Identification:</p> <ol style="list-style-type: none"> 1. Incorrect "From" Addresses. 2. Urgent action required. 3. Generic greeting 4. Fake links 5. Requests for personal information. <p>Countermeasures:</p> <ol style="list-style-type: none"> 1. Always double-check and make sure the address is correct. 2. Scrutinize urgent emails to make sure it is legitimate. 3. Check for generic greetings and whether the email has been personalized to you. 4. Do not click on random links received from an incorrect "From" Address. <p>Refer to SDS for more information.</p>	<p>LAN & PAN WiFi Tracking</p>   <p>Warning May allow device to be tracked. May expose personal information to attacker.</p> <p>Countermeasures:</p> <ol style="list-style-type: none"> 1. Frequently change hotspot network name. 2. Turn off Wi-Fi when not in use. <p>Refer to SDS for more information.</p>
<p>Payments Mobile Banking Vulnerability</p>  <p>Warning May cause disruption and/or loss of financial data.</p> <p>Ways of Identification:</p> <ol style="list-style-type: none"> 1. Please refer to countermeasures to protect yourself. <p>Countermeasures:</p> <ol style="list-style-type: none"> 1. Consider using online transactions through web browsers instead of 3rd party mobile banking apps. 2. Use pre-paid card services for any payment apps; this limits the potential financial threat. <p>Refer to SDS for more information.</p>	<p>Authentication NFC Payment attack</p>  <p>Warning May cause a loss in confidentiality, integrity, and availability of payment data.</p> <p>Ways of Identification:</p> <ol style="list-style-type: none"> 1. Please refer to countermeasures to protect yourself. <p>Countermeasures:</p> <ol style="list-style-type: none"> 1. Turn off NFC on device when not in use. 2. Make sure device is kept up to date. <p>Refer to SDS for more information.</p>	<p>LAN & PAN Wifi Eavesdropping</p>  <p>Warning May cause identity and data theft from device. Causes unauthorized use of personal information i.e., username, credit card information</p> <p>Countermeasures:</p> <ol style="list-style-type: none"> 1. Avoid public wi-fi network. 2. Install and keep updated antivirus software. 3. Use strong passwords. <p>Refer to SDS for more information.</p>

Appendix K



References

- Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, 32(3), 183-196.
- Abrams, M. (1998). *NIMS information security threat methodology (research report no. 98W0000094)*. Center for Advanced Aviation System Development. <https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.195.5420>
- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509-514.
- Adams, C. N., & Snider, D. H. (2018, April 19-22). *Effective Data Visualization in Cybersecurity* [Paper Presentation]. IEEE SoutheastCon, St. Petersburg, FL, United States
- Ahmed, A., Naji, A., & Tseng, M. L. (2020). A decision model for selecting a safety data sheet management system using fuzzy TOPSIS. *Journal of Modelling in Management*. Advance online publication. <https://doi.org/10.1108/JM2-05-2019-0109>.
- Alhabeeb, M., Almuhaideb, A., Le, P. D., & Srinivasan, B. (2010, April 20-23). *Information security threats classification pyramid* [Paper Presentation]. IEEE 24th International Conference on Advanced Information Networking and Applications Workshops, Perth, WA, Australia.
- Alhakami, W., Mansour, A., & Safdar, G. A. (2014). Spectrum sharing security and attacks in crns: A review. *International Journal of Advanced Computer Science and Applications*, 5(1), 76-87.
- Alias, N. (2015). Designing, developing and evaluating a learning support tool: A case of design and development research (DDR). *SAGE Research Methods Cases*. doi:10.4135/978144627305014558820
- Almutairi, M., & Riddle, S. (2017, May 10-12). *Security threat classification for outsourced IT projects* [Paper presentation]. 11th International Conference on Research Challenges in Information Science (RCIS), Brighton, United Kingdom.
- Almutairi, M., & Riddle, S. (2018, January). *A Framework for managing security risks of outsourced IT projects: An empirical study* [Paper presentation]. ICSIM2018: Proceedings of the 2018 International Conference on Software Engineering and Information Management, Casablanca, Morocco.
- Amoroso, E. G. (1994). *Fundamentals of computer security technology*. Prentice-Hall, Inc.

- Anwar, M. N., Nazir, M., & Mustafa, K. (2017, September 15-16). *Security threats taxonomy: Smart-home perspective* [Paper presentation]. 2017 3rd International Conference on Advances in Computing, Communication & Automation, Dehradun, India.
- Apatsidou, M., Konstantopoulou, I., Foufa, E., Tsarouhas, K., Papalexis, P., Rezaee, R., Spandidos, D., Kouretas, D., & Tsitsimpikou, C. (2018). Safe use of chemicals by professional users and health care specialists. *Biomedical reports*, 8(2), 160-165. <https://doi:10.3892/br.2018.1037>
- Applegate, S. D., & Stavrou, A. (2013, June 4-7). *Towards a cyber conflict taxonomy* [Paper presentation]. 5th International Conference on Cyber Conflict (CYCON 2013), Tallinn, Estonia.
- Avizienis, A., Laprie, J. C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE transactions on dependable and secure computing*, 1(1), 11-33.
- Bailey, J. E., & Pearson, S. W. (1983). Development of a tool for measuring and analyzing computer user satisfaction. *Management science*, 29(5), 530-545.
- Baldwin, A., Beres, Y., Duggan, G. B., Mont, M. C., Johnson, H., Middup, C., & Shiu, S. (2013). Economic methods and decision making by security professionals. In B. Schneier (Ed.), *Economics of information security and privacy III* (pp. 213-238). Springer.
- Bangor, A., Kortum, P. T., & Miller, J. T. (2008). An empirical evaluation of the system usability scale. *International Journal of Human-Computer Interaction*, 24(6), 574-594.
- Bano, M., Zowghi, D., & da Rimini, F. (2017). User satisfaction and system success: an empirical exploration of user involvement in software development. *Empirical Software Engineering*, 22(5), 2339-2372.
- Baptista, G., & Oliveira, T. (2015). Understanding mobile banking: The unified theory of acceptance and use of technology combined with cultural moderators. *Computers in Human Behavior*, 50, 418-430.
- Barn, R., & Barn, B. (2016, June 12-15). *An ontological representation of a taxonomy for cybercrime* [Paper presentation]. 24th European Conference on Information Systems, Istanbul, Turkey.
- Barros, I. M., Alcântara, T. S., Mesquita, A. R., Santos, A. C. O., Paixão, F. P., & Lyra Jr, D. P. (2014). The use of pictograms in the health care: a literature review. *Research in Social and Administrative Pharmacy*, 10(5), 704-719.

- Ben-Bassat, T., & Shinar, D. (2006). Ergonomic guidelines for traffic sign design increase sign comprehension. *Human factors*, 48(1), 182-195.
- Bertino, E. (2016). Security threats: Protecting the new cyberfrontier. *Computer* 49(6), 11-14.
- Bitton, R., Finkelshtein, A., Sidi, L., Puzis, R., Rokach, L., & Shabtai, A. (2018). Taxonomy of mobile users' security awareness. *Computers & Security*, 73, 266-293.
- Blees, G. J., & Mak, W. M. (2012). Comprehension of disaster pictorials across cultures. *Journal of Multilingual and Multicultural Development*, 33(7), 699-716.
- Boelhouwer, E., Davis, J., Franco-Watkins, A., Dorris, N., & Lungu, C. (2013). Comprehension of hazard communication: Effects of pictograms on safety data sheets and labels. *Journal of Safety Research*, 46, 145-155.
- Bompard, E., Huang, T., Wu, Y., & Cremenescu, M. (2013). Classification and trend analysis of threats origins to the security of power systems. *International Journal of Electrical Power & Energy Systems*, 50, 50-64.
- Brahm, F., & Singer, M. (2013). Is more engaging safety training always better in reducing accidents? Evidence of self-selection from chilean panel data. *Journal of Safety Research*, 47, 85-92.
- Brancheau, J. C., & Wetherbe, J. C. (1987). Key issues in information systems management. *MIS Quarterly*, 11(1), 23-45.
- Brooks, E. L., Keyt, B., & London, I. (2017). Chemical hazard communication: What US employers need to know about globally harmonized system standards. *Natural Resources & Environment*, 32(1), 43-47.
- Brown, C., Dog, S., Franklin, J. M., McNab, N., Voss-Northrop, S., Peck, M., & Stidham, B. (n.d.). Assessing threats to *mobile devices and infrastructure* (NISTIR 8144). Retrieved from <http://dx.doi.org/10.6028/NIST.IR.8144>
- Butler, R. (2020). A systematic literature review of the factors affecting smartphone user threat avoidance behaviour. *Information & Computer Security*. Advance online publication. <https://doi.org/10.1108/ICS-01-2020-0016>
- Caffaro, F., & Cavallo, E. (2015). Comprehension of safety pictograms affixed to agricultural machinery: A survey of users. *Journal of Safety Research*, 55, 151-158.
- Campbell, D. T., & Cook, T. D. (1979). *Quasi-experimentation: Design & analysis issues for field settings*. Chicago, IL: Rand McNally College Publishing Company.

- Carle, S. D. (1987). A hazardous mix: Discretion to disclose and incentives to suppress under OSHA's hazard communication standard. *The Yale Law Journal*, 97(4), 581-601.
- Carlton, M. (2016). *Development of a cybersecurity skills index: A scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills* (Publication No. 10240271) [Doctoral dissertation, Nova Southeastern University]. ProQuest Dissertations and Theses Global.
- Carlton, M., & Levy, Y. (2015, April 9-12). *Expert assessment of the top platform independent cybersecurity skills of non-IT professionals* [Paper presentation]. SoutheastCon 2015, Fort Lauderdale, FL, United States.
- Chan, A. H., & Ng, A. W. (2010a). Effects of sign characteristics and training methods on safety sign training effectiveness. *Ergonomics*, 53(11), 1325-1346.
- Chan, A. H., & Ng, A. W. (2010b). Investigation of guessability of industrial safety signs: Effects of prospective-user factors and cognitive sign features. *International Journal of Industrial Ergonomics*, 40(6), 689-697.
- Cheng, L., & Wang, J. (2019). Walls have no ears: A non-intrusive WiFi-based user identification system for mobile devices. *IEEE/ACM Transactions on Networking*, 27(1), 245-257.
- Chidambaram, V. (2004). Threat modeling in enterprise architecture integration. *Enterprise architecture & business competitiveness*, 2(4), 29-36.
- Choi, J. (2011). Literature review: Using pictographs in discharge instructions for older adults with low-literacy skills. *Journal of clinical nursing*, 20(21), 2984-2996.
- Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 30(8), 719-731.
- Cisco. (2018). *Annual cybersecurity report*. Retrieved from https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf.
- Cook, T. D., & Campbell, D. T. (1979). *Quasi-experimentation: Design and analytical*. Chicago, IL: Rand McNally.
- Cybersecurity Curricula 2017 (CSEC2017), Joint Task Force. (2017). *Curriculum guidelines for post-secondary degree programs in cybersecurity*. Retrieved from <https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf>

- Dalkey, N., & Helmer, O. (1963). An experimental application of the delphi method to the use of experts. *Management Science*, 9(3), 458-467.
- Davies, S., Haines, H., Norris, B., & Wilson, J. R. (1998). Safety pictograms: Are they getting the message across? *Applied Ergonomics*, 29(1), 15-23.
- Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior*, 26(6), 1739-1747.
- Deloitte, Deloitte Global Mobile Consumer Survey. (2016). *There's no place like phone: consumer usage patterns in the era of smartphone*. Retrieved from <http://www.deloitte.co.uk/mobileUK/assets/pdf/DeloitteMobile-Consumer-2016-There-is-no-place-like-phone.pdf>
- Demchenko, Y., Gommans, L., de Laat, C., & Oudenaarde, B. (2005, November 3). *Web services and grid security vulnerabilities and threats analysis and model* [Paper presentation]. The 6th IEEE/ACM International Workshop on Grid Computing, Seattle, WA, United States.
- Dooley, P. (2015). *An Empirical Development of Critical Value Factors for System Quality and Information Quality in Business Intelligence Systems Implementations* (Publication No. 3703380) [Doctoral dissertation, Nova Southeastern University]. ProQuest Dissertations and Theses Global.
- Dooley, P. P., Levy, Y., Hackney, R. A., & Parrish, J. L. (2018). Critical value factors in business intelligence systems implementations. In A. V. Deokar, A. Gupta, L. S. Iyer & M. C. Jones (Eds.), *Analytics and data science: Advances in research and pedagogy* (pp. 55-78). Springer. https://doi.org/10.1007/978-3-319-58097-5_6
- Doll, W. J., & Torkzadeh, G. (1991). The measurement of end-user computing satisfaction: Theoretical and methodological issues. *MIS Quarterly*, 15(1), 5-9.
- Doll, W. J., Xia, W., & Torkzadeh, G. (1994). A confirmatory factor analysis of the end-user computing satisfaction instrument. *MIS quarterly*, 18(4), 453-461.
- Donalds, C., & Osei-Bryson, K.-M. (2019). Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior*, 92, 403-418.
- Dorris, A. L., & Purswell, J. L. (1978, October 1). *Human factors in the design of effective product warnings* [Paper presentation]. Human Factors and Ergonomics Society Annual Meeting, Los Angeles, CA, United States.
- Dowse, R., & Ehlers, M. (2005). Medicine labels incorporating pictograms: Do they influence understanding and adherence? *Patient Education and Counseling*, 58(1), 63-70.

- Dowse, R., & Ehlers, M. S. (2001). The evaluation of pharmaceutical pictograms in a low-literate South African population. *Patient Education and Counseling*, 45(2), 87-99.
- Duarte, E., Rebelo, F., Teles, J., & Wogalter, M. S. (2014). Safety sign comprehension by students, adult workers and disabled persons with cerebral palsy. *Safety Science*, 62, 175-186.
- Duarte, M. E. C., & Rebelo, F. (2005). *Comprehension of safety signs: internal and external variable influences and comprehension difficulties by disabled people* [Paper presentation]. CybErg, Johannesburg, South Africa.
- Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science & Information Technology*, 6, 323-337.
- Fahlman, D. (2017). Mobiles in the workplace. In J. Traxler (Ed.), *Capacity building in a changing ICT environment* (pp. 47-57). Geneva, Switzerland: International Telecommunication Union.
- Farahmand, F., Navathe, S. B., Sharp, G. P., & Enslow, P. H. (2005). A management perspective on risk of security threats to information systems. *Information Technology and Management*, 6(2-3), 203-225.
- Feng, N., Wang, H. J., & Li, M. (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Information sciences*, 256, 57-73.
- Ferrando, R., & Stacey, P. (2017). *Classification of device behaviour in internet of things infrastructures: towards distinguishing the abnormal from security threats*. International Conference on Internet of Things and Machine Learning, Liverpool, United Kingdom.
- Furnell, S. (2005). Why users cannot use security. *Computers & Security*, 24(4), 274-279.
- Furnell, S. (2007). Making security usable: Are things improving? *Computers & Security*, 26(6), 434-443.
- Furnell, S. M., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security*, 25(1), 27-35.
- Geric, S., & Hutinski, Ž. (2007). Information system security threats classifications. *Journal of Information and Organizational Sciences*, 31(1), 51-61.
- Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). 2005 CSI/FBI computer crime and security survey. *Computer Security Journal*, 21(3), 21-40.

- GSM Association. (2018). *The mobile economy*. Retrieved from <https://www.gsmainelligence.com/research/?file=b9a6e6202ee1d5f787cfebb95d3639c5&download>
- Gupta, S., & Kumar, P. (2013). Taxonomy of cloud security. *International Journal of Computer Science, Engineering and Applications*, 3(5), 47-67.
- Hancock, H. E., Fisk, A. D., & Rogers, W. A. (2005). Comprehending product warning information: age-related effects and the roles of memory, inferencing, and knowledge. *Human Factors*, 47(2), 219-234.
- Hancock, H. E., Rogers, W. A., Schroeder, D., & Fisk, A. D. (2004). Safety symbol comprehension: Effects of symbol type, familiarity, and age. *Human Factors*, 46(2), 183-195.
- Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer attacks. *Computers & Security*, 24(1), 31-43.
- Hara, K., Mori, M., Ishitake, T., Kitajima, H., Sakai, K., Nakaaki, K., & Jonai, H. (2007). Results of recognition tests on Japanese subjects of the labels presently used in Japan and the UN-GHS labels. *Journal of Occupational Health*, 49(4), 260-267.
- Hart, C. (2018). *Doing a literature review: Releasing the research imagination*. London, United Kingdom: Sage Publications Ltd.
- Hasan, B., Rajski, E., Gómez, J. M., & Kurzhöfer, J. (2016). A proposed model for user acceptance of mobile security measures—business context. In K. Kim, N. Wattanapongsakom, & N. Joukov (Eds.), *Lecture Notes in Electrical Engineering: Vol 391. Mobile and Wireless Technologies* (pp. 97-108).
- Hewitt, B., Dolezel, D., & McLeod, A., Jr. (2017). Mobile device security: Perspectives of future healthcare workers. *Perspectives in Health Information Management*, 14(1c), 1-14.
- Hong, J. C., Tai, K. H., Hwang, M. Y., Kou, Y. C., & Chen, J. S. (2017). Internet cognitive failure relevant to users' satisfaction with content and interface design to reflect continuance intention to use a government e-learning system. *Computers in Human Behavior*, 66, 353-362.
- Hovav, A., & Gray, P. (2014). The ripple effect of an information security breach event: A stakeholder analysis. *Communications of the Association for Information Systems*, 34(50), 893-912.

- Howard, J. D. (1997). *An analysis of security incidents on the Internet 1989-1995* (Doctoral Dissertation, Carnegie-Mellon). Retrieved from <https://apps.dtic.mil/dtic/tr/fulltext/u2/a389085.pdf>
- Howard, M., & Lipner, S. (2006). *The security development lifecycle* (Vol. 8). Redmond: Microsoft Press.
- Hughes, N., & Burke, J. (2018). Sleeping with the frenemy: How restricting ‘bedroom use’ of smartphones impacts happiness and wellbeing. *Computers in Human Behavior*, 85, 236-244.
- IBM global technology services. (2014). *IBM security services 2014 cyber security intelligence index*. Retrieved from https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligence_20450.pdf
- Igure, V. M., & Williams, R. D. (2008). Taxonomies of attacks and vulnerabilities in computer systems. *IEEE Communications Surveys & Tutorials*, 10(1), 6-19.
- International Organization for Standardization. (2019). *Ergonomics of Human-System Interaction—Part 210: Human-Centred Design for Interactive Systems (ISO-9241-210:2019)*. <https://www.iso.org/standard/77520.html>
- International Telecommunication Union (ITU). (2017a). *Measuring the information society report*. Retrieved from <https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017.aspx>
- International Telecommunication Union (ITU). (2017b). *ICT facts and figures*. Retrieved from <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf>
- Ives, B., Olson, M. H., & Baroudi, J. J. (1983). The measurement of user information satisfaction. *Communications of the ACM*, 26(10), 785-793.
- Jones, H. S., & Towse, J. (2018). Examinations of email fraud susceptibility: Perspectives from academic research and industry practice. In J. McAlaney, L. Frumkin, & V. Benson (Eds.), *Psychological and Behavioral Examinations in Cybersecurity* (pp. 80-97). IGI Global.
- Joshi, Y., & Kothiyal, P. (2011). A pilot study to evaluate pharmaceutical pictograms in a multispecialty hospital at Dehradun. *Journal of Young Pharmacists*, 3(2), 163-166.
- Jouini, M., & Ben Arfa Rabai, L. (2016, July). *A scalable threats classification model in information systems* [Paper presentation]. SIN '16: 9th International Conference on Security of Information and Networks, Newark, NJ, United States.

- Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, 32, 489-496.
- Kalmegh, S. R., & Deshmukh, S. N. (2014). Effective Evaluation of Classification of Indigenous News Using Decision Table and OneR Algorithm. *International Journal of Advanced Information Science and Technology*, 26(26), 6-11.
- Kalsher, M. J., Wogalter, M. S., & Racicot, B. M. (1996). Pharmaceutical container labels: enhancing preference perceptions with alternative designs and pictorials. *International Journal of Industrial Ergonomics*, 18(1), 83-90.
- Kearns, G. S. (2016). Countering mobile device threats: A mobile device security model. *Journal of Forensic & Investigative Accounting*, 8(1), 36-48.
- Kido, Y., Tou, N.P., Yanai, N., & Shimojo, S. (2020). sD&D: Design and Implementation of Cybersecurity Educational Game with Highly Extensible Functionality. In K. Arai, S. Kapoor, & R. Bhatia (Eds.), *Advances in Intelligent Systems and Computing* (Vol. 1129, p. 857 - 873). Springer. https://doi.org/10.1007/978-3-030-39445-5_62
- Kim, K. K. (1989). User satisfaction: A synthesis of three different perspectives. *Journal of Information Systems*, 4(1), 1-12.
- Kjaerland, M. (2006). A taxonomy and comparison of computer security incidents from the commercial and government sectors. *Computers & Security*, 25(7), 522-538.
- Kolp, P., Sattler, B., Blayney, M., & Sherwood, T. (1993). Comprehensibility of material safety data sheets. *American Journal of Industrial Medicine*, 23(1), 135-141.
- Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, 29(8), 840-847.
- Kumar, S., Viinikainen, A., & Hamalainen, T. (2017, December 11-14). *Evaluation of ensemble machine learning methods in mobile threat detection* [Paper presentation]. International Conference for Internet Technology and Secured Transactions (ICITST), Cambridge, United Kingdom.
- Kurucay, M., & Inan, F. A. (2017). Examining the effects of learner-learner interactions on satisfaction and learning in an online undergraduate course. *Computers & Education*, 115, 20-37.
- Laughery, K. R. (2006). Safety communications: Warnings. *Applied Ergonomics*, 37(4), 467-478.

- Leavitt, N. (2011). Mobile security: Finally a serious problem? *IEEE Computer*, 44(6), 11-14.
- Lee, S. M., Kim, Y. R., & Lee, J. (1995). An empirical study of the relationships among end-user information systems acceptance, training, and effectiveness. *Journal of management information systems*, 12(2), 189-202.
- Leedy, P. D., Ormrod, J. E., & Johnson, L. R. (2019). *Practical research: Planning and design*. New York: Pearson Education.
- Lesch, M. F. (2003). Comprehension and memory for warning symbols: Age-related differences and impact of training. *Journal of Safety Research*, 34(5), 495-505.
- Lesch, M. F. (2008). Warning symbols as reminders of hazards: Impact of training. *Accident Analysis & Prevention*, 40(3), 1005-1012.
- Levy, Y. (2006). *Assessing the value of e-learning systems*. Hershey, PA: Idea Group Inc (IGI).
- 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, 181-212.
- Levy, Y., Murphy, K. E., & Zanakis, S. H. (2009). A value-satisfaction taxonomy of IS effectiveness (VSTISE): A case study of user satisfaction with IS and user-perceived value of IS. *International Journal of Information Systems in the Service Sector (IJISSS)*, 1(1), 93-118.
- Levy, Y., & Ramim, M. M. (2004). Financing expensive technologies in an era of decreased funding: Think Big... Start Small... Build Fast... In C. Howard, K. Schuenk, & R. Discenza (Eds.), *Distance Learning and University Effectiveness: Changing Educational Paradigms for Online Learning* (pp. 278-301). Hershey, PA : Idea-Group Publishing.
- Lichvar, B. T. (2011). *An empirical investigation of the effect of knowledge sharing and encouragement by others in predicting computer self-efficacy and use of information systems in the workplace* (Publication No. 3461673) [Doctoral dissertation, Nova Southeastern University]. ProQuest Dissertations and Theses Global.
- Lindqvist, U., & Jonsson, E. (1997, May 4-7). *How to systematically classify computer security intrusions* [Paper presentation]. IEEE Symposium on Security and Privacy (Cat. No.97CB36097), Oakland, CA, United States.
- Liu, T., Zhong, M., & Xing, J. (2005). Industrial accidents: Challenges for China's economic and social development. *Safety Science*, 43(8), 503-522.

- Liu, Y. C., & Ho, C. H. (2012). The effects of age on symbol comprehension in central rail hubs in Taiwan. *Applied Ergonomics*, 43(6), 1016-1025.
- Lui, L., & Hoelscher, U. (2006). Evaluation of graphical symbols. In W. Karwowski (Eds.), *International Encyclopedia of Ergonomics and Human Factors* (pp. 1053-1057). doi:10.1201/9780849375477
- Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly*, 16(2), 173-186.
- Mansoor, L. E., & Dowse, R. (2004). Design and evaluation of a new pharmaceutical pictogram sequence to convey medicine usage. *Ergonomics SA*, 16(2), 29-41.
- Masetic, Z., Hajdarevic, K., & Dogru, N. (2017, May 22-26). *Cloud computing threats classification model based on the detection feasibility of machine learning algorithms* [Paper presentation]. International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia.
- McAfee. (2018). *Mobile threat report: The next 10 years*. Retrieved from <https://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2018.pdf>
- McFarland, L. A., & Ployhart, R. E. (2015). Social media: A contextual framework to guide research and practice. *Journal of Applied Psychology*, 100(6), 1653-1677.
- Mertler, C. A., & Reinhart, R. V. (2016). *Advanced and multivariate statistical methods: Practical application and interpretation*. New York: Taylor and Francis Group.
- Mitre Corporation. (2017). *Common vulnerabilities and exposures: Android and iOS CVEs*. Retrieved from <https://cve.mitre.org/>
- Mitrokotsa, A., Rieback, M. R., & Tanenbaum, A. S. (2010). Classifying RFID attacks and defenses. *Information Systems Frontiers*, 12(5), 491-505.
- Montagne, M. (2013). Pharmaceutical pictograms: A model for development and testing for comprehension and utility. *Research in Social & Administrative Pharmacy*, 9(5), 609-620.
- Monteiro, S., Ispolnov, K., & Heleno, L. (2018, June 27-29). *Perception level of hazard pictograms by future engineers* [Paper presentation]. International Conference of the Portuguese Society for Engineering Education (CISPEE), Aveiro, Portugal.
- Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, 34, 47-66.

- Narwal, B., Mohapatra, A. K., & Usmani, K. A. (2019). Towards a taxonomy of cyber threats against target applications. *Journal of Statistics and Management Systems*, 22(2), 301-325.
- National Institute of Standards and Technology (NIST). (2006). *Minimum security requirements for federal information and information Systems* (FIPS PUB 200). Retrieved from <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf>
- Nayar, G., Wehrmeyer, W., Phillips, C., Crankshaw, N., Marsh, N., & France, C. (2016). The efficacy of safety data sheets in informing risk based decision making: A review of the aerospace sector. *Journal of Chemical Health and Safety*, 23(3), 19-29.
- National Institute of Standards and Technology (NIST). (2012). *An introduction to computer security: The nist handbook* (Special Publication 800-12).
- Ng, A. W., & Chan, A. H. (2007). The guessability of traffic signs: Effects of prospective-user factors and sign design features. *Accident Analysis & Prevention*, 39(6), 1245-1257.
- Ng, A. W., & Chan, A. H. (2008). The effects of driver factors and sign design features on the comprehensibility of traffic signs. *Journal of Safety Research*, 39(3), 321-328.
- Ng, A. W., & Chan, A. H. (2011). Investigation of the effectiveness of traffic sign training in terms of training methods and sign characteristics. *Traffic Injury Prevention*, 12(3), 283-295.
- Niewohner, J., Cox, P., Gerrard, S., & Pidgeon, N. (2004). Evaluating the efficacy of a mental models approach for improving occupational chemical risk protection. *Risk Analysis: An International Journal*, 24(2), 349-361.
- O'Connor, C. J., & Lirtzman, S. I. (1984). *Handbook of chemical industry labeling*. Park Ridge, IL: William Andrew.
- Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: An example, design considerations and applications. *Information & Management*, 42(1), 15-29.
- Onwuegbuzie, A. J., Bustamante, R. M., & Nelson, J. A. (2010). Mixed research as a tool for developing quantitative instruments. *Journal of Mixed Methods Research*, 4(1), 56-78.
- Occupational Safety and Health Act (OSHA). (n.d.). *OSHA quick card*. Retrieved from https://www.osha.gov/Publications/HazComm_QuickCard_SafetyData.html

- Occupational Safety and Health Act (OSHA). (2016). *Hazard classification guidance for manufacturers, importers, and employers* (OSHA 3844-02). Retrieved from <https://www.osha.gov/Publications/OSHA3844.pdf>
- Panigrahy, S. K., Jena, S. K., & Turuk, A. K. (2011, February). *Security in Bluetooth, RFID and wireless sensor networks* [Paper presentation]. International Conference on Communication, Computing & Security, Odisha, India.
- Paré, G., Trudel, M.-C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. *Information & Management*, 52(2), 183-199.
- Pascuet, E., Dawson, J., & Vaillancourt, R. (2008). A picture worth a thousand words: the use of pictograms for medication labelling. *International Journal of Pharmaceutics*, 23(1), 1-4.
- Patten, K. P., & Harris, M. A. (2013). The need to address mobile device security in the higher education IT curriculum. *Journal of Information Systems Education*, 24(1), 41.
- Peha, J. M. (2013). *The dangerous policy of weakening security to facilitate surveillance*. Retrieved from <https://ssrn.com/abstract=2350929>
- Penning, N., Hoffman, M., Nikolai, J., & Wang, Y. (2014, May 19-23). *Mobile malware security challenges and cloud-based detection* [Paper presentation]. International Conference on Collaboration Technologies and Systems (CTS), Minneapolis, MN, United States.
- Phillips, C. C., Wallace, B. C., Hamilton, C. B., Pursley, R. T., Petty, G. C., & Bayne, C. K. (1999). The efficacy of material safety data sheets and worker acceptability. *Journal of Safety Research*, 30(2), 113-122.
- Pew research center. (2018). *Mobile fact sheet*. Retrieved from <https://www.pewinternet.org/fact-sheet/mobile/>
- Pratt, I. S. (2002). Global harmonization of classification and labeling of hazardous chemicals. *Toxicology Letters*, 128(1-3), 5-15.
- Ramim, M. M., & Lichvar, B. T. (2014). Eliciting expert panel perspective on effective collaboration in system development projects. *Online Journal of Applied Knowledge Management*, 2(1), 122-136.
- Rauchs, M., & Hileman, G. (2017). *Global cryptocurrency benchmarking study* (No. 201704-gcbs). Retrieved from Cambridge Centre for Alternative Finance, Cambridge Judge Business School, University of Cambridge website:

<https://cdn.crowdfundinsider.com/wp-content/uploads/2017/04/Global-Cryptocurrency-Benchmarking-Study.pdf>

- Rhoades, T. P., Frantz, J. P., & Miller, J. M. (1990). Emerging methodologies for the assessment of safety related product communications. *Human Factors Society, 34*(14), 998-1002.
- Richardson, R. (2008). *CSI computer crime & security survey*. Retrieved from <http://www.sis.pitt.edu/jjoshi/courses/IS2150/Fall11/CSISurvey2008.pdf>
- Richey, R. C., & Klein, J. D. (2014). *Design and development research*. New York, NY: Springer.
- Robinett, F., & Hughes, A. (1984). Visual alerts to machinery hazards: A design case study. In R. Easterby & H. Zwaga, *Information design: The design and evaluation of signs and printed material* (pp. 405-417). Chichester, United Kingdom: Wiley.
- Rocha Flores, W., Holm, H., Svensson, G., & Ericsson, G. (2014). Using phishing experiments and scenario-based surveys to understand security behaviours in practice. *Information Management & Computer Security, 22*(4), 393-406.
- Rokeach, M. (1969). *Beliefs, attitudes, and values*. San Francisco, CA: Jossey-Bass Inc. Publishers.
- Rokeach, M. (1973). *The nature of human values*. New York, NY: The Free Press.
- Rother, H.-A. (2008). South African farm workers' interpretation of risk assessment data expressed as pictograms on pesticide labels. *Environmental Research, 108*(3), 419-427.
- Rothman, B. S., Gupta, R. K., & McEvoy, M. D. (2017). Mobile technology in the perioperative arena: Rapid evolution and future disruption. *Anesthesia & Analgesia, 124*(3), 807-818.
- Rowe, G., & Wright, G. (1999). The Delphi technique as a forecasting tool: Issues and analysis. *International Journal of Forecasting, 15*(4), 353-375.
- Rubbiani, M. (2010). Survey among agricultural workers about interpretation of plant protection product labels and safety data sheets. *Annali dell'Istituto Superiore di Sanità, 46*, 323-329.
- Ruf, L., Thorn, A., Christen, T., Gruber, B., & Portmann, R. (2008). *Threat modeling in security architecture-the nature of threats*. Retrieved from <https://pdfs.semanticscholar.org/09fc/831b360dce8f9924a67aed274f15bebf3e9b.pdf>

- Sadhra, S., Petts, J., McAlpine, S., Pattison, H., & MacRae, S. (2002). Workers' understanding of chemical risks: Electroplating case study. *Occupational and Environmental Medicine*, 59(10), 689-695.
- Sangchoolie, B., Folkesson, P., & Vinter, J. (2018, September 10-14). *A study of the interplay between safety and security using model-implemented fault injection* [Paper presentation]. European Dependable Computing Conference (EDCC), Iasi, Romania.
- Scheele, D. (1975). Reality construction as a product of delphi interaction. In H.A. Linstone, & M. Turoff (Eds.), *The delphi method: Techniques and applications* (pp. 37-71). Addison-Wesley Publishing Company.
- Schmidt, R., Lyytinen, K., Keil, M., & Cule, P. (2001). Identifying software project risks: An international delphi study. *Journal of management information systems*, 17(4), 5-36.
- Sedera, D., Lokuge, S., Grover, V., Sarker, S., & Sarker, S. (2016). Innovating with enterprise systems and digital platforms: A contingent resource-based theory view. *Information & Management*, 53(3), 366-379.
- Sekaran, U. (2003). *Research methods for business: A skill building approach*. New York, NY: John Wiley & Sons.
- Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill building approach*. West Sussex, United Kingdom: John Wiley & Sons.
- Seki, A., Takehara, H., Takigawa, T., Hidehira, T., Nakayama, S., Usamt, M., Uchida, G., & Kira, S. (2001). Use of material safety data sheets at workplaces handling harmful substances in Okayama, Japan. *Journal of Occupational Health*, 43(2), 95-100.
- Sheng, S., Broderick, L., Koranda, C. A., & Hyland, J. J. (2006, July 12-14). *Why Johnny still can't encrypt: Evaluating the usability of email encryption software* [Paper presentation]. Symposium on Usable Privacy and Security, Pittsburg, PA, United States.
- Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing internet users to protect themselves. *Computers in Human Behavior*, 48, 199-207.
- Sigaard, K. T., & Skov, M. (2015). Applying an expectancy-value model to study motivators for work-task based information seeking. *Journal of Documentation*, 71(4), 709-732.

- Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., & Wu, Q. (2014, June 3-4). *AVOIDIT: A cyber attack taxonomy* [Paper presentation]. NYS Cybersecurity Conference, Albany, NY, United States.
- Smith-Jackson, T., & Wogalter, M. (2007). Application of a mental models approach to MSDS design. *Theoretical Issues in Ergonomics Science*, 8(4), 303-319.
- Smith-Jackson, T., & Wogalter, M. S. (1998). Determining the preferred order of materials safety data sheets (MSDS): A user-centered approach. *Human Factors and Ergonomics Society*, 42(15), 1073-1077.
- Smith-Jackson, T., Wogalter, M. S., & Quintela, Y. (2010). Safety climate and pesticide risk communication disparities in crop production by ethnicity. *Human Factors and Ergonomics in Manufacturing & Service Industries*, 20(6), 511-525.
- Smith-Jackson, T. L., & Essuman-Johnson, A. (2002). Cultural ergonomics in Ghana, West Africa: A descriptive survey of industry and trade workers' interpretations of safety symbols. *International Journal of Occupational Safety and Ergonomics*, 8(1), 37-50.
- Souppaya, M., & Scarfone, K. (2013). *Guidelines for managing the security of mobile devices in the enterprise* (NIST SP 800). Retrieved from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf>
- Spinillo, C. G. (2012). Graphic and cultural aspects of pictograms: An information ergonomics viewpoint. *Work*, 41(1), 3398-3403.
- Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, 13(24), 380-429.
- Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, 13(2), 147-169.
- Su, T.-S., & Hsu, I.-Y. (2008). Perception towards chemical labeling for college students in Taiwan using globally harmonized system. *Safety Science*, 46(9), 1385-1392.
- Ta, G. C., Mokhtar, M. B., Mokhtar, H. A. B. M., Ismail, A. B., & Yazid, M. F. B. H. A. (2010). Analysis of the comprehensibility of chemical hazard communication tools at the industrial workplace. *Industrial Health*, 48(6), 835-844.
- Tang, J., Wang, D., Ming, L., & Li, X. (2012). A scalable architecture for classifying network security threats. *Science and Technology on Information System Security Laboratory*, 2012, 1-4.

- International Organization for Standardization (ISO). (2014). *Graphical symbols—test methods—part 1: Method for testing comprehensibility* (ISO 9186-1: 2014). Retrieved from <https://www.iso.org/standard/59226.html>
- Terrell, S. R. (2012). *Statistics translated: A step-by-step guide to analyzing and interpreting data*. New York, NY: Guilford Press.
- Trivedi, K. S., Kim, D. S., Roy, A., & Medhi, D. (2009, October 25-28). *Dependability and security models* [Paper presentation]. International Workshop on Design of Reliable Communication Networks, Washington, DC, United States.
- United Nations (2011). *Globally harmonized system of classification and labelling of chemicals (GHS)*. Retrieved from https://www.unece.org/fileadmin/DAM/trans/danger/publi/ghs/ghs_rev04/English/ST-SG-AC10-30-Rev4e.pdf
- United Nations. (2013). Guidance on the preparation of safety data sheets (SDS). In United Nations (Eds.), *Globally harmonized system for the classification and labelling of chemicals* (pp. 409-428). United Nations.
- Vaillancourt, R., Khoury, C., & Pouliot, A. (2018b). Validation of pictograms for safer handling of medications: comprehension and recall among pharmacy students. *The Canadian journal of hospital pharmacy*, 71(4), 258-266.
- Vaillancourt, R., Pouliot, A., Streitenberger, K., Hyland, S., & Thabet, P. (2016). Pictograms for safer medication management by health care workers. *Canadian Journal of Hospital Pharmacy*, 69(4), 286-293.
- Vaillancourt, R., Zender, M. P., Coulon, L., & Pouliot, A. (2018a). Development of pictograms to enhance medication safety practices of health care workers and international preferences. *Canadian Journal of Hospital Pharmacy*, 71(4), 243-257.
- Van Heerden, R., Irwin, B., Burke, I. D., & Leenen, L. (2012). A computer network attack taxonomy and ontology. *International Journal of Cyber Warfare and Terrorism*, 2(3), 12-25.
- Vecchiato, D., Vieira, M., & Martins, E. (2016, October 23-27). *Risk assessment of user-defined security configurations for android devices* [Paper presentation]. 2016 IEEE 27th International Symposium on Software Reliability Engineering (ISSRE), Ottawa, ON, Canada.
- Walters, A. U., Lawrence, W., & Jalsa, N. K. (2017). Chemical laboratory safety awareness, attitudes and practices of tertiary students. *Safety Science*, 96, 161-171.

- Wang, A.-H., & Chi, C.-C. (2003). Effects of hazardous material symbol labeling and training on comprehension according to three types of educational specialization. *International Journal of Industrial Ergonomics*, 31(5), 343-355.
- Watson, B., & Zheng, J. (2017, April). *On the user awareness of mobile security recommendations*. ACM SE '17: Proceedings of the SouthEast Conference, New York, NY, United States.
- Winder, C., Azzi, R., & Wagner, D. (2005). The development of the globally harmonized system (GHS) of classification and labelling of hazardous chemicals. *Journal of Hazardous Materials*, 125(1-3), 29-44.
- Web application security consortium. (2010). *WASC threat classification* (Version 2.0). Retrieved from <http://www.webappsec.org>
- Wogalter, M. S., & Laughery, K. R. (1996). Warning! sign and label effectiveness. *Current Directions in Psychological Science*, 5(2), 33-37.
- Wogalter, M. S., Sojourner, R. J., & Brelsford, J. W. (1997). Comprehension and retention of safety pictorials. *Ergonomics*, 40(5), 531-542.
- Wogalter, M. S., Conzola, V. C., & Smith-Jackson, T. L. (2002). Research-based guidelines for warning design and evaluation. *Applied ergonomics*, 33(3), 219-230.
- Wogalter, M. S., Silver, N. C., Leonard, S. D., & Zaikina, H. (2006). Warning symbols. In M. Wogalter, *Handbook of warnings* (pp. 159-176). Mahwah, NJ: Lawrence Erlbaum Associates.
- Worrell, J. L., Di Gangi, P. M., & Bush, A. A. (2013). Exploring the use of the Delphi method in accounting information systems research. *International Journal of Accounting Information Systems*, 14(3), 193-208.
- Yalew, S. D., Maguire, G. Q., Haridi, S., & Correia, M. (2017, October 30 – November 1). *Hail to the Thief: Protecting data from mobile ransomware with ransomsafedroid* [Paper presentation]. International Symposium on Network Computing and Applications (NCA), Cambridge, MA, United States.
- Yeh, Q.-J., & Chang, A. J.-T. (2007). Threats and countermeasures for information system security: A cross-industry study. *Information & Management*, 44(5), 480-491.
- Young, S. L., & Wogalter, M. S. (2000). Predictors of pictorial symbol comprehension. *Information Design Journal*, 10(2), 124-132.

Zimperium mobile threat defense. (2017). *Zimperium global threat report*. Retrieved from <https://blog.zimperium.com/zimperium-global-threat-report-q3-2017/>

Zumerle, D., & Girard, J. (2017). *Market guide for mobile threat defense solutions* (Gartner G00293658). Retrieved from <https://www.gartner.com/en/documents/3789664>