2019

Cyber Situational Awareness and Cyber Curiosity Taxonomy for Understanding Susceptibility of Social Engineering Attacks in the Maritime Industry

Guillermo Francisco Perez

Cyber Situational Awareness and Cyber Curiosity Taxonomy for Understanding Susceptibility of Social Engineering Attacks in the Maritime Industry

by

Guillermo Perez

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

College of Engineering and Computing
Nova Southeastern University

2019

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

12/17/2019

Yair Levy, Ph.D.
Chairperson of Dissertation Committee
Date

Dr. Melissa Carlton

12/17/19

Melissa Carlton, Ph.D.
Dissertation Committee Member
Date

12/17/19

Anat Hovav, Ph.D.
Dissertation Committee Member
Date

Approved:

Meline Kevorkian

12/17/19

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

College of Computing and Engineering
Nova Southeastern University

2019

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

Cyber Situational Awareness and Cyber Curiosity Taxonomy for Understanding Susceptibility of Social Engineering Attacks in the Maritime Industry

By
Guillermo Perez

The maritime information system (IS) user has to be prepared to deal with a potential safety and environmental risk that can be caused by an unanticipated failure to a cyber system used onboard a vessel. A hacker leveraging a maritime IS user's Cyber Curiosity can lead to a successful cyber-attack by enticing a user to click on a malicious Web link sent through an email and/or posted on a social media website. At worst, a successful cyber-attack can impact the integrity of a ship's cyber systems potentially causing disruption or human harm. A lack of awareness of social engineering attacks can increase the susceptibility of a successful cyber-attack against any organization. A combination of limited cyber situational awareness (SA) of social engineering attacks used against IS users and the user's natural curiosity create significant threats to organizations.

The theoretical framework for this research study consists of four interrelated constructs and theories: social engineering, Cyber Curiosity, Cyber Situational Awareness, and activity theory. This study focused its investigation on two constructs, Cyber Situational Awareness and Cyber Curiosity. These constructs reflect user behavior and decision-making associated with being a victim of a social engineering cyber-attack. This study designed an interactive Web-based experiment to measure an IS user's Cyber Situational Awareness and Cyber Curiosity to further understand the relationship between these two constructs in the context of cyber risk to organizations. The quantitative and qualitative data analysis from the experiment consisting of 174 IS users (120 maritime & 54 shoreside) were used to empirically assess if there are any significant differences in the maritime IS user's level of Cyber SA, Cyber Curiosity, and position in the developed Cyber Risk taxonomy when controlled for demographic indicators.

To ensure validity and reliability of the proposed measures and the experimental procedures, a panel of nine subject matter experts (SMEs) reviewed the proposed measures/scores of Cyber SA and Cyber Curiosity. The SMEs' responses were incorporated into the proposed measures and scores including the Web-based experiment. Furthermore, a pilot test was conducted of the Web-based experiment to assess measures of Cyber SA and Cyber Curiosity. This research validated that the developed Cyber Risk taxonomy could be used to assess the susceptibility of an IS user being a victim of a social engineering attack. Identifying a possible link in how both Cyber SA and Cyber Curiosity can help predict the susceptibility of a social engineering attack can be beneficial to the IS research community. In addition, potentially reducing the likelihood of an IS user being a victim of a cyber-attack by identifying factors that improve Cyber SA can reduce risks to organizations. The discussions and implications for future research opportunities are provided to aid the maritime cybersecurity research and practice communities.

Acknowledgements

Thank you God, Jesus Christ, for giving me the strength and perseverance to complete this academic journey in the midst of a personally challenging period. To my wife Greydys, who has been an endless supply of love, support, encouragement, and course correction when required throughout the doctoral program. Even though you knew that embarking on this journey would take time away from you and our children, you nevertheless gave me the freedom to finish without making me feel guilty for the time of solitude on the evenings and weekends when I needed to work on the paper. To my daughters Genevieve, Tatiana, and Sofia for always giving me love and continued affirmations that you were proud of me for pursuing a PhD. Thanks to my family and close friends who have always been a source of rechargeable batteries of encouragement.

I am indebted to my advisor, Dr. Yair Levy, for his wise counsel in helping me navigate the labyrinth of doctoral research. Without Dr. Levy's candid feedback and patience in reviewing the many versions of the doctoral papers, from idea, proposal, to report, my paper would not have morphed into the final product. I also want to thank my committee members, Dr. Anat Hovav and Dr. Melissa Carlton, for their time and insightful feedback which improved the overall research.

Many thanks to the professors in the doctoral program at Nova Southeastern University such as Dr. Ling Wang, Dr. Steve Terrel, Dr. Laurie P. Dringus for helping me develop my research skills throughout the core courses. I also want to thank the Ph.D. students that I met during the cluster weekends, I will always have fond memories of our interactions that helped fuel my desire to continue in the program.

Much gratitude to Royal Caribbean for their sponsorship of my educational pursuit. A special thanks to the many IT executives, HR, Shipboard, and Maritime Cybersecurity team members who provided various means of encouragement and support for embarking and completing the doctoral program.

Lastly, I dedicate this endeavor to my late father Ruben Perez who without his and my mother's personal sacrifices to immigrate and provide a better life in the United States, it would have never given me the abundance of opportunities provided throughout my life. I hope that from above you are proud of what I have achieved as a son.

Table of Contents

Chapters

Methodology 50

Results 72

Appendices

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

The maritime industry, a global, complex ecosystem that requires people to safely transport cargo and people, is highly dependent on operational technology (OT) such as navigation systems, propulsion, and power generation that is managed by information systems (IS) (Tucci, 2016). According to Kramek (2013), U.S. economic prosperity is dependent on maritime security. Maritime IS users are not exempt from the possibility of a cyber-attack because modern ships are equipped with broadband, high speed satellite to access the Internet and communicate with other networks. What is not well understood are specific cyber vulnerabilities of today's modern maritime industry that may be susceptible to cyber-attacks. In the commercial maritime industry, there is a prevalent belief that cyber threats are theoretical in nature and usually linked to a doubt to whether there are individuals with a genuine motivation to perform a cyber-attack against their own company (Cyberkeel, 2014). Modern ship captains and their crew are responsible for safely navigating a ship using IS that are used to control electronic chart displays, radar systems, safety monitors, and propulsion systems. Navigation bridge officers rely on situational awareness depending on cyber technology to make rapid decisions to safely steer a ship and avoid a collision (Sandhåland, Oltedal, & Eid, 2015). The majority of maritime accidents “are not caused by technical problems but by the failure of the crew to respond appropriately to the situation” (Barnett, Gatfield, & Pekcan, 2017, p. 2). In cybersecurity, the user is also identified as the weakest link, because even the strongest technical security controls can be bypassed easily through a social engineering attack (Chen, 2006; Mitnick, 2002; Schneier, 2000). In maritime safety, people are also the weakest link, not because of the people themselves, but because of the increased dependency on the use of IS in the way they perform their daily duties (Rothblum et al., 2002). The use of IS to safely navigate and operate ships is becoming more complex in an industry that is typically diverse in cultures, values, and backgrounds (Progoulaki & Theotakas, 2016). The combination of the dependency of IS to safely navigate a ship and the susceptibility of IS users provides a window of opportunity for a successful social engineering cyber-attack. A social engineering attack is a technique used by hackers, leveraging human interactions or social skills, to gain useful information to infiltrate an organizational network (US-CERT, 2016). These human manipulations, used by hackers, have evolved from attempting to get a business user to divulge their credentials, to leveraging social media sites to perform reconnaissance to gain useful information about an organization (Algarni, Xu, Chan, & Tian, 2013; Mills, 2009). Given the likelihood of IS users being the victim of a social engineering cyber-attack, this study will develop and empirically validate an IS cyber situational awareness (SA) taxonomy in the context of Cyber Curiosity that can be used as a benchmark to measure the susceptibility of mitigating a cyber-attack using social engineering techniques among critical maritime crew.

The main sections of this paper are: Problem Statement, Dissertation Goal, Research Questions, Relevance and Significance, Resources, and References. These sections build the research worthiness of the problem, elucidating the goals of the research, specifying the research questions that will be studied, the supporting literature, challenges that may be encountered in conducting the research, how the research and analysis will be conducted, a high level schedule to complete the research, any resources required, and a complete listing of the references used throughout the paper.

Problem Statement

The research problem that this study will address is the limited Cyber SA of social engineering threat vector used against information systems (IS) users, and the natural human curiosity that creates a significant cybersecurity threat to organizations (Iuga, Nurse, & Erola, 2016). The term Cyber SA in this context is defined by Tadda and Salerno (2010), where Cyber SA is the perception of cyber risk elements with respect to time and space, the understanding of their meaning, and anticipation of their status in the near future. Many IS users lack awareness of cybersecurity risks because their primary intention is to check email, browse Web pages, or use software (Whitten & Tygar, 1999). Despite recent efforts to improve Cyber SA, such as enabling cues on Web browsers warning users of a suspicious Website, IS users continue to fall prey to phishing attacks (Dhamija, Tygar, & Hearst, 2006; Herzberg, 2009). Human curiosity can increase or reduce the success of a cyber-attack. Social engineering techniques leverage emotions, such as curiosity, to capture the attention of users to lure them to open malicious email attachments or web links (Abraham & Smith, 2010). Baiting, a form of a social engineering attack, leverages human curiosity to lure a user to pick up a malware infected flash drive left abandoned on the floor (Fan, Lwakatare, & Rong, 2016).

An industry that is highly susceptible to social engineering attacks is the maritime industry, because awareness of cybersecurity risks in the maritime sector is currently low to non-existent (European Network and Information Security Agency, 2011). This observation is pervasive across all maritime organizational layers including government bodies, port authorities, and maritime companies (Kramek, 2013). An explanation for the current level of Cyber SA in the maritime sector is the lack of publicly known cybersecurity incidents occurring within the maritime sector (ENISA, 2011). Moreover, a further explanation by Cyberkeel (2014) for the current level of Cyber SA is "unawareness of the actual incidents that have taken place in the maritime sector" (p. 3). As evidence that maritime cybersecurity incidents have occurred in the past, in 2014, several maritime companies, specifically shipping lines and bunker fuel suppliers, were infiltrated with a remote access tool (RAT). The RAT was used to monitor and spoof email resulting in fraud by changing their bank account information to re-route large payments (Cyberkeel, 2014). The relevance of maritime cyber risk is confirmed by Fitton, Prince, Gersmond, and Lacy (2015) in noting that:

> In the maritime environment people interact with computer systems extensively. Whether that is a ship's navigation system, a drilling rig, a ballistic missile system or something as mundane as employee records. At every intersection of man/woman and machine there is the possibility for error, manipulation, coercion or sedition. (p. 15)

Human curiosity can increase or reduce the success of a cyber-attack. Social engineering techniques leverage emotions, such as curiosity, to capture the attention of users to lure them to open malicious email attachments or Web links (Abraham & Smith, 2010). For example, baiting, a form of a social engineering attack, leverages human curiosity to lure a user to pick up a malware infected flash drive left abandoned on the floor (Fan, Lwakatare, & Rong, 2016). Reducing the likelihood of a successful social engineering cyber-attack can be accomplished through increasing situational awareness by becoming more knowledgeable of the indicators of a cyber-attack (Dutt, Ahn, & Gonzalez, 2012). The inquisitiveness for interacting with the domain of IS, information technology, and the Internet can be defined as Cyber Curiosity. Combining the lack of awareness in the maritime industry of targeted cyber-attacks (Cyberkeel, 2012; ENISA, 2011) along with IS user's Cyber Curiosity, influences the susceptibility of being victims of a social engineering attack (Iuga et al., 2016). However, there is a lack of established validated instruments to measure Cyber SA and Cyber Curiosity in an effort to mitigate social engineering cyber-attack, especially in the maritime industry. Therefore, additional research is warranted to investigate the ways to measure IS user's Cyber SA and Cyber Curiosity, while using it to help identify the possibility of a successful social engineering cyber-attack.

Dissertation Goal

The main goal of this proposed research study is to design, develop, and to empirically validate an IS Cyber SA, in the context of Cyber Curiosity, taxonomy that measures the susceptibility of mitigating a cyber-attack using social engineering techniques on IS users in the maritime industry. The proposed taxonomy will be reviewed and validated by subject matter experts (SMEs). The SMEs review of the developed taxonomy will improve content validity, construct validity, and reliability (Straub, 1989). This proposed study will use maritime IS users as the context. This proposed study suggests that two dimensions of the susceptibility of a successful social engineering cyber-attack are user Cyber SA and Cyber Curiosity. The need for this proposed research is supported by Saridakis, Benson, Ezingeard and Tennakoon (2016) who advocated that "awareness of risk has been shown to be an antecedent of the intention to perform security behaviors, both in personal and professional contexts" (p. 326). Recent research investigated the human factor of sensitivity of using Web browser warnings to IS users of a possible phishing attack as a training method to raise Cyber SA that an attack was likely (Iuga et al., 2016). Another earlier study by Downs, Holbrook, and Cranor (2006) looked into phishing attack susceptibility based on user's decision strategies and their use of available cues to determine the "mental modes" used by people when reading emails. This proposed research builds on the aforementioned research by proposing a taxonomy to aid in the understanding of social engineering attacks based on a user's level of Cyber SA and Cyber Curiosity.

There are five specific goals of this proposed research study. The first goal of this proposed study is to identify, classify, and validate, using SMEs, the components for the measures of Cyber SA and Cyber Curiosity. The second goal is to identify the scores of the identified components of the measures of Cyber SA and Cyber Curiosity, using SMEs that enable a validated aggregation to the proposed Cyber Risk taxonomy. The third goal is to develop and validate, using SMEs, a Cyber Risk taxonomy to classify maritime IS users by their level of Cyber SA and Cyber Curiosity. The fourth goal of this proposed study is to use the validated Cyber Risk taxonomy in an experiment to classify the maritime IS users. The last and fifth goal of this research study is to empirically assess if there are any significant differences in the maritime IS user's level of Cyber SA, Cyber Curiosity, and position in the Cyber Risk taxonomy when controlled for demographics indicators such as: age, gender, nationality, department, years performing job function, and education level.

Figure 1 illustrates the proposed taxonomy of a 2x2 matrix that will classify maritime IS users' cyber risk by their level of Cyber SA and Cyber Curiosity (D-Type and I-Type).

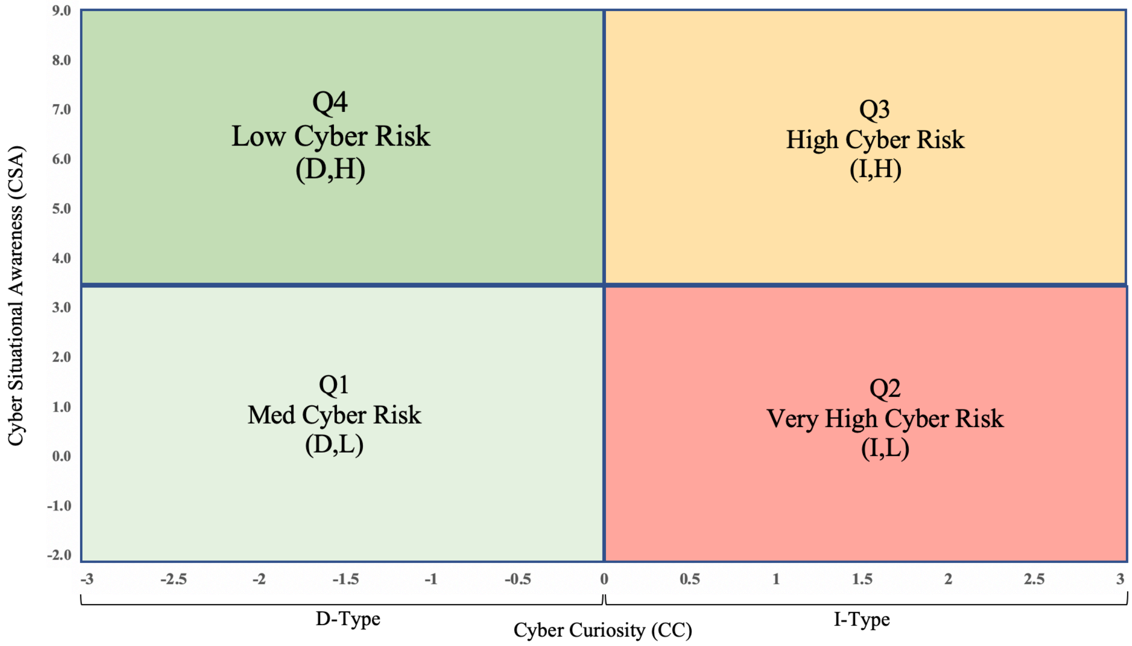


Figure 1. Cyber Risk taxonomy for susceptibility of being a victim of a social engineering cyber-attack

The x-axis represents the level of IS user Cyber Curiosity (I-Type and D-Type) and the y-axis represents the level of IS users Cyber SA. The coordinates (x,y) represents the combined value of both Cyber Curiosity and Cyber SA. The proposed taxonomy is comprised of four quadrants Q1, Q2, Q3, and Q4 as depicted in Figure 1. Each quadrant reflects the aggregate level of IS user cyber risk and their susceptibility to a social engineering attack. In the proposed risk matrix, there is direct relationship between the level of I-Type Cyber Curiosity and an inverse relationship with the level of Cyber SA and the resultant cyber risk to an organization.

The first quadrant, Q1, is labeled 'Medium Cyber Risk' because it consists of IS users with high D-Type Cyber Curiosity, low I-Type Cyber Curiosity and low Cyber SA score. IS users positioned in this quadrant maybe capable of reducing their likelihood of being susceptible to a successful social engineering attack by increasing their Cyber SA. The second quadrant, Q2, is labeled 'Very High Cyber Risk' because it consists of IS users with high I-Type Cyber Curiosity, low D-Type Cyber Curiosity, and low Cyber SA. Cyber risk in this quadrant is very high because IS users are more susceptible to a successful social engineering attack because of their high level of Cyber Curiosity and low SA of a possible cyber-attack. The third quadrant, Q3, is labeled 'High Cyber Risk' because it consists of IS users with high I-Type Cyber Curiosity, low D-Type Cyber Curiosity, and high Cyber SA. IS users positioned in this quadrant maybe capable of reducing their likelihood of being susceptible to a successful social engineering attack by decreasing their I-Type Cyber Curiosity and increasing D-Type Cyber Curiosity. The fourth quadrant, Q4, consists IS users with high D-Type Cyber Curiosity, low I-Type Cyber Curiosity and high Cyber SA and is labeled 'Low Cyber Risk'. IS users, in this quadrant, are keen of social engineering tools, techniques, and procedures (TTPs) meaning that they will be the least susceptible to a successful future attack.

Research Questions

The main research question that this proposed study will address is: Does the measured level of IS Cyber SA and Cyber Curiosity assist in the determination of a maritime IS user's susceptibility of a social engineering cyber-attack? In addition, this proposed study will address five specific research questions as follows:

RQ1a: What are the SMEs identified components of the measures of an IS user's level of Cyber SA which may influence the susceptibility of being a victim of a social engineering cyber-attack?

RQ1b: What are the SMEs identified components of the measures of an IS user's level of Cyber Curiosity which may influence the susceptibility of being a victim of a social engineering cyber-attack?

RQ2a: What are the specific scores of the SMEs identified components of the IS user's measures of Cyber SA that enable a validated hierarchical aggregation to the Cyber SA measure of the Cyber Risk taxonomy?

RQ2b: What are the specific scores of the SMEs identified components of the IS user's measures of Cyber Curiosity that enable a validated hierarchical aggregation to the Cyber Curiosity measure of the Cyber Risk taxonomy?

RQ3: What are the experts' approved classification of the Social Engineering Attack Experiment using the hierarchical aggregation of Cyber SA and Cyber Curiosity for the Cyber Risk Taxonomy using a social engineering attack experiment?

RQ4: How are the aggregated scores for Cyber SA and Cyber Curiosity positioned on the Cyber Risk taxonomy for maritime IS users?

RQ5a: Are there any statistically significant mean differences to maritime IS users' aggregated level of Cyber SA based on their age, gender, nationality, department, years at performing job, education level, or psychological state of mind?

RQ5b: Are there any statistically significant mean differences to maritime IS users' aggregated level of Cyber Curiosity based on their age, gender, nationality, department, years performing job, education level, or psychological state of mind?

RQ5c: Are there any statistically significant mean differences to an IS user's Cyber Risk score based on their age, gender, nationality, department, years performing job, education level, or psychological state of mind?

Relevance and Significance

Relevance

The purpose of this proposed study is to reduce the susceptibility of IS users being the victim of a social engineering cyber-attack. A review of the literature reveals that few studies have focused on Cyber SA as it relates to social engineering attacks. A multitude of the Cyber SA studies have focused on the role of IS users in cyber defense operations and analysis (Barford et al., 2010; Champion, Rajivan, Cooke, & Jariwala, 2012; Hoffman, Buchler, Doshi, & Cam, 2016). There has been limited work examining cyber-attacks from a human-centric perspective such as the effectiveness of phishing attacks

(Hong, Kelley, Tembe, Murphy-Hill, & Mayhorn, 2013; Kelly, Hong, Mayhorn, & Murphy-Hill, 2012; Mancuso, Strang, Funke, & Finomore, 2014). Cyber Curiosity, as a term, has very limited research studies published. The nearest studies are those involving human elements of social engineering where curiosity is mentioned as one of the influencing factors. Identifying a possible link in how both Cyber SA and Cyber Curiosity can help measure and predict the susceptibility of social engineering attack can be beneficial to the research community and organizations.

Significance

This study can help advance current research in cybersecurity and contribute to the body of knowledge regarding IS users as it relates to their awareness of social engineering cyber-attacks. According to Verizon's most recent Data Breach Investigations Report, social engineering attacks were used in 43% of all breaches with phishing and pretexting as the most common social engineering tactics (2018). The success rate of users clicking on phishing emails continues to rise. The success rate of users clicking on phishing emails was 30% and continues to rise year to year in comparing previous reports (Verizon, 2016). Despite the advancement of email security phishing detection and prevention technologies, social engineering phishing attacks continues to be a prevalent and easy form of cyber-attack (Gupta, Tewari, Jain & Agrawal, 2016). A successful cyber-attack can have significant financial impacts to a business. According to a recently published security report by Cisco (2017), almost a quarter of the surveyed businesses found that organizations that experienced a successful cyber-attack lost business opportunities. Out of those impacted businesses, four in ten said those losses were substantial and one in five lost customers nearly lost 30% revenue

(Cisco, 2017). Insight into factors that influence IS users' level of cybersecurity SA and Cyber Curiosity can help reduce the success rate of social engineering attacks.

Another significance of this study is the unusual context of the research setting. The maritime industry, specifically passenger vessels, present a unique research study environment where crew spend a significant amount of time in constant interaction with passengers and are also away from family for extended periods of time. This interaction and enclosed environment provides an interesting dynamic to cyber situational awareness and Cyber Curiosity research further contributing to the IS body of knowledge.

Barriers and Issues

One potential barrier for this proposed study is obtaining permission to measure the Cyber SA and Cyber Curiosity of maritime IS users. Another challenge is the continual introduction of new maritime IS users who are assigned to ships on a variable rotation of schedule such as eleven weeks on and eleven weeks off or have extended six-month contracts with six weeks off. As new staff especially ship chief staff like captains and chief engineers are introduced, their support and approval will be required. Institutional Review Board (IRB) approval is required to use maritime IS users as participants. Approval for this proposed study must be obtained prior to pursuing IRB approval. A third barrier is the duality of Cyber Curiosity. As identified in the literature review, Cyber Curiosity can be a motivating factor to gain knowledge (Litman, 2008) and improve Cyber SA (Hake, 2016) or it can be a weakness if an IS user is curious and clicks on a malicious email (Anti-Phishing Working Group, 2016). A fourth barrier is validating and conducting the experiment to measure SA and Cyber Curiosity. Measuring the internal level of Cyber SA and curiosity is challenging. Seminal SA research by Endsley (1995) identified the difficulty in assessing the extent observers can accurately rate the internal construct of SA. Measuring SA requires multiple techniques because the "actual internal level of SA cannot be accurately measured by observation alone" (Salmon, Stanton, Walker, & Green, 2006, p. 29). Conducting a Delphi technique to validate the experiment components can be time consuming (Hsu & Sandford, 2007). Identifying a group of Delphi experts who are equivalent in knowledge and experience can also be challenging. Developing an interactive Web-based application that captures IS user's response to measure SA and Cyber Curiosity can be daunting. There are direct (such as accurate identification of a phishing email), indirect (curiosity level), and mental workload (decision making) measures that must be incorporated in the overall measurement plan (Wright, Taekman, & Endsley, 2004).

Assumptions, Limitations and Delimitations

Assumptions

The following are assumptions made for this proposed study:

- Experiment approval and consent forms will be obtained from IS users participating in the survey and experiment.
- There will be an adequate number of SMEs for the expert panel reviews in Phase 2 and Phase 3.
- Experiment participants will be engaged and will answer honestly to the survey and experiment.
- All experiment participation will be voluntarily, and participants will have decision-making autonomy and not feel obligated to participate.

Limitations

There are several research study limitations to the proposed study. The first is that the proposed interactive social engineering attack experiment can create artificial situations that do not represent real-life situations impacting the gathered data since the reactions of the participants may not be true indicators of their behaviors in a real environment. Leveraging previously encountered social engineering attacks in published research or documented archives for the interactive experiment limits the risks of not creating real-life scenarios.

A second limitation is in the validity of the methods of measuring Cyber Curiosity and Cyber SA during the interactive Web-based experiment. Validity and reliability would be at question if the interactive experiment was incorrectly recording the participants' responses. To mitigate the risk of data collection methods, an expert panel of SMEs, using the Delphi technique, will review the proposed interactive experiment. In development research, a consensus building process such as the Delphi Process, can help establish the reliability and validity of the methods used (Ellis & Levy, 2010).

A third limitation is in the ability for a globally dispersed maritime workforce to participate in the experiment and data collection survey. A majority of the maritime participants will be sailing on a ship that has limited Internet connectivity and bandwidth. To limit the participating risk, the interactive Web-based experiment will need to be designed to limit bandwidth usage and duration to a minimum.

Delimitations

A delimitation of this proposed study is limited to scope of the investigations of the two constructs, Cyber SA and Cyber Curiosity. Another delimitation of this proposed study is that the population is limited to the maritime industry as the study may present different experiment results at other types of industries.

Definitions of Terms

The following represent terms and definitions.

Cyber Situational Awareness - The perception of cyber risk elements with respect to time and space, the understanding of their meaning, and anticipation of their status in the near future (Tadda & Salerno, 2010).

Cyber – Involving, using, or relating to computers, especially the Internet (Cambridge, n.d.).

Cybersecurity – The protection of cyberspace, the electronic information, the infrastructure that supports cyberspace, and the users of cyberspace in their personal, societal, and national capacity including any of their interests that are vulnerable to attacks originating in cyberspace (Solms & Niekerk, 2013).

Cyber Curiosity - Cyber Curiosity is the desire for information and knowledge about information systems (IS) and the Internet.

Epistemic Curiosity – Epistemic curiosity is a state of arousal that impels the search for knowledge that can only be relieved by the acquisition of knowledge (Berlyne, 1960).

Information Systems– A collection of multiple pieces of information involved in the dissemination of information. Hardware, software, computer system connections and information, information system users, and the system's housing are all part of an IS (Technopedia, n.d.).

Maritime industry – Enterprises engaged in the business of designing, constructing, manufacturing, acquiring, operating, supplying, repairing and/or maintaining vessels. Also enterprise operating shipping lines, and customs brokerage services, shipyards, dry docks, marine railways, marine repair shops, shipping and freight forwarding services and similar enterprises (PwC, 2016).

Operational Technology (OT) – Devices, sensors, software and associated networking that monitor and control shipboard onboard systems (BIMCO, 2016).

Phishing attack - A criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials (APWG, 2016).

Social engineering - A technique used by hackers, leveraging human interactions or social skills, to obtain or compromise IS information to infiltrate an organizations network (US-CERT, 2016).

Subject Matter Expert (SME) – A highly knowledgeable individual who performs specialized functions in given organizational processes (Encyclopedia, n.d.).

Summary

This proposed study will address the threats to organizations due to limited Cyber SA of socially engineered cyber-attacks (Cyberkeel, 2012; ENISA, 2011; Dhamija, Tygar, & Hearst, 2006; Herzberg, 2009) and natural human curiosity (Iuga, Nurse, & Erola, 2016; Fan, Lwakatare, & Rong, 2016) by empirically testing measures for levels of Cyber SA and Cyber Curiosity. Therefore, by using an expert validated set of Cyber SA and Cyber Curiosity measure components, scores, and Web-based experiment, this study will establish and validate a set of measurable Cyber SA and curiosity levels. Given the likelihood of IS users being the victim of a social engineering cyber-attack (Cisco, 2017; Verizon, 2018), this study will develop and empirically validate an IS cyber situational awareness (SA) taxonomy in the context of Cyber Curiosity that can be used as a benchmark to measure the susceptibility of mitigating a cyber-attack using social engineering techniques among IS users.

Chapter 2

Review of the Literature

Introduction

In this section, a literature review is presented to provide a synopsis of the relevant literature pertaining to areas and theories that provide a theoretical foundation for this proposed study. The main areas are social engineering, cyber situational awareness, Cyber Curiosity, and activity theory. This literature review will include the four characteristics mentioned, by Levy and Ellis (2006), which are 1) methodically analyze and synthesize quality literature, 2) establish a firm foundation for the research topic, 3) establish a solid foundation to the selection of research methodology, and 4) demonstrate that the proposed research is a novel contribution to the overall body of knowledge. To improve on the quality of the literature review, peer reviewed academic papers from reputable sources were used. Whenever appropriate, seminal researcher's material were included to provide historical or foundational.

Social Engineering

Social engineering can be considered the "art of persuasion" (Mitnick, 2002), influencing people to aid hackers to achieve their goal of gaining access to corporate IS systems. Most social engineering techniques are used to compromise IT while attacking individuals (Algarni, Xu, & Chan, 2015). Many organizations acknowledge the importance of predicting and controlling social engineering, but a multitude fail to reach that goal (Brody, 2012). Social engineering malware propagates through a variety of infiltration channels such as email, social media Websites, portable storage devices, and mobile devices (Abraham & Chengalur-Smith, 2010).

Phishing

An email phishing attack is a form of social engineering where an attacker uses an email to send a malicious attachment or web link to a victim with the intent of tricking the recipient to open an attachment (Anti-Phishing Working Group, 2016). In opening the attachment or clicking on the web link, the attacker attempts to steal the victims network account credentials or infect their machine with malware. There are many forms of email phishing attacks like broad target botnet-generated spam phishing to targeted spear-phishing. A spear-phishing is targeted toward a specific user, organization or demographic (Heartfield & Loukas, 2016). In a PriceWaterhouseCoopers (PwC) survey, phishing has "emerged as a significant risk to businesses of all sizes and across industry" (2017, p. 9) and re-emergence of traditional social engineering tactics. In one month, phishing was estimated to have caused $282M in global losses (RSA, 2014). Verizon Enterprise Solutions (2017) reported that attackers leverage email as the primary means of communication to the target, followed by in-person deception, and phone calls. The attackers' primary goal in the social phase of an attack is the installation of malware or disclosure of credentials (Verizon Enterprise Solutions, 2017). IS user's failure to report suspicious emails also impacts an organization's ability to increase Cyber SA. In an annual data breach investigative report, Data Breach Investigative Report (Verizon Enterprise Solutions, 2016), of the approximately 636,000 confirmed phishing emails, approximately 3% of targeted individuals alerted management of a possible phishing email. Increasing employee Cyber SA is a critical and often neglected arsenal in cybersecurity preparedness (PricewaterhouseCoopers, 2017).

Business Email Compromise

Business email compromise (BEC) is a sophisticated scam targeting organizations and IS users with the intention of committing fraud or obtaining sensitive information such as financial wire transfers, personally identifiable information (PII), undisclosed proprietary data, or user credentials (FBI, 2018). BEC attackers rely on social engineering tactics like impersonation to trick unaware IS users (TrendMicro, 2016). According to TrendMicro (2016), there are three common types of phishing BEC scams. One type is the “Bogus Invoice Scheme” that involves an organization that has an established relationship with a supplier and the attacker asks to wire funds for a bogus invoice payment. A second type of BEC is “CEO Fraud” where an attacker impersonates a high-level executive and requests, via email, an urgent time-sensitive wire transfer to an unsuspecting employee. The third type of BEC attack is “Data Theft” is a compromised email account of a role-specific employee that the attacker uses to send emails with the goal of obtaining sensitive information from other IS users. Data theft BEC attacks are difficult to detect since the email is coming from a legitimate employee circumventing cybersecurity awareness training SA advice to check for legitimate senders.

BEC phishing cyber-attacks is a growing and evolving issue for organizations regardless of its size. The Internet Crime Compliance Center (IC3), FBI’s center for users to submit complaints of Internet crime, since its inception, has received about 4 million complaints resulting in $5.52 billion in losses (FBI, 2017). In a 2017 analysis report, researchers at SecureWork's Counter Threat Unit (CTU) identified a BEC social engineering scheme led by a threat group named GOLD GALLEON targeting the maritime shipping industry (Secureworks, 2018). GOLD GALLEON is a collection of at least 20 criminal associates collectively carrying out BEC campaigns. These types of groups are able to successfully exploit IS users by using publicly available malware such as inexpensive or free remote access trojans (RATs) and crypters to avoid malware detection tools (Secureworks, 2018).

Impersonation

As mentioned in the BEC section, a type of impersonation, social engineering cyber-attack is called "CEO Fraud" where an attacker impersonates a high-level executive and requests an urgent time-sensitive wire transfer to an unsuspecting IS user. In an impersonation phishing attack, an attacker first compromises or spoofs the email of an executive or business partner. In both cases the goal is for the attacker to exploit the trust of the IS user receiving the email to them to divulge targeted information or process a requested bogus transaction (Tripwire, 2017). In the 2017 Internet Crime Report, BEC accounted type attacks for 15,690 victims with a loss of $675 million (FBI, 2017). Many of these BEC attacks leveraged impersonation as the means of successfully exploiting the victims.

Combating social engineering phishing attacks requires organizations to develop shared social responsibility and not solely rely on technical solutions (Abraham & Chengular, 2010). Increasing Cyber SA of social engineering attacks can significantly reduce the likelihood of being a victim of an attack (Bullée, Montoya, Pieters, Junger, &

Hartel, 2015). A summary of research studies regarding social engineering are listed in Table 1.

Table 1

Summary of Social Engineering Literature

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Abraham & Chengalur-Smith, 2010	Literature review and synthesis		Social engineering malware proliferation through a variety of infiltration channels such as e-mail, social software, websites, and portable media	Social engineering malware is both pervasive and persistent. Emphasized the importance for organizations to develop a shared social responsibility to combat social engineering malware and not solely on technical solutions
Algarni et al., 2015	Scenario-based experiment	377 participants in the experiment	Social engineering victimization and the perceived sincerity, competence, attraction, and worthiness of source	The results of this study showed that every factor of the perceived sincerity, competence, attraction, and worthiness of a source are significant predictors of susceptibility to social engineering victimization. Perceived sincerity was found to induce the most influence on users' judgment toward accepting or rejecting social engineering-based attacks

Table 1
Summary of Social Engineering Literature (Cont.)

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Bullée et al., 2015	Empirical study via controlled experiment	118 participants in the experiment	Intervention and effect of authority in social engineering attack	A training (intervention) of the risks security engineering attacks reduced the probability of a successful attack by almost half versus those not exposed to the training
Heartfield & Loukas, 2016	Survey		Social engineering semantic attacks	Introduced a structured baseline for classifying semantic attacks by breaking down into components and identifying countermeasures

Situational Awareness

SA has received considerable attention from the psychology and human factors research communities over the past 20 years. Although the original impetus for research came from military aviation, it has now developed into a critical research theme in almost any domain that involves humans performing tasks in complex, dynamic systems. SA research is widespread and ongoing in a variety of domains, including military operations (Endsley & Garland, 2000; Matthews, Pleban, Endsley, & Strater, 2000), aviation (Kaber, Endsley, Wright, & Warren, 2002; Keller, Lebiere, Shay, & Latorella, 2004), air traffic control (Hauss & Eyferth, 2003; Endsley & Smolensky, 1998), and automotive (Zheng, McConkie & Tai, 2004). In recent years SA research has also been extended to the cyber domain in cyber defense (Barford et al., 2010), modeling detection (Dutt, Ahn, & Gonzalez, 2013) and industrial control systems (Hoffman et al., 2016).

SA in aviation

There have been numerous research studies of SA in aviation. In a controlled experiment conducted of 16 pilots by Kaber, Endsley, Wright, and Warren (2002), it was discovered that workload automation of flight controls may compromise pilot situational awareness after a critical event as compared to manual flight operation. In another longitudinal study spanning four years of SA and demands of short-term memory system, Isaac (2017) research confirmed previous studies that short-term memory is capable of storing information for a few seconds without active rehearsal, but that short-term memory has also limited capacity unless a controlled process like repeating information.

SA in automobile safety

SA has been used in automobile safety by various studies. In one empirical study using a driving simulation experiment by Zeng, McConkie, and Tai (2004), SA and awareness of a car driver identified that vehicle location is coarsely remembered in driver’s memory. This investigation helped explain why drivers fail to notice a decreasing distance to the car ahead resulting in rear-end collisions. Benefits of driving training and improving SA where studied by Walker, Stanton, Kazi, Salmon, and Jenkins (2008) where they demonstrated that drivers who undergo advanced driving training show an increase in the number of new information elements that comprise their SA.

SA in maritime industry

In the maritime industry SA studies have focused primarily on safety. In a study of offshore drilling personnel (N=378) on stress levels and its impact on SA, the researchers discovered that higher levels of stress and fatigue are linked to lower levels of work SA (Sneddon, Mearns & Flin, 2012). In another study of dynamic position operators SA and decision-making, operators chose to follow predetermined procedures, in accordance with their training, to avoid accidents and rectify the situation whenever automation systems no longer function properly (Øvergård, Sorensen, Nazir, & Martinsen, 2015).

Goal oriented situational awareness

SA is a concept widely used to understand individuals reasoning in highly dynamic technical systems in safety-critical domains such as aviation, military operations and maritime (Westrenen & Praetorius, 2014). A goal-oriented definition of situational awareness requires what must be known to solve a class of problems encountered when interacting with a dynamic environment. In this view, SA is viewed as the "capacity to direct consciousness to generate competent performance given a particular situation as it unfolds" (Smith & Hancock, 1995, p. 138). The cognitive side of SA relates to human capacity of being able to comprehend the technical implications, for example navigational system displays, and draw conclusions to derive informed decisions.

Endsley and Jones (2016) identified three levels of SA. The first level is perception (Level 1 SA), second level comprehension (Level 2 SA), and third level projection (Level 3 SA). Level 1 SA is the perception of cues that is used to form a picture of the situation. Level 2 SA is comprehension which is the integration of multiple pieces of information and their relevance to a person's goal. A person with Level 2 SA "been able to derive operationally relevant meaning and significance from the Level 1 SA data" (Endsley & Garland, 2000, p. 6). Level 3 SA is the highest level of SA which is the ability for a person to forecast future situation events. According to Endsley and Garland (2000), "experienced operators rely heavily on future projects. It is the mark of a skilled expert" (p. 6). Figure 2 shows a model of SA in dynamic decision making.

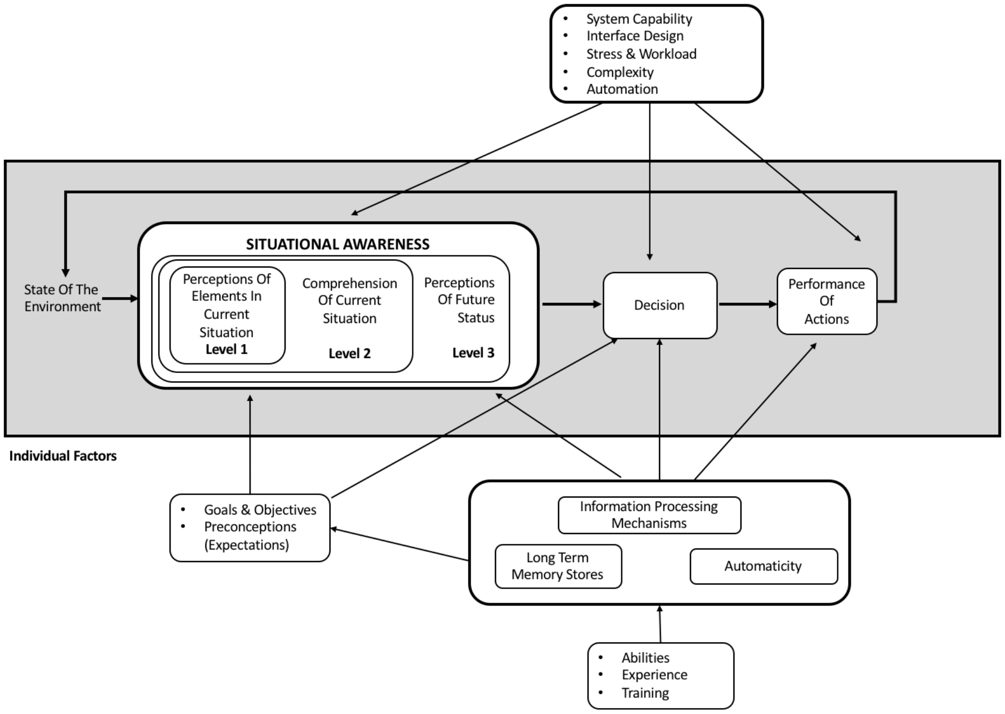


Figure 2. Model of SA in dynamic decision making adopted from Endsley (1995)

SA Perception, Comprehension, and Projection Elements in Different Domains

SA perception, comprehension and projection examples vary by type of job domain (i.e. navigation officer, chief engineer, and cybersecurity operational technology (OT) engineer). The three elements of SA can be defined by SMEs in the domain who can provide what they consider important using goal-oriented task analysis processes (Endsley & Jones, 2012). A listing of examples of the three SA elements by job domain are listed in Table 2. A summary of research studies regarding situational awareness are listed in Table 3.

Table 2
Examples of Perception, Comprehension, and Projection Elements for Different Job Domains (Adapted from Endsley, 2015).

Domain	Perception	Comprehension	Projection
Vessel Navigation Officer	Ship location	Impact of weather on itinerary	Predicted changes in visibility
Ship Navigation Officer	System failures or downgrades	Ability to reach alternate port	Projected impact of changes on safety of vessel
Vessel Chief Engineer	Scheduled outages	Effected vessel systems	Projected impact on vessel systems adding or removing element
Vessel Chief Engineer	Power load levels	Confidence level in parameter values	Potential for voltage collapse
Cybersecurity OT Engineer	Malware detected in OT system	Behavior of malware in OT system	Projected impact of malware on vessel systems
Cybersecurity OT Engineer	Suspicious network activity in OT network	Behavior of network activity to OT systems	Projected impact of systems in OT network

Table 3
Summary of Situational Awareness Literature

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Dutt et al., 2013	Simulation using modeling techniques		Cyber situation awareness	It is important to train defenders with cases involving multiple threats that will improve threat-prone memory and prepare defenders with impatient attackers
Endsley & Garland, 2000	Literature review and synthesis		Situation awareness	Provides a comprehensive overview of situation awareness and an analysis of nine different approaches to measuring situational awareness

Table 3

Summary of Situational Awareness Literature (Cont.)

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Endsley & Jones, 2016	Literature review and synthesis		User-centered design and situation awareness	A comprehensive book on user-centered design to improve situational awareness
Endsley & Smolensky, 1998	Literature review and analysis		Situational awareness	SA awareness focusing on air traffic controllers (ATC) providing SA requirements for ATC and measuring and evaluating SA
Hauss & Eyferth, 2003	Simulation using modeling techniques		Situation awareness measurement	A new on-line probe SA assessment technique was developed (SALSA) for air traffic management that is more applicable than previous measurement models like SAGAT
Hoffman et al., 2016	Literature review and synthesis		Situation awareness in industrial control systems	Highlight specific challenges created by physical, cyber, and people risks that must be understood for analyst to defend against potential industrial control systems cyber attacks
Isaac, A., 2017	Empirical study via controlled experiment	34 flight radar controllers	Situation awareness and demands on short-term memory	Situational awareness is sensitive to the demands of the short-term memory system. Immediate problems encountered by a radar controller will be to as a result of limitations of short-term memory

Table 3

Summary of Situational Awareness Literature (Cont.)

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Kaber et al., 2002	Empirical study via controlled experiment	16 private pilots	Situation awareness and levels of automation (LOA)	Workload automation may compromise pilot situational awareness after a critical event as compared to manual flight control
Keller, et al., 2004	Simulation using modeling techniques		Human performance modeling	Study demonstrate that existing human performance modeling tools can be used to predict the situational awareness of systems designed to provide information to human operators in high workload or high-risk environments
Matthews et al., 2000	Theoretical		Situation awareness measurement	Development of situation awareness measurement rating scales and a SA self-assessment questionnaire.
Øvergård et al., 2015	Accident review and analysis	24 critical incidents	Situation awareness and decision making	Identified that dynamic position operators chose to follow predetermined procedures, in accordance with their training, to avoid accidents and rectify the situation whenever automation systems no longer function properly
Smith & Hancock, 1995	Literature review and analysis		Risk space and situational awareness	Introduces the concept of risk space to represent the invariant relations in the environment that enable an agent to adopt to novel situations and to attain prespecified goals

Table 3

Summary of Situational Awareness Literature (Cont.)

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Sneddon et al., 2012	Empirical study via questionnaire	378 offshore drilling personnel	Work situational awareness and stress levels	Higher levels of stress and fatigue are linked to lower levels of work SA
Van Westrenen & Praetorius, 2014	Comparison and contrast analysis		Maritime traffic situation awareness	Critically reviewed SA and how it has been defined and measured in various domains. Argued that freeze techniques are an inadequate way of assessing operator's situation awareness
Walker et al., 2008	Longitudinal study with analysis	75 drivers	Situational awareness and advanced driving	Drivers who undergo advanced driving training show an increase in the number of new information elements that comprise their SA
Zheng et al., 2004	Empirical study via driving simulator experiment	17 adults	Situation awareness of auto driver	Vehicle location is coarsely represented in driver's memory and is used to visually monitor more fine-grained location information that helps explain why drivers fail to notice a decreasing distance to the auto ahead resulting in rear-end collisions

Cyber Situational Awareness

Cyber SA, in the context of this proposed study, is the perception of cyber risk elements with respect to time and space, the understanding of their meaning, and anticipation of their status in the near future (Tadda & Salerno, 2010). Cyber SA is a subset of situational awareness that deals with the “cyber” environment (Franke & Brynielsson, 2014). An IS user’s increased level of Cyber SA may be dependent on the level of experience in threat detection and awareness. Decision support tools and human-computer interaction design have been areas of research to aid IS analysts in increasing Cyber SA. For example, Erbacher et al., (2010) developed a task-flow diagram using collected feedback such as processes, goals, and concern from IS network analysts. Erbacher (2012) also designed a visualization technique to aid decision makers in making rapid assessments and prioritization of identified cyber anomalies. Along similar research, Mahony et al. (2010) used cognitive task analysis to design a cyber situational awareness tool. In contrast to the abundance of traditional SA in improving human decision making (Van Westrenen & Praetorius, 2014), less research has been devoted to IS user SA because recent research has focused on tools (Jonker, Langevin, Schretlen, & Canfield, 2012) or specialized training for security analysts (Ahrend, Jirotka, & Jones, 2016). A summary of research studies regarding cyber situational awareness are listed in Table 4.

Table 4

Summary of Cyber Situational Awareness Literature

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Ahrend et al., 2016	Qualitative data gathering and analysis using semi-structured interviews	Five interviewees	Development of threat and defense knowledge to increase Cyber SA	Analyzed and describe the tacit knowledge, practices, skills, and tools that IS practitioners use to create and utilize threat and defense knowledge (TDK) to improve Cyber SA

Table 4

Summary of Cyber Situational Awareness Literature (Cont.)

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Erbacher, 2012	Case study	Interviews with network analysts and network managers	Cyber situational awareness	Created a next generation situation awareness visualization technique of cyber data to improve cyber decision-making challenges
Franke & Brynielsson, 2014	Literature review and synthesis		Cyber situational awareness	Thorough literature review of Cyber SA consisting of analysis of 102 articles by clustering them by category such as industrial control systems, emergency management, tools, architectures, and algorithms
Jonker et al., 2012	Developmental research		Visual analytics and cyber situational awareness	Demonstrated the use of visualization tools of "big data" to increase cyber situational awareness
Mahony et al., 2010	Developmental research	Analytically-driven knowledge acquisition sessions with operational SMEs	Cyber situational awareness	Developed a list of preliminary Cyber SA categories that can help drive the design and development of a SA tool
Tadda & Salerno, 2010	Survey with analysis		Metrics for measuring the capability supporting cyber situational awareness	A thorough analysis of metrics that can be mapped to SA reference model to help evaluate the quality of performance measures consisting of four dimensions: confidence, purity, cost utility, and timeliness

Curiosity and Cyber Curiosity

Historically there have been many attempts at defining curiosity. Hume (1888) distinguished between curiosity as a passion for scientific discovery and the innate, human nature curiosity such as the "insatiable desire of knowing the action and circumstances of their neighbors" (p. 237). Cicero viewed curiosity as a passionate act, human nature's innate love of learning and knowledge without the lure of profit (Elster, 2000). Modern psychologist defined curiosity as an appetite for knowledge (Lowenstein, 1994). Curiosity is often considered the desire to gain information, which, in turn, results in exploratory behavior and knowledge acquisition (Berlyne, 1960, 1963). Further work into knowledge acquisition's link to curiosity led to Lowenstein's (1994) development of a knowledge-gap model that focuses on curiosity as resulting from the identification of unknown pieces of information. According to Lowenstein (1994), there are two dimensions of curiosity, one epistemic and perceptual and the other, specific and diverse. Epistemic curiosity (EC) refers to a desire for information and knowledge (Berlyne, 1960). Litman and Jimerson's (2004) analysis of Berlyne's formulation of EC, identified that "unpleasant state of uncertainty" (p. 1586) were more important for motivating knowledge seeking than "pleasurable states of interest." (p. 1586). From this analysis, Litman and Jimerson (2004) identified two types of curiosity based on interest induction (I) and deprivation (D) elimination. I-type curiosity involves the pleasure of new discoveries, whereas D-Type is concerned with reducing uncertainty and eliminating unwanted states of ignorance (Litman, 2008).

Lowenstein (1994) considered the greater motivator for knowledge seeking to be uncertainty reduction versus anticipation of learning something interesting not taking into account individual differences (Litman, Hutchins & Russon, 2005). Litman and Jimerson (2004) further theorized that there are also individual differences in the types of emotions people experience when their curiosity is aroused whether as a result of pleasurable feelings of interest or unpleasant experience of uncertainty. In an empirical study of EC of 321 undergraduate students by Litman, Hutkins, and Russon (2005), the findings suggested that when “participants felt more distant from the desired knowledge, curiosity was both less intense and also involved more positive emotions; when they felt close to figuring out the knowledge, curiosity was more intense, but also less pleasant” (p. 578).

In Cyber SA context, D-Type curiosity can help IS users develop more awareness about cyber threats such as a phishing attack if they are uncertain or ignorant of the indicators or impact of a social engineering attack. I-Type curiosity, in contrast, can create an opportunity for a social engineering cyber-attack by using curiosity to lure users to clicking on a web link or visit a website. Cyber Curiosity in this context is the desire for information and knowledge about information systems (IS).

A better understanding of Cyber Curiosity and a possible link to reducing risks (Hake, 2016) such as a social engineering attack might assist organizations in designing more effective Cyber SA programs or in identifying personality characteristics that help with cybersecurity job requirements (Libicki, Senty, & Pollack, 2014). A summary of research studies regarding curiosity and Cyber Curiosity are listed in Table 5.

Table 5

Summary of Curiosity and Cyber Curiosity Literature

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Berlyne, 1960, 1963	Literature review and synthesis		Exploratory and epistemic behavior	Increases the knowledge of concepts and principles of exploratory and epistemic behavior
Elster, 2000	Literature review and synthesis		Constraint theory	People may benefit from being constrained in their options from being ignorant
Hume, 1888	Treatise		Human nature	A comprehensive attempt to base philosophy on a new, observationally grounded study of human nature
Libicki et al., 2014	Empirical study via interviews and literature review and synthesis	Interviews with representatives of 5 U.S. government organizations	Cybersecurity labor market	In addressing cybersecurity resource gaps companies are defining personality characteristics notably intense curiosity to help identify potential candidates
Litman, 2008	Empirical study via questionnaires	2660 undergraduate students	Interest (I-type) and deprivation (D-type) curiosity	The results of the study helped clarify the differences between I-type and D-type epistemic curiosity (EC). I-type EC is concerned with adding new ideas to improve intellectual mastery while D-type EC reflects an unsatisfied need-like state that motivates exploration and performance-oriented learning goals.

Table 5

Summary of Curiosity and Cyber Curiosity Literature (Cont.)

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Litman et al., 2005	Empirical study via questionnaires	265 university students	Epistemic curiosity	Further substantiation of previous research by Lowenstein (1994) that exploration of knowledge is more strongly motivated when the goal is to reduce feelings of uncertainty rather than to increase feelings of interest
Litman & Jimerson, 2004	Empirical study via questionnaires	321 undergraduate students (248 women, 73 men)	Curiosity as a feeling of deprivation (CFD) and feeling of interest (CFI)	CFD and CFI are psychometrically distinguishable constructs but overlap substantially in relation to epistemic curiosity
Lowenstein, 1994	Literature review and synthesis		Curiosity	A new account of curiosity as a form of cognitively induced deprivation that comes from the perception in a gap in knowledge

Activity Theory

History of Theory

Activity theory originated in the 1920’s and was developed by a group of Russian psychologists. Activity theory threefold origins come from classical German philosophy, in the writing of Marx and Engels, and in the Soviet Russian cultural-historical psychology of Vygotsky, Leont’ev, and Luria (Engestrom, Miettinen, & Punamaki, 1999). Throughout activity theory’s history, three generations of activity theory developed. The first generation was influenced in the 1920’s and 1930’s by Vygotsky, focused on the individual and culture. Vygotsky (1978) proposed that humans deeply understand the things around them and acquire knowledge through their meaningful actions, interaction and other social activities.

The second generation led by Leont’ev (1978, 1981), focused on collective activity, mediational means, and division of labor as the basis of historical processes. Activity theory was introduced into an international audience in the late 1970’s through Leont′ev’s English translation of *Activity, Consciousness, and Personality* (1978). Broadly defined, activity theory “is a philosophical and cross-disciplinary framework for studying different forms of human practices as development processes, which both individuals and social levels interlink at the same time” (Kuutti, 1995, p. 23). Activities are at the center of human behavior (Fishbein & Ajzen, 1975) and these activities are actions and operations that people perform to achieve a desired outcome (Hasan & Crawford, 2003).

The third generation, led by Engeström and Cole, gravitated towards dialogue, multiple perspectives, and cultural diversity (Engeström, Miettinen, & Punamäki, 1999). Cole and Engeström further refined the concept of an activity by adding there is also a transformation of the relationship between the subject and object through their interaction (Salomon, 1997). Luria (1928) asserted a similar observation that tools “radically change his conditions of existence, they even react on him in that they effect a change in him and his psychic condition (p. 493). The basic structure of human cognition that develops from tool mediation and widely known representation of activity theory (AT) is the triadic schema shown below (Figure 3).

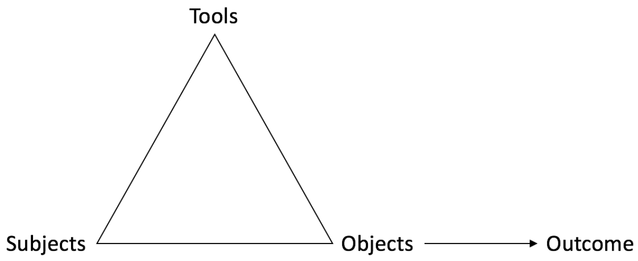


Figure 3. Activity theory triadic schema adopted from Engeström (2006).

At the most basic level, the concept of an activity is the “purposeful interaction of the subject with the world” (Kaptelinin & Nardi, 2006, p. 31), resulting in a mutual transformation (Outcome) between the subject and object (Leontiev, 1978). Kaptelinin and Nardi (2006) described activity as the “basic *unit of analysis* providing a way to understand subject and objects, an understanding that cannot be achieved by focusing on the subject or object separately” (p. 3).

Evolution of Theory

According to activity theory, not any entity is a subject. Subjects have needs that can be met by being and acting in the world (Kaptelinin & Nardi, 2006). In other words, subjects live in the world. Tools in activity theory are not limited to physical artifacts. Vygotsky (1978) made no distinction between things that only exists in the mind from physical artifacts. According to Vygotsky (1978)’s expanded definition of a tool, curiosity or situational awareness would function as tools to accomplish a particular outcome. For example, a Subject includes a user who accesses (Activity) a website with a computer (Object) to learn (Outcome) something new (Curiosity) but uses cyber situational awareness (Tool) to avoid suspicious websites. Bedny and Meister (1999) linked activity theory with situational awareness by stating that "the goals in the theory of activity are closely related to notions of expectations, forecasting, anticipation, or extrapolation" (p. 64). Activity theory has been used in numerous studies and applications, such as in mobile learning (Hsu & Ching, 2013), information sharing systems (Alhefeiti, 2018), personal learning environments (Buchem, Attwell, & Torres, 2011), and the maritime industry (Viktorelius & Lundh, 2019).

Activity Theory Use in the Maritime Industry

In a study by Viktorelius and Lundh (2019), activity theory was used as the framework in analyzing contradictions and tensions in the work practices onboard ships following the implementation of energy monitoring. In using activity theory in this research study, a better understanding of sociotechnical change processes were identified. In another study, activity theory was used to identify interface design human factor issues that impacted situational awareness during remote ship monitoring (Man, Weber, Cimbritz, Lundh, & MacKinnon, 2018).

Activity Theory Use in Safety and Other Industries

Recent empirical research by Vries and Bligård (2019), demonstrates activity theory as a useful model in navigational safety assessment and design. Their research leverage linked activity triangles to show the advisory relationship between pilots (Subject) local knowledge and foresight (Tools), and safe navigation (Goal) with the vessel's crew. A relationship established by Vries and Bligård (2019) was linking activity triangles between goals of one actor may be used as a tool by another actor. This linking can be extended to more complex activity triangle relationships. In a longitudinal observation research focusing on mobile workforce (Francisco, Klein, Engestrom, &

Sannino, 2018), activity theory framework was used to create supportive learning pathways for mobile workers performing knowledge intensive activities. A summary of research studies regarding activity theory are listed in Table 6.

Table 6
Summary of Activity Theory Literature

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Alhefeiti & Abdulla, 2018	Case study	32 participants	Activity theory-based information sharing analysis	Developed a systematic approach to the design of information sharing systems
Allen et al., 2013	Empirical research	50 semi-structured interviews	Critical realism and activity theory	Demonstrated that critical realism and activity theory are essential to IS research
Bedny & Meister, 1999	Case study		Situation awareness	Situation awareness must be viewed as part of cognitive activity that is intensely dynamic
Buchem, et al., 2011	Scientific analysis of publications	100 publications	Personal learning environments (PLE) and activity theory	Created a better understanding of PLEs and developed a knowledge base to inform further research
Engeström, Miettien, & Punamäki, 1999	Literature review and synthesis		Activity Theory	Comprehensive overview, history, and theoretical background of Activity Theory
Fishbein & Ajzen, 1975	Literature review and synthesis		Attitude	Activities are at the center of human behavior.

Table 6

Summary of Activity Theory Literature (Cont.)

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Francisco, et al., 2018	Literature review and synthesis		Activity theory and expansive learning	Theoretical contribution of exploring expansive learning in mobile work to analyze practices of knowledge creation and sharing.
Kaptelinin & Nardi, 2006	Literature review and synthesis		Activity Theory	A systematic entry-level introduction to the major principles of activity theory and applied to our relationship with technology.
Kuutti, 1995	Literature review and synthesis		Human-Computer Interaction and Activity Theory	Paper discusses the potentials of activity theory as an alternative framework for HCI research and design.
Leont′ev, 1978	Literature review and synthesis		Activity and consciousness	Demonstrates the primacy of Marxists methodology in the resolution of fundamental problems of contemporary psychology
Luria,1928	Literature review and synthesis			Cultural development
Viktorelius & Lundh, 2019	Case study		Energy efficiency and cultural-historical activity theory	A better understanding of the social technical change processes can be achieved if the existing practitioners every day practices paradoxes are examined

IS User Activity Theoretical Framework

A solid theoretical framework “identifies and defines the important variables in the situation that are relevant to the problem and describes and explains the interconnections among the variables” (Sekaran & Bougie, 2013, p. 78). The IS user activity system model illustrated in Figure 4 adopts activity theory to investigate the relationship between IS users (Subject), Cyber Curiosity (Tool), Cyber SA (Tool), actions (Object) and outcome (Goal). Figure 4 adapts the triangular activity system developed by Engeström (1990) that is considered a valuable descriptional framework for use and analysis of technologies (Kaptelinin & Nardi, 2006).

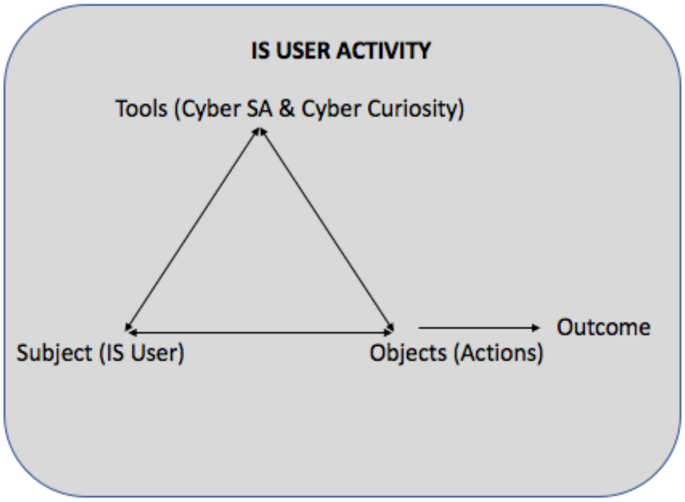


Figure 4. The IS user activity system model adopted from Kaptelinin and Nardi (2006)

Demographic Indicators

Age

Age has been a demographic indicator in research related to curiosity, social engineering, and situational awareness. A study by Robinson, Demetre and Litman

(2017), showed a decline in epistemic curiosity, an intellectual desire for new knowledge, from early to late adulthood. Age-related declines in exploratory behavior are also evident in animal research (Collier et al., 2004). Motivational factors also affect curiosity at various ages. According to socioemotional selectivity theory (SST), when individuals are young, they tend to focus on information seeking goals over emotion-regulation goals in preparation for the uncertain future. In contract, older people tend to favor emotion-regulation goals and optimization of their psychological wellbeing. This focus in emotion-regulation goals at older age is due to their perception that time is limited (Sakaki & Murayama, 2018). In summary, previous studies in personality psychology, animal behavior, and social psychology confirm that curiosity declines with advanced age.

There have been numerous studies that have identified age-related cognitive declines and its impact to situational awareness. In evaluating the impacts of aging in situational awareness, one type of intelligence, fluid intelligence, declines as an individual age (Caserta & Abrams, 2007). For example, driving in an unfamiliar city during high traffic requires fluid intelligence to deal with the rapid processing of new information. Age-related declines in the perception of rich relevant cues impact level 1 situational awareness (Korteling, 1993; Salthouse, 1991). Level 2 and 3 SA also suffer from age-related declines due to the increased load in working memory (Bolstad, 2001).

Years performing job

In the maritime industry, the years performing job may influence detection of a social engineering cyber-attack or improve their cyber situational awareness. Asher and

Gonzalez (2015) examined the knowledge gap between experts and novices in cybersecurity and how it influences their ability to detect cyber-attacks. Experts do better when their decisions relate to their judgement and when under static as compared to dynamic stimulus. Along similar previous research findings, experience makes an expert more attuned to cues that are overlooked by a novice (Randel, Pugh, & Reed, 1996). Beyond experience, situated knowledge, knowledge specific to an organization or operating environment may offer an additional layer of situational awareness to detect cyber-attacks beyond just years of experience in performing a particular job (Goodall, Jutters & Komlodi, 2004).

Gender

Gender has been studied as a demographic indicator in research related to curiosity, social engineering, and situational awareness. In one study by Huang, Wang, Zhou, and Zhang (2010), there were no significant differences observed in epistemic curiosity between males and females. In a study by Anwar et al. (2017), they observed gender differences in security self-efficacy, where women's mean self-efficacy score was 0.95 standard deviations lower than men's mean ratings. Further research is warranted whether gender has an influence on Cyber SA and Cyber Curiosity.

Nationality

National culture is defined as the “values, beliefs, and assumptions learned in early childhood that distinguishes one group of people from another” (Testa, 2002, p. 427). One particular maritime industry, the cruise industry, capitalizes on sourcing its human resources in an environment that is hierarchical in organization and nationality structure. Weaver (2005) generalized that the lowest ranking employees are usually from

Eastern Europe, Central America, and Southeast Asia. Middle ranking crew such as supervisors are frequently from eastern and western Europe. While higher ranking crew members are from wealthier countries like the United States, United Kingdom, Canada, or Australia. A summary of research studies regarding demographic indicators are listed in Table 7.

Table 7

Summary of Demographic Indicators Literature

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Anwar et al., 2017	Cross-sectional survey study	481 students	Cybersecurity behaviors and gender	Gender has effect in security self-efficacy, prior experience, and computer skills and minimal effect in cues-to-action and self-reported cybersecurity behaviors
Ben-Asher & Gonzalez, 2015	Experiment and questionnaire	55 students; 20 security professionals	Dynamic decision making, intrusion detection system	A better understanding of the human decision-making process in the detection of cyber-attacks. Experts do well in tasks where the stimulus is static. Performance of detecting cyber-attacks where similar for experts and novices
Bolstad, 2001	Driving simulator experiment	48 participants	Situational awareness and age	Older adults have lower SA and with increasing complexity they are more susceptible to a narrowing of attention

Table 7

Summary of Demographic Indicators Literature (Cont.)

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Collier et al., 2004	Experimental research	344 rats	Spatial learning and age	Discovery of age related reduction in neurotransmission resulting in deficits in spatial learning and memory performance
Goodall et al., 2004			Intrusion detection and expertise	Effective intrusion detection requires expertise that combines deep understanding of networking, system behavior, and situated knowledge of the local operating environment.
Huang, et al., 2010	Survey and data analysis	2871 students	Epistemic curiosity	Boys and girls experience and express both I-type EC and D-type EC to the same extent and frequency, invalidating any biased gender-based expectation
Korteling, 1993	Experiment	28 adults	Dual-task performance and age	Further substantiated the slowing-complexity hypothesis that general slowing causes age effects to increase with overall task complexity

Table 7

Summary of Demographic Indicators Literature (Cont.)

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Randel et al., 1996	Experiment	28 warfare technicians	Situation awareness and naturalistic decision making	Experts were more proficient in recalling radar emitters and their ability to make correct decision based on better SA
Robinson et al., 2017	Quasi-experimental design	963 adults	Curiosity and age	Individuals in the crisis period of various age groups were more curious (D-type) than those of the same life stage
Sakaki & Murayama, 2018	Literature review and analysis		Cognitive preservation and aging	Despite that curiosity declines with age, it plays an important role in maintaining cognitive function, mental health, and physical health in older adults
Salthouse, 1991	Literature review and analysis		Cognitive functioning and age	Reviewed and evaluated the major explanations proposed to account for the negative relationship between age and cognition
Testa, 2002	Survey and data analysis	367 cruise line managers	Multiculturalism and dyad congruence	National culture systematically impacts how subordinates evaluate and feel about their leaders

Table 7

Summary of Demographic Indicators Literature (Cont.)

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Weaver, 2005	Literature review and analysis		Performative metaphors	Performance metaphors can be used to explain the difficult conditions and circumstances that cruise-ship service employees work

Summary of What is Known and Unknown in the Literature

A review of literature provides an overview of important constructs such as Cyber SA, Cyber Curiosity, and foundational theories that include activity theory all of which provide the foundation for this proposed study. A detailed description of what is known and unknown is included in this literature review. The following paragraph gives a summary of what is known and unknown within this area of research.

In information security, users are the weakest link (Anderson, 1993; Boss, Kirsh, Angermeier, Shingler, & Boss, 2009; Mahfuth, Yussof, Baker, & Ali, 2017). Attackers exploit this fact using social engineering (Mouton, Leenen, & Venter, 2016). IS user curiosity can lead to compromise and safety of systems such as in baiting types of socially engineered attacks where the user is enticed by a gift or reward (Fan, Lwakatare, & Rong, 2017). In contrast, IS user curiosity can possibly improve IS security by users being more aware of social engineering attacks. Lack of Cyber SA limits an IS user's ability to detect a social engineering cyber-attack. Increasing Cyber SA, as demonstrated in other domains such as medical, transportation, driving safety, may improve IS users awareness of potential cyber-attack and reduce cyber incidents. The medical and transportation domains have benefitted from situational awareness simulation training to improve perception ability. A recent medical SA study by Chang et al. (2017), resulted in modest differences between simulation training versus lecture training on SA. What is unknown is whether increasing Cyber SA for individuals with a propensity to engage in risky activity such as surfing questionable websites, clicking on email links without worrying about the ramifications can lower their risks. In similar studies of SA analyzing offshore drilling accidents and unsafe work behaviors, showed a positive relation to the safety of non-compliance workers with a history of unsafe behaviors (Sneddon, Means, & Flin, 2013). A review of the literature associated with Cyber SA and Cyber Curiosity seems to indicate that these two constructs likely impact the susceptibility and success of a social engineering attack. However, limited research on these relationships has been conducted and as a result, additional research is warranted.

Chapter 3

Methodology

Overview of Research Design

This research study used a developmental approach. A developmental research approach was an appropriate approach because the study required developing a Cyber SA and Cyber Curiosity risk taxonomy to address an identified problem. According to Ellis and Levy (2009), developmental research attempts to answer how the building of an artifact ameliorates a problem. A comparison approach was also used to better understand the relationship between the constructs of Cyber SA and Cyber Curiosity. Figure 5 shows the research design consisting of three phases for this research study. Developmental research has three essential elements: 1) creating and validating the criteria the product must meet; 2) following an accepted process for developing a product; 3) subjecting the product to an accepted process to assess if it satisfies the criteria (Ellis & Levy, 2009). This research design process began with the exploration of the literature to identify a research problem that led to the formulation of research questions. This was followed by the identification and proposal for the initial classification of components for the measures of Cyber SA and Cyber Curiosity. After this initial exploration and formulation stage, the research study transitioned to the first phase of three phases. In Phase One, the Cyber SA and Cyber Curiosity measures and scores used in the Cyber Risk taxonomy was validated by SMEs' input utilizing the Delphi method. In Phase Two, of this research study, using the validated Cyber SA and Cyber Curiosity components and scores, a proposed interactive social engineering attack experiment was SME validated utilizing the Delphi method. At the beginning of Phase Three, a successful pilot testing of the Cyber SA and Cyber Curiosity measures was conducted. Phase Three then proceeded with data collection, pre-analysis data screening, and data analysis. The entire research study culminated with the conclusions and recommendations. Figure 5 shows the research design for this research study.

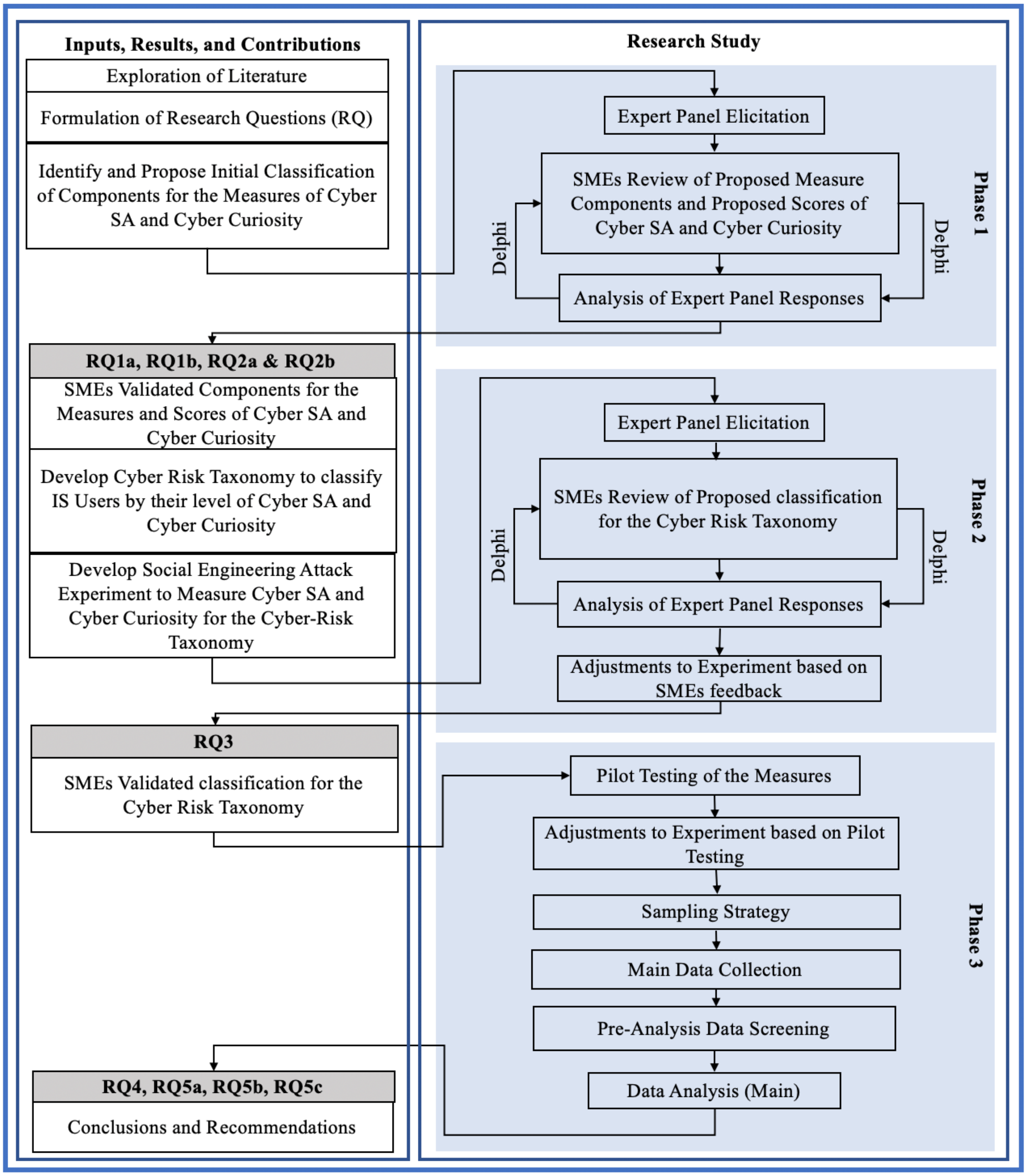

Inputs, Results, and Contributions
Exploration of Literature
Formulation of Research Questions (RQ)
Identify and Propose Initial Classification of Components for the Measures of Cyber SA and Cyber Curiosity
RQ1a, RQ1b, RQ2a & RQ2b
SMEs Validated Components for the Measures and Scores of Cyber SA and Cyber Curiosity
Develop Cyber Risk Taxonomy to classify IS Users by their level of Cyber SA and Cyber Curiosity
Develop Social Engineering Attack Experiment to Measure Cyber SA and Cyber Curiosity for the Cyber-Risk Taxonomy
RQ3
SMEs Validated classification for the Cyber Risk Taxonomy
RQ4, RQ5a, RQ5b, RQ5c
Conclusions and Recommendations
Research Study
Expert Panel Elicitation
SMEs Review of Proposed Measure Components and Proposed Scores of Cyber SA and Cyber Curiosity
Analysis of Expert Panel Responses
Delphi
Delphi
Phase 1
Expert Panel Elicitation
SMEs Review of Proposed classification for the Cyber Risk Taxonomy
Analysis of Expert Panel Responses
Adjustments to Experiment based on SMEs feedback
Delphi
Delphi
Phase 2
Pilot Testing of the Measures
Adjustments to Experiment based on Pilot Testing
Sampling Strategy
Main Data Collection
Pre-Analysis Data Screening
Data Analysis (Main)
Phase 3

Figure 5. Research Design Process

Phase One

Prior to beginning Phase One, this research study obtained site approval and Institutional Review Board (IRB) approval as seen in Appendix A and B respectively. Phase One of this research SMEs reviewed the proposed measure components and scores of Cyber SA and Cyber Curiosity. The SMEs review used the Delphi technique, to review and validate the proposed Cyber Risk taxonomy: 1) components for the measures of Cyber SA; 2) components for the measures of Cyber Curiosity levels; and 3) the scores of the identified components of the measures of Cyber SA and Cyber Curiosity. A target group of nine SMEs were solicited to participate in the review using Google Forms® to gather the data (See Appendix C & Figure 6). The SMEs background included a mixture of cybersecurity and cyber maritime experts with at least ten years of professional experience. The expert panel questionnaire began with an explanation of the questionnaire and the SMEs role in the research. The questionnaire then proceeded with SMEs demographics section to obtain their background and professional credentials. The last portion of the questionnaire, that collected the SME's validation responses and feedback, had two parts. Part one consisted of validating the proposed components and scores for the measures of Cyber SA through a multiple-choice grid with rows to validate each component for the measures of Cyber SA. There was multiple choice option to 1-Keep, 2-Adjust, or 3-Remove the proposed component. If the SMEs selected option 2 or 3 then the SMEs would need to provide feedback on the recommended adjustments. Part two consisted of validating the proposed components and scores for the measures of Cyber Curiosity using a similar multiple-choice option with SMEs validation requirements. Phase One concluded with successfully addressing research RQ1a, RQ1b, RQ2a, and RQ2b by successfully getting a consensus on the proposed Cyber Risk taxonomy.

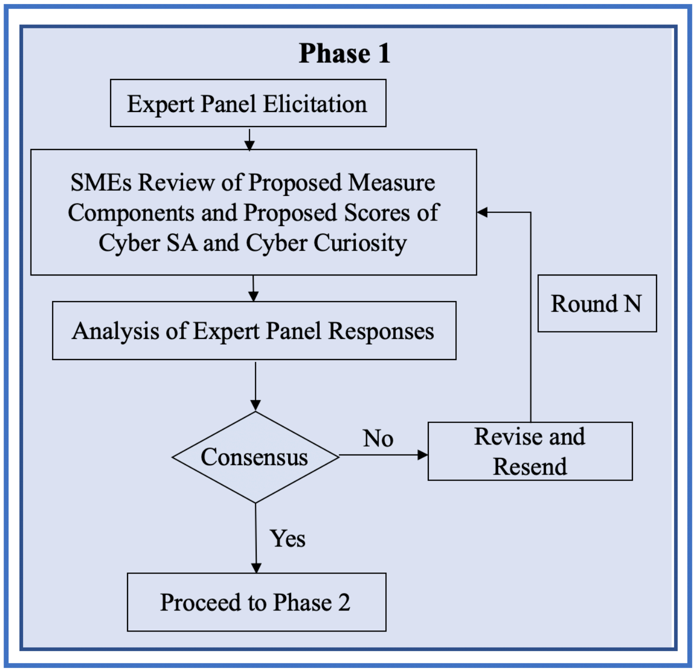

Phase 1
Expert Panel Elicitation
SMEs Review of Proposed Measure Components and Proposed Scores of Cyber SA and Cyber Curiosity
Analysis of Expert Panel Responses
Round N
Consensus
No
Revise and Resend
Yes
Proceed to Phase 2

Figure 6. Phase 1 - Research design to review and validate proposed measure components and proposed scores of Cyber SA and Cyber Curiosity

Phase Two

Phase Two SME validated the proposed Cyber Risk Taxonomy using a consensus-building process implementing the Delphi technique. A target group of seven SMEs were solicited to participate in the review using Google Forms® to gather the data (See Appendix F & Figure 7). The SMEs background included a mixture of cybersecurity and cyber maritime experts with at least ten years of professional experience. The expert panel questionnaire began with an explanation of the questionnaire and the SMEs role in the research. The questionnaire then proceeded with SMEs demographics section to obtain their background and professional credentials. The last portion of the questionnaire collected the SME’s validation responses and feedback. There was multiple choice option to 1-Keep, 2-Adjust, or 3-Remove the proposed Cyber Risk taxonomy components. If the SME selected option 2 or 3 then the SMEs would need to provide feedback on the recommended adjustments. The successful review and validation of the Cyber Risk Taxonomy concluded Phase 3 with addressing RQ3.

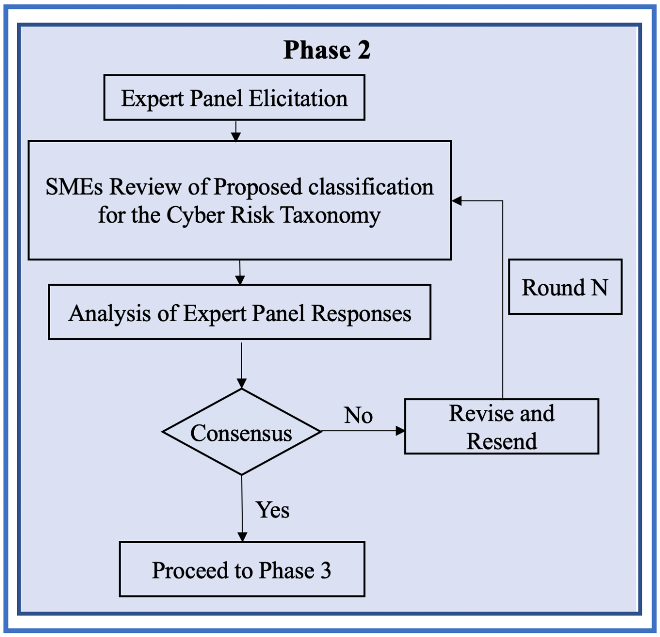

Phase 2
Expert Panel Elicitation
SMEs Review of Proposed classification for the Cyber Risk Taxonomy
Analysis of Expert Panel Responses
Round N
Consensus
No
Revise and Resend
Yes
Proceed to Phase 3

Figure 7. Phase 2 Research design to review and validate proposed classification for the Cyber Risk Taxonomy

Phase Three

Phase Three began with a pilot test of the Web-based experiment using a mixture of qualitative and quantitative data collection, to assess measures of Cyber SA and Cyber Curiosity. Minor adjustments were made to the experiment based on the feedback from the pilot experiment. After minor refinements were made to the experiment, Phase Three successfully conducted a quantitative empirical study by collecting Cyber SA and Cyber Curiosity data from 120 maritime IS and 54 shoreside IS users. Lastly, the collected data was analyzed to address RQ4, RQ5a, RQ5b, and RQ5c. The research methodology required several issues to be addressed including: 1) expert panel validation of Cyber Risk taxonomy; 2) experiment development; 3) experiment validity; 4) experiment reliability; 5) sampling strategy; 6) pre-analysis data preparation; and 7) data analysis.

The main research question that this research study addressed is: Does the measured level of IS Cyber SA and Cyber Curiosity assist in the determination of a maritime IS user's susceptibility of a social engineering cyber-attack? The research context in this proposed study will be Cyber SA and Cyber Curiosity in the maritime industry. The maritime industry is an ideal environment to study Cyber SA and Cyber Curiosity because maritime IS users must rely on SA to safely operate and navigate a ship. The maritime system “is a people system, and human errors figure prominently in casualty situations” (Rothblum, 2000, p. 1). Bridge officers frequently rely on SA using IS systems and their surroundings to make quick decisions when navigating in inclement weather or when safely piloting through a condensed port (Chauvin & Lardjane, 2008; Olsson & Jansson, 2007).

Experiment Development

This research study Web-based interactive experiment consisted of four steps (See Figure 8) that took between 15 through 20 minutes for participants to complete. Step one began with an audio and presentation overview of the research study that took less than two minutes to complete. Step two required the participants to review and electronically sign the informed consent form that took approximately two minutes to complete. Step three gathered the participant’s demographics by requesting the participant to fill out a Google Form® pre-experiment survey that consisted of two sections. Step three took less than 3 minutes. Section one, as illustrated in Appendix I, gathered demographic items from the survey participants consisting of age range (D1), gender identification (D2), nationality (D3), department (D4), years performing job (D5), and education level (D6).

Section two of the survey gathered participants psychological state of being consisting of two items P1 and P2 using a four-point Likert scale ranging from "not at all" to "nearly every day." The rationale for these survey items were described in the literature demographics section.

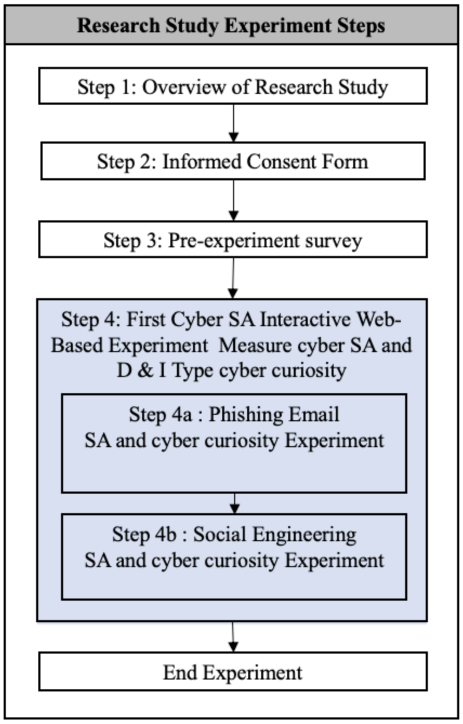

Research Study Experiment Steps
Step 1: Overview of Research Study
Step 2: Informed Consent Form
Step 3: Pre-experiment survey
Step 4: First Cyber SA Interactive Web-Based Experiment Measure cyber SA and D & I Type cyber curiosity
Step 4a : Phishing Email SA and cyber curiosity Experiment
Step 4b : Social Engineering SA and cyber curiosity Experiment
End Experiment

Figure 8. Research Study Experiment Steps

After the survey form was submitted, step four began with the two-part interactive Web-based experiment took less than 13 minutes to complete. The first experiment collected the participants Cyber SA and Cyber Curiosity D-Type measures by presenting a simple social engineering scenario that integrated the measures of the two constructs: Cyber SA and Cyber Curiosity (D-type). The second portion of the experiment collected the participants Cyber SA and Cyber Curiosity (I-Type) by presenting an advanced social engineering scenario that integrated the measures of the two constructs: Cyber SA and

Cyber Curiosity (D-Type & I-Type). See Figure 9 for the conceptual design of the Cyber SA and Cyber Curiosity measurement approach.

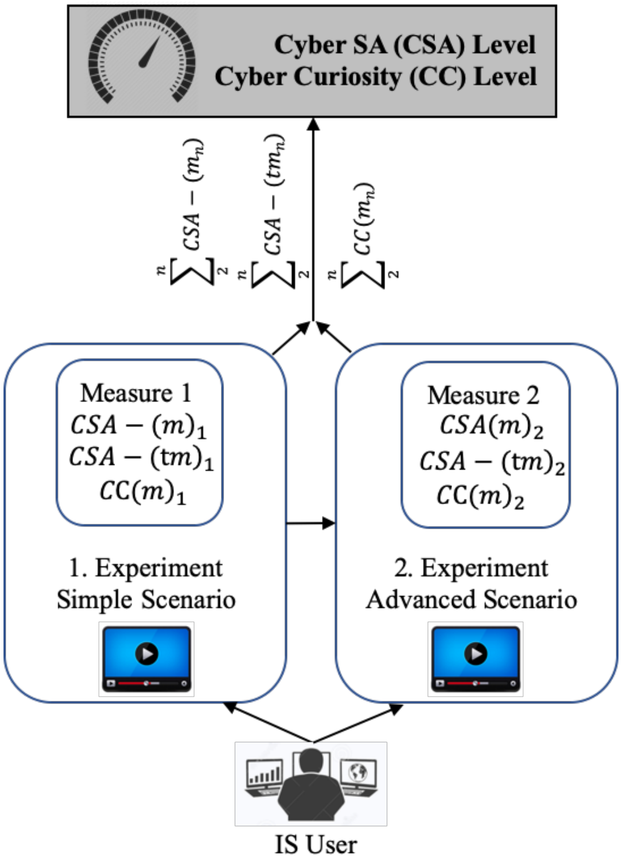


Figure 9. Conceptual design of the Cyber SA and Cyber Curiosity measurement approach

Expert Panel & Delphi Technique

The use of an expert panel using the Delphi technique was used validate the Cyber SA and Cyber Curiosity measures and scores and the Web-based experiment. The Delphi method assists with construct validity (Okoli & Pawlowski, 2004). The Delphi technique has been used to develop a range of possible alternatives, to explore underlying assumptions leading to different judgments, to seek out information which may generate a consensus on the part of the respondent group, and to correlate informed judgements on a topic spanning a wide range of disciplines (Delbecq, Van de Ven, & Gustafon, 1975). There are three characteristics associated with the Delphi method which are anonymity, controlled feedback, and aggregations of responses. There are typically three to four rounds used in the Delphi method but three is sufficient to collect needed information and reach a consensus (Brooks, 1979; Custer, Scarcella, & Steward, 1999). The first round begins with an open-ended questionnaire that solicits specific information from the SMEs (Custer et al., 1999). An acceptable modification to round one of the Delph method is to use a structured questionnaire that is based upon an extensive review of the literature (Kerlinger, 1973). The second round the SMEs are required to rank-order items to establish priorities among items and to reach consensus or disagreement among items (Ludwig, 1994). In this study, the first and second round were combined into a two-part questionnaire structured questionnaire and a rank-order of items for the SMEs to validate the components for the measures and scores of Cyber SA and Cyber Curiosity constructs. In Delphi reviews where complete consensus was achieved in earlier rounds, additional rounds was not necessary as the number of Delphi iterations depends on the degree of consensus sought by researchers and can vary (Delbecq, Van De Ven, & Gustafson, 1975).

Pilot Testing

Prior to data collection, the proposed pre-experiment survey and experiment was reviewed by an expert panel and a pilot test was conducted on a subset of the sample population. Ten IS users were used in the pilot to assess the measures of Cyber SA and Cyber Curiosity. A pilot is defined as an experimental investigation (Hawker & Waite, 2007) that allows the researcher to test of the methods and procedures to be used later on a larger scale. Conducting a pilot test is one of the most important steps in successful quantitative research because it provides a preliminary assessment of the theory (Dennis & Valacich, 2001) including identifying areas where the proposed experiment may be complicated and fail (Teijlingen & Hundley, 2001). Furthermore, the pilot experiment further substantiate that the experiment was valid and reliable before its implementation to the experiment sample. Appendix E provides the pilot study recruitment email used to enlist participants. Prior to beginning the pilot test, a consent form as seen in Appendix F was acknowledged and signed.

Measuring Cyber Situational Awareness

Several methods for measuring SA have been developed. The SA data collection approaches are self-rating technique (McGuiness & Foy, 2000; Matthews & Beal, 2002), observer rating (Matthews & Beal, 2002), freeze online probe (Endsley, 1995; Hauss & Eyferth, 2003), performance measures, real-time probe (Jeannott, Kelly, & Thompson, 2003), post-trial questionnaire (Jeannott et al., 2003) and physiological measurement techniques (e.g. eye tracking devices). The majority of such measures often use simulators (Wright, Taekman, & Endsley, 2004). Other than simulators, SA data collection methods have used post task completion SA rating questionnaires where respondents rate factors affecting their performance and understanding to provide a global measure of SA (Taylor, 1990). Freeze probe techniques require the administration of SA queries online during ‘freezes’ in a simulation of the task under analysis (Salmon et al., 2009). For this proposed study, a freeze probe technique was used to gather IS user responses from the social engineering attack, interactive Web-based Cyber SA and Cyber Curiosity experiment. Time is the factor that was used to measure the level Cyber SA.

The advantages of using freeze probe is that it is a direct approach, subject to number validation studies, and removes challenges with collecting SA post-trail data (Salmon et al., 2006). Performance measures to assess Cyber SA involved measuring relevant aspects of the IS participant performance during the Web-based experiment (i.e. identification of phishing attack indicators). For each correct identification of a social engineering attack type indicators the participant gets a point. Table 8 and Table 9 shows the SMEs validated Cyber SA measurement points for each correct attack identification and the duration for the identification of the attack.

Table 8

Cyber SA Measurement Points (CSA-m)

Experiment User Action Categories	**Points**
Simple social engineering attack identified	1
Advanced social engineering attack identified	2
Unable to identify social engineering attack or no response	0
Incorrect social engineering attack identified	-1

Table 9

Cyber SA Time Measurement Points (CSA-tm)

Level	**Experiment User Action Timing Categories**	**Points**
Advanced	Advanced social engineering attack identified under 10 seconds	4
	Advanced social engineering attack identified between 10 seconds and 20 seconds	2
	Advanced social engineering attack identified longer than 20 seconds	0
Simple	Simple social engineering attack identified under 10 seconds	2
	Simple social engineering attack identified between 10 seconds and 20 seconds	1
	Simple social engineering attack identified longer than 20 seconds	0

Measuring Cyber Curiosity

In the context of this research study, the two types of epistemic curiosity (EC) were measured I-Type (interest induction) and D-type (deprivation elimination). I-Type EC deals with the pleasure of new discoveries and diverse exploration. D-Type EC is concerned with reducing uncertainty, eliminating unwanted levels of ignorance, aimed at solving problems, and setting performance-oriented learning goals (Litman, 2008). Two EC measurements used in curiosity research are the Epistemic Curiosity Scale (ECS) (Litman & Spielberger, 2003) and the Curiosity as a Feeling-of-Deprivation Scale (CFDS) (Litman & Jimerson, 2004). An adaption of the ECS and CFDS EC measurement using an indirect versus direct (questionnaire or survey) will be used for this proposed experiment.

Cyber Curiosity I-Type and D-Type measurements were taken during the Cyber SA interactive Web-based experiment. Both I-Type and D-Type Cyber Curiosity measurements were obtained by keeping track of the various Web links the participants click on during the interactive experiment. I-Type and D-Type curiosities are inversely related in terms of scoring Cyber Curiosity. I-Type curiosity reduces Cyber Curiosity scores while D-Type increases Cyber Curiosity scores. For example, if the participant clicked on a simple explanation of identifying a social engineering attack, they got a negative point (D-type curiosity). If the participant clicked on a more in-depth explanation, they got negative 2 points (D-Type curiosity). If the participant clicked on a Web link that was potentially malicious, they got a point increased (I-Type curiosity). Table 10 shows the SMEs validated Cyber Curiosity measurement points per action selected.

Table 10

Cyber Curiosity Measurement Points

	Curiosity Type		
Experiment User Action Selection	**I-Type**	**D-Type**	**Points**
Simple explanation (User was presented with link to expand on explaining the section of the experiment such as "Learn more about Phishing Email Situational Awareness")		x	-1
In-depth explanation (User was presented with a link in the simple explanation section to seek further information such as "To learn further information about Phishing Email Situational Awareness")		x	-2
Enticing Web link (User was presented with a link to a non-SA awareness page with an entertaining story or topic)	x		1
Enticing Pop-up Web link (User was presented with a pop-up to a non-SA awareness page with an entertaining story or topic)	x		2

Reliability and Validity

Instrument Validity

Validity in research refers to the researches ability to infer meaningful and justifiable inferences from data about a sample or population (Creswell, 2005). Validity of an instrument refers to the degree an instrument measures what it is supposed to measure (Leedy & Ormrod, 2005). To ensure the validity and reliability of the Web-based experiment and surveys, a panel of SMEs reviewed the proposed interactive social engineering attack experiment to measure Cyber SA and Cyber Curiosity. A pilot was also conducted to test the experiment and gathered measures to refine the experiment based on the results.

Internal Validity

Internal validity is the confidence placed in the cause-and-effect relationship or more simply stated, “To what extent does the research design permit us to say that the independent variable causes a change in a variable” (Sekaran & Bougie, 2013, p. 174). This study leveraged SA experimental techniques previously used by notable researchers in SA. To further reduce the threats to internal validity, an expert panel reviewed and validated the experimental procedures and scorings.

External Validity

External validity is the extent of generalizability of the results of a causal study to other environments, people, or events (Sekaran & Bougie, 2013). Because research study gathering data in a field experiment and not in a controlled, lab environment, this approach increases the external validity. According to Sekaran and Bougie (2013), field experiments have more external validity meaning that the results are more generalizable to similar organizational settings.

Construct Validity

Construct validity “testifies to how well the results obtained from the use of the measure fit the theories around which the test is designed” (Sekeran & Bougie, 2013, p. 227). Incorporating the validation of a measure can help substantiate research findings, as well as “move the IS field forward toward meaningful replicated studies” (Straub, 1989, p. 162). This research study focused on two constructs, Cyber SA and Cyber Curiosity. Using published measures for similar constructs such as situational awareness and curiosity improved the “goodness” of the measure (Sekeran & Bougie, 2013). Requiring feedback from SMEs, using the Delphi technique, ensured that the criteria used in the method of measuring Cyber SA and Cyber Curiosity was further validated.

Instrument Reliability

The Web-based experiment was designed to accurately measure levels of Cyber SA and Cyber Curiosity. To increase the reliability of the experiment, detailed logging was enabled to track the measured points for both Cyber SA and Cyber Curiosity. These captured measurements were compared with the expected results and compared with what was being recorded. Further measurement calculations were validated during the pilot testing of 10 users to make sure that experiment data recorded was accurately and reliably sent to Amazon’s DynamoDB NoSQL database. A manual, visual inspection of each participants measurements were validated to what was observed during the experiment. There was a risk to instrument reliability in this experiment in that it utilized an interactive Web-based experiment that needed to use a provided computer and satellite Internet. To increase reliability, several performance tests were conducted on the experiment site (ship) to identify the minimum requirements for the computer and Internet speed. To improve the performance and higher reliability of the cyber SA timed measures, non-essential components to the experiment were removed such as the audio overview of the experiment and high-resolution graphics. To test for internal consistency a mixture of split-half, Cronbach Coefficient Alpha, or Kuder-Richardson correlation tests were used.

Population and Sample

The population of the study is approximately 1,200 maritime IS users in the marine operations, hotel operations, and shipboard information technology (IT) departments. A randomized selection of the sampling frame was the sample of the study. A sample size of 174 IS users was used to support the validity and generalization of the results. To further increase the generalizability of the study, the sample group, due to the global nature of the maritime industry, had diversity such as nationality, education level, department, and number of years performing job.

Data Collection and Analysis

Prior to data analysis, pre-analysis of data was performed on the data collected from the SMEs and the experiment participants. Levy and Ellis (2006) recommend pre-analysis data screening to prevent data collection issues. This research study had two forms of quantitative data gathered from the pre-experiment survey and interactive Web-based experiment with the sample participants to measure the two constructs, IS user Cyber SA and Cyber Curiosity. Using the demographics information and personal mood data gathered from the pre-experiment survey using Google Forms, this set of additional data was measured and analyzed against the two constructs. The measures from the experiment will be plotted on the Cyber SA and Cyber Curiosity Cyber Risk taxonomy.

Data Aggregation

The measurement of IS participants Cyber SA and Cyber Curiosity required measuring relevant aspects of the IS participant performance during the interactive Web-based experiment such as the identification of a phishing attack or an IS participant clicking on a Web-link. This research study required three data aggregations. The first data aggregation was calculating overall Cyber SA. Equation 1 (Eq. 1) was used to compute the total Cyber SA score for each experiment participant.

Eq. 1 $$Cyber\ SA\ Total\ =\ \sum_{1}^{n} CSA(m_n) + CSA(tm_n)$$

Here $CSA(m_n)$ is the average specific score of the SMEs identified components of the IS user's measures of Cyber SA. $CSA(tm_n)$ is the average specific score of the SMEs identified components of the IS user's *time* measurement of Cyber SA. $CSA(tm_n)$ is the specific score of the SMEs identified components of the IS user's time measurement of Cyber SA. And *n* is a specific Cyber SA experiments, which is two (2) in this study. The second data aggregation was calculating overall Cyber Curiosity. Equation 2 (Eq. 2) was used to compute the total Cyber Curiosity score for each experiment participant.

Eq. 2 $$Cyber\ Curiosity\ Total\ =\ \sum_{1}^{n} CC(m_n)$$

Here $CC(m_n)$ is the average specific score of the SMEs identified components of the IS user's measures of Cyber Curiosity. And *n* is the specific Cyber Curiosity experiments, which is two in this study. The third data aggregation, the Cyber Risk score, is the product of the overall Cyber SA and Curiosity score adjusted scores (transformations). Such transformation was needed, given that two components of the measures had a range of scores from negative to positive. Thus, the transformations conducted unable the overall product to represent accurately the magnitude of the specific measures combined. Equation 3 (Eq. 3) was used to compute the total Cyber Curiosity score for each experiment participant.

Eq. 3 $$Cyber\ Risk\ score = \left(Cyber\ SA\ Total + (1 - minCSA)\right) \times\ (Cyber\ Curiosity\ Total + (1 - minCC))$$

Here $minCSA$ is the minimum value for the Cyber SA score range and $minCC$ is = the minimum value for the Cyber Curiosity score range.

Research Question 4 (RQ4)

The fourth research question determined where the IS users are positioned in the Cyber Risk taxonomy based on their Cyber SA and Cyber Curiosity measurements captured in the interactive Web-based experiment. RQ4 is stated as:

RQ4: How are the aggregated scores for Cyber SA and Cyber Curiosity positioned on the Cyber Risk taxonomy for the maritime IS users?

Analysis of RQ4 was determined by calculating the aggregates for Cyber SA and Cyber Curiosity and plotting the values on the Cyber Risk taxonomy (2x2 matrix). As described earlier, each quadrant represents one of the four groups labeled “Low Cyber Risk”, “Medium Cyber Risk”, “High Cyber Risk” and “Very High Cyber Risk.”

Research Question 5 (RQ5)

The fifth research question determined if there were any statistically significant mean differences to IS users aggregated Cyber SA and Cyber Curiosity levels, and Cyber Risk score based on the captured demographics in the pre-experiment survey (See Appendix I & J) such as age range, gender identification, nationality, department, years performing job function, or education level. RQ5 is stated as:

RQ5a: Are there any statistically significant mean differences to maritime IS users' aggregated level of Cyber SA based on their age, gender, department, years performing job function, or education level?

RQ5b: Are there any statistically significant mean differences to maritime IS users' aggregated level of Cyber Curiosity based on their age, gender, department, years performing job function, or education level?

RQ5c: Are there any statistically significant mean differences to an IS user's Cyber Risk score based on their age, gender, department, years performing job function, or education level?

According to Sekaran and Bougie (2013), it is necessary to include a frequency distribution for demographic variables. This research study included a tabulation to compute an IS user's Cyber SA and Cyber Curiosity aggregated score based on their gender, age, nationality, department, years performing job function, and education level. This research used the means of the aggregated scores for the two constructs, Cyber SA and Cyber Curiosity, to analyze RQ5a-RQ5b and tests the significance of group differences using one-way analysis of variance (ANOVA). To calculate the Cyber Risk score to analyze RQ5c and tests the significance of group differences using one-way analysis of variance (ANOVA), the product of the adjusted Cyber SA and Cyber Curiosity was used. According to Mertler and Vannatta (2010), ANOVA is the appropriate statistical test to evaluate differences when there is one dependent variable (DV) with two or more categories and multiple quantitative independent variables IVs. The IVs in this research study are the demographics indicators D1-D6. The given that there were two independent DVs, Cyber SA and Cyber Curiosity, as well as one integrated multiplication of the two, the Cyber Risk score, ANOVA was conducted three times. The first ANOVA1 analyzed Cyber SA and the IVs (age, gender, nationality, department, years performing job, and education level). The second ANOVA2 analyzed

Cyber Curiosity and the same set of IVs. The third ANOVA3 analyzed the IS user's Cyber Risk score and the IVs (age, gender, nationality, department, years performing job, and education level). In addition, a t-test was used to help further evaluate differences between the two groups (maritime vs. shoreside) based on the IS users aggregated levels of Cyber SA and Cyber Curiosity (Mertler & Vannatta, 2010).

Resources

In order to complete this research study, the following resources were used:

- Access to a pool of maritime IS users: An adequate sample of IS maritime responsible for ship operations was recruited from a passenger vessel. This sample was accessible and approved through experiment site and IRB approval.
- Expert panel: This research required an expert panel of industry and academic professionals in the IS cybersecurity field. Feedback from the expert panel was used to validate the experiment used to measure the constructs of Cyber SA and Cyber Curiosity.
- Statistical analysis tool: A statistical analysis tool (SPSS) was used to analyze the data gathered and compile the results.
- Google Forms®: A cloud-based tool was used to develop the expert panel qualitative survey, consent forms, and pre-experiment survey instrument.
- Amazon AWS: An infrastructure-as-a-service (IaaS) platform was used to host the Web-based interactive experiment. The technology components consisted of an Apache web server, a MySQL database, a gateway API for the client-side script to submit experiment responses, a AWS S3 data storage to store the results of the Google Forms® and the experiment data (AWS DynamoDB).

- Technology: A mixture of tools such as hardware, software, networking, and library resources was used to facilitate the communication with advisor and committee, researching the literature, and writing the dissertation report.

Summary

In closing the methodology section, Chapter Three detailed the research design, experiment development, a review of the population and sample, data analysis and aggregation. Concluding with a summary of the research questions posed and resources used to carry out research. This research study consisted of three phases culminating in the analysis and responding of the four research questions (RQ4, RQ5a, RQ5b, & RQ5c) with a conclusion and recommendations for future research. The main goal of this research was to design, develop, and to empirically validate an IS Cyber SA in the context of Cyber Curiosity that measures the susceptibility of mitigating a cyber-attack using social engineering techniques on maritime IS users.

Chapter 4

Results

Overview

This chapter contains the results and data analysis conducted in this research study. In Phase One of this research, SMEs reviewed the proposed measure components and scores of Cyber SA and Cyber Curiosity. Phase One concluded with addressing research questions RQ1a, RQ1b, RQ2a, and RQ2b. Phase Two involved the SMEs, who validated the proposed interactive social engineering attack experimental procedures to measure Cyber SA and Cyber Curiosity using the Delphi technique. Phase Two concluded with addressing RQ3. Phase Three began with a pilot test of the experiment to assess the measures of Cyber SA and Cyber Curiosity. Needed adjustments were made to the experiment based on the feedback from the pilot experiment. After refinements were made to the experiment, Phase Three completed the analysis of Cyber SA and Cyber Curiosity data from 120 maritime IS and 54 shoreside IS users. The data that was gathered and analyzed addressed RQ4, RQ5a, RQ5b, and RQ5c.

Qualitative Research and Expert Panel (Phase One)

The beginning of Phase One consisted of a Delphi Method data collection method using a well-structured questionnaire based on literature review of Cyber SA and Cyber

Curiosity filled out by cybersecurity SMEs to validate the proposed measure components and scores for Cyber SA and Cyber Curiosity. It is an acceptable and common modification of the Delphi review to use a structured questionnaire versus open ended questionnaire (Kerlinger, 1973; Hsu & Sanford, 2007). For Phase One, the SMEs were solicited from LinkedIn professional contacts working in the maritime and cybersecurity industry. The SMEs data collection was started in early August 2019 and was completed by the end of August 2019.

Phase One – Data Collection

The goal for this phase of the study was to complete an expert panel solicitation to review and validate the proposed Cyber Risk taxonomy using a consensus-building process implementing the Delphi technique. Upon data collection, the SMEs reviewed and validated the following:

1. Components for the measures of Cyber SA and experimental procedures
2. Components for the measures of Cyber Curiosity levels and experimental procedures
3. The scores of the identified components of the measures of Cyber SA and Cyber Curiosity

A group of nine SMEs participated in the review and validation using an online questionnaire to gather the data. The SMEs background were mixture of cybersecurity and cyber maritime experts with at least ten years of professional experience. The questionnaire consisted of two parts. Part 1 consisted of three sections (A, B, & C). Section A gathered the SMEs validation of the components for the measures of Cyber SA. Section B gathered the validation for scores for the identified components of Cyber

SA. The last section C of Part 1 gathered the time scores for identified components of the measures of Cyber SA. The second part of the questionnaire consisted of only two sections (A & B). Part 2 Section gathered the SMEs validation of the components for the measures of Cyber Curiosity. Part 2 Section B gathered the validation for scores for the identified components of Cyber Curiosity.

Phase One – Pre-Analysis Data Screening

Prior to beginning data analysis, pre-analysis data screening was conducted on the data collected from the SMEs. Pre-analysis data screening needed to be conducted to prevent data collection issues (Levy & Ellis, 2006), ensure accurate data is collected and there are no missing or outlier data values (Mertler & Vannatta, 2012). SMEs responses were collected using Google Forms®. To ensure data integrity, editing of data was prevented after submission from the participants. To ensure data completely, each question in the SMEs review was required to be filled in prior to submission. Pre-analysis data screening was done by saving the collected data to Google's spreadsheet. In Google's spreadsheet, the collected data has the submitted timestamp and responses entries for secure storage and retrieval. On performing pre-analysis data screening, only one outlier response out of the nine was identified and removed since the data submitted in free form had a response that was not able to be understood (Part 1 – Section C, P1-C4 feedback).

Phase One – Expert Panel Characteristics

Upon completing pre-analysis data screening, demographic analysis was performed on the collected SMEs Questionnaire (See Appendix D). Demographic information collected from the SMEs included gender, age, level of education, number of professional certifications, and years of professional experience. To qualify the expertise level of the SMEs, number of professional certifications, level of education, and years of professional experience were gathered to potentially remove SMEs responses who did not meet minimum requirements. For the SMEs that participated in Phase One, all of them had at least a Bachelor's or Technical Degree, majority held one or more professional certifications, and more than 12 years of professional experience.

Table 11

Descriptive Statistics of the SMEs (n=9)

Demographic Item	**Frequency**	**Percent**
Gender		
Female	1	11.1%
Male	8	88.9%
Age Category		
35-44	4	44.4%
45-54	5	55.6%
Education		
Bachelor's Degree or Technical Degree	6	66.7%
Master's Degree	3	33.3%
Certifications		
0	1	11.1%
1	5	55.6%
2	3	33.3%
Years of Professional Experience		
12-15	5	55.6%
>=16	4	44.4%

Phase One – Data Analysis

The purpose of the SMEs two-part questionnaire was to validate the proposed components for the measures and scores of Cyber Situational Awareness (CSA) and

Cyber Curiosity levels to help develop and empirically validate an IS Cyber Risk taxonomy in the context of cyber risk that can be used as a benchmark to measure the susceptibility of mitigating a cyber-attack using social engineering techniques among IS users. Section A of Part One of the questionnaire asked the SMEs to provide feedback on the performance measures to assess Cyber SA measuring relevant aspects of the IS participant performance during the Web-based experiment (i.e. identification of phishing attack indicators). The SMEs were asked to review and validate the proposed Cyber SA components for the measures for each type of social engineering attack user action. Their options were to 1-Keep, 2-Adjust, or 3-Remove. For Section A, eight of the nine SMEs had a consensus to "Keep" the components for the measures of Cyber SA (See Table 12). Upon reviewing the feedback from the SMEs response to "Adjust", the SME was making a clarification on the term 'social engineering attack' that did not impact the recommended components since the difference between 'simple' and 'advanced' were on the level of effort to craft an attack (sophistication) and the level of Cyber SA required for an IS user to identify an attack.

Table 12

SMEs Validation and Review of Cyber SA Components User Action

	SMEs Responses (N=9)		
Experiment User Action Categories	**Keep**	**Adjust**	**Remove**
Simple social engineering attack identified	8	1	-
Advanced social engineering attack identified	8	1	-
Unable to identify social engineering attack or no response	8	1	-
Incorrect social engineering attack identified	8	1	-

Section B of Part One of the questionnaire asked the SMEs to review and validate the measurement scores to assess Cyber SA measuring relevant aspects of the IS participant performance during the Web-based experiment. The SMEs were asked to review and validate the proposed Cyber SA scores for each type of social engineering attack user action. Their options were to 1-Keep, 2- Adjust, or 3-Remove. For Section B, there was 100% consensus from the SMEs to "Keep" the recommended scores for Cyber SA. Table 13 shows the Cyber SA User Action Score SMEs responses.

Table 13
SMEs Validation and Review of Cyber SA User Action Scores

		SMEs Responses (N=9)		
Experiment User Action Categories	**Points**	**Keep**	**Adjust**	**Remove**
Simple social engineering attack identified	1	9	-	-
Advanced social engineering attack identified	2	9	-	-
Unable to identify social engineering attack or no response	0	9	-	-
Incorrect social engineering attack identified	-1	9	-	-

Section C of Part One of the questionnaire asked the SMEs to review and validate the time measurement scores to assess Cyber SA measuring relevant aspects of the IS participant performance during the Web-based experiment. The SMEs were asked to review and validate the proposed Cyber SA time scores for each type of social engineering attack user action. Their options were to 1-Keep, 2-Adjust, or 3-Remove. For Section C, there was 90% consensus from the SMEs to "Keep" the recommended scores for Cyber SA. According to Green (1982) and Ulschak (1983), consensus on a topic can be achieved by having at least 70% of the Delphi SMEs agree. One of the originally proposed timing scoring options removed which was “Unable to detect simple nor advanced social engineering attack” since that was replaced with the same scoring as “attack identified longer than 20 secs.” Table 14 shows the Cyber SA Time Measurement Score SMEs responses.

Table 14

SMEs Validation and Review of Cyber SA Time Measurement Scores

			SMEs Responses (N=9)		
Level	**Experiment User Action Timing Categories**	**Points**	**Keep**	**Adjust**	**Remove**
Advanced	Advanced social engineering attack identified under 10 seconds	4	9	-	-
	Advanced social engineering attack identified between 10 seconds and 20 seconds	2	9	-	-
	Advanced social engineering attack identified longer than 20 seconds	0	8	1	-
Simple	Simple social engineering attack identified under 10 seconds	2	9	-	-
	Simple social engineering attack identified between 10 seconds and 20 seconds	1	9	-	-
	Simple social engineering attack identified longer than 20 seconds	0	9	-	-

Part Two of the questionnaire asked the SMEs to review and validate the proposed components for the measures and scores of Cyber Curiosity relevant aspects of the IS participant performance during the Web-based experiment. The SMEs were asked to review and validate the proposed cyber curiosity measurements for each type of scenario. Their options were to 1-Keep, 2-Adjust, or 3-Remove. For Section C, there was 100% consensus from the SMEs to “Keep” the recommended scores for Cyber SA. Table 15 shows the Cyber Curiosity SMEs responses. Phase One of the research study was completed successfully addressing research RQ1a, RQ1b, RQ2a, and RQ2b.

Table 15

Cyber Curiosity Measurement Points

Experiment User Action Selection	**Points**	**Curiosity Type**		**SMEs Responses (N=9)**		
		I-Type	**D-Type**	**Keep**	**Adjust**	**Remove**
Simple explanation (User will be presented with link to expand on explaining the section of the experiment such as "Learn more about Phishing Email Situational Awareness"	-1		x	9	-	-
In-depth explanation (User will be presented with a link in the simple explanation section to seek further information such as "To learn further information about Phishing Email Situational Awareness"	-2		x	9	-	-
Enticing Web link (User will be presented with a link to a non-SA awareness page with an entertaining story or topic.)	1	x		9	-	-
Enticing Pop-up Web link (User will be presented with a pop-up to a non-SA awareness page with an entertaining story or topic.)	2	x		9	-	-

Qualitative and Quantitative Research and Expert Panel (Phase Two)

The development and SMEs validation of the proposed measure components and scores for Cyber SA and Cyber Curiosity from Phase One was used to operationalize the Web-based application and determine the Risk Taxonomy matrix scoring ranges (min and max) for Cyber SA and Cyber Curiosity. For Phase Two, the SMEs were solicited from LinkedIn professional contacts working in the maritime and cybersecurity industry. The SMEs data collection was started in early September 2019 and was completed by the end of September 2019.

Phase Two – Data Collection

The beginning of Phase Two data collection consisted of using a questionnaire filled out by cybersecurity SMEs to validate the proposed Cyber Risk Taxonomy. The goal for this phase of the study was to complete an expert panel solicitation to review and validate the proposed Cyber Risk Taxonomy using a consensus-building process implementing the Delphi technique. Upon data collection, the SMEs reviewed and validated the proposed classification for the Cyber Risk Taxonomy.

A group of five SMEs participated in the review and validation using Google Forms® questionnaire to gather the data. The SMEs background were mixture of cybersecurity and cyber maritime experts with at least ten years of professional experience. The questionnaire consisted two sections. The first section gathered the SMEs' demographics. The second section gathered the validation responses for the Risk Taxonomy components.

Phase Two – Data Pre-Analysis and Screening

Prior to beginning data analysis, pre-analysis data screening was conducted on the data collected from the SMEs. SMEs responses were collected using Google Forms®. To ensure data integrity, editing of data was prevented after submission from the participants. To ensure data completeness, each question in the SME review was required to be filled in prior to submission. Pre-analysis data screening was done by saving the collected data to Google's spreadsheet. In Google's spreadsheet, the collected data has the submitted timestamp and responses entries for secure storage and retrieval. On performing pre-analysis data screening no responses were excluded, thus obtaining the full set of responses from the Delphi Review.

Phase Two – Expert Panel Characteristics

Upon completing pre-analysis data screening, demographic analysis was performed on the collected SMEs Questionnaire (See Appendix F). Demographic information collected from the SMEs included gender, age, level of education, number of professional certifications, and years of professional experience. To qualify the expertise level of the SMEs, number of professional certifications, level of education, and years of professional experience were gathered to potentially remove SMEs responses who did not meet minimum requirements. For the SMEs that participated in Phase Two, all the them had at least a Bachelor's or Technical Degree, majority held one or more professional certifications, and more than 12 years of professional experience (See Table 16).

Table 16

Descriptive Statistics of the Phase Two SMEs Round (n=5)

Demographic Item	**Frequency**	**Percent**
Gender		
Female	1	20%
Male	4	80%
Age Category		
35-44	2	40%
45-54	3	60%

Table 16

Descriptive Statistics of the Phase Two SMEs Round (n=5) (Cont.)

Demographic Item		Frequency	Percent
Education			
	Bachelor’s Degree or Technical Degree	3	60%
	Master’s Degree	2	40%
Certifications			
	1	1	20%
	2	1	20%
	3	2	40%
	4	1	20%
Years of Professional Experience			
	12-15	2	55.6%
	>=16	3	44.4%

Phase Two – Data Analysis

The purpose of the SMEs two-part questionnaire was to validate the proposed Cyber Risk Taxonomy to help develop and empirically validate the taxonomy in the context of cyber risk that can be used as a benchmark to measure the susceptibility of mitigating a cyber-attack using social engineering techniques among IS users. The SMEs were asked to review and validate the proposed Cyber Risk Taxonomy quadrants. Their options were to 1-Keep, 2-Adjust, or 3-Remove. All five SMEs had a consensus to “Keep” the quadrant labels and placement in the Cyber Risk Taxonomy for Low, Medium, High, and Very High quadrants (See Table 17). Phase Two of the research study was completed successfully addressing research RQ3.

Table 17

SMEs validation of Proposed Cyber Risk Taxonomy (n=5)

Item	Review and Validation Item	Keep	Adjust	Remove
Low Risk Quadrant Components	Quadrant label	5	-	-
	Quadrant placement on Risk Taxonomy	5	-	-

Table 17

SMEs validation of Proposed Cyber Risk Taxonomy (n=5) (Cont.)

Item	Review and Validation Item	Keep	Adjust	Remove
Medium Risk	Quadrant label	5	-	-
Quadrant Components	Quadrant placement on Risk Taxonomy	5	-	
High Risk	Quadrant label	5	-	-
Quadrant Components	Quadrant placement on Risk Taxonomy	5	-	-
Very High Risk	Quadrant label	5	-	-
Quadrant Components	Quadrant placement on Risk Taxonomy	5	-	-

Quantitative Research (Phase Three)

The beginning of Phase Three consisted of pilot testing of 10 maritime IS users onboard a ship. Pilot testing was conducted to ensure that the Web-based experiment had adequate response times in loading the various Webpages, and that the experiment scores for Cyber SA and Cyber Curiosity were being recorded and submitted accurately to Amazon’s data storage location. Due to the limited ship satellite Internet bandwidth, adjustments needed to be made to the Web-based experiment application to improve the response and loading times of various Webpages. Minor adjustments such as limiting audio prompts and instructions to text, significantly improved the loading times so that the experiment can be completed within the expected time frame. After completing the pilot testing and making necessary but minor adjustments to the experiment, main data collection started with the maritime participants. Pilot and main data collection was started on October 20, 2019 and was completed on October 26, 2019.

Phase Three – Data Collection

In Phase Three, participants onboard the ship, the experiment site, were recruited by email and through verbal communication in crew areas to voluntary attend the cybersecurity awareness campaign where they would participant in the maritime research study experiment. The ship has 1,180 crew member capacity. Out of the potential 1,180 crew members, about 261 (22.1%) are IS users. Out of the 261 potential shipboard IS users, 120 participants where collected, generating a 45.9% participation rate. To compare Cyber Curiosity and Cyber SA measures of shipboard with shoreside IS users, a small group of 54 participants were recruited through verbal and instant message communication. The shoreside participants were a convenience selected sample. In summary the total sample size for data analysis was 174 records.

Prior to starting the Cyber SA and Cyber Curiosity Web-based experiment, participants were asked demographic and "state-of-mind" questions. These survey responses were saved at Google Forms® Web-based tool prior to starting the Web-based experiment. To ensure survey data completeness, all of the demographics section survey questions had enabled restrictions to require each question to be filled out prior to form submission. Accuracy of the experiment data captured was ensured by performing repeated testing of the Cyber SA and Cyber Curiosity Web-based experiment prior to conducing the experiment to evaluate the measured scores for both constructs Cyber SA and Cyber Curiosity. Lastly, collected survey forms and experiment results were downloaded from Google Forms® and Amazon's DynamoDB® into a MySQL database for pre-processing to prepare the data. Below were the steps taken to merge the survey form data and the experiment data.

- Step 1 – Merge survey form data with experiment data using unique identified of ParticipantID
- Step 2 – Merged data that had orphaned records meaning non-matching ParticipantID’s were discarded

Pre-analysis experiment data screening identified 23 out of the total 197 participants that started the experiment did not complete successfully the two parts of the experiment. These were identified by filtering where the pre-experiment survey and the captured experiment data has missing participant ID’s which was the method of matching the two data sets. The reason for the two data sets not having matching participant ID’s was either the survey was started and submitted but the experiment was not completed, or the pre-experiment survey data was not successfully submitted to Google Forms during the start of the experiment.

Once data pre-analysis was completed and a working data set was obtained, data coding of the pre-experiment questionnaire responses was performed. A data coding legend was created for demographic information such as age, gender, nationality, department, years performing job function, and education level to help with data analysis. After this initial pre-processing, the data was then exported from MySQL in comma separated format (CSV) and imported into IBM’s Statistical Package for the Social Sciences (SPSS) for further pre-analysis data screening.

Phase Three – Data Pre-Analysis and Screening

To ensure the accuracy and integrity of the data collected for this research study, frequency distribution and descriptive statistics were used using IBM’s SPSS tool.

Frequency distribution analysis was performed on the measures collected during the experiment to assess if the range of values for Cyber Curiosity and Cyber SA were within anticipated ranges. See Figure 10 and 11 for the frequency distribution of Cyber SA and Cyber Curiosity. The Cyber SA mean score was 1.01 (N=174, St.Dev = 1.958) with a range from -2 to 9. The Cyber Curiosity mean score was 0.2 (N=174, St.Dev = 1.226) with a range from -3 to 3. While one case was detected as potential multivariate outlier, upon closer investigation, it was decided to keep the record in and assess with and without it to verify. Initial assessments did not result in any differences, thus the case was retained for all further analyses. After the pre-analysis phase, a total of 174 or 88.3% of the survey and experiment results used for phase three data analysis.

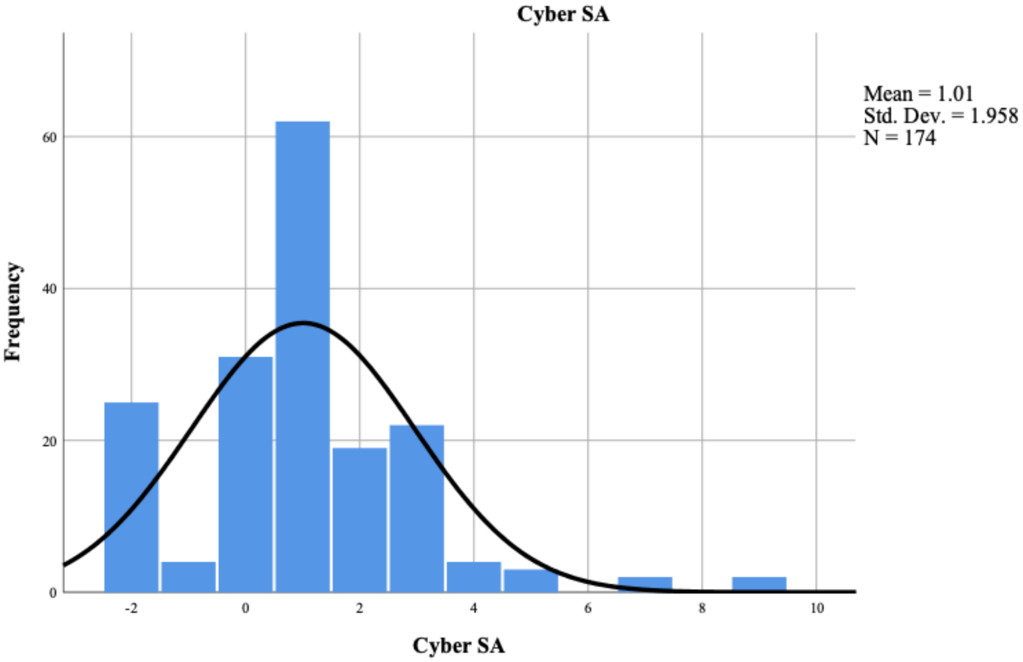


Figure 10. Frequency Distribution of Cyber SA scores (total) for both maritime IS and shoreside users (N=174).

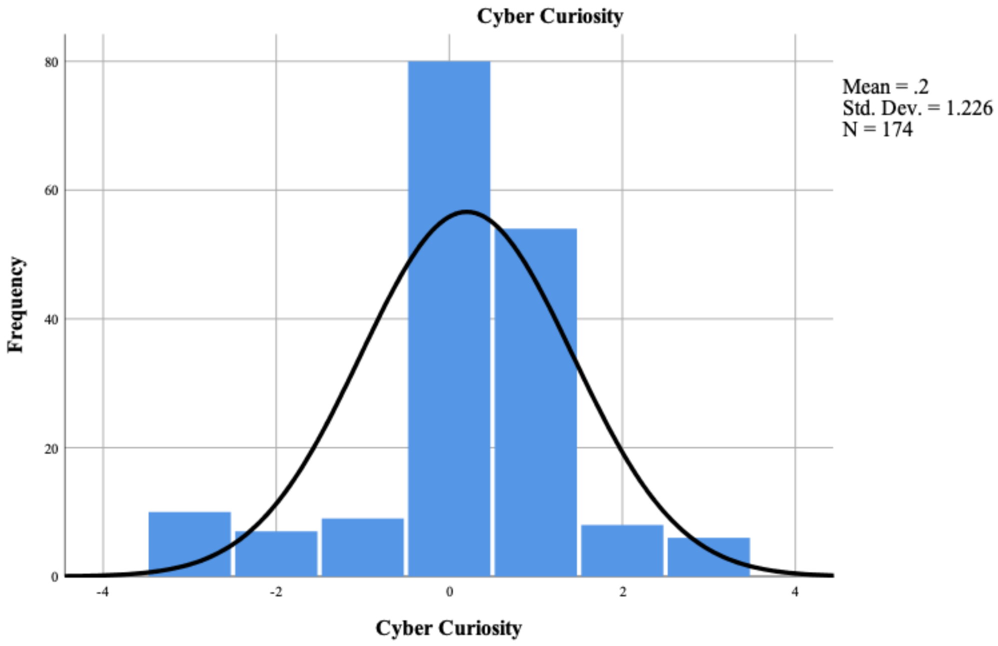


Figure 11. Frequency Distribution of Cyber Curiosity scores for both maritime IS and shoreside users (N=174).

Phase Three - Data Analysis

Phase Three consisted of a quantitative data analysis of the collected Cyber SA and Cyber Curiosity data from 120 maritime IS and 54 shoreside IS users. The collected data was analyzed to address RQ4, RQ5a, RQ5b, and RQ5c.

Demographic Analysis

After finishing the pre-analysis and data screening phase, 174 or 88.3% results remained for analysis. The data collected represents a likeness to that of the general sample targeted which was maritime IS and shoreside IS users working for a passenger vessel company. An analysis of the participants gender identity revealed the majority were male (113 or 64.9%) and then followed by female (58 or 33.3%). A very minor group were identified as transgender female, transgender male or did not prefer to answer and were grouped as “Other.” Analysis of the participants’ age ranges revealed that the majority were within three age groups, 25-34 or 28.7%, 35-44 or 33.9%, and 45.54 or 28.7%. An analysis of participants' nationality or geographic region of identification had a wide range of representation with the majority identified as from Europe (47 or 27%), Asia (46 or 26.4%), South-Central America (25 or 14.4%), North America (23 or 13.2%) and Caribbean (22 or 12.6%). The participants' working area revealed a wide range of representation of over 15 departments with the top two of the users from Hotel (33 or 19%) as well as Food and Beverage (26 or 14.9%). Details of the demographics of the total population are presented in Table 18.

Table 18

Descriptive Statistics of the Participants (N=174)

Demographic Item		**Frequency**	**Percent**
Gender			
	Female	58	33.3%
	Male	113	64.9%
	Other	3	1.8%
Age Category			
	18-24	5	2.9%
	25-34	50	28.7%
	35-44	59	33.9%
	45-54	50	28.7%
	55-64	10	5.7%
Nationality			
	Africa	6	3.4%
	Asia	46	26.4%
	Caribbean	22	12.6%
	Europe	47	27.0%
	Middle East	3	1.7%
	North America	23	13.2%
	Oceania	2	1.1%
	South-Central America	25	14.4%
Department			
	Cruise Division	6	3.4%
	Deck	10	5.7%

Table 18
Descriptive Statistics of the Participants (N=174) (Cont.)

Demographic Item		Frequency	Percent
Department			
	Engine	13	7.5%
	Financial	7	4.0%
	Food & Beverage	26	14.9%
	Guest Services	14	8.0%
	Hotel Department	33	19.0%
	Housekeeping	14	8.0%
	Human Resources	4	2.3%
	Inventory	7	4.0%
	IT	20	11.5%
	Marketing & Revenue	11	6.3%
	Medical	6	3.4%
	Other	2	1.1%
	Security	1	0.6%
Years Performing Job			
	<=2	5	2.9%
	3-5	40	23.0%
	6-8	31	17.8%
	9-11	24	13.8%
	12-15	36	20.7%
	>=16	38	21.8%
Education			
	Primary or some High School	3	1.7%
	Secondary or High School	14	8.0%
	Some College or Technical School	44	25.3%
	Bachelor’s Degree or Technical Degree	81	46.6%
	Master’s Degree	32	18.4%

A data analysis of frequencies, percentages, and one-way analysis of variance (ANOVA) was conducted to assess for any differences between the two experimental groups, maritime and shoreside. The two-group identification were labeled as Group A for the maritime IS users (n_1=120), and Group B for the shoreside IS users (n_2=54). Group A, the maritime IS users, consisted of 120 or 69% of the total sample. Group B, the shoreside IS users, consisted of 54 or 31% of the total sample. In comparing the two groups, Group A and Group B, there were no significant differences in gender percentages between the groups. Details of the demographics of the total population for the two groups are presented in Table 19.

Table 19

Descriptive Statistics of Participants by Group (N=174)

Demographic Item	**Group A (n_1=120) Maritime**		**Group B (n_2=54) Shoreside**	
	Frequency	**Percent**	**Frequency**	**Percent**
Gender				
Female	37	30.8%	21	38.9%
Male	80	66.7%	33	61.1%
Other	3	2.5%	0	0%
Age Category				
18-24	5	4.2%	0	0%
25-34	41	34.2%	9	16.7%
35-44	43	35.8%	16	29.6%
45-54	28	23.3%	22	40.7%
55-64	3	2.5%	7	13.0%
Nationality				
Africa	6	5.0%	0	
Asia	40	33.3%	6	11.1%
Caribbean	9	7.5%	13	24.1%
Europe	36	30.0%	11	20.4%
Middle East	2	1.7%	1	1.9%
North America	8	6.7%	15	27.8%
Oceania	2	1.7%	0	
South-Central America	17	14.2%	8	14.8%
Department				
Cruise Division	6	5.0%	0	0%
Deck	9	7.5%	1	1.9%
Engine	10	8.3%	3	5.6%
Financial	3	2.5%	4	7.4%
Food & Beverage	24	20.0%	2	3.7%
Guest Services	7	5.8%	7	13.0%
Hotel Department	33	27.5%	0	0%

Table 19

Descriptive Statistics of Participants by Group (N=174) (Cont.)

Demographic Item	Group A (n_1=120) Maritime		Group B (n_2=54) Shoreside	
	Frequency	**Percent**	**Frequency**	**Percent**
Housekeeping	14	11.7%	0	0%
Human Resources	1	0.8%	3	5.6%
Inventory	2	1.7%	5	9.3%
IT	0	0%	20	37.0%
Marketing & Revenue	9	7.5%	2	3.7%
Medical	1	0.8%	5	9.3%
Other	1	0.8%	1	1.9%
Security	0	0%	1	1.9%
Years Performing Job				
<=2	5	4.2%	0	0%
3-5	30	25.0%	10	18.5%
6-8	18	15.0%	13	24.1%
9-11	14	11.7%	10	18.5%
12-15	22	18.3%	14	25.9%
>=16	31	25.8%	7	13.0%
Education				
Primary or some High School	3	2.5%	0	0%
Secondary or High School	14	11.7%	0	0%
Some College or Technical School	40	33.3%	4	7.4%
Bachelor’s Degree or Technical Degree	46	38.3%	35	64.8%
Master’s Degree	17	14.2%	15	27.8%

To analyze if there exist mean group differences between maritime and shoreside groups an independent t-test was employed. The results from the procedures are presented in Table 20 through Table 21. The results indicate that there was a significant difference in Years Performing Job, Education, and Psychological State of Mind (P1 and P2) between the two groups. In reviewing the Years Performing Job for maritime (M = 3.93; St.Dev = 1.661) and shoreside (M = 3.91; St.Dev = 1.336) their categorical mean averages differences were negligible. When analyzing the frequency statistics between maritime and shoreside, the maritime participants had double percentage difference in equal or greater than 16 years of job experience; 13% for shoreside participants while maritime had 26%. Analysis of level of Education level revealed that 47% of the maritime participants had less than a Bachelor's degree while the majority of shoreside participants had a Bachelors or higher degree (See Table 19). In analyzing P1-Uplift and P2-Interest Phycological State of Mind responses, maritime participants were more open to sharing this information (13% Preferred not to answer) while the shoreside participants were less willing (64.8% Preferred not to answer).

Table 20

Group Statistics for Demographics

Item	**Group**	**N**	**Mean**	**St.Dev**
Age	Maritime	120	-	-
	Shoreside	54	-	-
Gender	Maritime	120	-	-
	Shoreside	54	-	-
Nationality	Maritime	120	-	-
	Shoreside	54	-	-
Department	Maritime	120	-	-
	Shoreside	54	-	-
Years Performing Job	Maritime	120	3.93	1.661
	Shoreside	54	3.91	1.336
Education	Maritime	120	3.50	.961
	Shoreside	54	4.20	.562
P1 - Uplift	Maritime	120	3.60	.991
	Shoreside	54	4.57	.633
P2 - Interest	Maritime	120	3.62	1.022
	Shoreside	54	4.61	.564

Table 21
Independent Samples Test of Demographics

	Levene's Test for Equality of Variances		t-test for Equality of Means					
							95% Confidence Interval of the Difference	
Item	F	Sig.	t	df	Sig. (2-talied)	Mean Difference	Lower	Upper
Age	0.440	0.508	-4.278	172	***0.000****	-0.642	-0.938	-0.346
Gender	0.041	0.839	1.397	172	0.164	0.139	-0.057	0.335
Nationality	0.117	0.732	0.225	172	0.822	0.073	-0.569	0.715
Department	0.024	0.876	-3.342	172	***0.001****	-1.835	-2.919	-0.751
Years Performing Job	8.426	***0.004***	0.068	172	0.945	0.018	-0.490	0.525
Education	22.704	***0.000****	-6.043	160.475	***0.000****	-0.704	-0.934	-0.474
P1 - Uplift	8.796	***0.003***	-7.802	152.072	***0.000****	-0.974	-1.221	-0.727
P2 - Interest	12.960	***0.000****	-8.233	165.019	***0.000****	-0.994	-1.233	-0.756

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

Cyber SA and Cyber Curiosity Positioning on Cyber Risk Taxonomy

To answer research Q4, "How are the aggregated scores for Cyber SA and Cyber Curiosity positioned on the Cyber Risk taxonomy for maritime IS users", the taxonomy chart is shown on Figure 13. Within the IS User Cyber SA (CSA) and Cyber Curiosity (CC) Risk Taxonomy charts, the x-axis represents the level of IS user Cyber Curiosity (I-Type and D-Type) and the y-axis represents the level of IS users Cyber SA. The coordinates (x,y) represents the combined experiment scores for both CC and CSA. The size of the bubble in each chart represents the count of how many participants had the same CSA and CC total score from the web-based experiment.

The developed and SMEs validated taxonomy is comprised of four quadrants Q1, Q2, Q3, and Q4 as depicted in Figure 12. Each quadrant reflects the aggregate level of IS user cyber risk and their susceptibility to a social engineering attack. In the risk matrix, there is direct relationship between the level of I-Type Cyber Curiosity and an inverse relationship with the level of Cyber SA and the resultant cyber risk to an organization. The first quadrant, Q1, is labeled ‘Medium Cyber Risk’ because it consists of IS users with high D-Type Cyber Curiosity, low I-type Cyber Curiosity, and low Cyber SA score. IS users positioned in this quadrant are capable of reducing their likelihood of being susceptible to a successful social engineering attack by increasing their Cyber SA. The second quadrant, Q2, is labeled ‘Very High Cyber Risk’ because it consists of IS users with high I-Type Cyber Curiosity, low D-Type Cyber Curiosity, and low Cyber SA. Cyber risk in this quadrant is very high because IS users are more susceptible to a successful social engineering attack because of their high level of I-Type Cyber Curiosity and low Cyber SA of a possible cyber-attack. The third quadrant, Q3, is labeled ‘High Cyber Risk’ because it consists of IS users with high I-Type Cyber Curiosity, low D-type Cyber Curiosity and high Cyber SA. IS users positioned in this quadrant maybe capable of reducing their likelihood of being susceptible to a successful social engineering attack by decreasing their I-Type Cyber Curiosity and increasing D-Type Cyber Curiosity. According to Litman, Hutkins, and Russon (2005), smaller knowledge gaps will “arouse more curiosity and stimulate more exploratory behavior” (p. 561). The fourth quadrant, Q4, consists IS users with high D-Type Cyber Curiosity and high Cyber SA and is labeled ‘Low Cyber Risk’. IS users in this quadrant are keen of social engineering tools, techniques, and procedures (TTPs) meaning that they will be the least susceptible to a successful future attack.

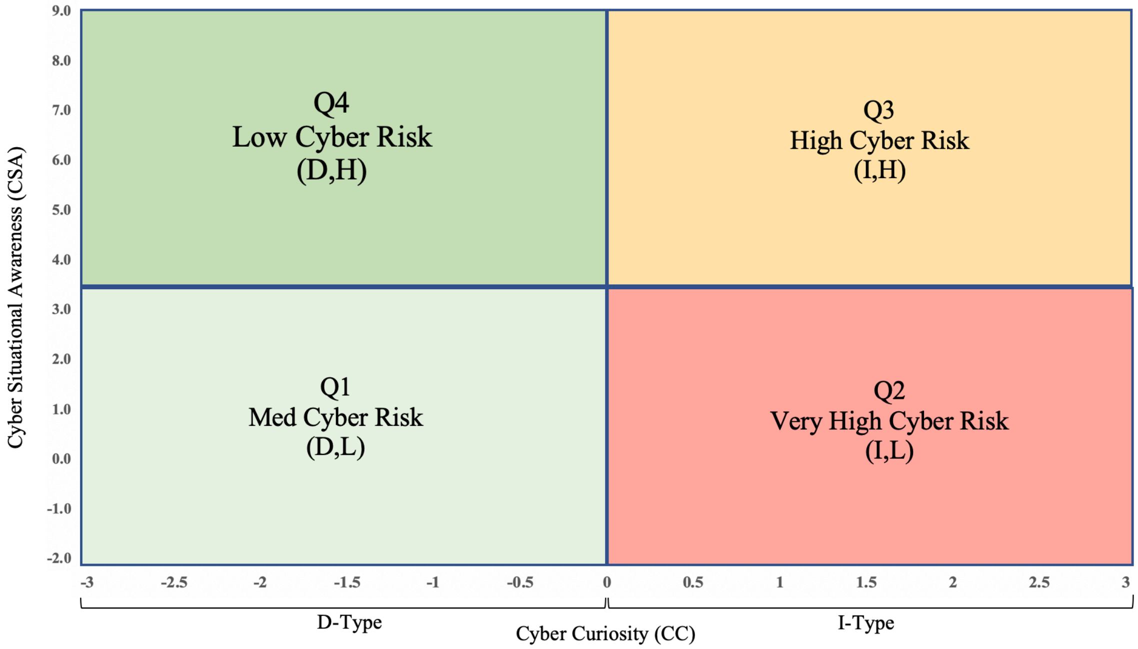


Figure 12. IS User Cyber SA and Cyber Curiosity Risk Taxonomy

The results of how the aggregated scores for CSA and CC are positioned on the Cyber Risk taxonomy for both maritime and shoreside IS users (N=174) are shown in Figure 13. In analyzing the participants aggregated scores obtained for both Cyber SA and Cyber Curiosity measurements, the largest groups are located in the lower right quadrant indicating that the majority of the users have a very high level of cyber risk. In reviewing the participants CC scores, the majority of IS users had an inclination towards I-Type curiosity. I-Type curiosity involves the pleasure of new discoveries versus D-Type that is concerned with reducing uncertainty or unwanted states of ignorance (Litman, 2008). In a Cyber SA context, IS users with higher I-Type curiosity scores also had lower Cyber SA scores thus possibly susceptible to a successful social engineering attack.

In analyzing the maritime participants (n=120) aggregated scores obtained for both Cyber SA and Cyber Curiosity measurements, the largest groups are located in the lower right quadrant indicating that the majority of the users have a very high level of cyber risk (See Figure 14). In reviewing the maritime participants CC scores, the IS users had an inclination towards I-Type curiosity. In analyzing the shoreside participants (n=54) aggregated scores obtained for both Cyber SA and Cyber Curiosity measurements, the largest groups are located in the lower left quadrant indicating that the majority of the users have a medium level of cyber risk (See Figure 15). In reviewing the shoreside participants CC scores, the IS users had an inclination towards D-Type curiosity. D-Type curiosity is concerned with reducing uncertainty or unwanted states of ignorance (Litman, 2008).

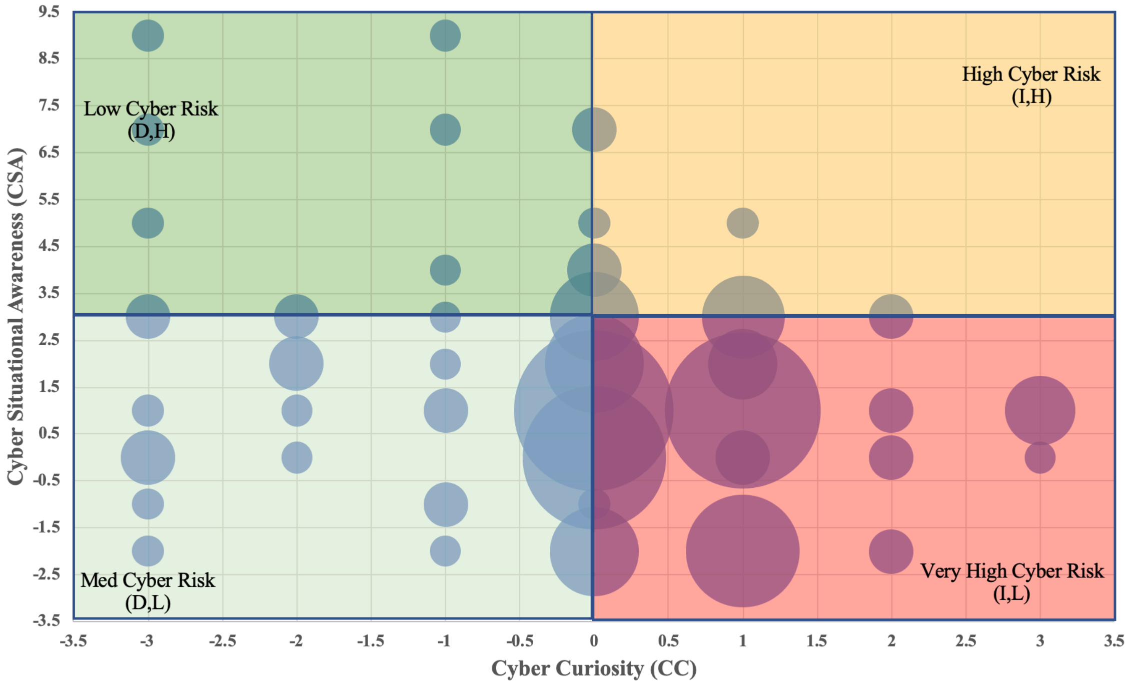


Figure 13. IS User Cyber SA and Cyber Curiosity Risk Taxonomy, Bubble size represents the participant count (N=174)

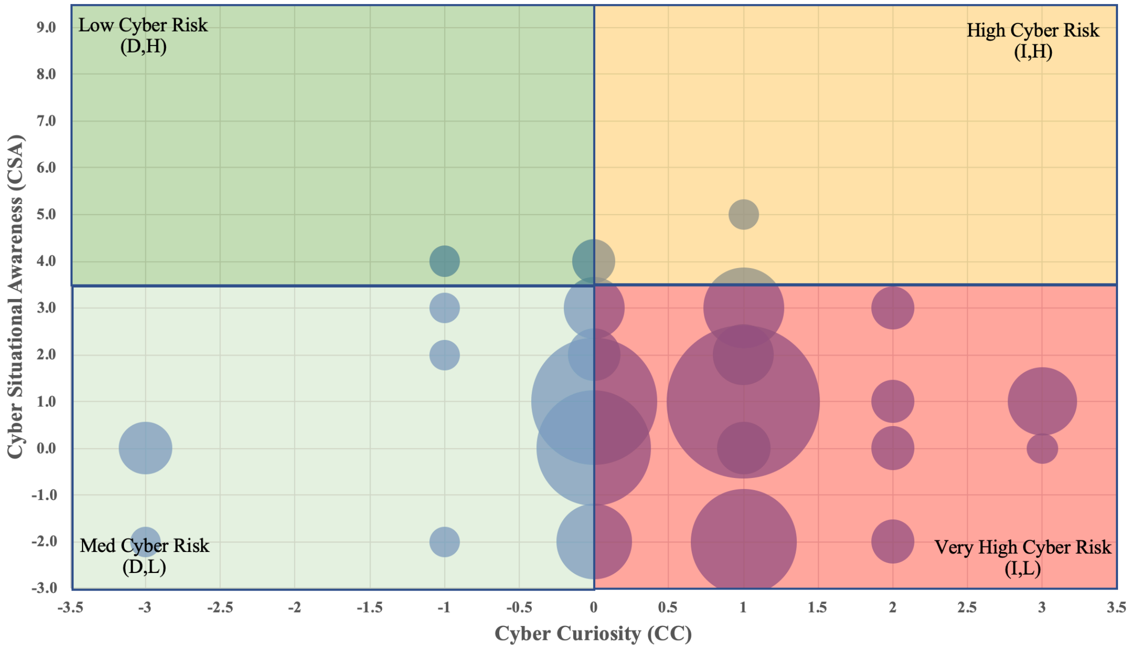


Figure 14. Maritime IS User Cyber SA and Cyber Curiosity Risk Taxonomy, Bubble size represents the participant count (n=120)

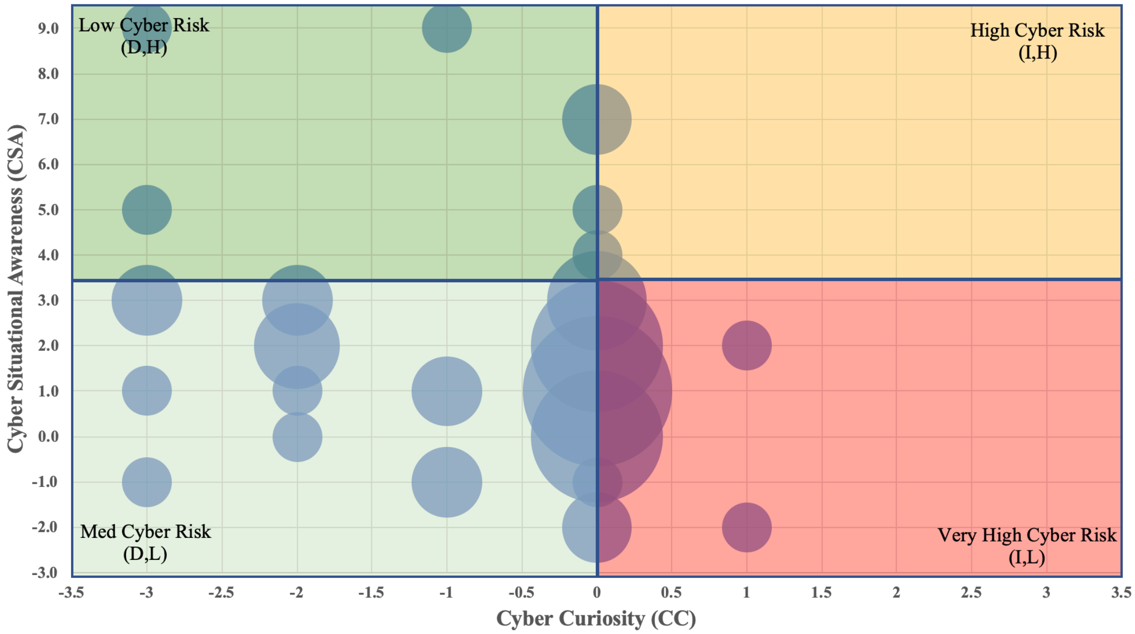


Figure 15. Shoreside IS User Cyber SA and Cyber Curiosity Risk Taxonomy, Bubble size represents the participant count (n=54)

Cyber SA Data Analysis

To answer RQ5a, which is "Are there any significant differences to maritime IS users' aggregated level of Cyber SA based on their age, gender, nationality, job function, years at performing job, education level, or psychological state of mind?", a one-way analysis of variance (ANOVA) was employed. The alpha level was set as α=0.05, as the conventional standard of statistical significance (p ≤ .05). In reviewing the age, gender, nationality, department, years performing job, education level, and psychological state of mind, for the maritime and shoreside IS users (N=174), the statistical tests show that an IS users' Department F(14, 159) = 2.128, p = 0.013 has the most significant difference in Cyber SA scores among the other groups. An ANOVA analysis of the other categories Age F(4, 169) = 0.529 , p = 0.715, Gender F(4, 169) = 1.479, p = 0.211, Nationality F(7, 166) = 0.918, p = 0.494, Years Performing Job F(5, 168) = 0.610, p = 0.693, Education Level F(4, 169) = 0.603, p = 0.661, Psychological state of mind P1-Uplift (F(4, 169) 1.770, p = 0.137) and P2-Interest (F(5, 168) 1.619, p = 0.158) were not significant. Table 22 provides an overview of the mean, standard deviation, and ANOVA results.

Table 22

ANOVA Results for Cyber SA (N=174)

Item	**Min**	**Max**	**Mean**	**St.Dev**	**F**	**Sig.**
Age	1	5	3.06	0.960	0.529	0.715
Gender	-	-	-	-	1.479	0.211
Nationality	-	-	-	-	0.918	0.494
Department	-	-	-	-	2.128	***0.013****
Years Performing Job	1	6	3.92	1.563	.610	0.693
Education Level	1	5	3.72	0.916	.603	0.661
P1 – Uplift	1	5	3.90	1.001	1.770	0.137
P2 – Interest	1	5	3.93	1.014	1.619	0.158

Note. Variables with missing min, max, min or St.Dev are nominal
*-p<.05, **-p<.01, *** -p<.001

Cyber SA Data Analysis by Group

In analyzing the mean score by Department, the Inventory Group A ((n_1=120), M = 3.0) had five-fold difference in the magnitude of Cyber SA mean score than Group B ((n_2=54), M = 0.60) (See Figure 16). Further analysis using a one-way ANOVA did not have any significant differences of Department analyzing the two groups individually, Group A maritime F(12, 107) 1.377, p = 0.188 and Group B shoreside F(11, 42) = 0.796, p = 0.643 (See Table 21). An analysis of age, gender, nationality, department, years performing job, education level, and psychological state of mind (P1 – Uplift & P2 – Interest) for maritime (Group A, n_1=120) and shoreside (Group B, n_2 = 54), did not have statistically significant differences with Cyber SA among the other groups. After the ANOVA analysis, a paired sample t-test was conducted to determine if there was a significant difference in Cyber SA scores between Group A and Group B. There was not a significant difference between the maritime (M = 0.67; St.Dev = 1.626) and shoreside (M = 1.76; St.Dev = 2.394) IS users. RQ5a was successfully addressed through the performed analysis. Table 23 provides an overview of the mean, standard deviation, and ANOVA results by Group for Cyber SA scores.

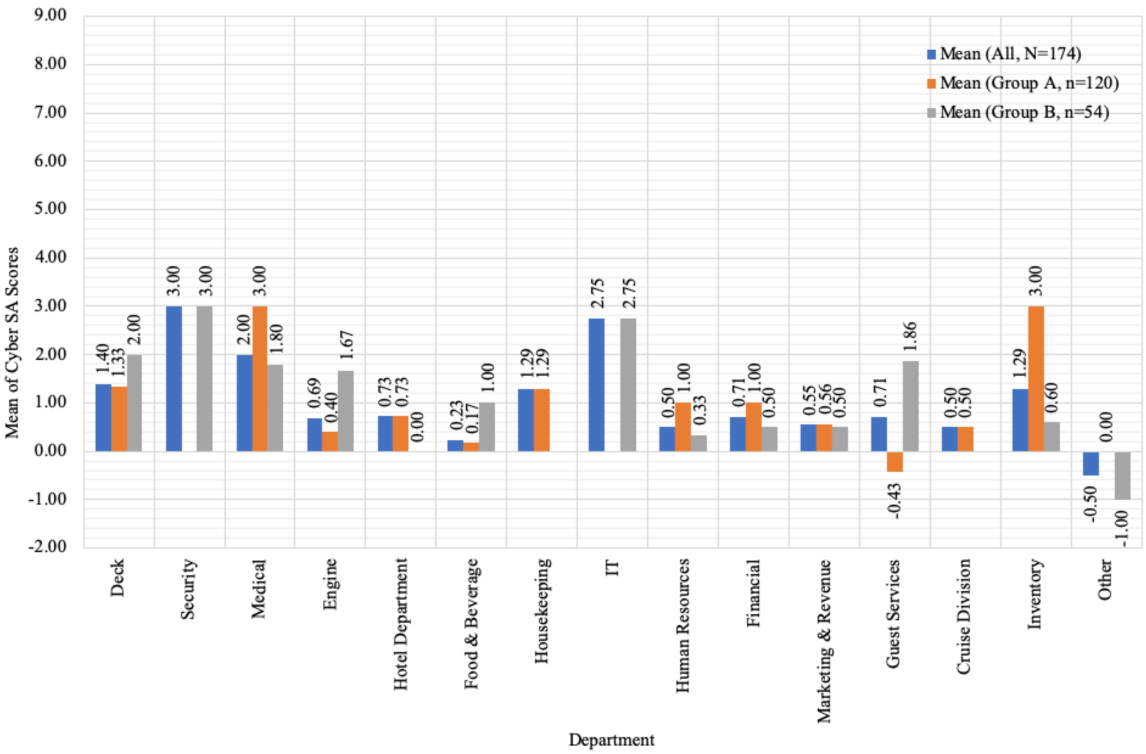


Figure 16. Means of the Cyber SA scores by Department (N=174)

Table 23

ANOVA Results of Participants by Group for Cyber SA

	Group A Maritime (n_1=120)				**Group B Shoreside (n_2=54)**			
Item	**Mean**	**St.Dev**	**F**	**Sig.**	**Mean**	**St.Dev**	**F**	**Sig.**
Age	2.86	0.910	2.028	0.095	3.50	0.927	0.184	0.907
Gender	-	-	2.291	0.064	-	-	1.089	0.301
Nationality	-	-	1.055	0.398	-	-	.520	0.760
Department	-	-	1.377	0.188	-	-	.796	0.643
Years Performing Job	3.93	1.661	0.899	0.484	3.91	1.336	1.332	0.271
Education Level	3.50	0.961	0.442	0.778	4.20	0.562	.287	0.752
P1 - Uplift	3.60	0.991	1.406	0.236	4.57	0.633	.726	0.489
P2 - Interest	3.62	1.022	0.898	0.485	4.61	0.564	2.183	0.123

Note. Variables with missing min, max, min or St.Dev are nominal
*-p<.05, **-p<.01, *** -p<.001

To analyze if there exist mean group differences in Cyber SA scores between maritime and shoreside IS users, an independent t-test was employed. The results from the procedures are presented in Table 24 through Table 25. The results indicate that shoreside IS users have more than double the Cyber SA mean scores than maritime IS users. There is also a significant statistical difference in the mean Cyber SA scores between maritime and shoreside IS users indicating that shoreside IS users had a better ability to identify a social engineering attack.

Table 24

Group Statistics for Cyber SA

Group	**N**	**Mean**	**St.Dev**
Maritime	120	0.67	1.626
Shoreside	54	1.76	2.394

Table 25

Independent Samples Test of Cyber SA

Levene's Test for Equality of Variances		t-test for Equality of Means					
						95% Confidence Interval of the Difference	
F	Sig.	t	df	Sig. (2-talied)	Mean Difference	Lower	Upper
5.318	***0.022****	-3.051	75.828	***0.003*****	-1.093	-1.806	-0.379

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

Cyber Curiosity Data Analysis

To answer RQ5b, which is "Are there any significant differences to maritime IS users' aggregated level of Cyber Curiosity based on their age, gender, nationality, job function, years at performing job, education level, or psychological state of mind?", a one-way analysis of variance (ANOVA) was used. In reviewing the age, gender, nationality, department, years performing job, education level, and psychological state of mind, for the maritime and shoreside IS users (N=174), the statistical tests show that an IS users' Department F(14, 159) = 1.980, p = 0.022 has the most significant difference in Cyber Curiosity scores among the other groups (See Table 24). In analyzing the mean score by Department, Group B had a double the magnitude mean score of D-Type Cyber Curiosity for the Deck (M = -2.0) and Other (M = -3.0) department (See Figure 17). The "Other" department had a high D-type curiosity score, but this only represented one shoreside participant. Further analysis using a one-way ANOVA did not have any significant differences of Department analyzing the two groups individually, Group A maritime F(12, 107) 0.612, p = 0.828 and Group B shoreside F(11, 42) = 1.524 , p = 0.159 (See Table 27). Table 26 provides an overview of the mean, standard deviation, and ANOVA results.

Table 26

ANOVA Results for Cyber Curiosity(N=174)

IV	**Mean**	**St.Dev**	**F**	**Sig.**
Age	3.06	0.960	1.372	0.246
Gender	-	-	2.069	0.087
Nationality	-	-	1.542	0.156
Department	-	-	1.980	***0.022****
Years Performing Job	3.92	1.563	0.225	0.951
Education Level	3.72	0.916	2.096	0.084
P1 – Uplift	3.90	1.001	1.506	0.203
P2 – Interest	3.92	1.014	2.066	0.072

Note. Variables with missing min, max, min or St.Dev are nominal
*-p<.05, **-p<.01, *** -p<.001

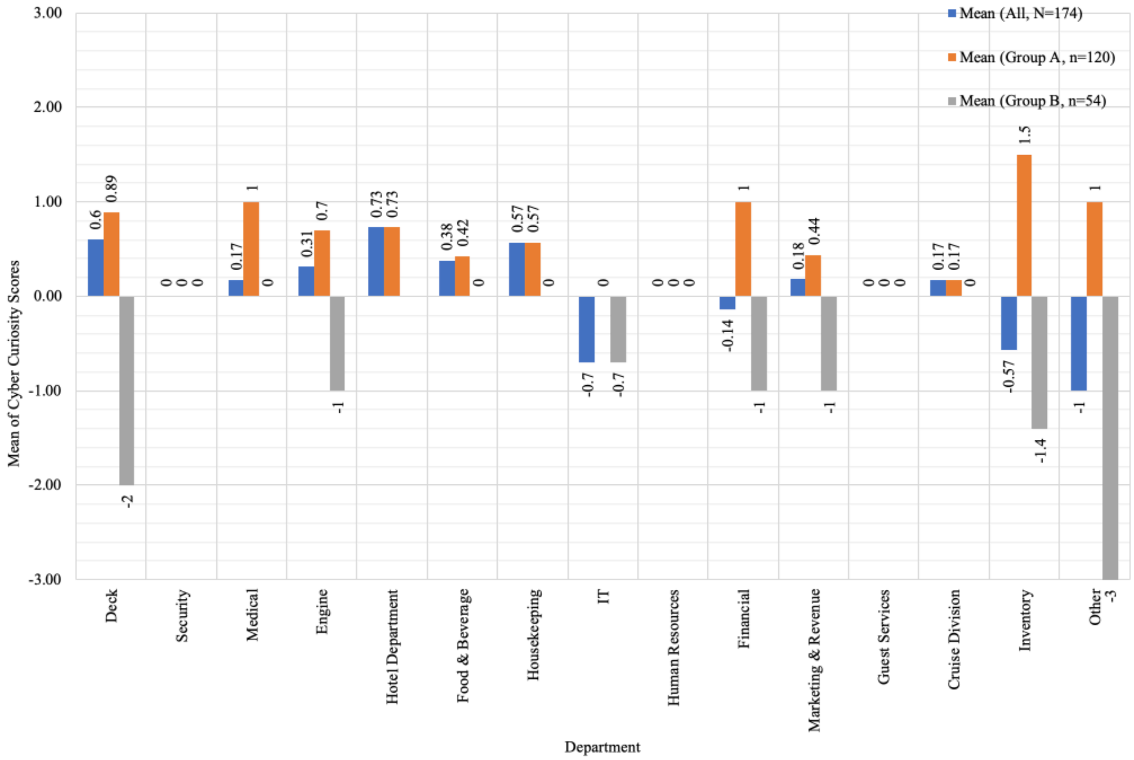


Figure 17. Means of the Cyber Curiosity scores by Department (N=174)

Cyber Curiosity Data Analysis by Group

In reviewing the age, gender, nationality, department, years performing job, education level, and psychological state of mind, for both the maritime (Group A, n_1=120) and shoreside (Group B, n_2=54), the statistical tests show within Group A Gender F(4,159) = 2.128, p = 0.016 has a significant difference in Cyber Curiosity among the other groups. This variance was further analyzed and was caused by an outlier score by a single transgender male with a score CC score of -3. After performing an ANOVA and filtering for Gender within Group A not equal to transgender male, the Gender variance was F(3,115) .249, p = 0.862. After the ANOVA analysis, a paired sample t-test was conducted to determine if there was a significant difference in Cyber SA scores between Group A and Group B. There was not a significant difference between the maritime (M = 0.67; St.Dev = 1.626) and shoreside (M = 1.76; St.Dev = 2.394) IS users. RQ5b was successfully addressed through the performed analysis. Table 27 provides an overview of the mean, standard deviation, and ANOVA results for each group.

Table 27

ANOVA Results of Participants by Group for Cyber Curiosity

	Group A Maritime (n_1=120)				**Group B Shoreside (n_2=54)**			
Item	**Mean**	**St.Dev**	**F**	**Sig.**	**Mean**	**St.Dev**	**F**	**Sig.**
Age	2.86	0.910	1.249	0.294	3.50	0.927	1.411	0.251
Gender	-	-	3.203	***0.016****	-	-	1.332	0.254
Nationality	-	-	0.602	0.753	-	-	4.068	***.004*****
Department	-	-	0.612	0.828	-	-	1.524	0.159
Years Performing Job	3.93	1.661	1.133	0.347	3.91	1.336	1.262	0.298
Education Level	3.50	0.961	.037	0.997	4.20	.562	.962	0.389
P1 - Uplift	3.60	0.991	1.969	0.104	4.57	.633	2.968	0.060
P2 - Interest	3.62	1.022	1.404	0.228	4.61	.564	4.783	***0.012****

Note. Variables with missing min, max, min or St.Dev are nominal
*-p<.05, **-p<.01, *** -p<.001

To analyze if there exist mean group differences in Cyber Curiosity scores between maritime and shoreside IS users, an independent t-test was employed. The results from the procedures are presented in Table 28 through Table 29. The results indicate that maritime IS users are more inclined to have I-Type curiosity while shoreside IS users are inclined to have D-Type curiosity.

Table 28

Group Statistics for Cyber Curiosity

Group	**N**	**Mean**	**St.Dev**
Maritime	120	0.58	1.074
Shoreside	54	-0.65	1.119

Table 29

Independent Samples Test of Cyber Curiosity

Levene's Test for Equality of Variances		t-test for Equality of Means					
						95% Confidence Interval of the Difference	
F	Sig.	t	df	Sig. (2-talied)	Mean Difference	Lower	Upper
1.705	0.193	6.909	172	**0.000*** **	1.231	0.880	1.583

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

Cyber Risk Data Analysis

To answer RQ5c, which is "Are there any significant differences to an IS user's Cyber Risk score based on their age, gender, nationality, department, years performing job, education level, or psychological state of mind?", a one-way analysis of variance (ANOVA) was employed. This study assumes the Cyber Risk score as the representation of the participants Cyber SA and Cyber Curiosity scores combined as indicated by the Cyber Risk score calculations previously stated in the research methodology data aggregation section. An analysis of age, gender, nationality, department, years performing job, education level, and psychological state of mind (P1 – Uplift & P2 – Interest) for the total sample (N=174) did not show a significant difference with the product score of Cyber SA and Cyber Curiosity in comparison with the other independent variables. Table 30 provides an overview of the mean, standard deviation, and ANOVA results.

Table 30

ANOVA Results for Cyber Risk Score (N=174)

IV	**Mean**	**St.Dev**	**F**	**Sig.**
Age	3.06	0.960	1.114	0.352
Gender	-	-	1.811	0.129
Nationality	-	-	0.317	0.945
Department	-	-	1.158	0.313
Years Performing Job	3.92	1.563	1.050	0.390
Education Level	3.72	0.916	.975	0.422
P1 - Uplift	3.90	1.001	.285	.888
P2 - Interest	3.92	1.014	.088	.994

Note. Variables with missing min, max, min or St.Dev are nominal
*-p<.05, **-p<.01, *** -p<.001

In reviewing the age, gender, nationality, department, years performing job, education level, and psychological state of mind for the maritime IS users (Group A, n_1=120), this study determined that Gender and Department had the most statistically significant difference in comparison with the other independent variables. There was a close significant difference between Gender groups as calculated by an ANOVA F(4,115) = 2.430, p = 0.052. There was also a close significant difference between Department groups as calculated by an ANOVA F(12,107) = 1.793, p = .058. An ANOVA analysis of the other categories Age F(4,115) =0.924 , p = 0.452, Nationality F(7,112) = 0.859, p = 0.542, Years Performing Job F(5,114) = 0.633, p = 0.675, Education Level F(4,115) = 0.574, p = 0.682, Psychological state of mind P1-Uplift (F(4,115) = 0.507, p = 0.731), P2-Interest (F(5,114) = 0.641, p = 0.699) were not significant. In reviewing the age, gender, nationality, department, years performing job, education level, and psychological state of mind for the maritime IS users (Group B, n_1=54), this study determined that Psychological state of mind P1-Uplift F((2,51) = 6.116, p = 0.004) and P2-Uplift (F(2,51) = 6.107, p = 0.004) had the most statistically significant difference in comparison with the other independent variables. Table 31 provides an overview of the mean, standard deviation, and ANOVA results.

Table 31
ANOVA Results of Participants by Group for Cyber Risk

	Group A Maritime (n_1=120)				**Group B Shoreside (n_2=54)**			
Item	**Mean**	**St.Dev**	**F**	**Sig.**	**Mean**	**St.Dev**	**F**	**Sig.**
Age	2.86	0.910	.924	0.452	3.50	0.927	0.418	0.741
Gender	-	-	2.430	***0.052***	-	-	0.147	0.703
Nationality	-	-	0.859	0.542	-	-	1.534	0.197
Department	-	-	1.793	***0.058***	-	-	1.146	0.352
Years Performing Job	3.93	1.661	0.633	0.675	3.91	1.336	1.680	0.170
Education Level	3.50	0.961	0.574	0.682	4.20	0.562	0.319	0.728
P1 – Uplift	3.60	0.991	0.507	0.731	4.57	0.633	6.116	***0.004*****
P2 – Interest	3.62	1.022	0.641	0.699	4.61	0.564	6.107	***0.004*****

Note. Variables with missing min, max, min or St.Dev are nominal
*-p<.05, **-p<.01, *** -p<.001

To analyze if there exist mean group differences in Cyber Risk scores between maritime and shoreside IS users, an independent t-test was employed. The results from the procedures are presented in Table 32 through Table 33. The results indicate that maritime IS users do not have a significant statistical difference in Cyber Risk than shoreside IS users.

Table 32

Group Statistics for Cyber Risk

Group	N	Mean	St.Dev
Maritime	120	18.8333	9.68698
Shoreside	54	16.5741	10.14536

Table 33

Independent Samples Test of Cyber Risk

Levene's Test for Equality of Variances		t-test for Equality of Means					
						95% Confidence Interval of the Difference	
F	Sig.	t	df	Sig. (2-talied)	Mean Difference	Lower	Upper
0.146	0.703	1.403	172	0.163	2.25926	-0.92038	5.43890

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

Summary

This chapter contained the results and data analysis conducted in this research study. Phase One of this research SME reviewed the proposed measure components and scores of Cyber SA and Cyber Curiosity. Phase One concluded with addressing research RQ1a, RQ1b, RQ2a, and RQ2b. Phase Two SMEs validated the proposed Risk Taxonomy using the Delphi technique. Phase Two concluded with addressing RQ3. Phase Three began with a pilot test of the experiment to assess the measures of Cyber SA and Cyber Curiosity. Needed adjustments were made to the experiment based on the feedback from the pilot experiment. After refinements were made to the experiment, Phase Three completed the analysis of Cyber SA and Cyber Curiosity data from 120 maritime and 54 shoreside IS users.

The five goals of this study were accomplished using a three-phase research methodology approach. The first goal was to identify, classify, and validate, using SMEs, the components for the measures of Cyber SA and Cyber Curiosity. The second goal was to identify the scores of the identified components of the measures of Cyber SA and Cyber Curiosity, using SMEs and the Delphi method to validate aggregation to the proposed Cyber Risk taxonomy. The third goal was to develop and validate, using SMEs, a Cyber Risk taxonomy to classify maritime IS users by their level of Cyber SA and Cyber Curiosity. The fourth goal was to use the validated Cyber Risk taxonomy in an experiment to classify maritime IS users. The position of the participants in the Cyber Risk taxonomy were presented in Figure 14 and Figure 15. The last and fifth goal was to empirically assess if there are any significant differences in the maritime IS user's level of Cyber SA, Cyber Curiosity, and Cyber Risk when controlled for demographics indicators such as age, gender, nationality, department, years performing job, and education level. The results of the ANOVA were presented in Table 20 through Table 31 which met the fifth goal of this research study.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusions

Phishing is one the most common forms of social engineering attack and used in 43% of all breaches (Verizon, 2018). Because the success rate of IS users clicking on phishing emails steadily increases year to year (Verizon, 2016), phishing attacks continues to be a prevalent and easy form of cyber-attack (Gupta et al., 2016). This research attempts to better understand the human nature of these types of cyber risks with the development and SME validation of a Cyber Risk taxonomy. The Cyber Risk taxonomy assesses an IS user's susceptibility of being a victim of a social engineering cyber-attack. This chapter contains the conclusions of this research study. Followed by a discussion of the findings in the larger context of social engineering and cybersecurity. Proceeding with sharing the implications of this conducted research to the IS body of knowledge. And concluding with recommendations for further research. This study attempted to address the limited Cyber SA of social engineering threats used against IS users and the natural curiosity that creates a significant threat to organizations (Iuga, Nurse, & Erola, 2016). This research objective was achieved successfully addressing the five research goals and research questions. This research study used a three-phased developmental methodology approach. The first phase SME reviewed and validated, using the Delphi method, the proposed measure components and scores of Cyber SA and Cyber Curiosity. The second phase SME validated the proposed Cyber Risk taxonomy to help develop and empirically validate an IS cyber situational awareness (SA) taxonomy in the context of Cyber Curiosity that can be used as a benchmark to measure the susceptibility of mitigating a cyber-attack using social engineering techniques among IS users. The third phase consisted of field testing the developed web-experiment in a maritime environment with IS users to assess the measures of Cyber SA and Cyber Curiosity. Lastly, the final phase concluded with the analysis and summary of the gathered experiment data.

Discussion

The results of this study indicated that there was not a significant difference in IS users' Cyber SA and Cyber Curiosity by Age, Years Performing Job, nor Education Level. There was a significant difference in Cyber SA when evaluating both maritime and shoreside in the participants Department but not when analyzing each group separately. When analyzing Cyber SA scores individually by groups, maritime and shoreside, there were no statistically significant differences observed on Age, Gender, Nationality, Department, Years Performing Job, Education Level, or Psychological State. Another observation was that shoreside IS users were more reluctant to share their psychological state of mind than were maritime users.

When analyzing the participants' positioning on the Cyber SA and Cyber Curiosity Risk Taxonomy, the larger groups have a very high level of cyber risk. Another observation was that participants as a whole, had an inclination towards I-Type curiosity. IS users with higher I-Type Cyber Curiosity also had lower Cyber SA scores, thus possibly less successful at detecting a social engineering attack. Even though the sample size of 174 IS users was valid for this research study, further research onboard other types and size of vessels can increase the validation of the results and its generalizability. In analyzing the maritime and the shoreside groups individually on their placement on the Cyber Risk taxonomy, the maritime IS users were classified as high risk high. This result can be attributed to their higher levels of I-Type Cyber Curiosity and low level of D-type Cyber Curiosity. The unique operating conditions of maritime IS users where they are working extended periods of time away at sea can possibly impede their interest in D-Type curiosity and engage in more I-Type curiosity and impact their Cyber SA.

Implications

This study provides the maritime industry with valuable insights into the susceptibility of social engineering attacks because of the limited awareness of cybersecurity risks in the maritime sector. In leveraging experiment results from this study that determined participants are highly susceptible to socially engineering attacks due to their lower Cyber SA and higher levels of I-Type curiosity than D-Type curiosity, the maritime industry can develop cybersecurity awareness programs that increases Cyber SA by requiring IS users to reduce uncertainty in how to identify a social engineering cyber-attack.

Recommendations and Future Research

More research is needed to take place in other maritime industries beyond a passenger vessel setting. These would include supply chain ports, cargo vessels, and offshore facilities. Another recommendation for future research includes investigating other psychological states of mind beyond those measured in the pre-experiment questionnaire. Further investigating other psychological behaviors (i.e. boredom and depression) that impact the levels of Cyber Curiosity or Cyber SA can shed insights to reduce cybersecurity risks.

Summary

This research study addressed the research problem of limited Cyber SA of social engineering threat vector used against information system (IS) users, and the natural human curiosity that creates a significant cybersecurity threat to organizations (Iuga, Nurse, & Erola, 2016). The main goal of this research was to design, develop, and to empirically validate an IS Cyber SA in the context of Cyber Curiosity taxonomy that measures the susceptibility of mitigating a cyber-attack using social engineering techniques on IS users in the maritime industry

This study had five specific goals. The first research goal was to identify, classify, and validate, using SMEs the components for the measures of Cyber SA and Cyber Curiosity. The second goal was to identify the scores of the identified components of the measures of Cyber SA and Cyber Curiosity, using SMEs that enable a validated aggregation to the proposed Cyber Risk taxonomy. The third goal was to develop and validate, using SMEs, a Cyber Risk taxonomy to classify maritime IS users by their level of Cyber SA and Cyber Curiosity. The fourth research goal was to use the validated Cyber Risk taxonomy in an experiment to classify 174 maritime and shoreside IS users. The fifth research goal was to empirically assess if there are any significant differences in the 174 maritime and shoreside IS user's level of Cyber SA, Cyber Curiosity, and position in the Cyber Risk taxonomy when controlled for demographics indicators such as: age, gender, department, years performing job function, and education level.

In Phase One, a panel of SMEs were solicited from the maritime industry and cybersecurity to answer the following research questions:

RQ1a: What are the SMEs identified components of the measures of an IS user's level of Cyber SA which may influence the susceptibility of being a victim of a social engineering cyber-attack?

RQ1b: What are the SMEs identified components of the measures of an IS user's level of Cyber Curiosity which may influence the susceptibility of being a victim of a social engineering cyber-attack?

RQ2a: What are the specific scores of the SMEs identified components of the IS user's measures of Cyber SA that enable a validated hierarchical aggregation to the Cyber SA measure of the Cyber Risk taxonomy?

RQ2b: What are the specific scores of the SMEs identified components of the IS user's measures of Cyber Curiosity that enable a validated hierarchical aggregation to the Cyber Curiosity measure of the Cyber Risk taxonomy?

The SMEs background included a mixture of cybersecurity and cyber maritime experts with at least ten years of professional experience. The Delphi method was used to obtain consensus among SME's validate the proposed Cyber Risk taxonomy components for the measures of Cyber SA levels, Cyber Curiosity levels, and the scores of the identified components of the measures of Cyber SA and Cyber Curiosity.

In Phase Two another panel of SMEs were solicited from the maritime industry and cybersecurity to answer the following research question:

RQ3: What are the experts' approved classification of the Social Engineering Attack Experiment using the hierarchical aggregation of Cyber SA and

Cyber Curiosity for the cyber-Risk Taxonomy using a social engineering attack experiment?

The Delphi method was used to obtain consensus among SME's validate the proposed classification for the Cyber Risk Taxonomy.

In Phase Three, pilot test of the Web-based experiment was conducted using a mixture of qualitative and quantitative data collection, to assess measures of Cyber SA and Cyber Curiosity. After minor refinements were made to the experiment based on feedback of the pilot experiment, Phase Three successfully conducted a quantitative empirical study by collecting Cyber SA and Cyber Curiosity data from 120 maritime IS and 54 shoreside IS users. Lastly, the collected data was analyzed to address the following questions:

RQ4: How are the aggregated scores for Cyber SA and Cyber Curiosity positioned on the Cyber Risk taxonomy for maritime IS users?

RQ5a: Are there any statistically significant mean differences to maritime IS users' aggregated level of Cyber SA based on their age, gender, nationality, department, years at performing job, education level, or psychological state of mind?

RQ5b: Are there any statistically significant mean differences to maritime IS users' aggregated level of Cyber Curiosity based on their age, gender, nationality, department, years performing job, education level, or psychological state of mind?

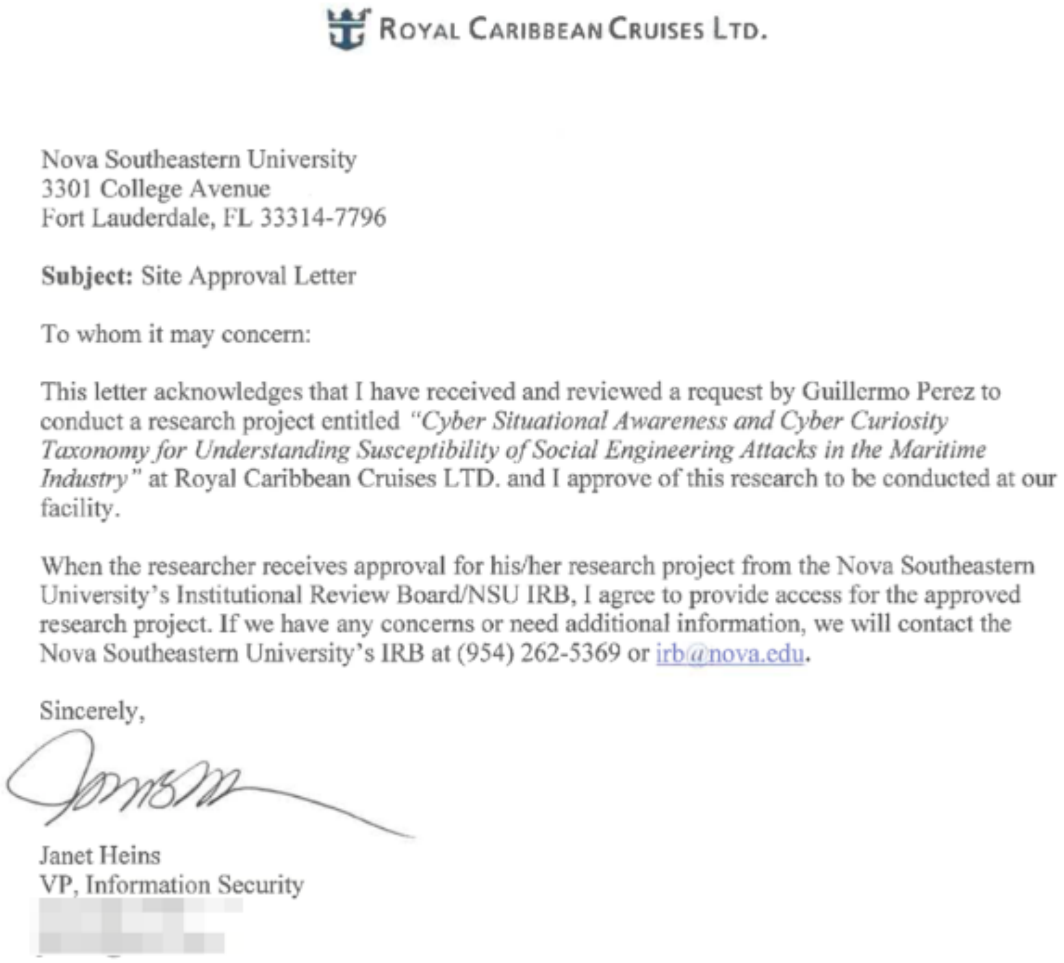
RQ5c: Are there any statistically significant mean differences to an IS user's Cyber Risk score based on their age, gender, nationality, department, years performing job, education level, or psychological state of mind?

This research study made several contributions to the Information Security body of knowledge. The first was by designing, developing, and empirically validating an IS Cyber SA, in the context of Cyber Curiosity, Cyber Risk taxonomy that measures the susceptibility of mitigating a cyber-attack using social engineering techniques on IS users in the maritime industry. The second is that this study helped advance current research in cybersecurity and contribute to the body of knowledge regarding IS users as it relates to their awareness of social engineering cyber-attacks. Another significance of this study is the unusual context of the research setting. The maritime industry, specifically passenger vessels, presented a unique research study environment where crew spend a significant amount of time in constant interaction with passengers and are also away from family for extended periods of time. This interaction and enclosed environment provided an interesting dynamic to cyber situational awareness and Cyber Curiosity research further contributing to the IS body of knowledge.

In conclusion, maritime organizations can use the developed cyber risk taxonomy and the research results to help reduce social engineering cyber risks and improve cyber situational awareness. Other researchers can use the developed cyber risk taxonomy to assess cyber situational awareness and cyber curiosity in other environments. Lastly, security and awareness programs can use the validated Cyber Curiosity components to better assess an IS users type of curiosity to better entice use to raise cyber situational awareness.

Appendix A

Site Approval Letter



ROYAL CARIBBEAN CRUISES LTD.

Nova Southeastern University
3301 College Avenue
Fort Lauderdale, FL 33314-7796

Subject: Site Approval Letter

To whom it may concern:

This letter acknowledges that I have received and reviewed a request by Guillermo Perez to conduct a research project entitled *"Cyber Situational Awareness and Cyber Curiosity Taxonomy for Understanding Susceptibility of Social Engineering Attacks in the Maritime Industry"* at Royal Caribbean Cruises LTD. and I approve of this research to be conducted at our facility.

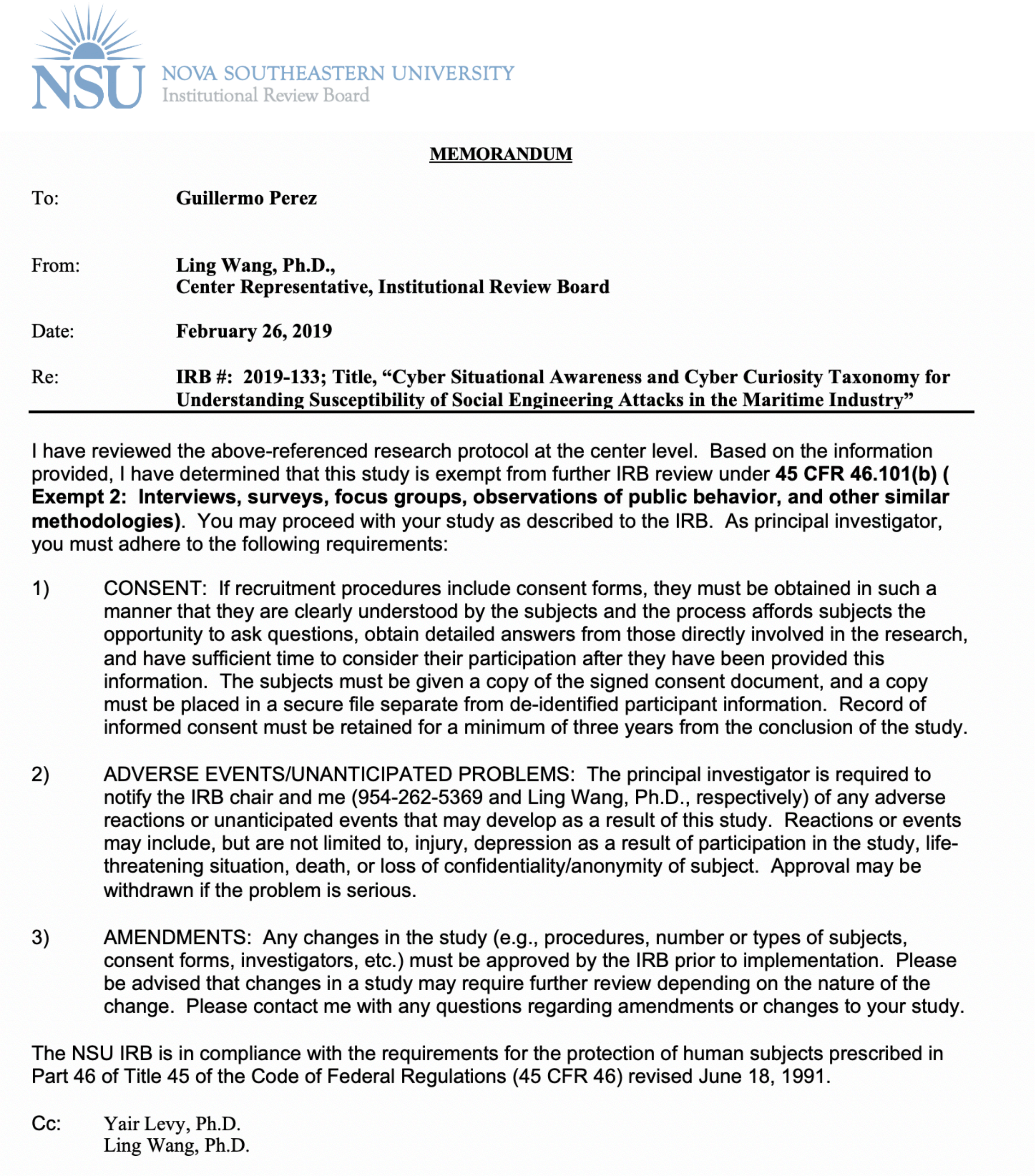
When the researcher receives approval for his/her research project from the Nova Southeastern University's Institutional Review Board/NSU IRB, I agree to provide access for the approved research project. If we have any concerns or need additional information, we will contact the Nova Southeastern University's IRB at (954) 262-5369 or irb@nova.edu.

Sincerely,

Janet Heins
VP, Information Security
[redacted]

Appendix B

Institutional Review Board Approval Letter



NOVA SOUTHEASTERN UNIVERSITY
Institutional Review Board

MEMORANDUM

To: **Guillermo Perez**

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

Date: **February 26, 2019**

Re: **IRB #: 2019-133; Title, "Cyber Situational Awareness and Cyber Curiosity Taxonomy for Understanding Susceptibility of Social Engineering Attacks in the Maritime Industry"**

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 C

Expert Panel Recruitment Email

Dear Cybersecurity Experts,

I need your assistance in providing expert feedback on set of measures for my upcoming doctoral research study. I am a Ph.D. Candidate in Information Assurance and Cybersecurity at the College of Engineering and Computing, Nova Southeastern University (NSU), working under the supervision of Professor Dr. Yair Levy. My research is seeking to develop a Cyber Risk taxonomy to classify maritime IS users by their level of cyber situational awareness (SA) and Cyber Curiosity of Information Systems (IS) users.

In this part of the research, I need your assistance in validating the proposed components for the measures and scores of cyber situational awareness (CSA) and Cyber Curiosity levels to help develop and empirically validate an IS cyber situational awareness (SA) taxonomy in the context of Cyber Curiosity that can be used as a benchmark to measure the susceptibility of mitigating a cyber-attack using social engineering techniques among IS users.

Below are definitions used in the research study:

- Cybersecurity – The protection of cyberspace, the electronic information, the infrastructure that supports cyberspace, and the users of cyberspace in their personal, societal, and national capacity including any of their interests that are vulnerable to attacks originating in cyberspace (Solms & Niekerk, 2013).

- Cyber Situational Awareness - The perception of cyber risk elements with respect to time and space, the understanding of their meaning, and anticipation of their status in the near future (Tadda & Salerno, 2010).

- Cyber Curiosity - Cyber Curiosity is the desire for information and knowledge about information systems (IS) and the Internet.

- Social engineering - A technique used by hackers, leveraging human interactions or social skills, to obtain or compromise IS information to infiltrate an organizations network (US-CERT, 2016).

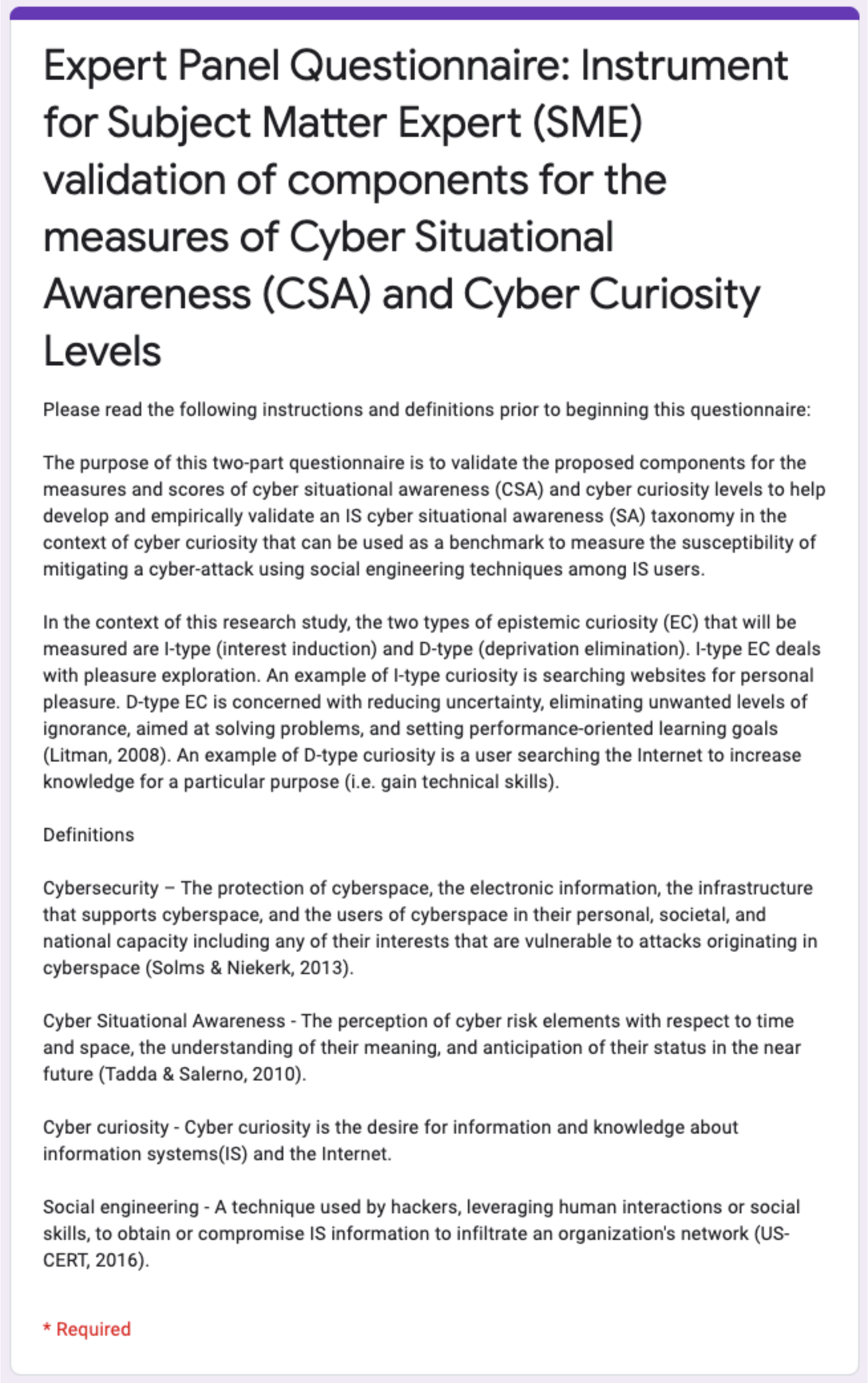
The information provided with your assistance will be used for this research study in aggregated form. No personally identifiable information (PII) will be collected. As a participate, you agree to keep all the information regarding this research confidential and refrain from disclosing any details related to this survey or the material contained within it.

Thank you in advance for your consideration. I appreciate your assistance and contribution for this research study.

Regards,
Guillermo Perez, Ph.D. Candidate
E-mail:gp90@mynsu.nova.edu
Information Assurance and Cybersecurity

Appendix D

Expert Panel Questionnaire: Instrument for Subject Matter Expert (SME) validation of components for the measures of Cyber Situational Awareness (CSA) and Cyber Curiosity Levels



Expert Panel Questionnaire: Instrument for Subject Matter Expert (SME) validation of components for the measures of Cyber Situational Awareness (CSA) and Cyber Curiosity Levels

Please read the following instructions and definitions prior to beginning this questionnaire:

The purpose of this two-part questionnaire is to validate the proposed components for the measures and scores of cyber situational awareness (CSA) and cyber curiosity levels to help develop and empirically validate an IS cyber situational awareness (SA) taxonomy in the context of cyber curiosity that can be used as a benchmark to measure the susceptibility of mitigating a cyber-attack using social engineering techniques among IS users.

In the context of this research study, the two types of epistemic curiosity (EC) that will be measured are I-type (interest induction) and D-type (deprivation elimination). I-type EC deals with pleasure exploration. An example of I-type curiosity is searching websites for personal pleasure. D-type EC is concerned with reducing uncertainty, eliminating unwanted levels of ignorance, aimed at solving problems, and setting performance-oriented learning goals (Litman, 2008). An example of D-type curiosity is a user searching the Internet to increase knowledge for a particular purpose (i.e. gain technical skills).

Definitions

Cybersecurity – The protection of cyberspace, the electronic information, the infrastructure that supports cyberspace, and the users of cyberspace in their personal, societal, and national capacity including any of their interests that are vulnerable to attacks originating in cyberspace (Solms & Niekerk, 2013).

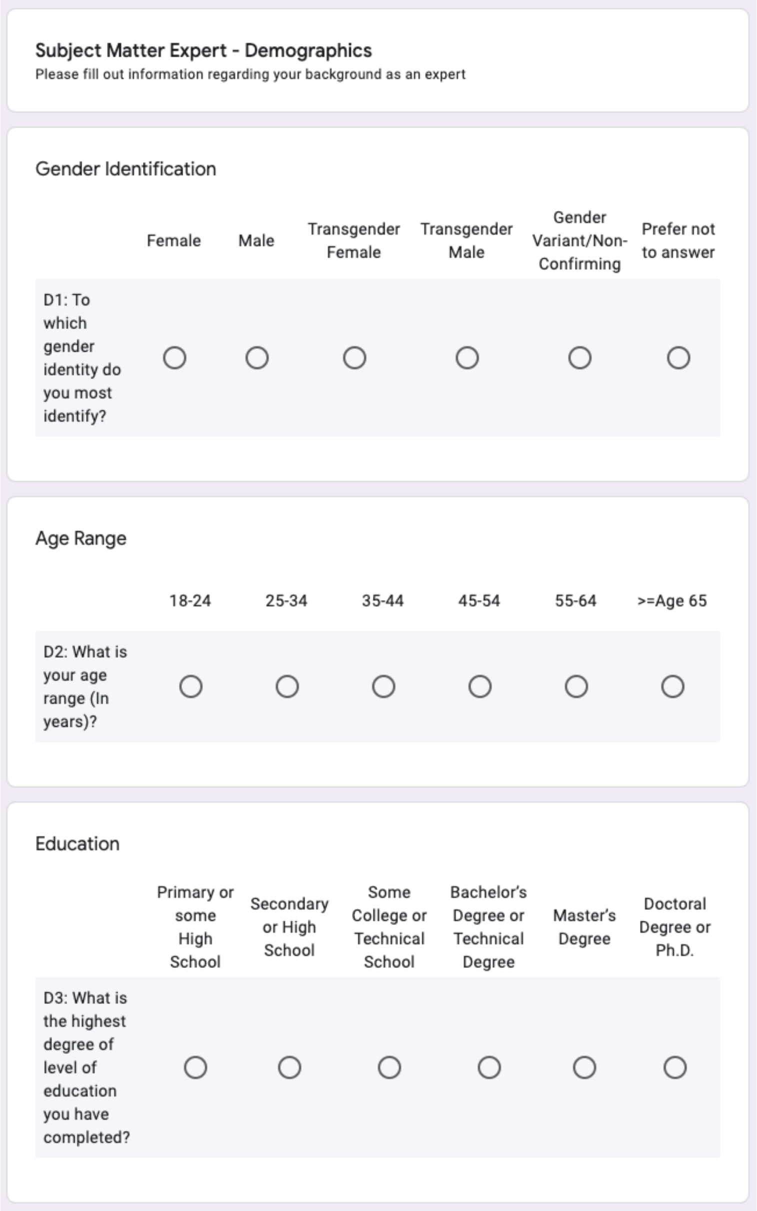
Cyber Situational Awareness - The perception of cyber risk elements with respect to time and space, the understanding of their meaning, and anticipation of their status in the near future (Tadda & Salerno, 2010).

Cyber curiosity - Cyber curiosity is the desire for information and knowledge about information systems(IS) and the Internet.

Social engineering - A technique used by hackers, leveraging human interactions or social skills, to obtain or compromise IS information to infiltrate an organization's network (US-CERT, 2016).

* Required

Expert Panel Questionnaire - Components & Measures (Cont.)



Subject Matter Expert - Demographics
Please fill out information regarding your background as an expert

Gender Identification

	Female	Male	Transgender Female	Transgender Male	Gender Variant/Non-Confirming	Prefer not to answer
D1: To which gender identity do you most identify?	○	○	○	○	○	○

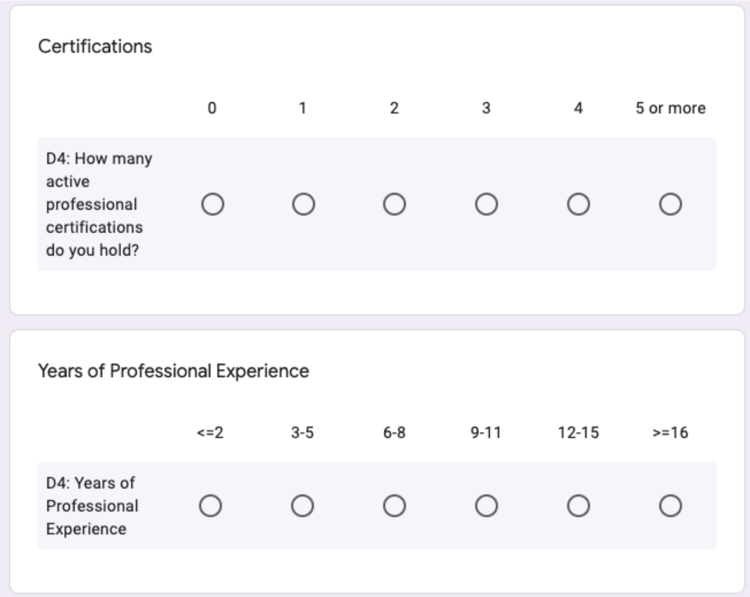
Age Range

	18-24	25-34	35-44	45-54	55-64	>=Age 65
D2: What is your age range (In years)?	○	○	○	○	○	○

Education

	Primary or some High School	Secondary or High School	Some College or Technical School	Bachelor's Degree or Technical Degree	Master's Degree	Doctoral Degree or Ph.D.
D3: What is the highest degree of level of education you have completed?	○	○	○	○	○	○

Expert Panel Questionnaire - Components & Measures (Cont.)



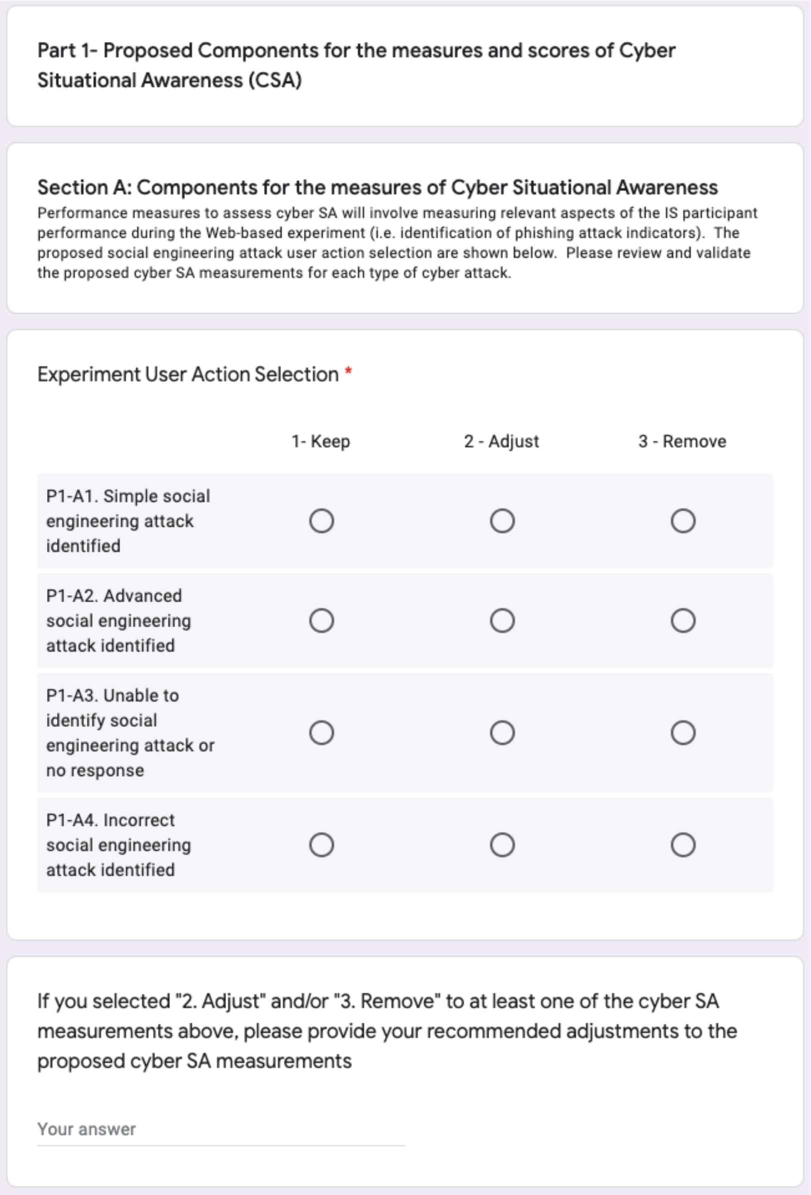
Certifications

	0	1	2	3	4	5 or more
D4: How many active professional certifications do you hold?	○	○	○	○	○	○

Years of Professional Experience

	<=2	3-5	6-8	9-11	12-15	>=16
D4: Years of Professional Experience	○	○	○	○	○	○

Expert Panel Questionnaire - Components & Measures (Cont.)



Part 1- Proposed Components for the measures and scores of Cyber Situational Awareness (CSA)

Section A: Components for the measures of Cyber Situational Awareness

Performance measures to assess cyber SA will involve measuring relevant aspects of the IS participant performance during the Web-based experiment (i.e. identification of phishing attack indicators). The proposed social engineering attack user action selection are shown below. Please review and validate the proposed cyber SA measurements for each type of cyber attack.

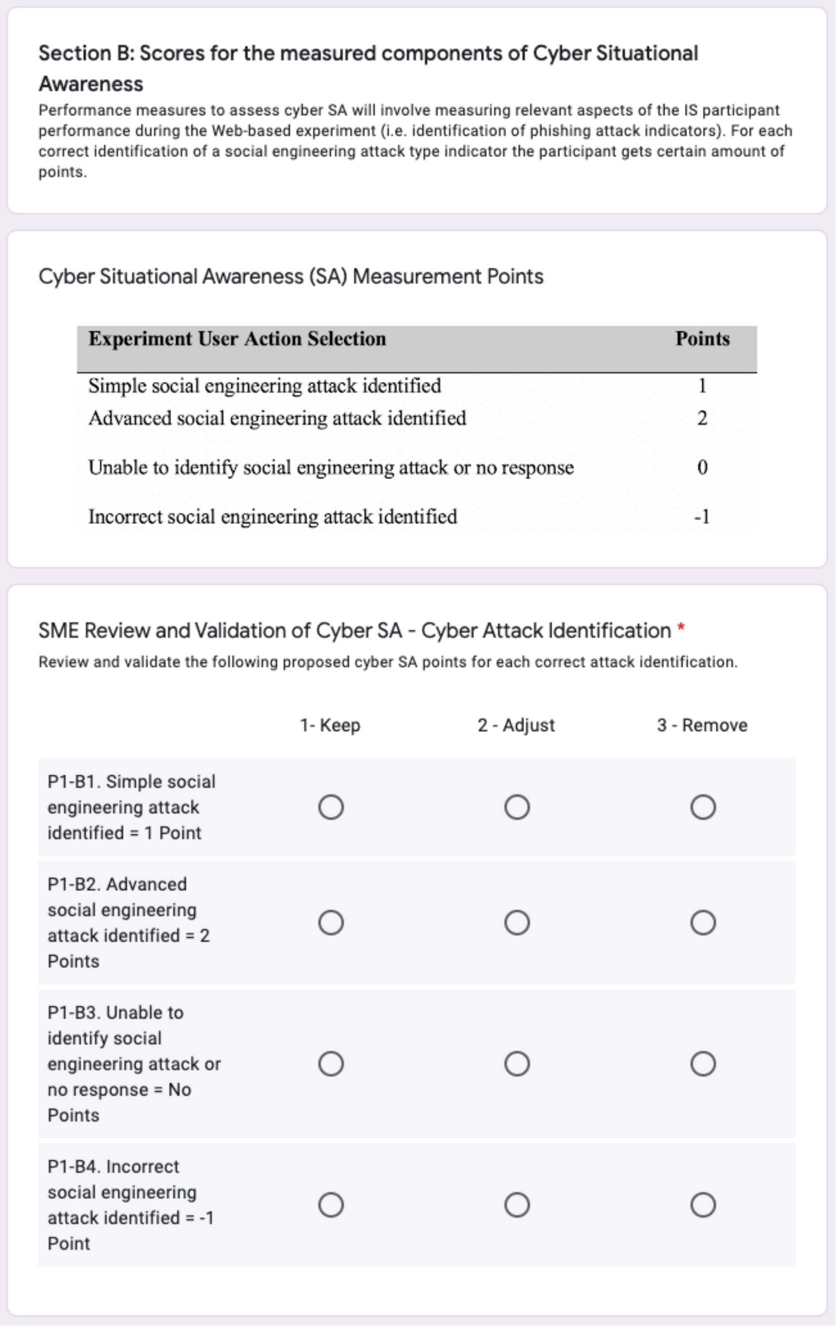
Experiment User Action Selection *

	1- Keep	2 - Adjust	3 - Remove
P1-A1. Simple social engineering attack identified	○	○	○
P1-A2. Advanced social engineering attack identified	○	○	○
P1-A3. Unable to identify social engineering attack or no response	○	○	○
P1-A4. Incorrect social engineering attack identified	○	○	○

If you selected "2. Adjust" and/or "3. Remove" to at least one of the cyber SA measurements above, please provide your recommended adjustments to the proposed cyber SA measurements

Your answer

Expert Panel Questionnaire - Components & Measures (Cont.)



Section B: Scores for the measured components of Cyber Situational Awareness

Performance measures to assess cyber SA will involve measuring relevant aspects of the IS participant performance during the Web-based experiment (i.e. identification of phishing attack indicators). For each correct identification of a social engineering attack type indicator the participant gets certain amount of points.

Cyber Situational Awareness (SA) Measurement Points

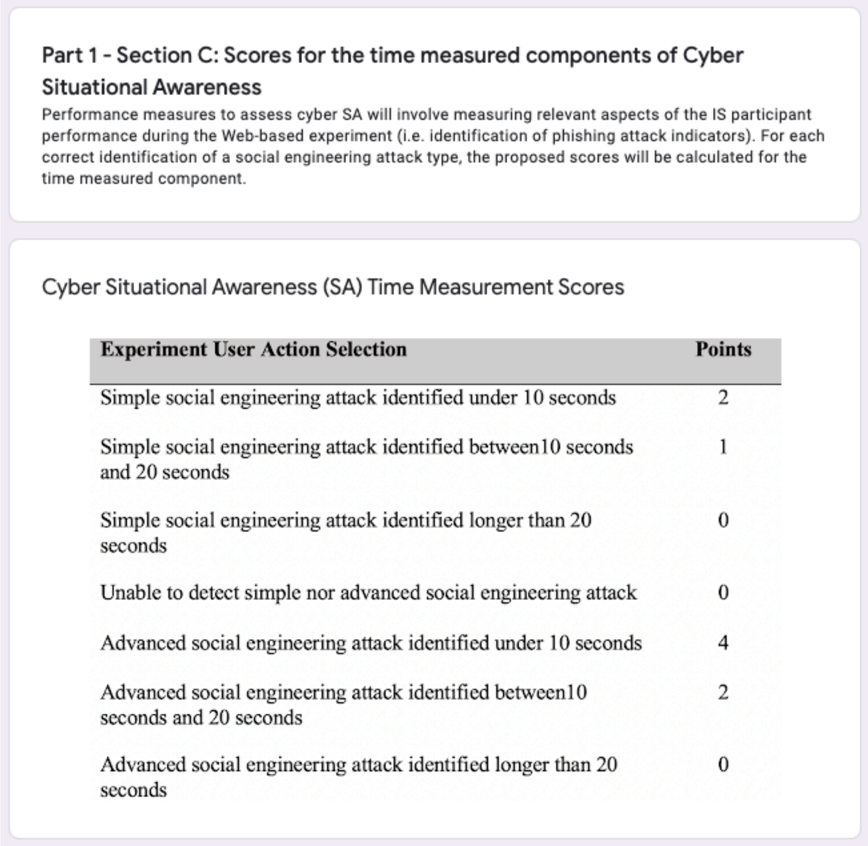
Experiment User Action Selection	Points
Simple social engineering attack identified	1
Advanced social engineering attack identified	2
Unable to identify social engineering attack or no response	0
Incorrect social engineering attack identified	-1

SME Review and Validation of Cyber SA - Cyber Attack Identification *

Review and validate the following proposed cyber SA points for each correct attack identification.

	1- Keep	2 - Adjust	3 - Remove
P1-B1. Simple social engineering attack identified = 1 Point	○	○	○
P1-B2. Advanced social engineering attack identified = 2 Points	○	○	○
P1-B3. Unable to identify social engineering attack or no response = No Points	○	○	○
P1-B4. Incorrect social engineering attack identified = -1 Point	○	○	○

Expert Panel Questionnaire - Components & Measures (Cont.)



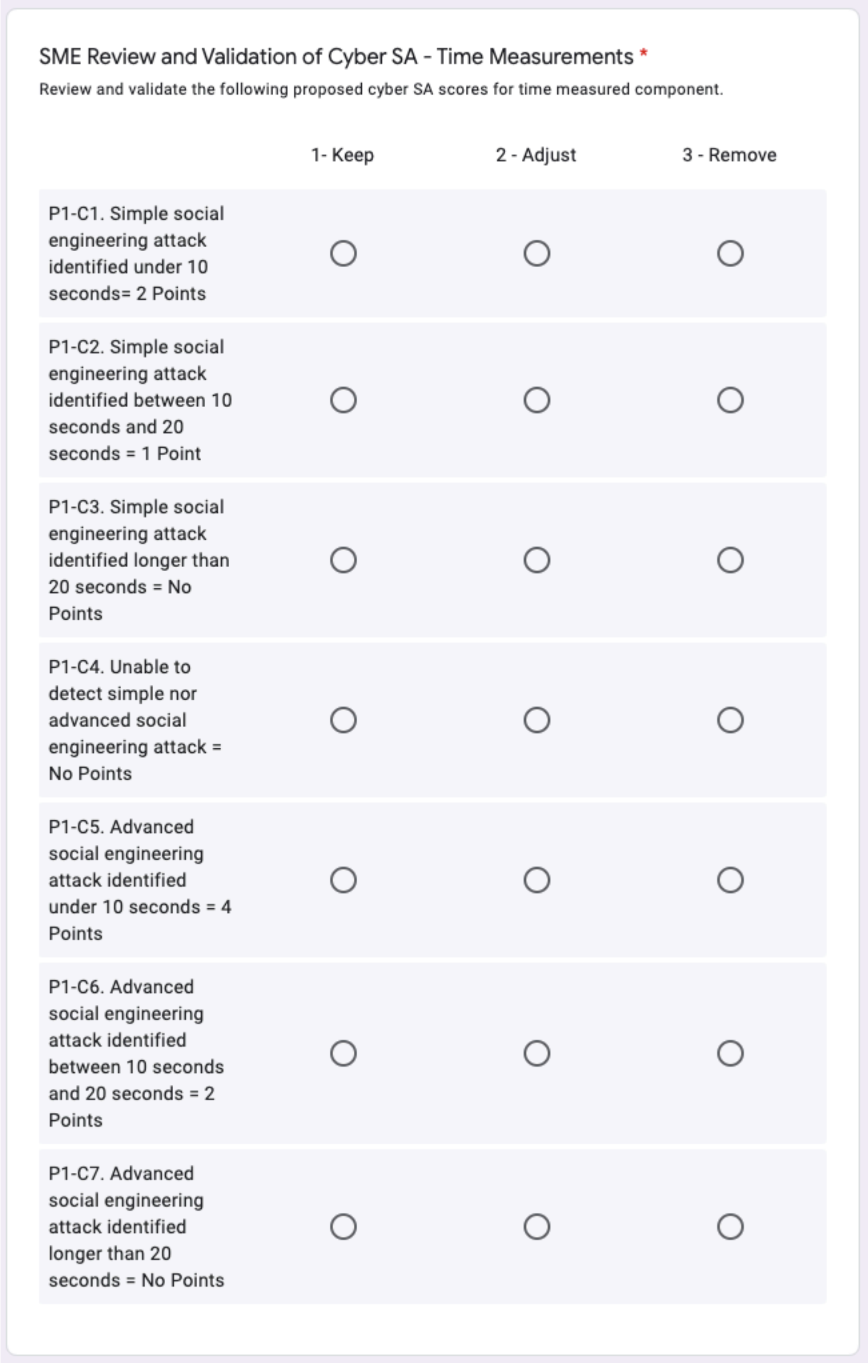
Part 1 - Section C: Scores for the time measured components of Cyber Situational Awareness

Performance measures to assess cyber SA will involve measuring relevant aspects of the IS participant performance during the Web-based experiment (i.e. identification of phishing attack indicators). For each correct identification of a social engineering attack type, the proposed scores will be calculated for the time measured component.

Cyber Situational Awareness (SA) Time Measurement Scores

Experiment User Action Selection	Points
Simple social engineering attack identified under 10 seconds	2
Simple social engineering attack identified between10 seconds and 20 seconds	1
Simple social engineering attack identified longer than 20 seconds	0
Unable to detect simple nor advanced social engineering attack	0
Advanced social engineering attack identified under 10 seconds	4
Advanced social engineering attack identified between10 seconds and 20 seconds	2
Advanced social engineering attack identified longer than 20 seconds	0

Expert Panel Questionnaire - Components & Measures (Cont.)

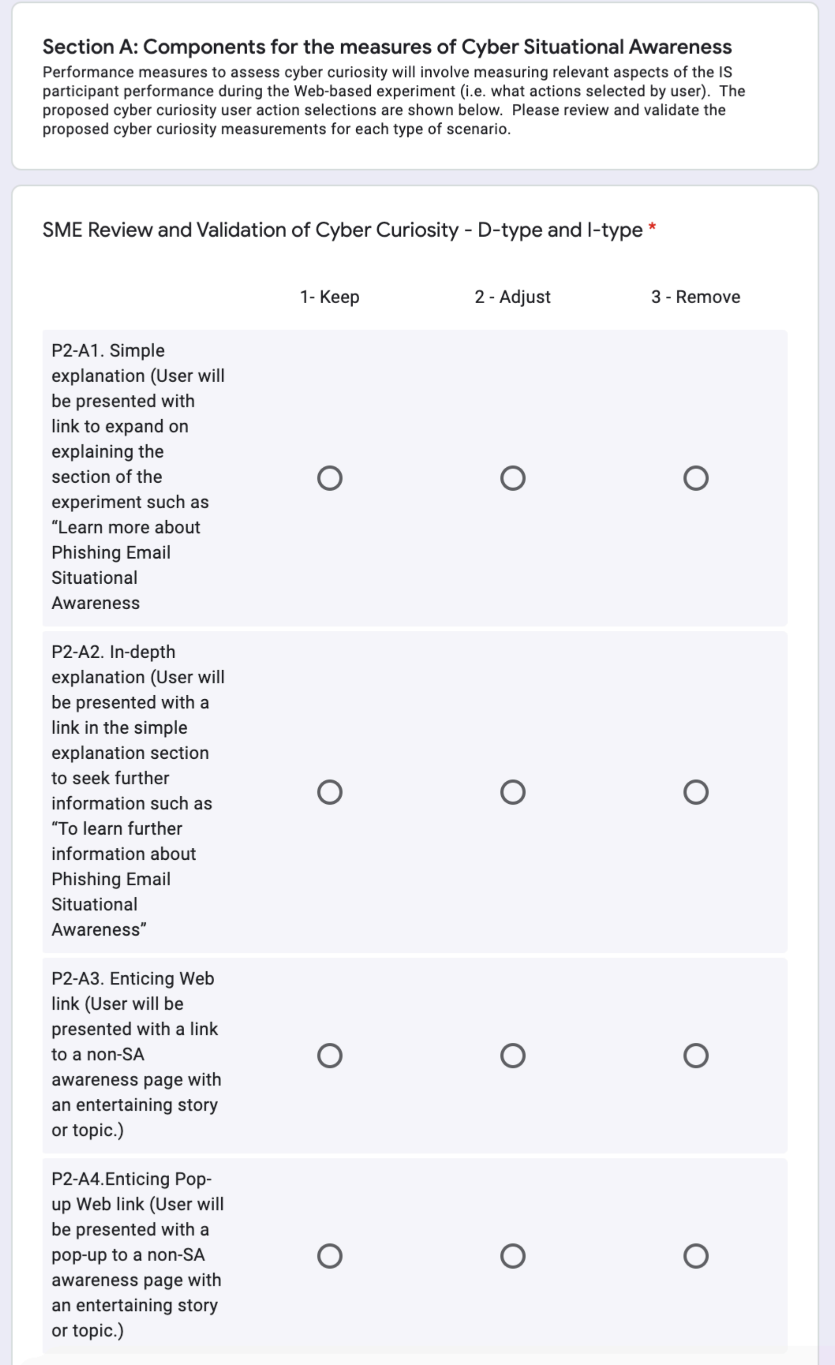


SME Review and Validation of Cyber SA - Time Measurements *

Review and validate the following proposed cyber SA scores for time measured component.

	1- Keep	2 - Adjust	3 - Remove
P1-C1. Simple social engineering attack identified under 10 seconds= 2 Points	○	○	○
P1-C2. Simple social engineering attack identified between 10 seconds and 20 seconds = 1 Point	○	○	○
P1-C3. Simple social engineering attack identified longer than 20 seconds = No Points	○	○	○
P1-C4. Unable to detect simple nor advanced social engineering attack = No Points	○	○	○
P1-C5. Advanced social engineering attack identified under 10 seconds = 4 Points	○	○	○
P1-C6. Advanced social engineering attack identified between 10 seconds and 20 seconds = 2 Points	○	○	○
P1-C7. Advanced social engineering attack identified longer than 20 seconds = No Points	○	○	○

Expert Panel Questionnaire - Components & Measures (Cont.)



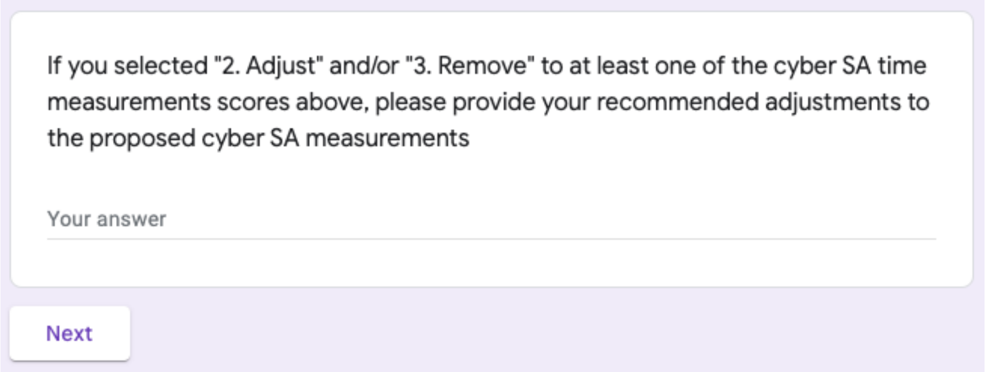
Section A: Components for the measures of Cyber Situational Awareness

Performance measures to assess cyber curiosity will involve measuring relevant aspects of the IS participant performance during the Web-based experiment (i.e. what actions selected by user). The proposed cyber curiosity user action selections are shown below. Please review and validate the proposed cyber curiosity measurements for each type of scenario.

SME Review and Validation of Cyber Curiosity - D-type and I-type *

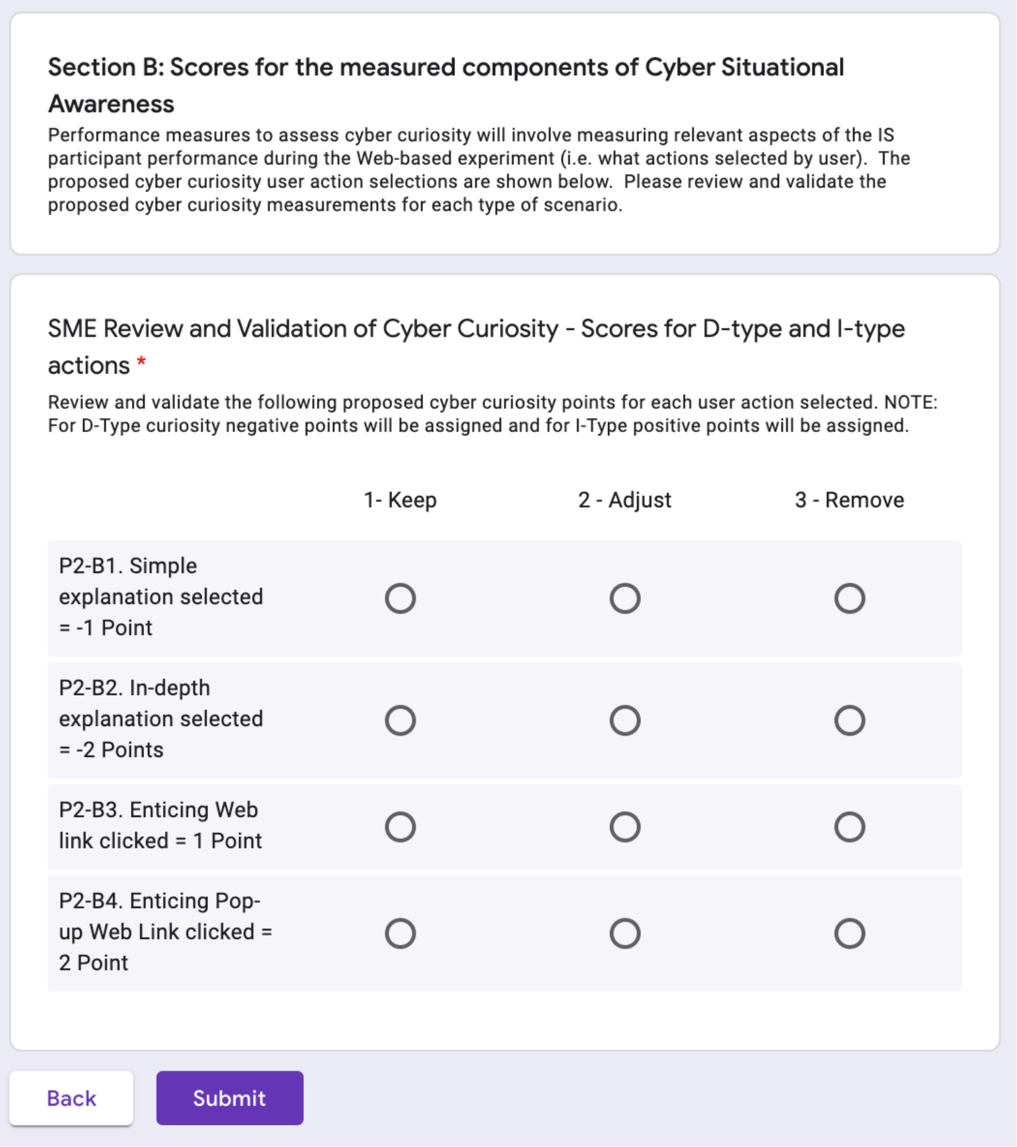
	1- Keep	2 - Adjust	3 - Remove
P2-A1. Simple explanation (User will be presented with link to expand on explaining the section of the experiment such as “Learn more about Phishing Email Situational Awareness	○	○	○
P2-A2. In-depth explanation (User will be presented with a link in the simple explanation section to seek further information such as “To learn further information about Phishing Email Situational Awareness”	○	○	○
P2-A3. Enticing Web link (User will be presented with a link to a non-SA awareness page with an entertaining story or topic.)	○	○	○
P2-A4.Enticing Pop-up Web link (User will be presented with a pop-up to a non-SA awareness page with an entertaining story or topic.)	○	○	○

Expert Panel Questionnaire - Components & Measures (Cont.)



If you selected "2. Adjust" and/or "3. Remove" to at least one of the cyber SA time measurements scores above, please provide your recommended adjustments to the proposed cyber SA measurements

Your answer



Section B: Scores for the measured components of Cyber Situational Awareness

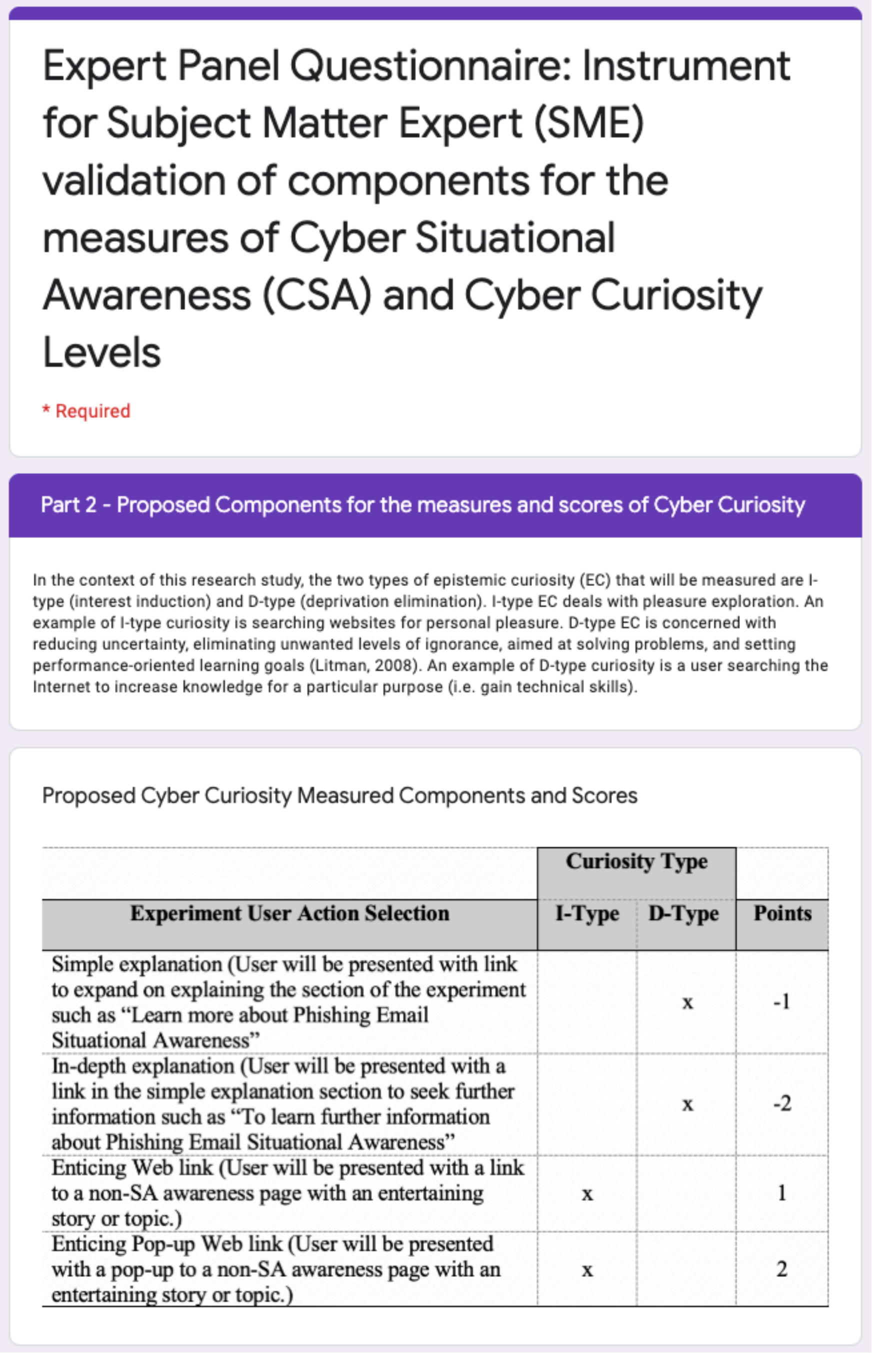
Performance measures to assess cyber curiosity will involve measuring relevant aspects of the IS participant performance during the Web-based experiment (i.e. what actions selected by user). The proposed cyber curiosity user action selections are shown below. Please review and validate the proposed cyber curiosity measurements for each type of scenario.

SME Review and Validation of Cyber Curiosity - Scores for D-type and I-type actions *

Review and validate the following proposed cyber curiosity points for each user action selected. NOTE: For D-Type curiosity negative points will be assigned and for I-Type positive points will be assigned.

	1- Keep	2 - Adjust	3 - Remove
P2-B1. Simple explanation selected = -1 Point	○	○	○
P2-B2. In-depth explanation selected = -2 Points	○	○	○
P2-B3. Enticing Web link clicked = 1 Point	○	○	○
P2-B4. Enticing Pop-up Web Link clicked = 2 Point	○	○	○

Expert Panel Questionnaire - Components & Measures (Cont.)



Expert Panel Questionnaire: Instrument for Subject Matter Expert (SME) validation of components for the measures of Cyber Situational Awareness (CSA) and Cyber Curiosity Levels

* Required

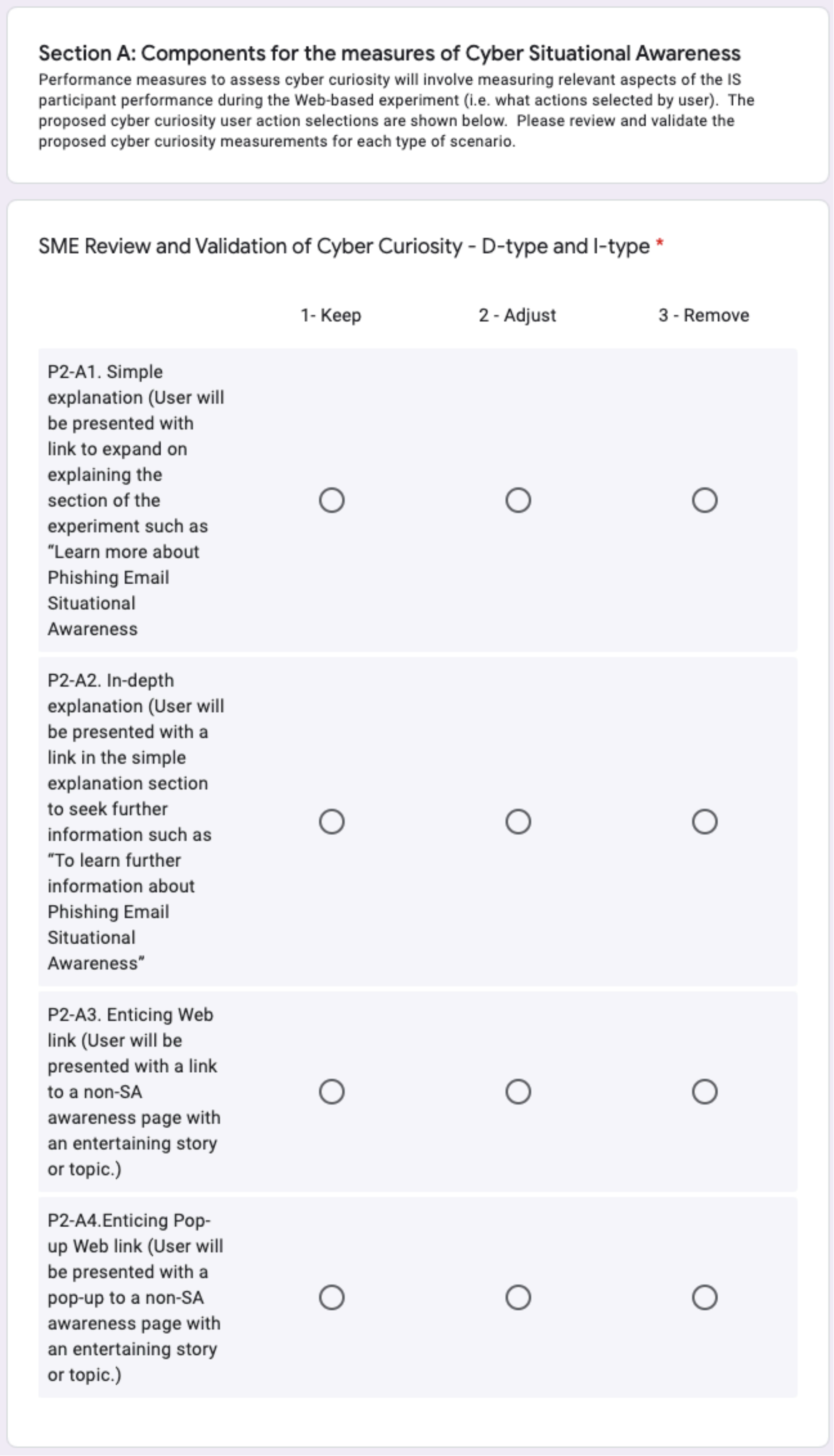
Part 2 - Proposed Components for the measures and scores of Cyber Curiosity

In the context of this research study, the two types of epistemic curiosity (EC) that will be measured are I-type (interest induction) and D-type (deprivation elimination). I-type EC deals with pleasure exploration. An example of I-type curiosity is searching websites for personal pleasure. D-type EC is concerned with reducing uncertainty, eliminating unwanted levels of ignorance, aimed at solving problems, and setting performance-oriented learning goals (Litman, 2008). An example of D-type curiosity is a user searching the Internet to increase knowledge for a particular purpose (i.e. gain technical skills).

Proposed Cyber Curiosity Measured Components and Scores

	Curiosity Type		
Experiment User Action Selection	**I-Type**	**D-Type**	**Points**
Simple explanation (User will be presented with link to expand on explaining the section of the experiment such as "Learn more about Phishing Email Situational Awareness"		x	-1
In-depth explanation (User will be presented with a link in the simple explanation section to seek further information such as "To learn further information about Phishing Email Situational Awareness"		x	-2
Enticing Web link (User will be presented with a link to a non-SA awareness page with an entertaining story or topic.)	x		1
Enticing Pop-up Web link (User will be presented with a pop-up to a non-SA awareness page with an entertaining story or topic.)	x		2

Expert Panel Questionnaire - Components & Measures (Cont.)



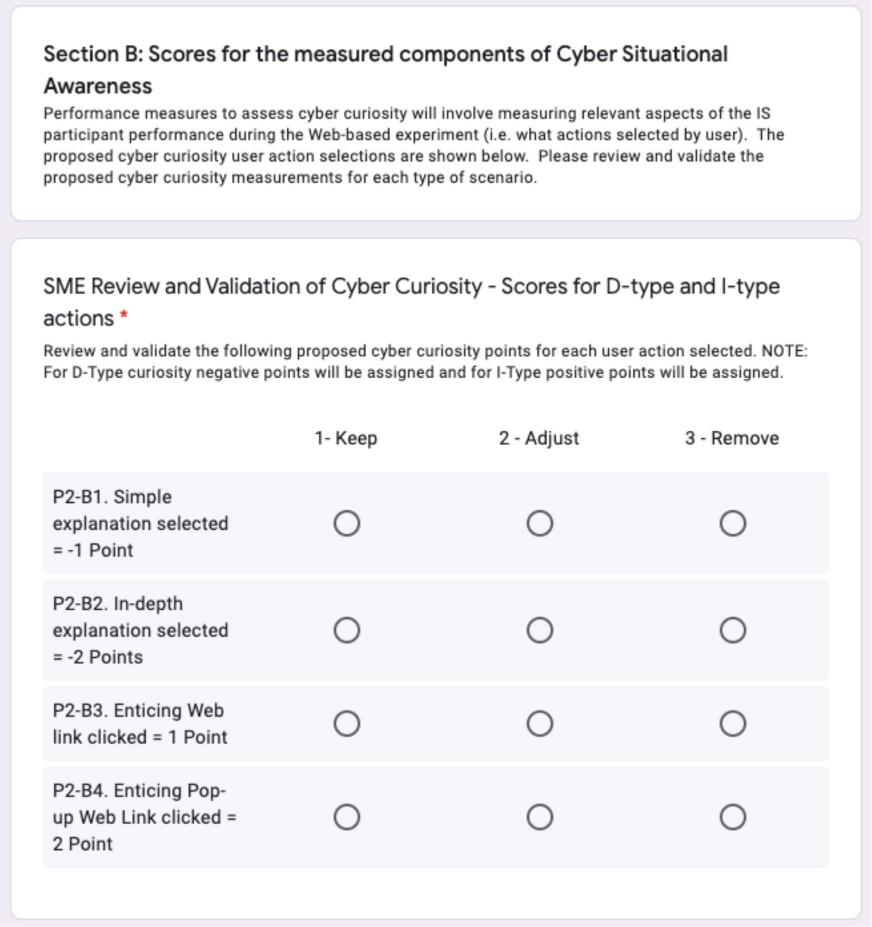
Section A: Components for the measures of Cyber Situational Awareness

Performance measures to assess cyber curiosity will involve measuring relevant aspects of the IS participant performance during the Web-based experiment (i.e. what actions selected by user). The proposed cyber curiosity user action selections are shown below. Please review and validate the proposed cyber curiosity measurements for each type of scenario.

SME Review and Validation of Cyber Curiosity - D-type and I-type *

	1- Keep	2 - Adjust	3 - Remove
P2-A1. Simple explanation (User will be presented with link to expand on explaining the section of the experiment such as “Learn more about Phishing Email Situational Awareness	○	○	○
P2-A2. In-depth explanation (User will be presented with a link in the simple explanation section to seek further information such as “To learn further information about Phishing Email Situational Awareness”	○	○	○
P2-A3. Enticing Web link (User will be presented with a link to a non-SA awareness page with an entertaining story or topic.)	○	○	○
P2-A4.Enticing Pop-up Web link (User will be presented with a pop-up to a non-SA awareness page with an entertaining story or topic.)	○	○	○

Expert Panel Questionnaire - Components & Measures (Cont.)



Section B: Scores for the measured components of Cyber Situational Awareness

Performance measures to assess cyber curiosity will involve measuring relevant aspects of the IS participant performance during the Web-based experiment (i.e. what actions selected by user). The proposed cyber curiosity user action selections are shown below. Please review and validate the proposed cyber curiosity measurements for each type of scenario.

SME Review and Validation of Cyber Curiosity - Scores for D-type and I-type actions *

Review and validate the following proposed cyber curiosity points for each user action selected. NOTE: For D-Type curiosity negative points will be assigned and for I-Type positive points will be assigned.

	1- Keep	2 - Adjust	3 - Remove
P2-B1. Simple explanation selected = -1 Point	○	○	○
P2-B2. In-depth explanation selected = -2 Points	○	○	○
P2-B3. Enticing Web link clicked = 1 Point	○	○	○
P2-B4. Enticing Pop-up Web Link clicked = 2 Point	○	○	○

Appendix E

Expert Panel Recruitment Email

Dear Cybersecurity Experts,

I need your assistance in providing expert feedback on set of measures for my upcoming doctoral research study. I am a Ph.D. Candidate in Information Assurance and Cybersecurity at the College of Engineering and Computing, Nova Southeastern University (NSU), working under the supervision of Professor Dr. Yair Levy. My research is seeking to develop a Cyber Risk taxonomy to classify maritime IS users by their level of cyber situational awareness (SA) and Cyber Curiosity of Information Systems (IS) users.

In this part of the research, I need your assistance in validating the proposed Cyber Risk Taxonomy components to help develop and empirically validate an IS cyber situational awareness (SA) taxonomy in the context of Cyber Curiosity that can be used as a benchmark to measure the susceptibility of mitigating a cyber-attack using social engineering techniques among IS users.

Below are definitions used in the research study:

- Cybersecurity – The protection of cyberspace, the electronic information, the infrastructure that supports cyberspace, and the users of cyberspace in their personal, societal, and national capacity including any of their interests that are vulnerable to attacks originating in cyberspace (Solms & Niekerk, 2013).

- Cyber Curiosity - Cyber Curiosity is the desire for information and knowledge about information systems (IS) and the Internet.

- Cyber Situational Awareness - The perception of cyber risk elements with respect to time and space, the understanding of their meaning, and anticipation of their status in the near future (Tadda & Salerno, 2010).

- Social engineering - A technique used by hackers, leveraging human interactions or social skills, to obtain or compromise IS information to infiltrate an organization's network (US-CERT, 2016).

- Subject Matter Expert (SME) – A highly knowledgeable individual who performs specialized functions in given organizational processes (Encyclopedia, n.d.).

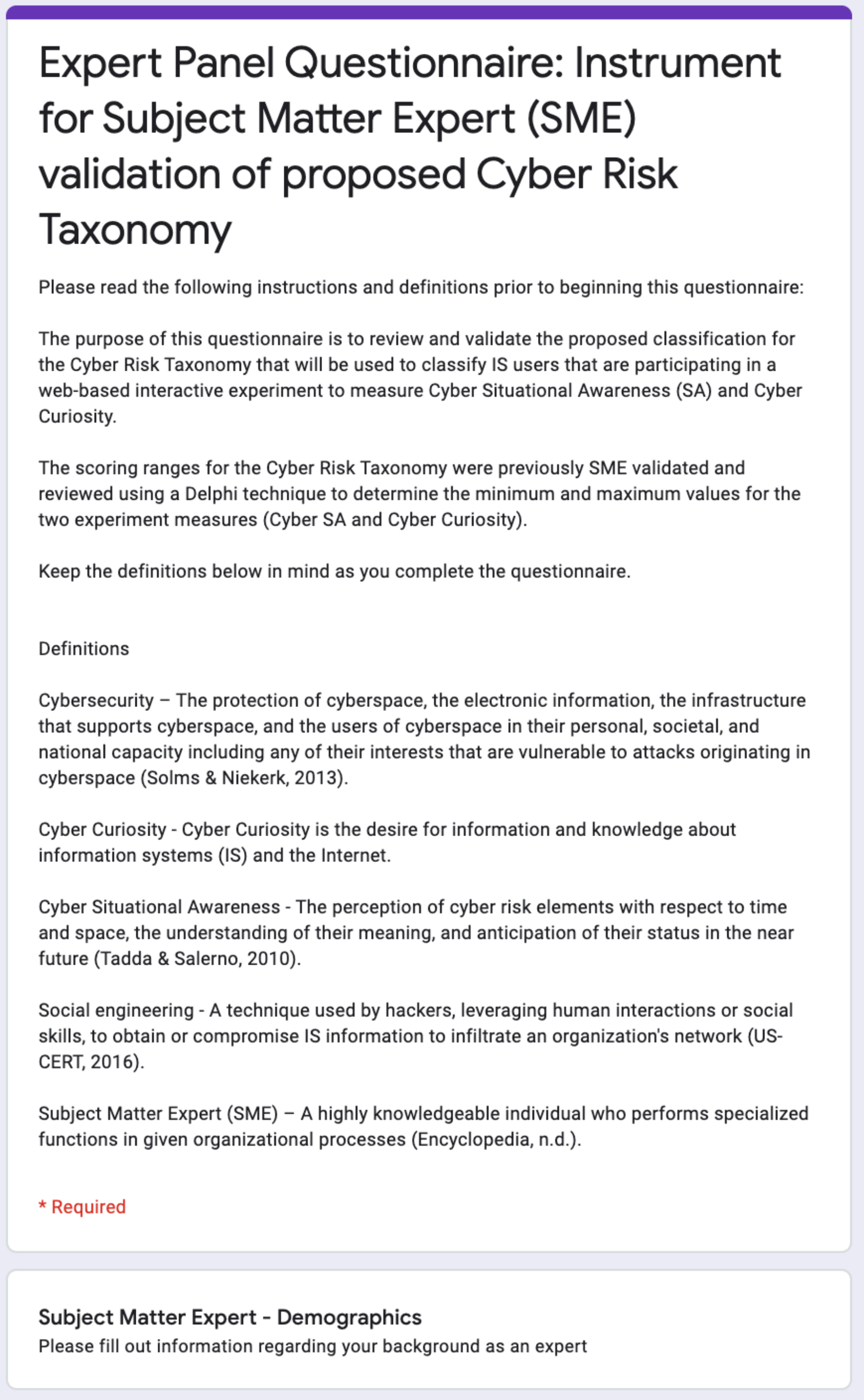
The information provided with your assistance will be used for this research study in aggregated form. No personally identifiable information (PII) will be collected. As a participate, you agree to keep all the information regarding this research confidential and refrain from disclosing any details related to this survey or the material contained within it.

Thank you in advance for your consideration. I appreciate your assistance and contribution for this research study.

Regards,
Guillermo Perez, Ph.D. Candidate
E-mail:gp90@mynsu.nova.edu
Information Assurance and Cybersecurity

Appendix F

Expert Panel Questionnaire: Instrument for Subject Matter Expert (SME) Validation of Proposed Cyber Risk Taxonomy



Expert Panel Questionnaire: Instrument for Subject Matter Expert (SME) validation of proposed Cyber Risk Taxonomy

Please read the following instructions and definitions prior to beginning this questionnaire:

The purpose of this questionnaire is to review and validate the proposed classification for the Cyber Risk Taxonomy that will be used to classify IS users that are participating in a web-based interactive experiment to measure Cyber Situational Awareness (SA) and Cyber Curiosity.

The scoring ranges for the Cyber Risk Taxonomy were previously SME validated and reviewed using a Delphi technique to determine the minimum and maximum values for the two experiment measures (Cyber SA and Cyber Curiosity).

Keep the definitions below in mind as you complete the questionnaire.

Definitions

Cybersecurity – The protection of cyberspace, the electronic information, the infrastructure that supports cyberspace, and the users of cyberspace in their personal, societal, and national capacity including any of their interests that are vulnerable to attacks originating in cyberspace (Solms & Niekerk, 2013).

Cyber Curiosity - Cyber Curiosity is the desire for information and knowledge about information systems (IS) and the Internet.

Cyber Situational Awareness - The perception of cyber risk elements with respect to time and space, the understanding of their meaning, and anticipation of their status in the near future (Tadda & Salerno, 2010).

Social engineering - A technique used by hackers, leveraging human interactions or social skills, to obtain or compromise IS information to infiltrate an organization's network (US-CERT, 2016).

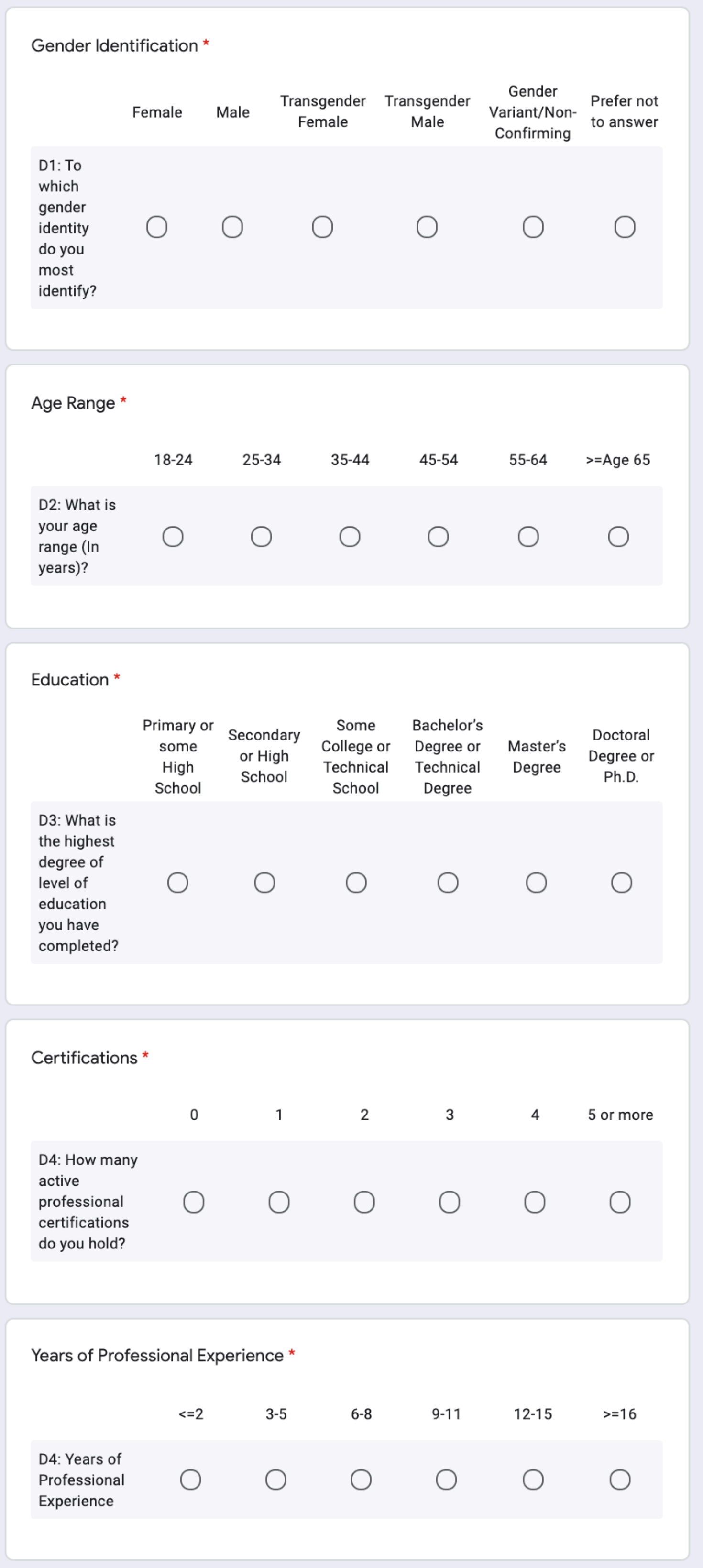
Subject Matter Expert (SME) – A highly knowledgeable individual who performs specialized functions in given organizational processes (Encyclopedia, n.d.).

* Required

Subject Matter Expert - Demographics

Please fill out information regarding your background as an expert

Expert Panel Questionnaire – Risk Taxonomy (Cont.)



Gender Identification *

	Female	Male	Transgender Female	Transgender Male	Gender Variant/Non-Confirming	Prefer not to answer
D1: To which gender identity do you most identify?	○	○	○	○	○	○

Age Range *

	18-24	25-34	35-44	45-54	55-64	>=Age 65
D2: What is your age range (In years)?	○	○	○	○	○	○

Education *

	Primary or some High School	Secondary or High School	Some College or Technical School	Bachelor's Degree or Technical Degree	Master's Degree	Doctoral Degree or Ph.D.
D3: What is the highest degree of level of education you have completed?	○	○	○	○	○	○

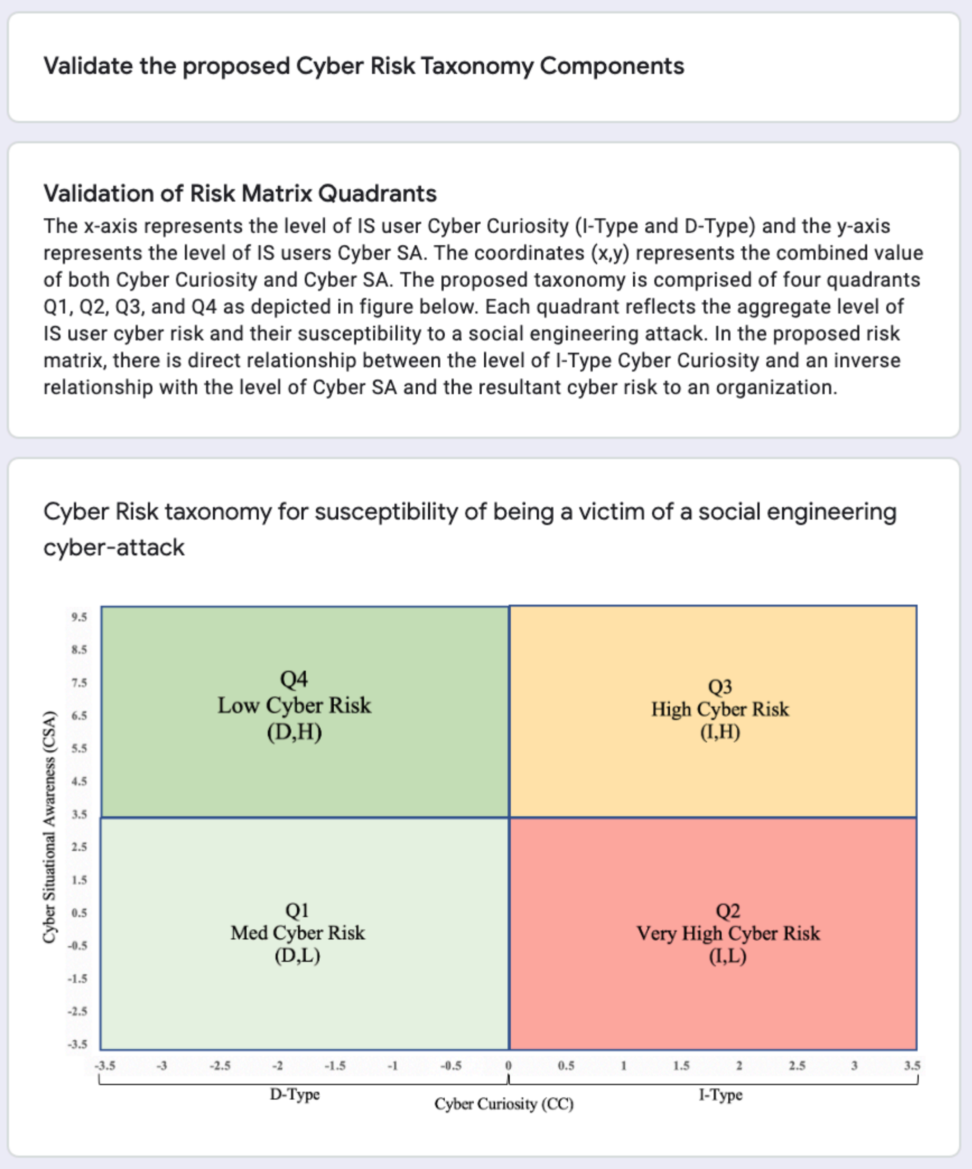
Certifications *

	0	1	2	3	4	5 or more
D4: How many active professional certifications do you hold?	○	○	○	○	○	○

Years of Professional Experience *

	<=2	3-5	6-8	9-11	12-15	>=16
D4: Years of Professional Experience	○	○	○	○	○	○

Expert Panel Questionnaire – Risk Taxonomy (Cont.)



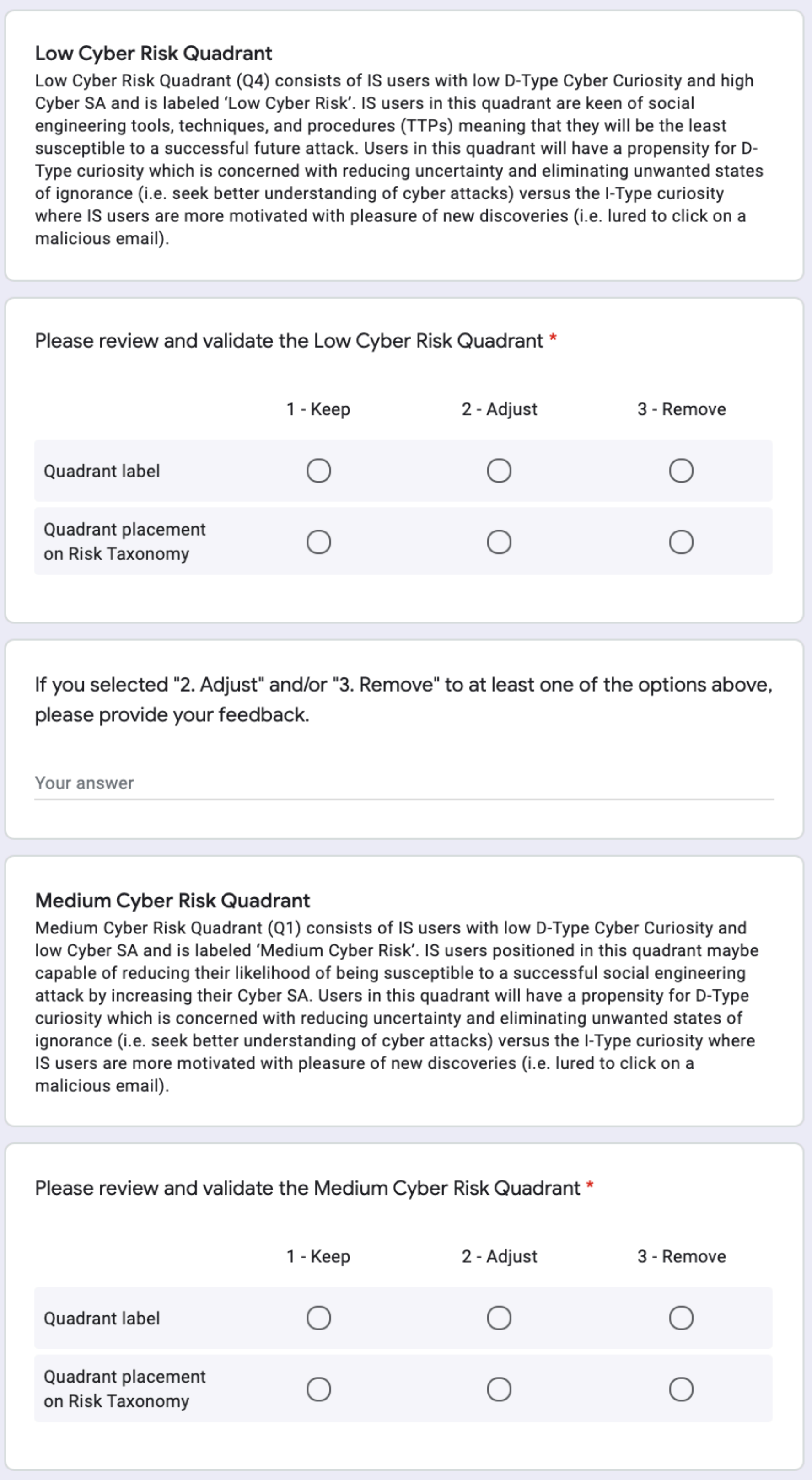
Validate the proposed Cyber Risk Taxonomy Components

Validation of Risk Matrix Quadrants

The x-axis represents the level of IS user Cyber Curiosity (I-Type and D-Type) and the y-axis represents the level of IS users Cyber SA. The coordinates (x,y) represents the combined value of both Cyber Curiosity and Cyber SA. The proposed taxonomy is comprised of four quadrants Q1, Q2, Q3, and Q4 as depicted in figure below. Each quadrant reflects the aggregate level of IS user cyber risk and their susceptibility to a social engineering attack. In the proposed risk matrix, there is direct relationship between the level of I-Type Cyber Curiosity and an inverse relationship with the level of Cyber SA and the resultant cyber risk to an organization.

Cyber Risk taxonomy for susceptibility of being a victim of a social engineering cyber-attack

Expert Panel Questionnaire – Risk Taxonomy (Cont.)



Low Cyber Risk Quadrant

Low Cyber Risk Quadrant (Q4) consists of IS users with low D-Type Cyber Curiosity and high Cyber SA and is labeled 'Low Cyber Risk'. IS users in this quadrant are keen of social engineering tools, techniques, and procedures (TTPs) meaning that they will be the least susceptible to a successful future attack. Users in this quadrant will have a propensity for D-Type curiosity which is concerned with reducing uncertainty and eliminating unwanted states of ignorance (i.e. seek better understanding of cyber attacks) versus the I-Type curiosity where IS users are more motivated with pleasure of new discoveries (i.e. lured to click on a malicious email).

Please review and validate the Low Cyber Risk Quadrant *

	1 - Keep	2 - Adjust	3 - Remove
Quadrant label	○	○	○
Quadrant placement on Risk Taxonomy	○	○	○

If you selected "2. Adjust" and/or "3. Remove" to at least one of the options above, please provide your feedback.

Your answer

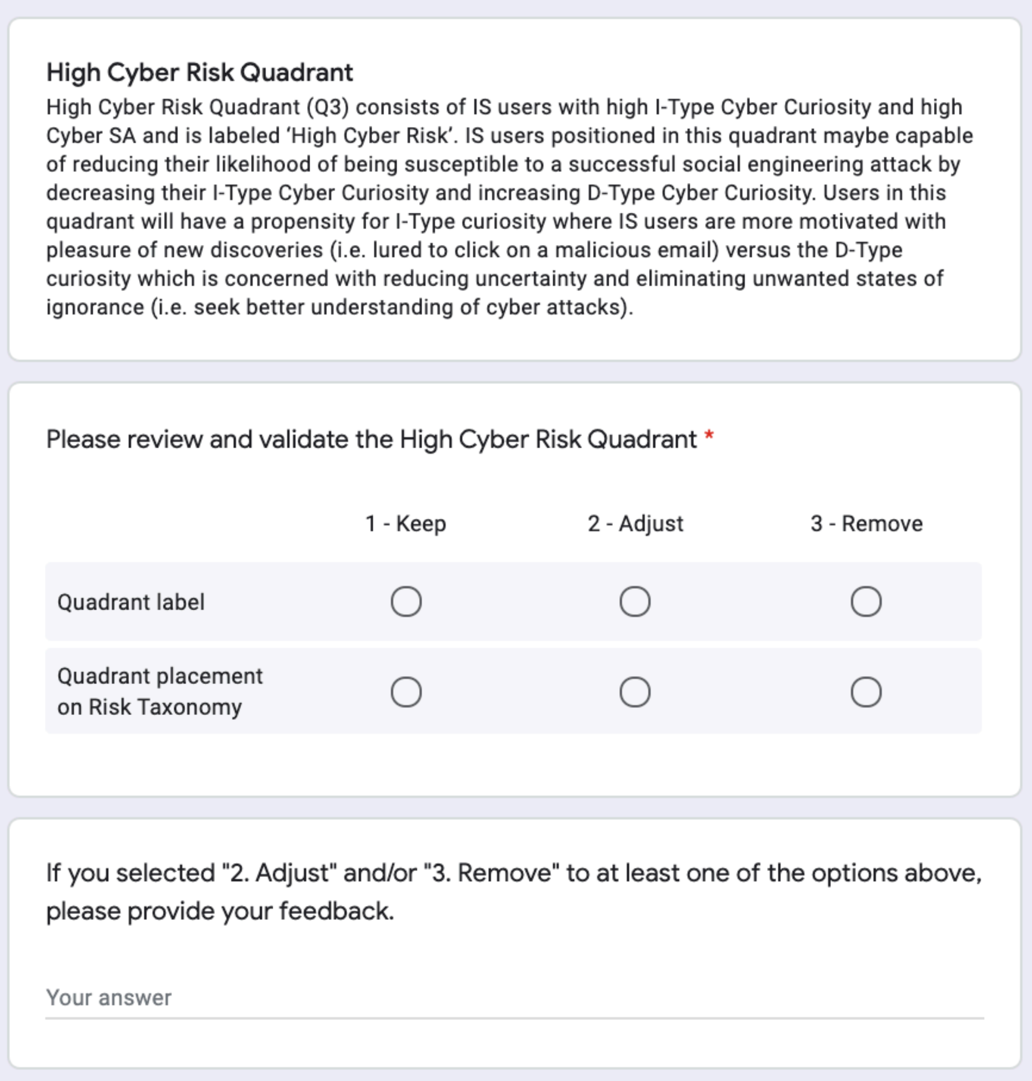
Medium Cyber Risk Quadrant

Medium Cyber Risk Quadrant (Q1) consists of IS users with low D-Type Cyber Curiosity and low Cyber SA and is labeled 'Medium Cyber Risk'. IS users positioned in this quadrant maybe capable of reducing their likelihood of being susceptible to a successful social engineering attack by increasing their Cyber SA. Users in this quadrant will have a propensity for D-Type curiosity which is concerned with reducing uncertainty and eliminating unwanted states of ignorance (i.e. seek better understanding of cyber attacks) versus the I-Type curiosity where IS users are more motivated with pleasure of new discoveries (i.e. lured to click on a malicious email).

Please review and validate the Medium Cyber Risk Quadrant *

	1 - Keep	2 - Adjust	3 - Remove
Quadrant label	○	○	○
Quadrant placement on Risk Taxonomy	○	○	○
)

Expert Panel Questionnaire – Risk Taxonomy (Cont.)



High Cyber Risk Quadrant

High Cyber Risk Quadrant (Q3) consists of IS users with high I-Type Cyber Curiosity and high Cyber SA and is labeled 'High Cyber Risk'. IS users positioned in this quadrant maybe capable of reducing their likelihood of being susceptible to a successful social engineering attack by decreasing their I-Type Cyber Curiosity and increasing D-Type Cyber Curiosity. Users in this quadrant will have a propensity for I-Type curiosity where IS users are more motivated with pleasure of new discoveries (i.e. lured to click on a malicious email) versus the D-Type curiosity which is concerned with reducing uncertainty and eliminating unwanted states of ignorance (i.e. seek better understanding of cyber attacks).

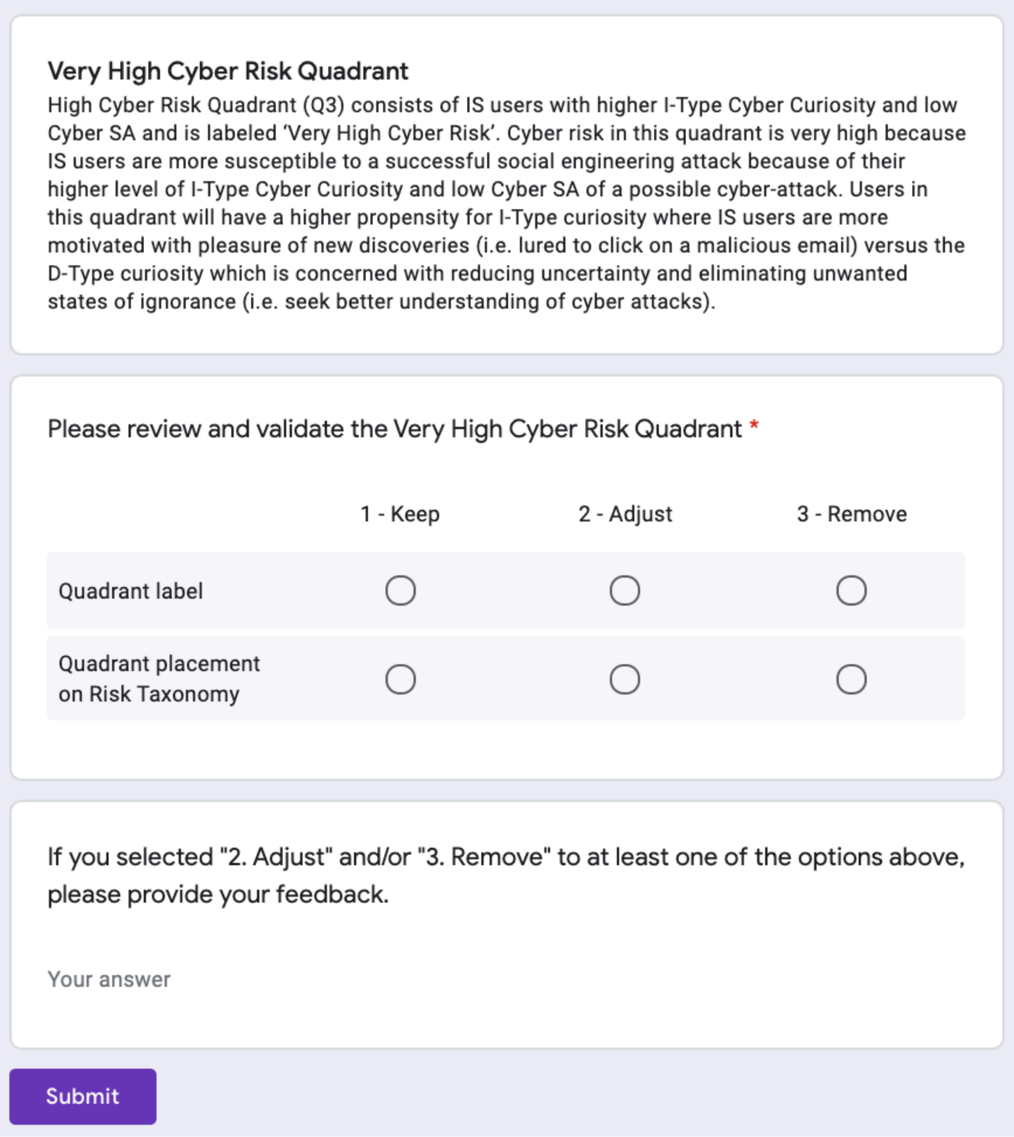
Please review and validate the High Cyber Risk Quadrant *

	1 - Keep	2 - Adjust	3 - Remove
Quadrant label	○	○	○
Quadrant placement on Risk Taxonomy	○	○	○

If you selected "2. Adjust" and/or "3. Remove" to at least one of the options above, please provide your feedback.

Your answer

Expert Panel Questionnaire – Risk Taxonomy (Cont.)



Very High Cyber Risk Quadrant

High Cyber Risk Quadrant (Q3) consists of IS users with higher I-Type Cyber Curiosity and low Cyber SA and is labeled 'Very High Cyber Risk'. Cyber risk in this quadrant is very high because IS users are more susceptible to a successful social engineering attack because of their higher level of I-Type Cyber Curiosity and low Cyber SA of a possible cyber-attack. Users in this quadrant will have a higher propensity for I-Type curiosity where IS users are more motivated with pleasure of new discoveries (i.e. lured to click on a malicious email) versus the D-Type curiosity which is concerned with reducing uncertainty and eliminating unwanted states of ignorance (i.e. seek better understanding of cyber attacks).

Please review and validate the Very High Cyber Risk Quadrant *

	1 - Keep	2 - Adjust	3 - Remove
Quadrant label	○	○	○
Quadrant placement on Risk Taxonomy	○	○	○

If you selected "2. Adjust" and/or "3. Remove" to at least one of the options above, please provide your feedback.

Your answer

Appendix G

Pilot Research Study Recruitment Email

Dear Cybersecurity Experts,

I need your assistance in a pilot research study in fulfillment of my doctoral research study. I am a Ph.D. Candidate in Information Assurance and Cybersecurity at the College of Engineering and Computing, Nova Southeastern University (NSU), working under the supervision of Professor Dr. Yair Levy. My research is seeking to develop a Cyber Risk taxonomy to classify maritime IS users by their level of cyber situational awareness (SA) and Cyber Curiosity of Information Systems (IS) users.

In this part of the research, I need your assistance to ensure the interactive Web-based experiment is working accurately. The experiment will measure cyber situational awareness (CSA) and Cyber Curiosity levels to help develop and empirically validate an IS cyber situational awareness (SA) taxonomy in the context of Cyber Curiosity that can be used as a benchmark to measure the susceptibility of mitigating a cyber-attack using social engineering techniques among IS users.

Below are definitions used in the research study:

- Cybersecurity – The protection of cyberspace, the electronic information, the infrastructure that supports cyberspace, and the users of cyberspace in their personal, societal, and national capacity including any of their interests that are vulnerable to attacks originating in cyberspace (Solms & Niekerk, 2013).

- Cyber Situational Awareness - The perception of cyber risk elements with respect to time and space, the understanding of their meaning, and anticipation of their status in the near future (Tadda & Salerno, 2010).

- Cyber Curiosity - Cyber Curiosity is the desire for information and knowledge about information systems (IS) and the Internet.

- Social engineering - A technique used by hackers, leveraging human interactions or social skills, to obtain or compromise IS information to infiltrate an organizations network (US-CERT, 2016).

The information provided with your assistance will be used for this research study in aggregated form. No personally identifiable information (PII) will be collected. As a participate, you agree to keep all the information regarding this research confidential and refrain from disclosing any details related to this survey or the material contained within it.

Pilot Research Study Recruitment Email (Cont.)

If you are willing to participate, please reply to this email and we will schedule an appointment.

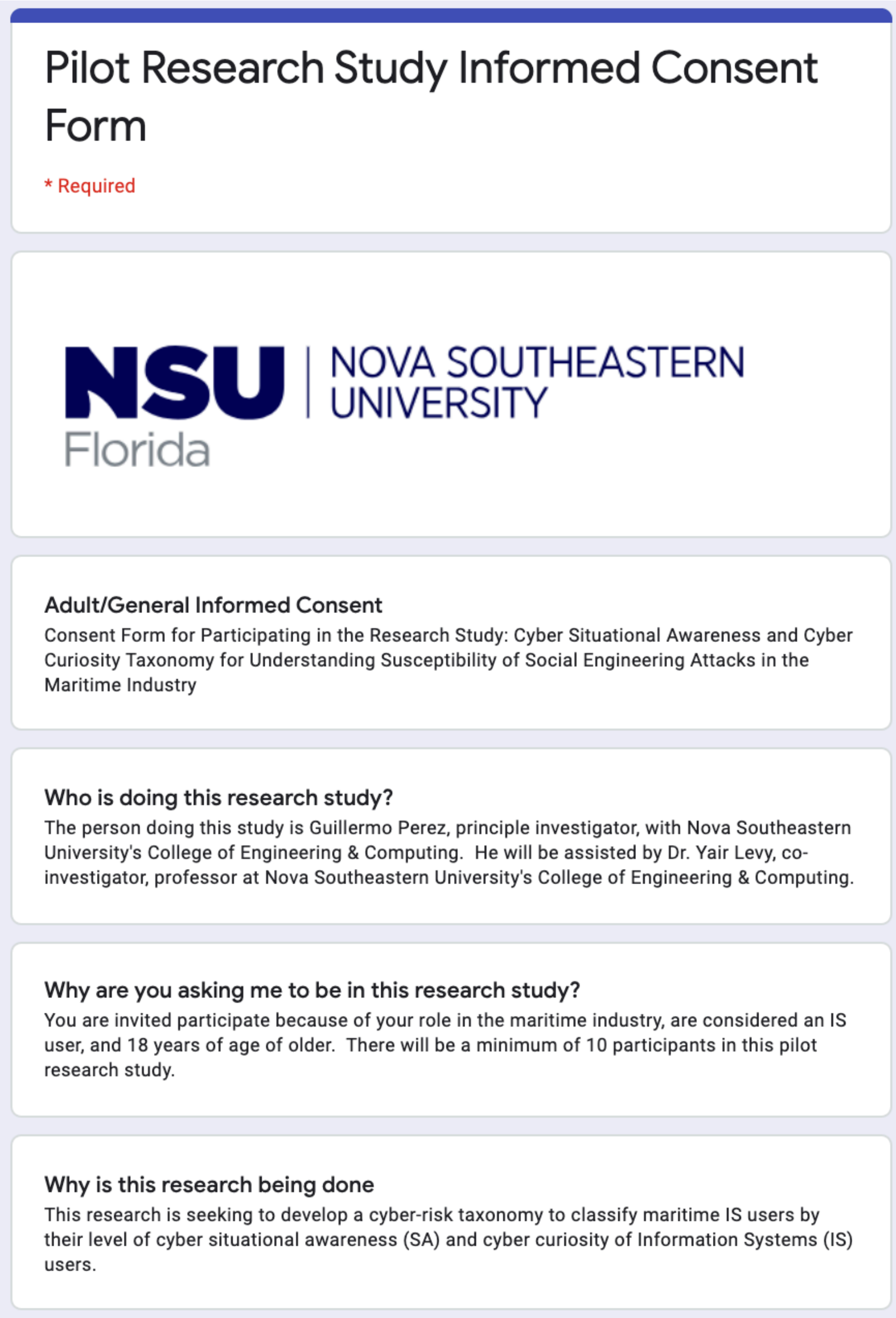
Thank you in advance for your consideration. I appreciate your assistance and contribution for this research study.

Should you wish to receive the findings of the study, please send me an email and I will gladly provide you with the information about the academic research publication(s) resulting from this study.

Regards,
Guillermo Perez, Ph.D. Candidate
E-mail:gp90@mynsu.nova.edu
Information Assurance and Cybersecurity

Appendix H

Pilot Study Informed Consent Form



Pilot Research Study Informed Consent Form

* Required

Adult/General Informed Consent

Consent Form for Participating in the Research Study: Cyber Situational Awareness and Cyber Curiosity Taxonomy for Understanding Susceptibility of Social Engineering Attacks in the Maritime Industry

Who is doing this research study?

The person doing this study is Guillermo Perez, principle investigator, with Nova Southeastern University's College of Engineering & Computing. He will be assisted by Dr. Yair Levy, co-investigator, professor at Nova Southeastern University's College of Engineering & Computing.

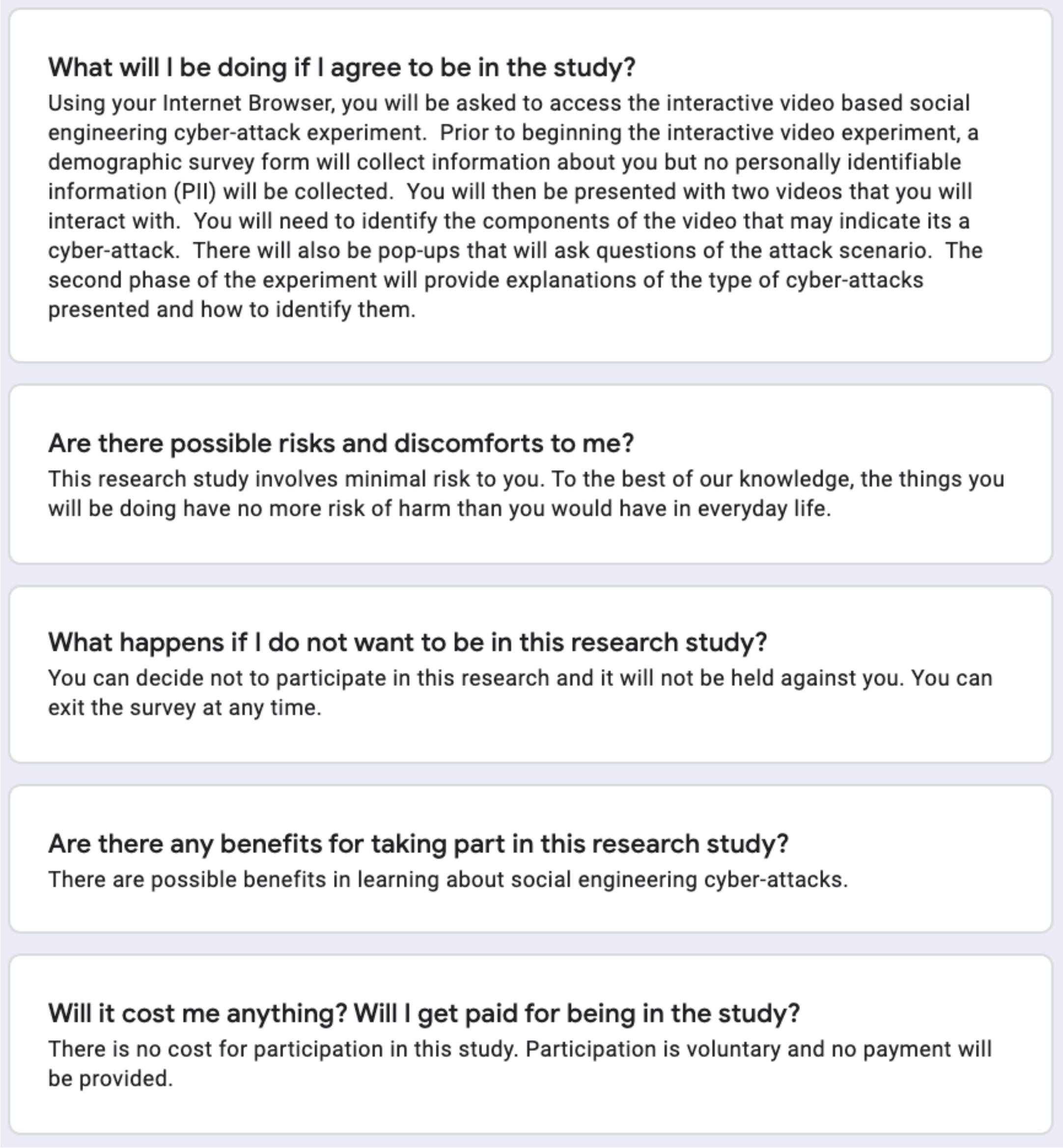
Why are you asking me to be in this research study?

You are invited participate because of your role in the maritime industry, are considered an IS user, and 18 years of age of older. There will be a minimum of 10 participants in this pilot research study.

Why is this research being done

This research is seeking to develop a cyber-risk taxonomy to classify maritime IS users by their level of cyber situational awareness (SA) and cyber curiosity of Information Systems (IS) users.

Pilot Study Informed Consent Form (Cont.)



What will I be doing if I agree to be in the study?

Using your Internet Browser, you will be asked to access the interactive video based social engineering cyber-attack experiment. Prior to beginning the interactive video experiment, a demographic survey form will collect information about you but no personally identifiable information (PII) will be collected. You will then be presented with two videos that you will interact with. You will need to identify the components of the video that may indicate its a cyber-attack. There will also be pop-ups that will ask questions of the attack scenario. The second phase of the experiment will provide explanations of the type of cyber-attacks presented and how to identify them.

Are there possible risks and discomforts to me?

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

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

You can decide not to participate in this research and it will not be held against you. You can exit the survey at any time.

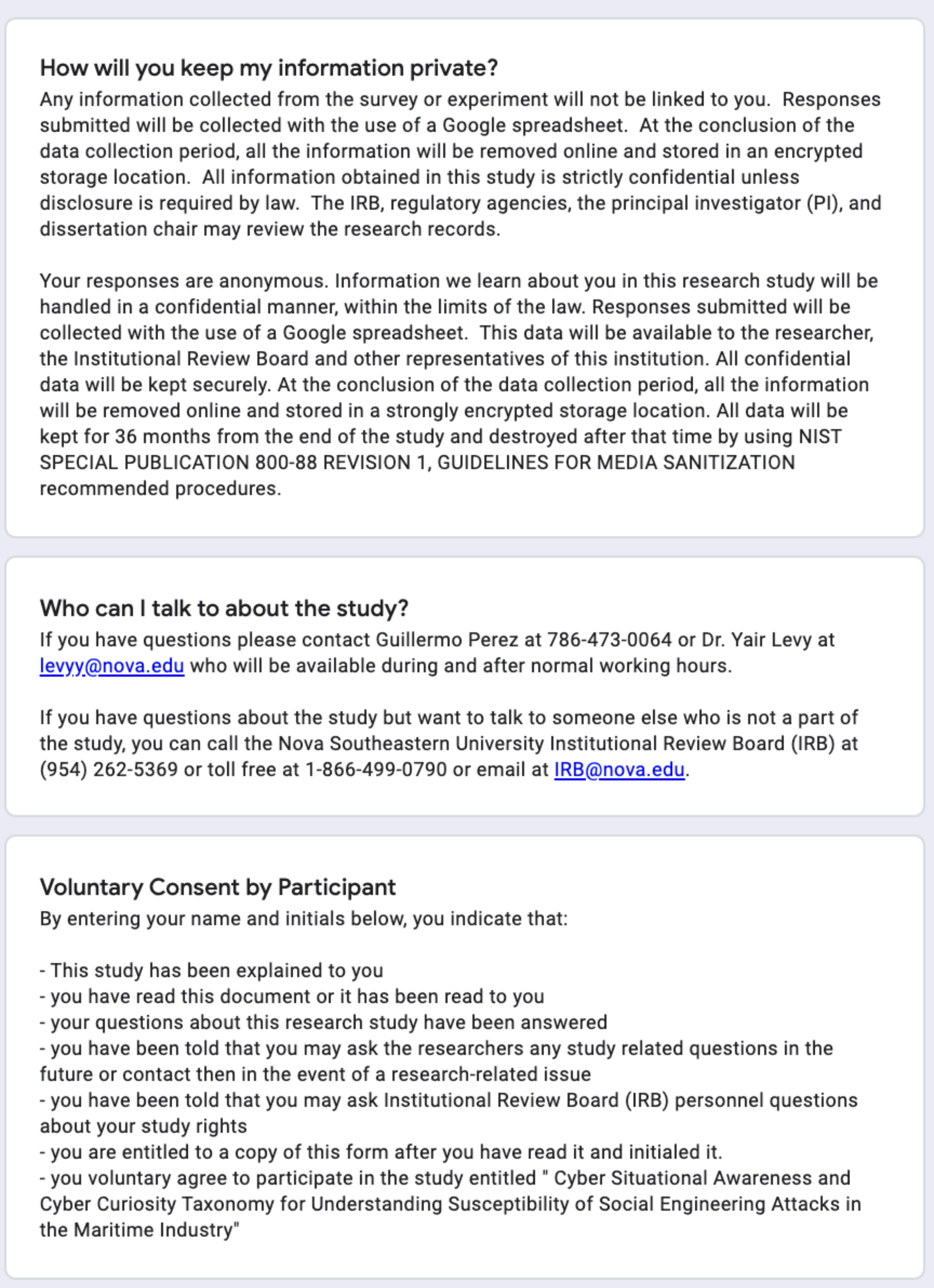
Are there any benefits for taking part in this research study?

There are possible benefits in learning about social engineering cyber-attacks.

Will it cost me anything? Will I get paid for being in the study?

There is no cost for participation in this study. Participation is voluntary and no payment will be provided.

Pilot Study Informed Consent Form (Cont.)



How will you keep my information private?

Any information collected from the survey or experiment will not be linked to you. Responses submitted will be collected with the use of a Google spreadsheet. At the conclusion of the data collection period, all the information will be removed online and stored in an encrypted storage location. All information obtained in this study is strictly confidential unless disclosure is required by law. The IRB, regulatory agencies, the principal investigator (PI), and dissertation chair may review the research records.

Your responses are anonymous. Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law. Responses submitted will be collected with the use of a Google spreadsheet. This data will be available to the researcher, the Institutional Review Board and other representatives of this institution. All confidential data will be kept securely. At the conclusion of the data collection period, all the information will be removed online and stored in a strongly encrypted storage location. All data will be kept for 36 months from the end of the study and destroyed after that time by using NIST SPECIAL PUBLICATION 800-88 REVISION 1, GUIDELINES FOR MEDIA SANITIZATION recommended procedures.

Who can I talk to about the study?

If you have questions please contact Guillermo Perez at 786-473-0064 or Dr. Yair Levy at levyy@nova.edu who will be available during and after normal working hours.

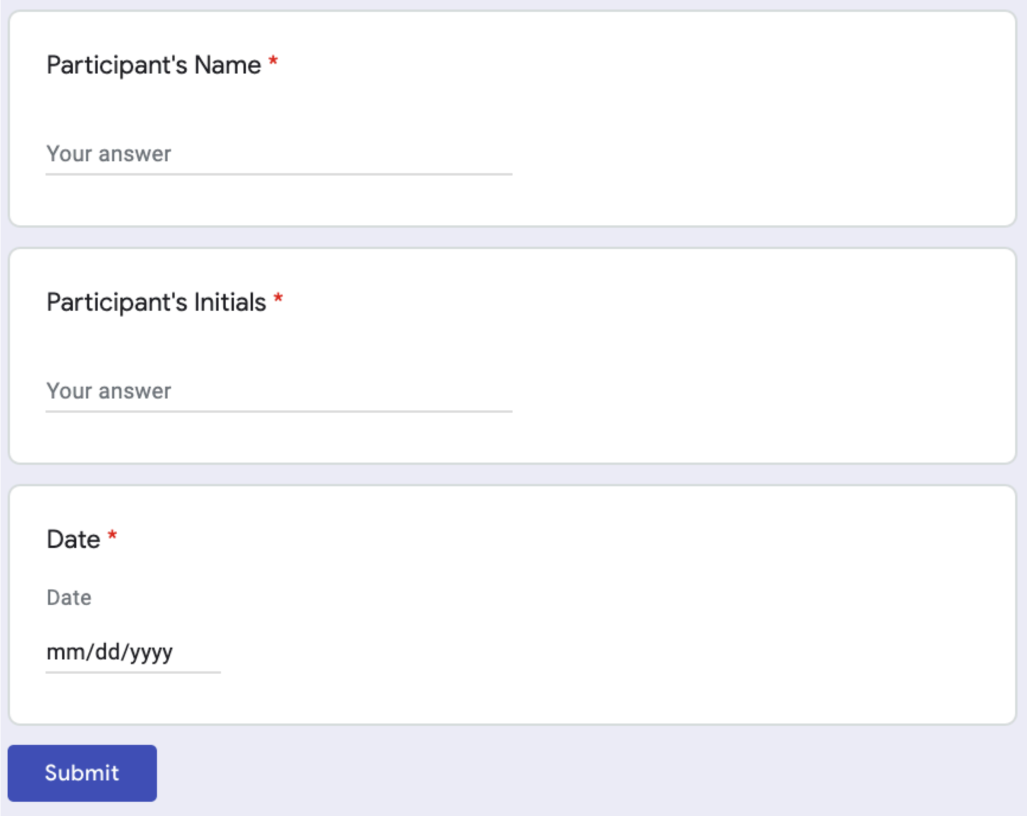
If you have questions about the study but want to talk to someone else who is not a part of the study, you can call the Nova Southeastern University Institutional Review Board (IRB) at (954) 262-5369 or toll free at 1-866-499-0790 or email at IRB@nova.edu.

Voluntary Consent by Participant

By entering your name and initials below, you indicate that:

- This study has been explained to you
- you have read this document or it has been read to you
- your questions about this research study have been answered
- you have been told that you may ask the researchers any study related questions in the future or contact then in the event of a research-related issue
- you have been told that you may ask Institutional Review Board (IRB) personnel questions about your study rights
- you are entitled to a copy of this form after you have read it and initialed it.
- you voluntary agree to participate in the study entitled " Cyber Situational Awareness and Cyber Curiosity Taxonomy for Understanding Susceptibility of Social Engineering Attacks in the Maritime Industry"

Pilot Study Informed Consent Form (Cont.)



Participant's Name *

Your answer

Participant's Initials *

Your answer

Date *

Date

mm/dd/yyyy

Appendix I

Research Study Recruitment Email

Dear Potential Research Participants,

I am a Ph.D. Candidate in Information Assurance and Cybersecurity at the College of Engineering and Computing, Nova Southeastern University (NSU), working under the supervision of Professor Dr. Yair Levy. I am reaching out to you to voluntarily take part in my research that is seeking to develop a Cyber Risk taxonomy to classify maritime Information Systems (IS) users by their level of cyber situational awareness (SA) and Cyber Curiosity.

Your participation will include filling out a pre-experiment survey and then interacting with a Web-based application. The information provided with your assistance will be used for this research study in aggregated form. No personally identifiable information (PII) will be collected. As a participate, you agree to keep all the information regarding this research confidential and refrain from disclosing any details related to this survey or the material contained within it.

If you are willing to participate, please reply to this email and we will schedule an appointment.

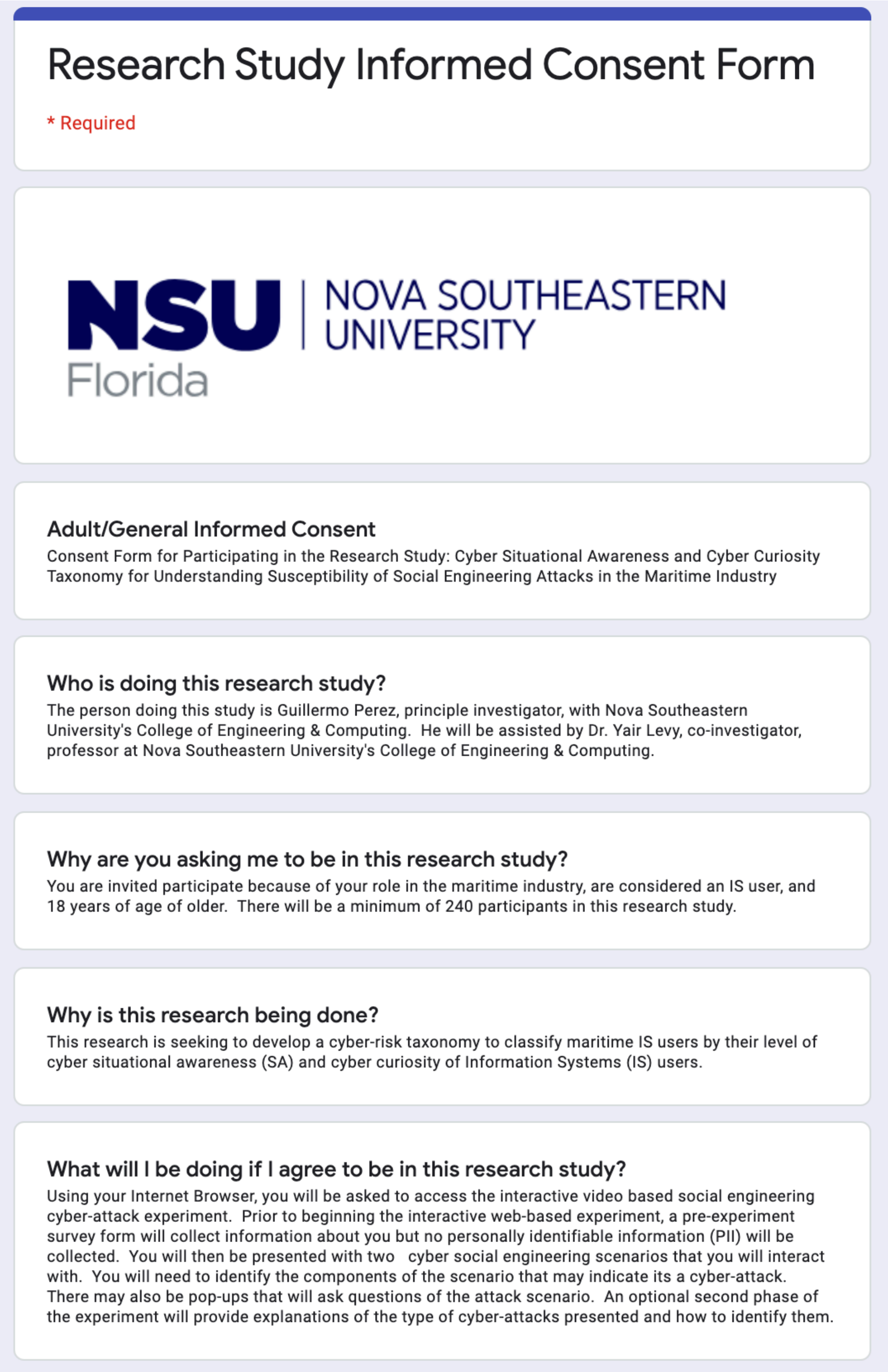
Thank you in advance for your consideration. I appreciate your assistance and contribution for this research study.

Should you wish to receive the findings of the study, please send me an email and I will gladly provide you with the information about the academic research publication(s) resulting from this study.

Regards,
Guillermo Perez, Ph.D. Candidate
E-mail:gp90@mynsu.nova.edu
Information Assurance and Cybersecurity

Appendix J

Research Study Informed Consent Form



Research Study Informed Consent Form

* Required

NSU | NOVA SOUTHEASTERN UNIVERSITY
Florida

Adult/General Informed Consent

Consent Form for Participating in the Research Study: Cyber Situational Awareness and Cyber Curiosity Taxonomy for Understanding Susceptibility of Social Engineering Attacks in the Maritime Industry

Who is doing this research study?

The person doing this study is Guillermo Perez, principle investigator, with Nova Southeastern University's College of Engineering & Computing. He will be assisted by Dr. Yair Levy, co-investigator, professor at Nova Southeastern University's College of Engineering & Computing.

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

You are invited participate because of your role in the maritime industry, are considered an IS user, and 18 years of age of older. There will be a minimum of 240 participants in this research study.

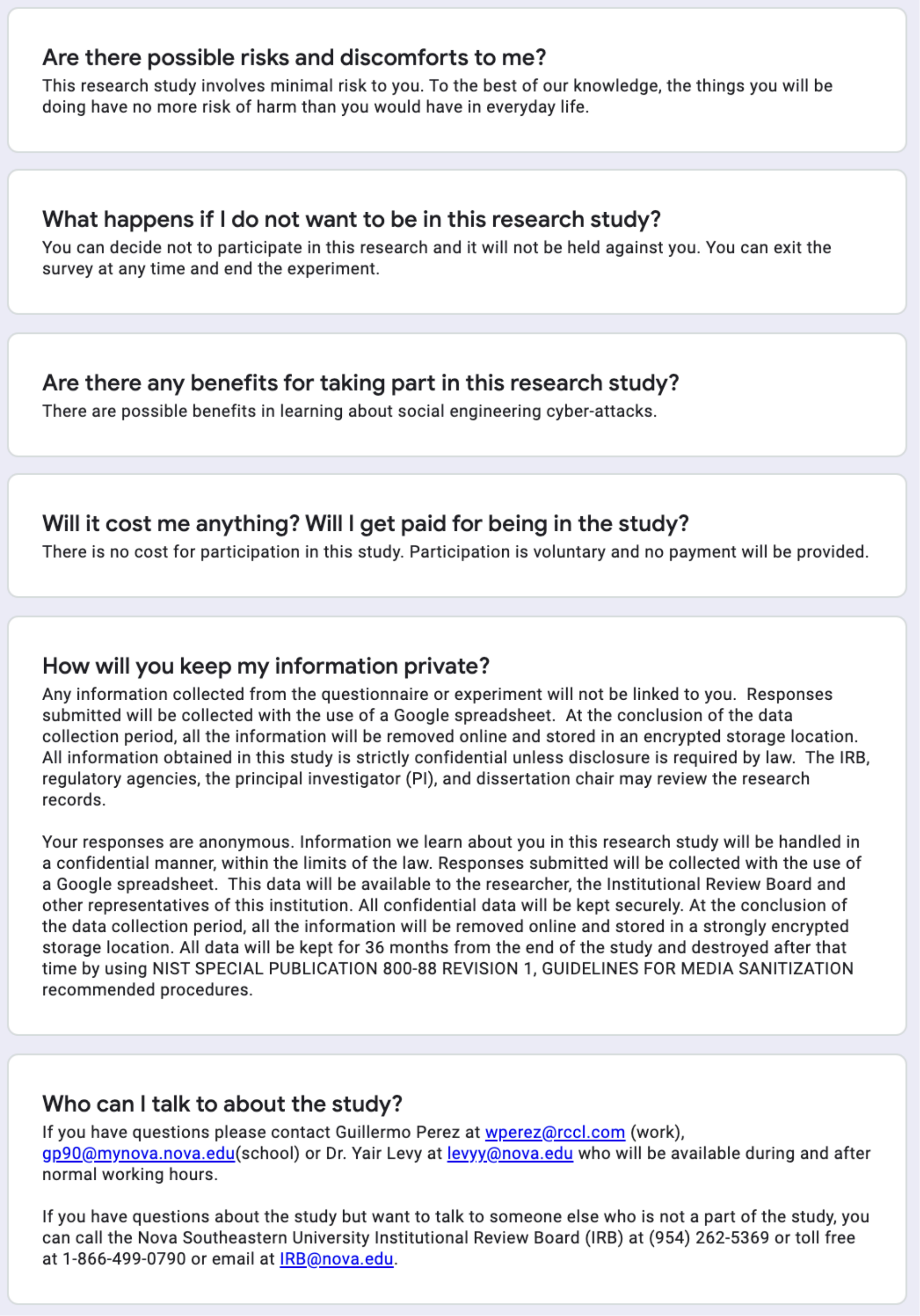
Why is this research being done?

This research is seeking to develop a cyber-risk taxonomy to classify maritime IS users by their level of cyber situational awareness (SA) and cyber curiosity of Information Systems (IS) users.

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

Using your Internet Browser, you will be asked to access the interactive video based social engineering cyber-attack experiment. Prior to beginning the interactive web-based experiment, a pre-experiment survey form will collect information about you but no personally identifiable information (PII) will be collected. You will then be presented with two cyber social engineering scenarios that you will interact with. You will need to identify the components of the scenario that may indicate its a cyber-attack. There may also be pop-ups that will ask questions of the attack scenario. An optional second phase of the experiment will provide explanations of the type of cyber-attacks presented and how to identify them.

Research Study Informed Consent Form (Cont.)



Are there possible risks and discomforts to me?

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

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

You can decide not to participate in this research and it will not be held against you. You can exit the survey at any time and end the experiment.

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

There are possible benefits in learning about social engineering cyber-attacks.

Will it cost me anything? Will I get paid for being in the study?

There is no cost for participation in this study. Participation is voluntary and no payment will be provided.

How will you keep my information private?

Any information collected from the questionnaire or experiment will not be linked to you. Responses submitted will be collected with the use of a Google spreadsheet. At the conclusion of the data collection period, all the information will be removed online and stored in an encrypted storage location. All information obtained in this study is strictly confidential unless disclosure is required by law. The IRB, regulatory agencies, the principal investigator (PI), and dissertation chair may review the research records.

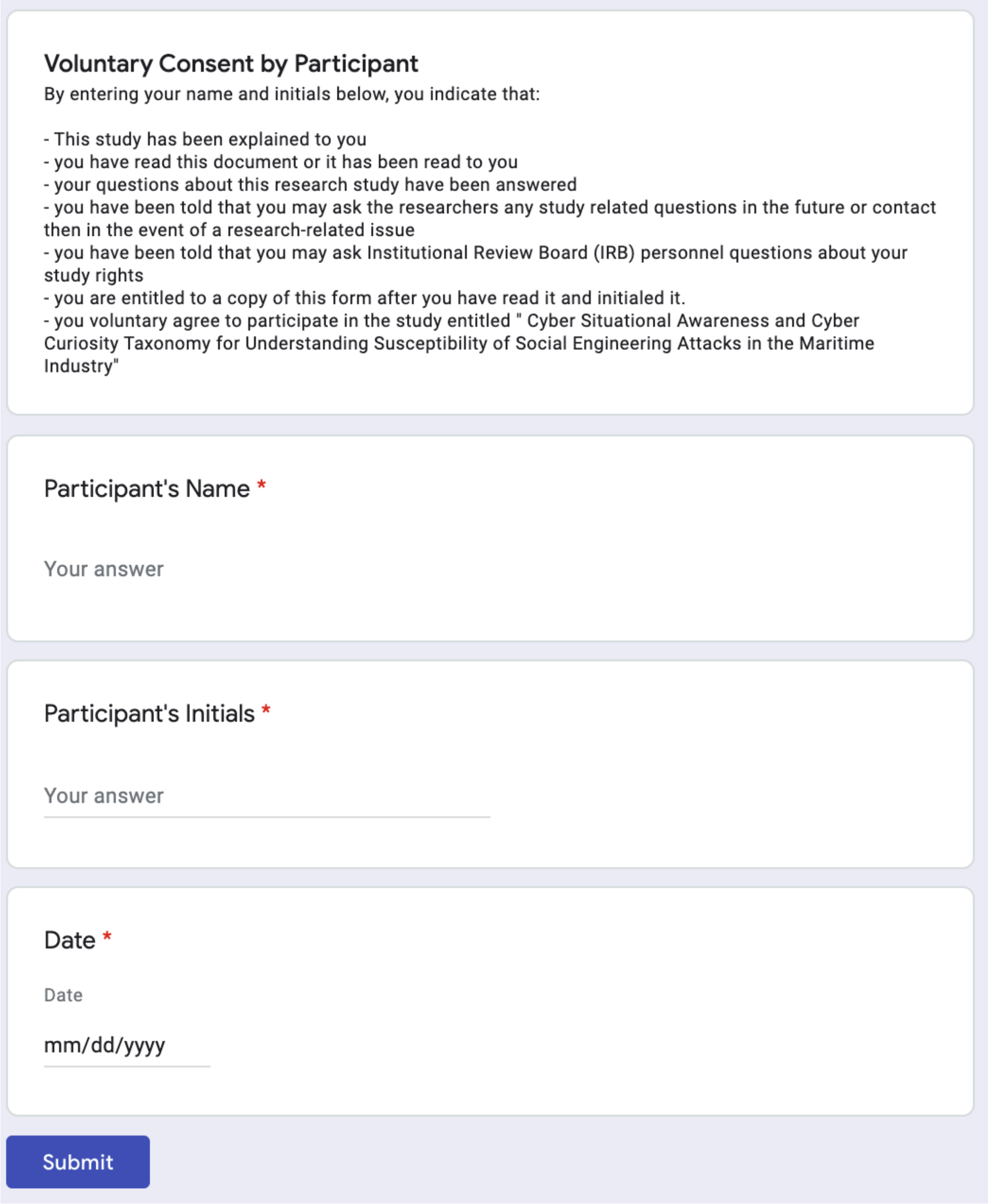
Your responses are anonymous. Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law. Responses submitted will be collected with the use of a Google spreadsheet. This data will be available to the researcher, the Institutional Review Board and other representatives of this institution. All confidential data will be kept securely. At the conclusion of the data collection period, all the information will be removed online and stored in a strongly encrypted storage location. All data will be kept for 36 months from the end of the study and destroyed after that time by using NIST SPECIAL PUBLICATION 800-88 REVISION 1, GUIDELINES FOR MEDIA SANITIZATION recommended procedures.

Who can I talk to about the study?

If you have questions please contact Guillermo Perez at wperez@rccl.com (work), gp90@mynova.nova.edu(school) or Dr. Yair Levy at levyy@nova.edu who will be available during and after normal working hours.

If you have questions about the study but want to talk to someone else who is not a part of the study, you can call the Nova Southeastern University Institutional Review Board (IRB) at (954) 262-5369 or toll free at 1-866-499-0790 or email at IRB@nova.edu.

Research Study Informed Consent Form (Cont.)



Voluntary Consent by Participant

By entering your name and initials below, you indicate that:

- This study has been explained to you
- you have read this document or it has been read to you
- your questions about this research study have been answered
- you have been told that you may ask the researchers any study related questions in the future or contact then in the event of a research-related issue
- you have been told that you may ask Institutional Review Board (IRB) personnel questions about your study rights
- you are entitled to a copy of this form after you have read it and initialed it.
- you voluntary agree to participate in the study entitled " Cyber Situational Awareness and Cyber Curiosity Taxonomy for Understanding Susceptibility of Social Engineering Attacks in the Maritime Industry"

Participant's Name *

Your answer

Participant's Initials *

Your answer

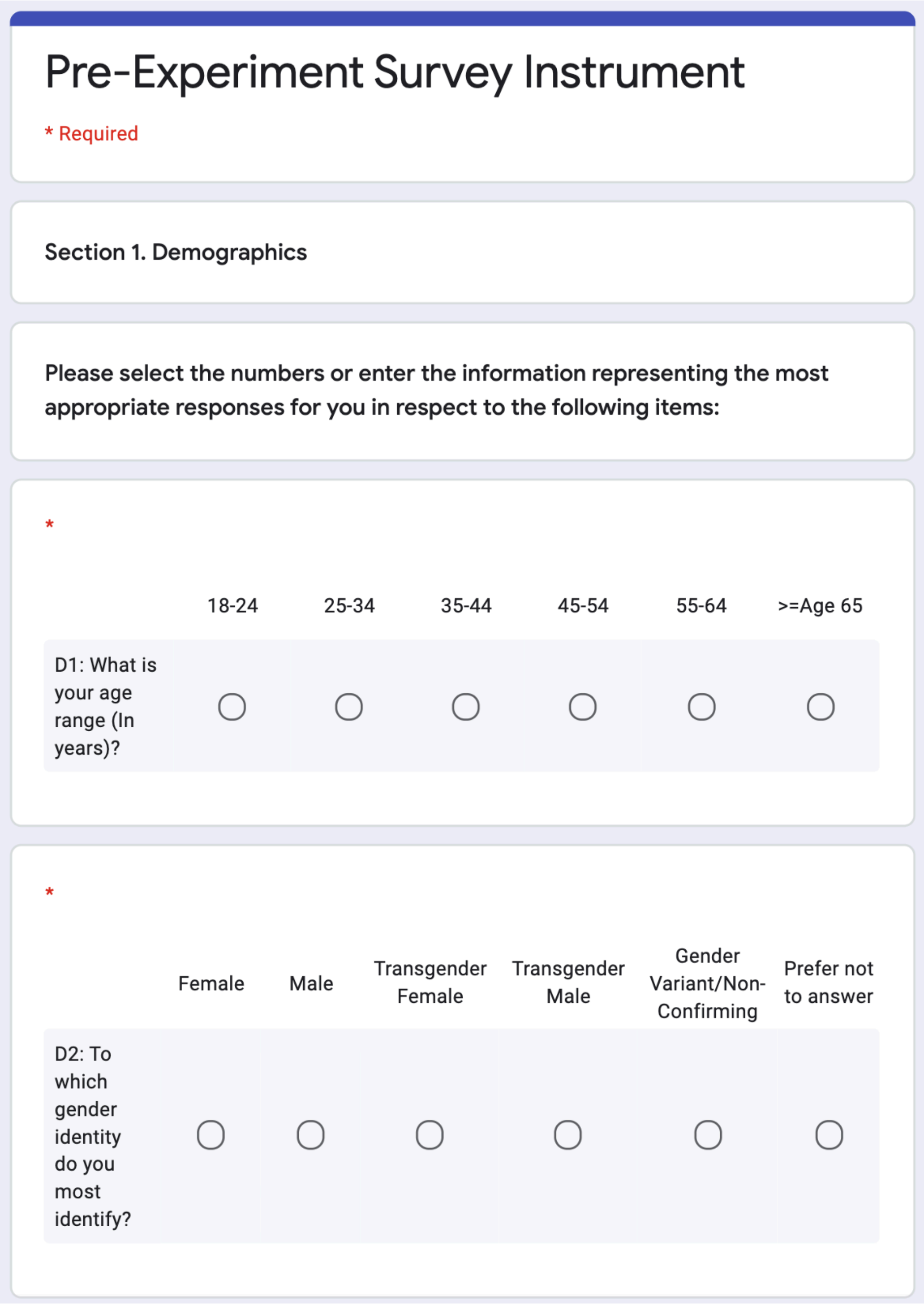
Date *

Date

mm/dd/yyyy

Appendix K

Pre-Experiment Survey Instrument (Shipboard)



Pre-Experiment Survey Instrument

* Required

Section 1. Demographics

Please select the numbers or enter the information representing the most appropriate responses for you in respect to the following items:

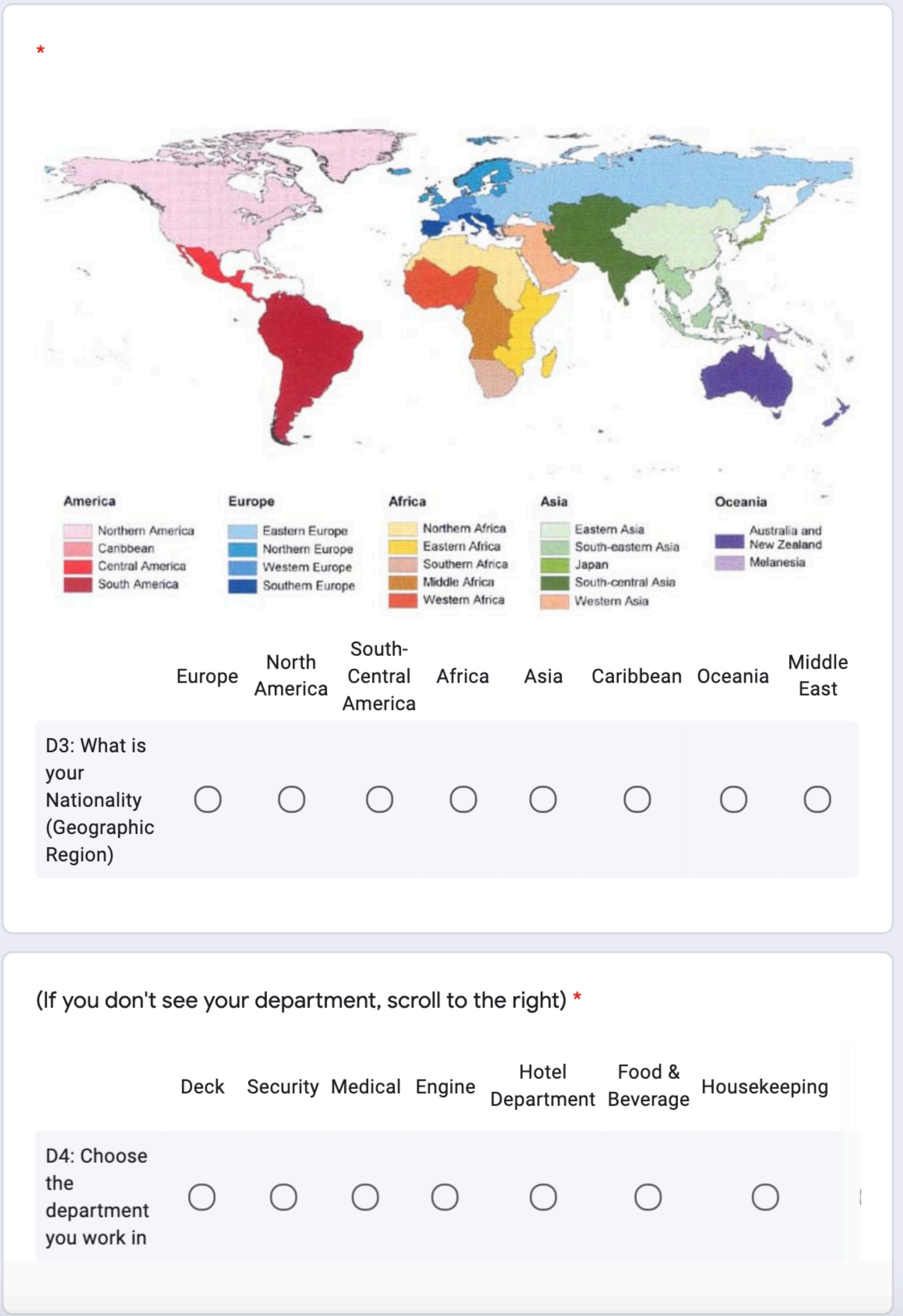
*

	18-24	25-34	35-44	45-54	55-64	>=Age 65
D1: What is your age range (In years)?	○	○	○	○	○	○

*

	Female	Male	Transgender Female	Transgender Male	Gender Variant/Non-Confirming	Prefer not to answer
D2: To which gender identity do you most identify?	○	○	○	○	○	○

Pre-Experiment Survey Instrument (Cont.)



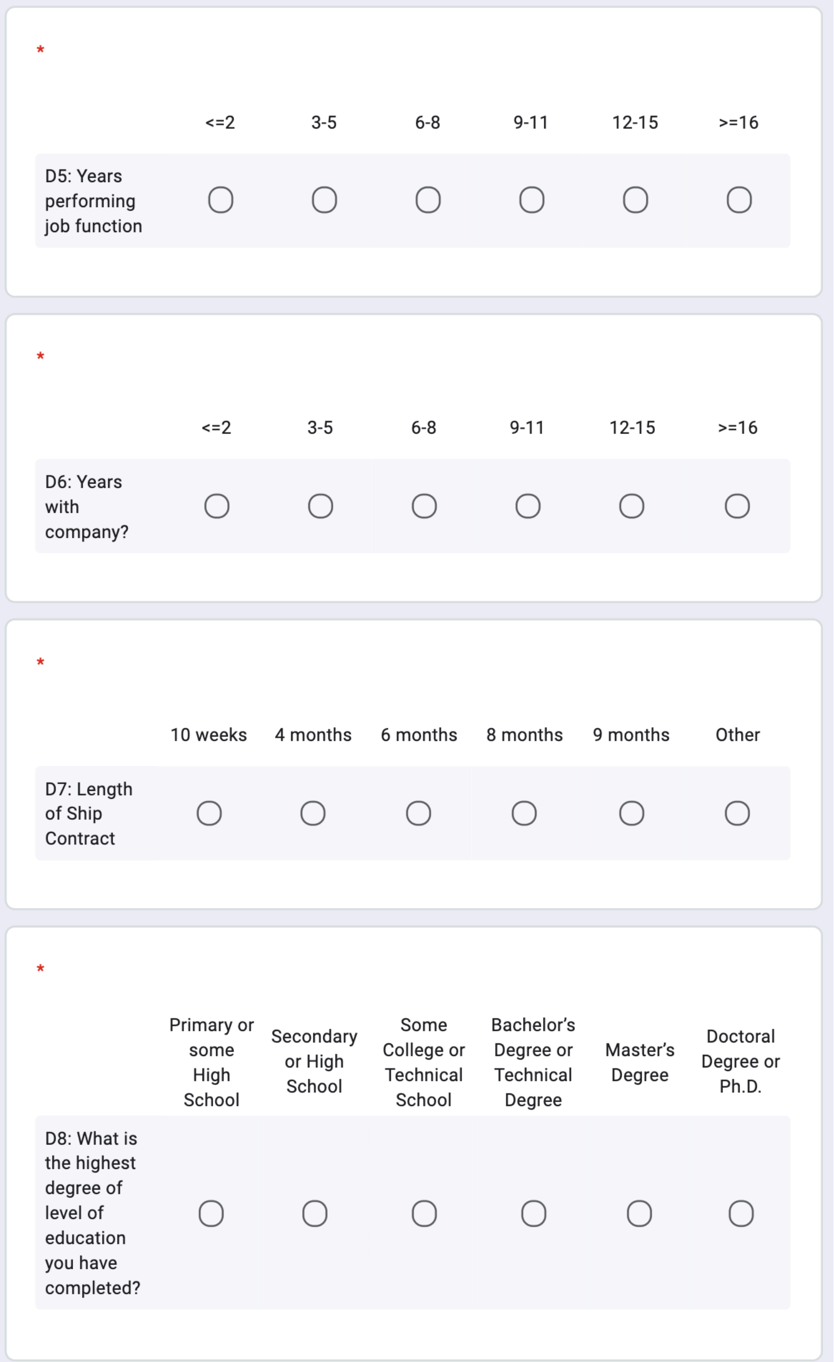
*

	Europe	North America	South-Central America	Africa	Asia	Caribbean	Oceania	Middle East
D3: What is your Nationality (Geographic Region)	○	○	○	○	○	○	○	○

(If you don't see your department, scroll to the right) *

	Deck	Security	Medical	Engine	Hotel Department	Food & Beverage	Housekeeping
D4: Choose the department you work in	○	○	○	○	○	○	○

Pre-Experiment Survey Instrument (Cont.)



*

	<=2	3-5	6-8	9-11	12-15	>=16
D5: Years performing job function	○	○	○	○	○	○

*

	<=2	3-5	6-8	9-11	12-15	>=16
D6: Years with company?	○	○	○	○	○	○

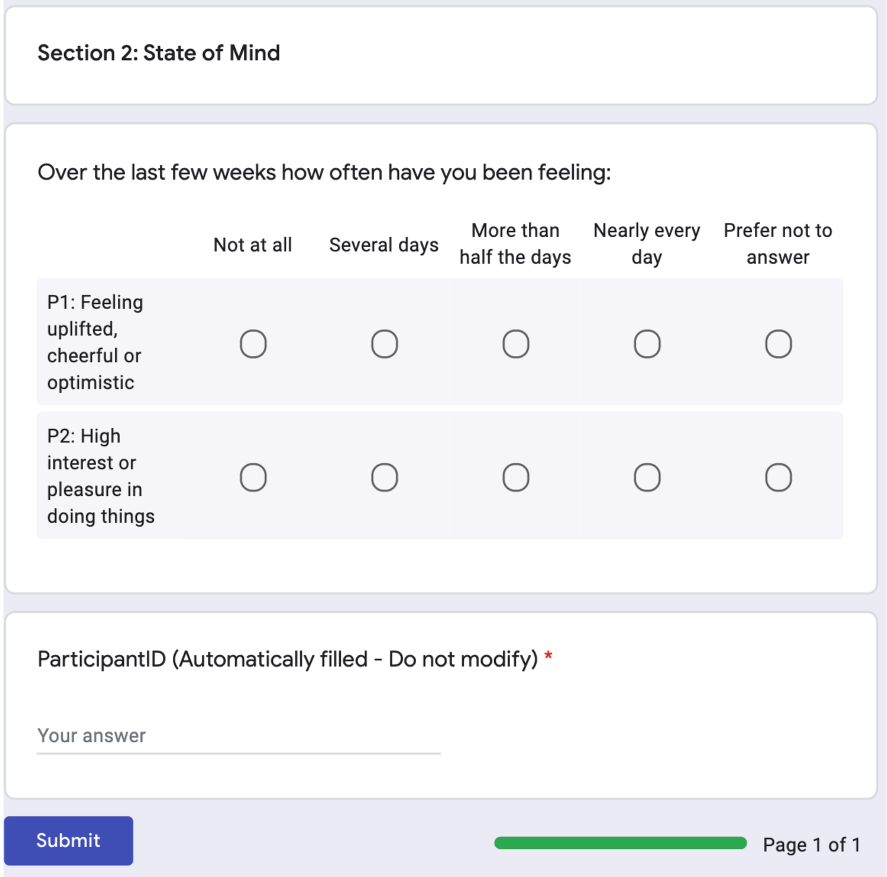
*

	10 weeks	4 months	6 months	8 months	9 months	Other
D7: Length of Ship Contract	○	○	○	○	○	○

*

	Primary or some High School	Secondary or High School	Some College or Technical School	Bachelor's Degree or Technical Degree	Master's Degree	Doctoral Degree or Ph.D.
D8: What is the highest degree of level of education you have completed?	○	○	○	○	○	○

Pre-Experiment Survey Instrument (Cont.)



Section 2: State of Mind

Over the last few weeks how often have you been feeling:

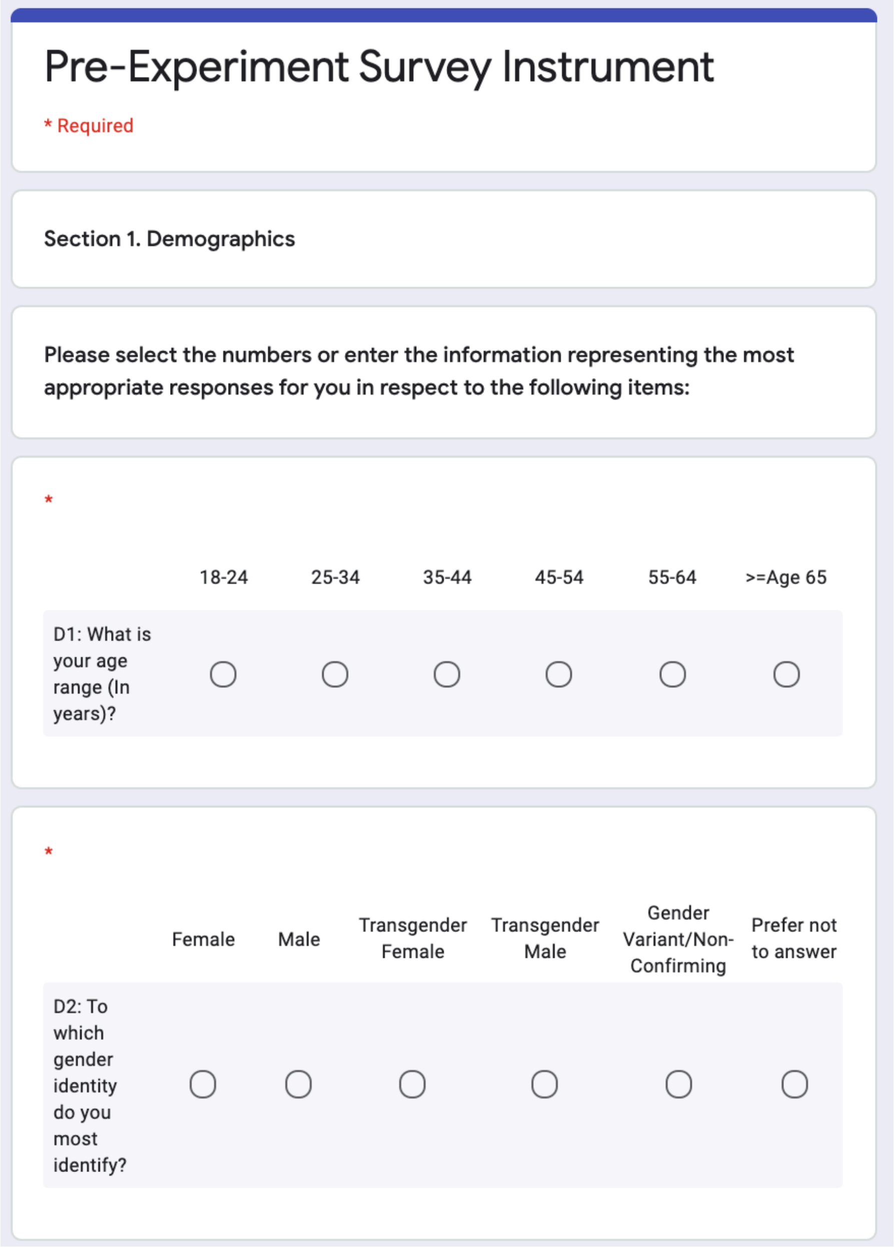
	Not at all	Several days	More than half the days	Nearly every day	Prefer not to answer
P1: Feeling uplifted, cheerful or optimistic	○	○	○	○	○
P2: High interest or pleasure in doing things	○	○	○	○	○

ParticipantID (Automatically filled - Do not modify) *

Your answer

Appendix L

Pre-Experiment Survey Instrument (Shoreside)



Pre-Experiment Survey Instrument

* Required

Section 1. Demographics

Please select the numbers or enter the information representing the most appropriate responses for you in respect to the following items:

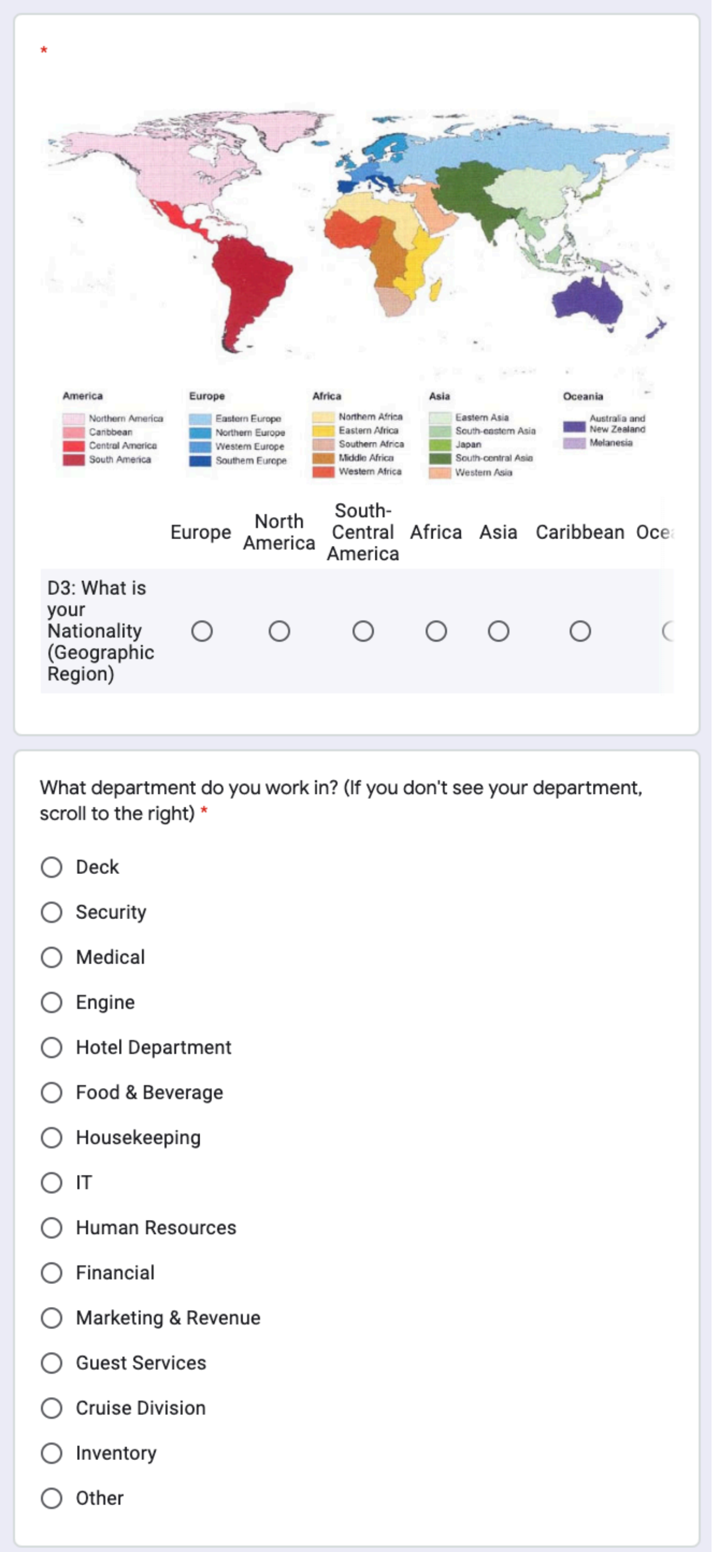
*

	18-24	25-34	35-44	45-54	55-64	>=Age 65
D1: What is your age range (In years)?	○	○	○	○	○	○

*

	Female	Male	Transgender Female	Transgender Male	Gender Variant/Non-Confirming	Prefer not to answer
D2: To which gender identity do you most identify?	○	○	○	○	○	○

Pre-Experiment Survey Instrument (Cont.)



*

	Europe	North America	South-Central America	Africa	Asia	Caribbean	Oce
D3: What is your Nationality (Geographic Region)	○	○	○	○	○	○	○

What department do you work in? (If you don't see your department, scroll to the right) *

○ Deck

○ Security

○ Medical

○ Engine

○ Hotel Department

○ Food & Beverage

○ Housekeeping

○ IT

○ Human Resources

○ Financial

○ Marketing & Revenue

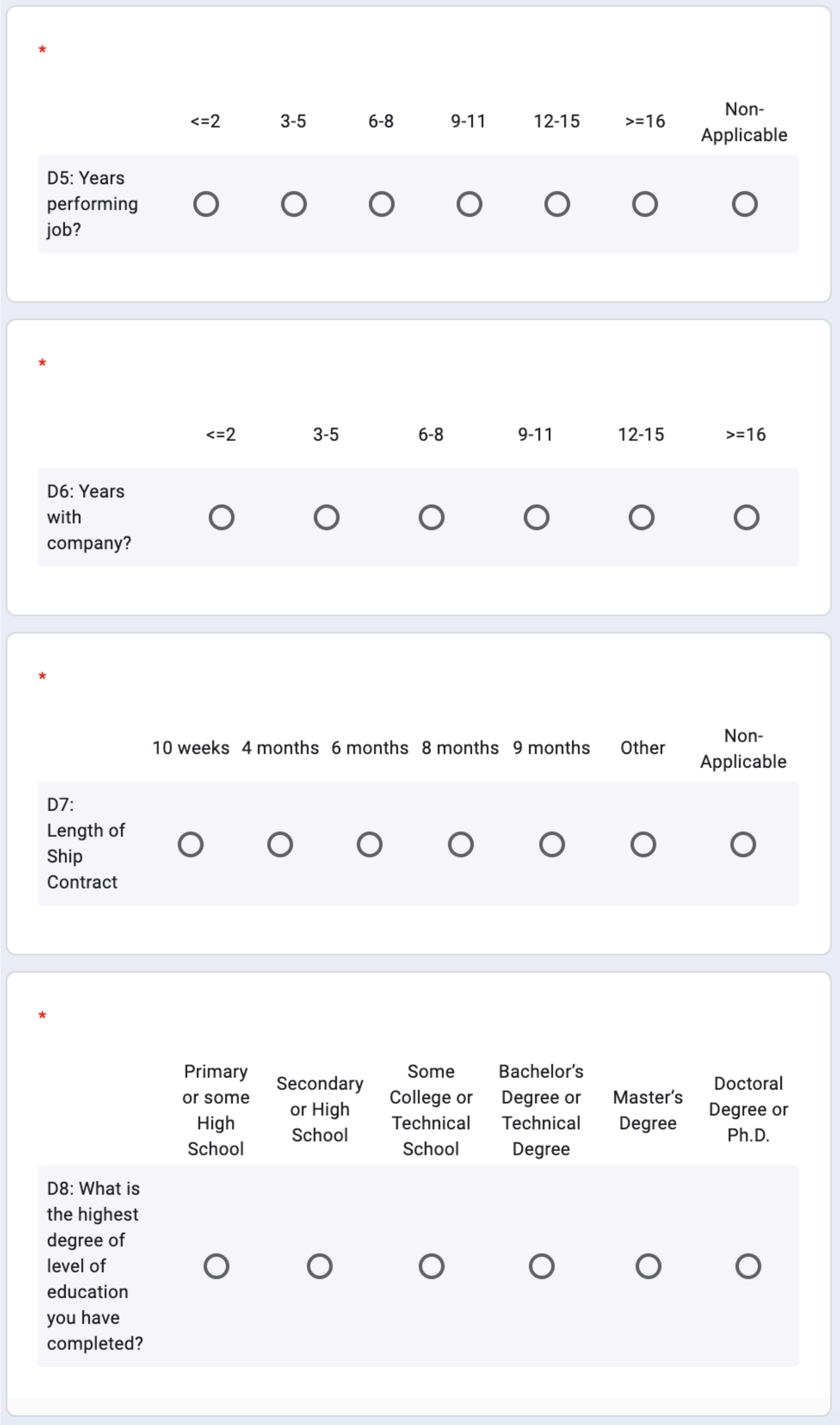
○ Guest Services

○ Cruise Division

○ Inventory

○ Other

Pre-Experiment Survey Instrument (Cont.)



*

	<=2	3-5	6-8	9-11	12-15	>=16	Non-Applicable
D5: Years performing job?	○	○	○	○	○	○	○

*

	<=2	3-5	6-8	9-11	12-15	>=16
D6: Years with company?	○	○	○	○	○	○

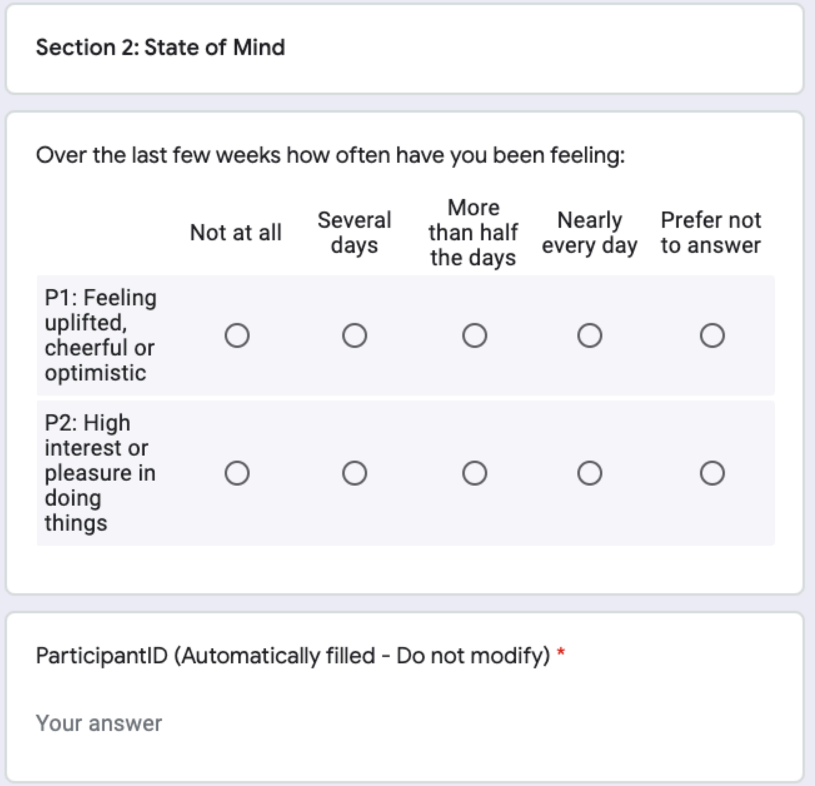
*

	10 weeks	4 months	6 months	8 months	9 months	Other	Non-Applicable
D7: Length of Ship Contract	○	○	○	○	○	○	○

*

	Primary or some High School	Secondary or High School	Some College or Technical School	Bachelor’s Degree or Technical Degree	Master’s Degree	Doctoral Degree or Ph.D.
D8: What is the highest degree of level of education you have completed?	○	○	○	○	○	○

Pre-Experiment Survey Instrument (Cont.)



Section 2: State of Mind

Over the last few weeks how often have you been feeling:

	Not at all	Several days	More than half the days	Nearly every day	Prefer not to answer
P1: Feeling uplifted, cheerful or optimistic	○	○	○	○	○
P2: High interest or pleasure in doing things	○	○	○	○	○

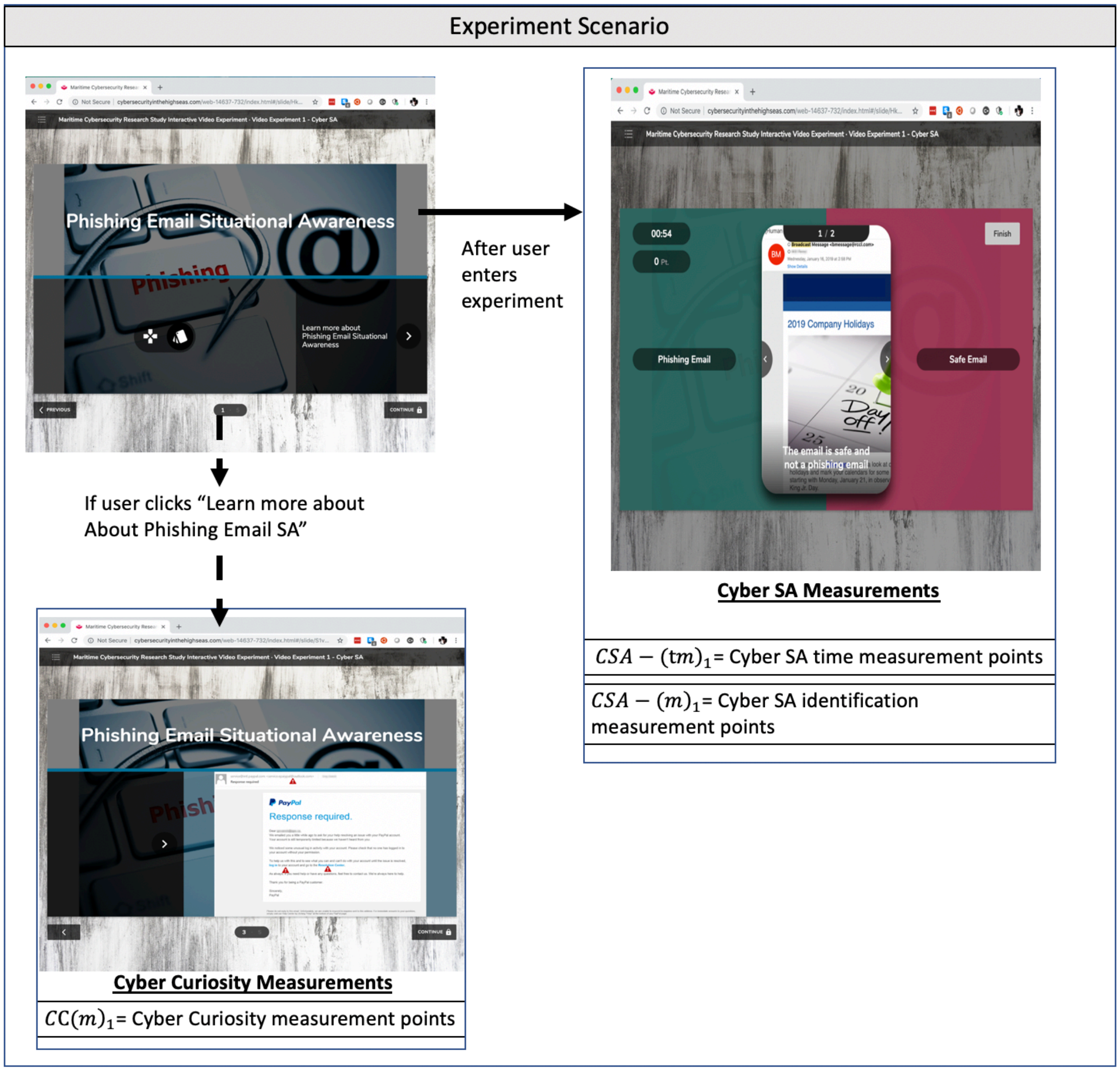
ParticipantID (Automatically filled - Do not modify) *

Your answer

Appendix M

Blueprint of the Proposed Initial Measures

The blueprint for the proposed initial measures for this research study consists of a series of experiment scenarios that presents the participant with links and choices to measures their level of Cyber Curiosity and Cyber SA. Table 9 and Table 10 show the proposed measures for the user action selection for Cyber SA and Cyber Curiosity.



Experiment Scenario

After user enters experiment

If user clicks "Learn more about About Phishing Email SA"

Cyber SA Measurements

$CSA-(tm)_1$ = Cyber SA time measurement points

$CSA-(m)_1$ = Cyber SA identification measurement points

Cyber Curiosity Measurements

$CC(m)_1$ = Cyber Curiosity measurement points

Maritime Cybersecurity Research Study Interactive Video Experiment - Video Experiment 1 - Cyber SA
Phishing Email Situational Awareness
Phishing
Learn more about Phishing Email Situational Awareness
PREVIOUS
CONTINUE
00:54
0 Pt.
Finish
1 / 2
2019 Company Holidays
Phishing Email
Safe Email
The email is safe and not a phishing email
PayPal
Response required.

Blueprint of the proposed initial measures (Cont.)

Table 9

Cyber SA Time Measurement Points (CSA-tm)

Level	Experiment User Action Timing Categories	Points
Advanced	Advanced social engineering attack identified under 20 seconds	4
	Advanced social engineering attack identified between 20 seconds and 30 seconds	2
	Advanced social engineering attack identified longer than 30 seconds	0
Simple	Simple social engineering attack identified under 30 seconds	2
	Simple social engineering attack identified between 20 seconds and 30 seconds	1
	Simple social engineering attack identified longer than 30 seconds	0

Table 10

Cyber Curiosity Measurement Points

	Curiosity Type		
Experiment User Action Selection	**I-Type**	**D-Type**	**Points**
Simple explanation (User will be presented with link to expand on explaining the section of the experiment such as “Learn more about Phishing Email Situational Awareness”		x	-1
In-depth explanation (User will be presented with a link in the simple explanation section to seek further information such as “To learn further information about Phishing Email Situational Awareness”		x	-2
Enticing Web link (User will be presented with a link to a non-SA awareness page with an entertaining story or topic.)	x		1
Enticing Pop-up Web link (User will be presented with a pop-up to a non-SA awareness page with an entertaining story or topic.)	x		2

References

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, *32*(3), 183–196.

Algarni, A., Xu, Y., Chan, T., & Tian, Y.-C. (2013). Social engineering in social networking sites: Affect-based model. In *Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for Internet Technology and Secured Transaction*, London, UK, pp. 508–515.

Alhefeiti, A. Abdulla. (2018). *A systematic method of developing information sharing systems based on activity theory*. Retrieved from Central Archive at the University of Reading.

Allen, D. K., Brown, A., Karanasios, S., & Norman, A. (2013). How should technology-mediated organizational change be explained? A comparison of the contributions of critical realism and activity theory. *MIS Quarterly*, 37(3), 835.

Anderson, R. J. (1994). Why cryptosystems fail. *Communications of the ACM*, *37*(11), 32–40.

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

Ahrend, J. M., Jirotka, M., & Jones, K. (2016). On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit threat and defense knowledge. In *2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment* (CyberSA), London, UK, pp. 1–10.

Anti-Phishing Working Group (2016). *Phishing activity trends report: Unifying the global response to cybercrime* (4th quarter 2016*)*. Retrieved from https://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf

APA. (n.d.). *Transgender people, gender identity and gender expression*. Retrieved from https://www.apa.org/topics/lgbt/transgender.aspx

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jajodia, S., & Ou, X. (2010). Cyber SA: Situational awareness for cyber defense. *Cyber Situational Awareness* (pp. 3-13). Boston, MA: Springer.

Barnett, M., Gatfield, D., & Pekcan, C. (2017). *Non-technical skills: The vital ingredient in world maritime technology?* Warsash Maritime Centre, Southampton Solent University, Southampton, UK.

Bedny, G., Meister, D. (1999). Theory of activity and situation awareness. *International Journal of Cognitive Ergonomics*, 3(1), 63-72.

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, 48, 51–61.

Berlyne, D. E. (1954). A theory of human curiosity. In *British Journal of Psychology ,45*, 180-191.

Berlyne, D. E. (1960). *Conflict, arousal and curiosity*. New York, NY: McGraw-Hill.

Berlyne, D. E. (1963). Motivational problems raised by exploratory and epistemic behavior. *Psychology: A Study of Science*, 5, 25- 33.

Bolstad, C. A. (2001). Situation awareness: Does it change with age? *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 45(4), 272–276.

Boss, S., Kirsch, L., Angermeier, I., Shingler, R., & Boss, R. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, 18(2), 151-164.

Brody, R. G. (2012). Flying under the radar: Social engineering. *International Journal of Accounting and Information Management,* 20(4), 335-347.

Buchem, I., Attwell, G., & Torres, R. (2011). Understanding personal learning environments: Literature review and synthesis through the activity theory lens. *Proceedings of the PLE Conference 2011*.Southampton, UK, 1–33.

Bullée, J.-W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of Experimental Criminology*, *11*(1), 97–115.

Caserta, R. J., & Abrams, L. (2007). The relevance of situation awareness in older adults' cognitive functioning: A review. *European Review of Aging and Physical Activity*, 4(1), 3–13.

Champion, M. A., Rajivan, P., Cooke, N. J., & Jariwala, S. (2012). Team-based cyber defense analysis. *Proceeding of the 2012 IEEE International Multi-Disciplinary Conference on Cognitive in Situational Awareness and Decision Support*, pp. 218-221.

Chang, A. L., Dym, A. A., Venegas-Borsellino, C., Bangar, M., Kazzi, M., Lisenenkov, D., Eisen, L. A. (2017). Comparison between simulation-based training and lecture-based education in teaching situation awareness: A randomized controlled study. *Annals of the American Thoracic Society*, *14*(4), 529-535.

Chauvin, C., & Lardjane, S. (2008). Decision making and strategies in an interaction situation: Collision avoidance at sea. *Transportation Research Part F: Traffic Psychology and Behaviour*, *11*(4), 259–269.

Chen, C. C., Shaw, R. S., & Yang, S. C. (2006). Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. *Information Technology, Learning, and Performance Journal, 24*(1), 1-14.

Cisco (2017). *2017 annual security report.* Retrieved from: http://b2me.cisco.com/en-us-annual-cybersecurity-report-2017.

Collier, T.J., Greene, J.G., Felten, D.L., Stevens, S.Y., Collier, K.S., (2004). Reduced cortical noradrenergic neurotransmission is associated with increased neophobia and impaired spatial memory in aged rats. *Neurobiological Aging*, 25(2), 209–221.

Creswell, J. W. (2005). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (2nd ed.). Upper Saddle River, NJ: Pearson.

Cyber. (n.d.). In *Cambridge's online dictionary*. Retrieved from https://dictionary.cambridge.org/dictionary/english/cyber

Cyberkeel. (2014). Maritime cyber-risks: Virtual pirates at large on the cyber seas. Retrieved from: https://maritimecyprus.files.wordpress.com/2015/06/maritime-cyber-risks.pdf

Delbeq, A., Van de Ven, Andrew & Gustafson, D. H. (1975). Group techniques for program planning: A guide to nominal group and Delphi processes. Glenview, USA: Scott, Foresman and Company, 124.

Dennis, A. R., & Valacich, J. S. (2001). Conducting experimental research in information systems. *Communications of the Association for Information Systems*, *7*(1), 5.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, NY, pp. 581–590.

Dutt, V., Ahn, Y. S., & Gonzalez, C. (2013). Cyber situation awareness modeling detection of cyber attacks with instance-based learning theory. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *55*(3), 605-618.

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. *Proceeding of the Second Symposium on Usable Privacy and Security*, New York, NY, pp. 79–90.

Ellis, T. J., & Levy, Y. (2010). A guide for novice researchers: Design and development research methods. *Proceeding of the Informing Science + Information Technology Education Conference 2010*, Casino, Italy, pp. 107-118.

Elster, J. (2000). *Ulysses unbound: Studies in rationality, precommitment, and constraints*. UK: Cambridge University Press.

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors, 37*(1), 32-64.

Endsley, M. R. (2015). Toward a theory of situation awareness in dynamic systems. *Journal of cognitive engineering and decision making, 9*(1), 4-32.

Endsley, M. R., & Garland, D. J. (2000). *Situation awareness analysis and measurement.* Mahwah, NJ: Lawrence Erlbaum Associates.

Endsley, M.R., & Jones, D.R, (2004). Designing for situation awareness. Boca Raton, FL: CRC Press.

Endsley, M. R., & Jones, D. G. (2012). Designing for situation awareness: An approach to human-centered design (2nd ed.). UK: Taylor & Francis.

Endsley, M. R., & Smolensky, M. W. (1998). Situation awareness in air traffic control: The picture. *Human factors in air traffic control.* (pp. 115–154). San Diego, CA: Academic Press.

Engeström, Y. (1990). *Learning, working and imagining: Twelve studies in activity theory*. Helsinki, Finland: Orienta-konsultit.

Engeström, Y., Miettinen, R., Theory, I. C. R. A., & Punamäki, R. L. (1999). Perspectives on Activity Theory. UK: Cambridge University Press. Retrieved from https://books.google.com/books?id=GCVCZy2xHD4C

Erbacher, R. F., Frincke, D. A., Wong, P. C., Moody, S., & Fink, G. (2010). A multi-phase network situational awareness cognitive task analysis. *Information Visualization*, *9*(3), 204–219.

Erbacher, R. F. (2012). Visualization design for immediate high-level situational assessment. *Proceedings of the Ninth International Symposium on Visualization for Cyber Security, ACM*, New York, NY, pp. 17–24.

European Network and Information Security Agency (2011). Analysis of cyber security aspects in the maritime sector. Retrieved from https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1/at_download/fullReport

Fan, W., Lwankatare, K., Rong, R. (2016). Social engineering: I-E based model of human weakness to investigate attack and defense. *SCIREA Journal of Information Science and Systems Science*, *1*(2), 34-57.

Federal Bureau of Investigations. (2017). 2017 Internet crime report. Retrieved from https://pdf.ic3.gov/2017_IC3Report.pdf

Federal Bureau of Investigations. (2018). Public service announcement. Retrieved from https://www.ic3.gov/media/2018/180712.aspx

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Retrieved from https://books.google.com/books?id=8o0QAQAAIAAJ

Fitton, O., Prince, D., Germond, B., & Lacy, M. (2015). The future of maritime cyber security. Retrieved from Lancaster University, School of Science and Technology website http://eprints.lancs.ac.uk/72696/1/Cyber_Operations_in_the_Maritime_Environment_v2.0.pdf

Francisco, R., Klein, A. Z., Engeström, Y., & Sannino, A. (2018). Knowledge on the move : Expansive learning among mobile workers. *Online Collaboration and Communication in Contemporary Organizations* (pp. 179–200). Denmark: Aalborg University.

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness – A systematic review of the literature. *Computers & Security*, *46*, 18–31.

Goodall, J. R, Lutters, W. G., & Komlodi, A. (2004). I know my network: Collaboration and expertise in intrusion detection. *Proceedings of the 2004 ACM conference on computer supported cooperative work*, ACM, New York, NY, pp. 342–345.

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2016). Fighting against phishing attacks: State of the art and future challenges. *Neural Computing and Applications*, *28*(12), 3629-3654.

Hake, D. (2016). The value of curiosity and other lessons learned from the New York stock exchange’s cyber risk board forum. Retrieved from https://www.securityroundtable.org/the-value-of-curiosity-and-other-lessons-learned-from-the-new-york-stock-exchanges-cyber-risk-board-forum.

Hasan, H., & Crawford, K. (2003). Codifying or enabling: The challenge of knowledge management systems. *Journal of the Operational Research Society*, *54*(2), 184–193.

Hauss, Y., & Eyferth, K. (2003). Securing future ATM-concepts' safety by measuring situation awareness in ATC. *Aerospace Science and Technology*, *7*(6), 417–427.

Hawker, S., & Waite, M. (2007). *Concise Oxford thesaurus*. Oxford: Oxford University Press.

Heartfield, R., & Loukas, G. (2016). A taxonomy of attacks and a survey of defense mechanisms for semantic social engineering attacks. *ACM Computing Surveys*, *48*(3). 37-76.

Herzberg, A. (2009). Why Johnny can't surf (safely)? Attacks and defenses for Web users. *Computers & Security*, *28*(1–2), 63–71.

Hoffman, B., Buchler, N., Doshi, B., & Cam, H. (2016). Situational awareness in industrial control systems. *Cyber-security of SCADA and Other Industrial Control Systems* (pp. 187-208). Switzerland: Springer International Publishing.

Hong, K. W., Kelley, C. M., Tembe, R., Murphy-Hill, E., & Mayhorn, C. B. (2013). Keeping up with the joneses: Assessing phishing susceptibility in an email task. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *57*(1), 1012-1016.

Hsu, Y. C., & Ching, Y. H. (2013). Mobile computer-supported collaborative learning: A review of experimental research. *British Journal of Educational Technology*, 44(5), E111–E114.

Hsu, C. C., & Sandford, B. A. (2007). The Delphi technique: Making sense of consensus. *Practical assessment, research & evaluation*, *12*(10), 1-8.

Huang, D., Wang, L., Zhou, M., & Zhang, J. (2010). Gender difference in motives of knowledge searching: Measurement invariance and factor mean comparison of the interest/deprivation epistemic curiosity. *2010 IEEE 2nd Symposium on Web Society* (pp. 258–263).

Hume, D. (1888). *A treatise of human nature*. Oxford, England: Clarendon.

IBM, (2014). *IBM security services 2014 cyber security intelligence index: Analysis of cyber attacks and incident data from IBM's worldwide security operations*. Retrieved from https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf

Information systems. (n.d.). In *Technopedia.Com*. Retrieved from https://www.techopedia.com/definition/24142/information-system-is

Isaac, A., (2017). Situational awareness in air traffic control: Human cognition and advanced technology. In Harris, D. (Eds.), *Engineering psychology and cognitive ergonomics. Volume 1: Transportation systems* (pp.185-192). New York, NY:Taylor & Francis.

Iuga, C., Nurse, J. R. C., & Erola, A. (2016). Baiting the hook: Factors impacting susceptibility to phishing attacks. *Human-Centric Computing and Information Sciences*, *6*(1), 1–20.

Jeannott, E., Kelly, C., & Thompson, D. (2003). The development of situation awareness measures in ATM systems. European Air Traffic Management Programme report. HRS/HSP-005-REP-01.

Jonker, D., Langevin, S., Schretlen, P., & Canfield, C. (2012). Agile visual analytics for banking cyber "big data". I*n 2012 IEEE Conference on Visual Analytics Science and Technology (VAST)*, Seattle, WA, pp. 299–300.

Kaber, D.B., Endsley, M.R., Wright, M.C., & Warren, H. (2002). The effects of levels of automation on performance, situation awareness, and workload in an advanced commercial aircraft flight simulation. Final Rep.: NASA Langley Research Center Grant #NAG-1-01002. Hampton, VA: NASA Langley Research Center.

Kaptelinin, V., & Nardi, B. A. (2006). *Acting with technology: Activity theory and interaction design*. Cambridge, MA: The MIT Press.

Keller, J., Lebiere, C., Shay, R., & Latorella, K. (2004). Cockpit system situational awareness modelling tool. *Proceedings of the 5th Human Performance, Situation Awareness and Automation Conference*, Daytona Beach, FL.

Kelley, C. M., Hong, K. W., Mayhorn, C. B., & Murphy-Hill, E. (2012). Something smells phishy: Exploring definitions, consequences, and reactions to phishing. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 56(1), pp. 2108-2112.

Korteling, J. E. (1993). Effects of age and task similarity on dual-task performance. *Human Factors*, 35(1), 99–113.

Kramek, J. (2013). The critical infrastructure gap: U.S. port facilities and cyber vulnerabilities. *Federal Executive Series Policy Papers,* Brookings Institute. Retrieved from https://www.brookings.edu/wp-content/uploads/2016/06/03-cyber-port-security-kramek.pdf

Kuutti, K. (1996). Activity theory as a potential framework for human-computer interaction research. *Context and consciousness: Activity theory and human-computer interaction*, (pp. 17-44). Cambridge, MA: Massachusetts Institute of Technology.

Leedy, P. D., & Ormrod, J. E. (2005). *Practical research: Planning and design* (8th ed.). Upper Saddle River, NJ: Prentice Hall.

Leont′ev, A. N. (1978). *Activity, consciousness, and personality*. Englewood Cliffs, N.J: Prentice-Hall.

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.

Libicki, M. C., Senty, D., & Pollak, J. (2014). Hackers wanted: An examination of the cybersecurity labor market. RAND Corporation. Retrieved from https://www.rand.org/pubs/research_reports/RR430.html

Litman, J. A. (2008). Interest and deprivation factors of epistemic curiosity. *Personality and Individual Differences*, *44*(7), 1585–1595.

Litman, J. A., Crowson, H. M., & Kolinski, K. (2010). Validity of the interest- and deprivation-type epistemic curiosity distinction in non-students. *Personality and Individual Differences*, *49*(5), 531–536.

Litman, J., Hutchins, T., & Russon, R. (2005). Epistemic curiosity, feeling-of-knowing, and exploratory behaviour. *Cognition and Emotion*, *19*(4), 559–582.

Litman, J. A., & L Jimerson, T. (2004). The measurement of curiosity as a feeling of deprivation. *Journal of Personality Assessment*, *82*(2), 147-157.

Litman, J. A., & Spielberger, C. D. (2003). Measuring epistemic curiosity and its diversive and specific components. *Journal of Personality Assessment*, *80*, 75–86.

Loewenstein, G. (1994). The psychology of curiosity: A review and reinterpretation. *Psychological Bulletin*, *116*, 75–98.

Luria, A.R. (1928). The problem of the cultural behavior of the child. *Pedagogal Seminary and Journal of Genetic Psychology*, *35*, 493-504.

Mahoney, S., Roth, E., Steinke, K., Pfautz, J., Wu, C., & Farry, M. (2010). A cognitive task analysis for cyber situational awareness. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 54*(4), 279–283.

Mancuso, V., Strang, A., Funke, G., Finomore, V. (2014). A framework for human-centered research. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *58*(1), pp. 437-441

Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. (2017). A systematic literature review: Information security culture. *Proceedings of the 2017 International Conference on Research and Innovation in Information Systems (ICRIIS),* Langkawi, Malaysia, pp. 1–6.

Matthews, M.D., Pleban, R.J., Endsley, M.R., & Strater, L.D., (2000). Measures of infantry situation awareness for a virtual MOUT environment. *Proceedings of the Human Performance, Situation Awareness and Automation: User Centered Design for the New Millennium*. Savannah, GA: SA Technologies, Inc.

Mertler, C., & Vannatta, R.A. (2012). Advanced and multivariate statistical methods: Practical application and interpretation (5th ed.). Glendale, CA: Pyrczak Publishing.

Mills, D. (2009). Analysis of a social engineering threat to information security exacerbated by vulnerabilities exposed through the inherent nature of social networking Websites. *Information Security Curriculum Development Conference*, New York, NY, pp. 139–141.

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. New York, NY: Wiley Publishing, Inc.

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, *59*, 186–209.

Olsson, E., & Jansson, A. (2006). Work on the bridge – studies of officers on high-speed ferries. *Behaviour & Information Technology*, *25*(1), 37–64.

Øvergård, K. I., Sorensen, L. J., Nazir, S., & Martinsen, T. J. (2015). Critical incidents during dynamic positioning: operators' situation awareness and decision-making in maritime operations. *Theoretical Issues in Ergonomics Science*, *16*(4), 366–387.

PricewaterhouseCoopers. (2017). *Toward new possibilities in threat management.* Retrieved from https://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/assets/gsiss-report-cybersecurity-privacy-possibilities.pdf

Progoulaki, M., & Theotokas, I. (2016). Managing culturally diverse maritime human resources as a shipping company's core competency. *Maritime Policy & Management*, 43(7), 860–873.

Randel, J. M., Pugh, H. L., & Reed, S. K. (1996). Differences in expert and novice situation awareness in naturalistic decision making. *International Journal of Human–Computer Studies*, 45(5), 579–597.

Robinson, O. C., Demetre, J. D., & Litman, J. A. (2017). Adult life stage and crisis as predictors of curiosity and authenticity: Testing inferences from Erikson's lifespan theory. *International Journal of Behavioral Development, 41*(3), 426–431.

Rothblum, A. M. (2000, October). Human error and marine safety. *National Safety Council Congress and Expo,* Orlando, FL.

Rothblum, A.M., Wheal, D., Withington, S., Shappell, S. A., Wiegmann, D. A., Boehm, & W., Chaderjan, M. (2002). Human factors in incident investigations and analysis. *2nd International Workshop of Human Factors in Offshore Operations*. Houston, Texas.

RSA (2014). *RSA monthly online fraud report – September 2014*. Retrieved from https://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-0914.pdf

Salmon, P. M., Stanton, N. A., Walker, G. H., Jenkins, D., Ladva, D., Rafferty, L., & Young, M. (2009). Measuring situation awareness in complex systems: Comparison of measures study. *International Journal of Industrial Ergonomics*, *39*(3), 490–500.

Salmon, P.M., Stanton, N.A., Walker, G.H., & Green, D., (2006). Situation awareness measurement: A review of applicability for C4i environments. *Applied Ergonomics*, *37* (2), 225–238.

Salomon, G. (1997). *Distributed cognitions: Psychological and educational considerations.* Cambridge, UK: Cambridge University Press.

Sakaki, M., Yagi, A., & Murayama, K. (2018). Curiosity in old age: A possible key to achieving adaptive aging. *Neuroscience & Biobehavioral Reviews*, 88, 106–116.

Salthouse, T. (1991). Theoretical perspectives on cognitive aging. New York, NY: Psychology Press.

Sandhåland, H., Oltedal, H., & Eid, J. (2015). Situation awareness in bridge operations – A study of collisions between attendant vessels and offshore facilities in the North Sea. *Safety Science*, *79*, 277–285.

Saridakis, G., Benson, V., Ezingeard, J.-N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*, *102*, 320–330.

Schneier, B. (2000). *Secrets & lies: Digital security in a networked world*. New York, NY: Wiley Publishing, Inc.

Secureworks. (2018). *Gold galleon: How a Nigerian cyber crew plunders the shipping industry*. Retrieved from https://www.secureworks.com/research/gold-galleon-how-a-nigerian-cyber-crew-plunders-the-shipping-industry

Sekaran, U., & Bougie, R. (2013). *Research methods for business: A skill-building approach* (6th Ed.). West Sussex, UK: John Wiley & Sons Ltd.

Subject Matter Expert. (n.d.). In *Encyclopedia.Com*. Retrieved from http://www.encyclopedia.com/management/encyclopedias-almanacs-transcripts-and-maps/subject-matter-experts

Smith, K., & Hancock, P. A. (1995). Situation awareness is adaptive, externally directed consciousness. *Human Factors*, *37*(1), 137–148.

Sneddon, A., Mearns, K., & Flin, R. (2012). Stress, fatigue, situation awareness and safety in offshore drilling crews. *Safety Science*, *56*(Supplement C), 80–88.

Solms, R., & Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*(Supplement C), 97–102.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, *13*(2), 147-169.

Tadda, G. P., & Salerno, J. S. (2010). Overview of cyber situation awareness. *Cyber Situational Awareness: Issues and Research,* 46, 15-35. doi:10.1007/978-1-4419-0140-8

Tadda, G. P., & Salerno, J. S. (2010). Overview of Cyber Situation Awareness BT - Cyber Situational Awareness: Issues and Research. In S. Jajodia, P. Liu, V. Swarup, & C. Wang (Eds.) (pp. 15–35). Boston, MA: Springer US. doi:10.1007/978-1-4419-0140-8_2

Taylor, R. M. (1990). Situational awareness rating technique (SART): The development of a tool for aircrew systems design. *Situational Awareness In Aerospace Operations* (AGARD-CP-478) (pp. 3/1–3/17). Neuilly Sur Seine, France: NATO-AGARD.

Van Teijlingen, E. R., & Hundley, V. (2001). The importance of pilot studies. *Nursing Standard*. 16(40), 33-36.

Testa, M. R. (2002). Leadership dyads in the cruise industry: the impact of cultural congruency. *International Journal of Hospitality Management*, *21*(4), 425–441.

TrendMicro (2016). *Security 101: Business email compromise (BEC) schemes*. Retrieved from https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/business-email-compromise-bec-schemes

Tripwire (2017). *Don't be a whale – How to detect the business email compromise (BEC) scam*. Retrieved from https://www.tripwire.com/state-of-security/featured/how-detect-business-email-compromise-bec-scam/

Tucci, A. E. (2016). Cyber risks in the marine transportation system. *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level,* (3), 113–131.

Ulschak, F. L. (1983). Human resource development: The theory and practice of need assessment. Reston, VA: Reston Publishing Company, Inc.

Verizon Enterprise Solutions. (2016). *Verizon 2016 data breach investigations report*. Retrieved from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016

Verizon Enterprise Solutions. (2017). *Verizon 2017 data breach investigations report*. Retrieved from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017

Verizon Enterprise Solutions. (2018). *Verizon 2018 data breach investigations report.* Retrieved from https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

US-CERT. (2016). National cyber alert system: Cyber security tip ST04-0141. Retrieved from http://www.us-cert.gov/cas/tips/ST04-014.html

Van Westrenen, F., & Praetorius, G. (2014). Situation awareness and maritime traffic: Having awareness or being in control? *Theoretical Issues in Ergonomics Science*, *15*(2), 161–180.

Viktorelius, M., & Lundh, M. (2019). Energy efficiency at sea: An activity theoretical perspective on operational energy efficiency in maritime transport. *Energy Research & Social Science*, 52, 1–9.

Vries, L., & Bligård, L.-O. (2019). Visualising safety: The potential for using sociotechnical systems models in prospective safety assessment and design. *Safety Science*, 111, 80–93.

Vygotsky, L.S. (1978). *Mind and society*. Cambridge, MA: Harvard University Press.

Weaver, A. (2005). Interactive service work and performative metaphors: The case of the cruise industry. *Tourist Studies*, *5*(1), 5–27.

Wright, M. C., Taekman, J. M., & Endsley, M. R. (2004). Objective measures of situation awareness in a simulated medical environment. *Quality and Safety in Health Care*, *13*(Supplement 1), 65-71.

Whitten, A., & Tygar, J. D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. *Proceedings of the 8th Conference USENIX Security Symposium*, Berkeley, CA, *8*(1), 14-29.

Winkler, I. S., & Dealy, B. (1995). Information security technology? Don’t rely on it: A case study in social engineering. *Proceedings of the 5th Conference on USENIX UNIX Security Symposium,* Berkeley, CA.

Zheng, X. S., Tai, Y.-C., & McConkie, G. W. (2004). Exploring drivers’ situation awareness in a dynamic traffic environment. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *48*(19), 2374–2377.