CERIAS Tech Report 2023-8
Human Factors in Cybersecurity: A Cross-Cultural Study on Trust
by Isslam Alhasan
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

HUMAN FACTORS IN CYBERSECURITY: A CROSS-CULTURAL STUDY ON TRUST

by

Isslam Alhasan

A Dissertation

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Doctor of Philosophy

Department of Technology

West Lafayette, Indiana

August 2023

THE PURDUE UNIVERSITY GRADUATE SCHOOL

STATEMENT OF COMMITTEE APPROVAL

Dr. John Springer, Chair

Department of Computer & Information Technology

Dr. Smriti Bhatt

Department of Computer & Information Technology

Dr. Dawn Laux

Department of Computer & Information Technology

Dr. Tatiana Ringenberg

Department of Computer & Information Technology

Approved by:

Dr. Kathryne A. Newton

With a heart overflowing with gratitude and appreciation, I dedicate this dissertation to the individuals who have been my pillars of strength throughout this journey.

My parents hold a special place in my heart, they have always been there for me, showering me with love and making dua'a for my success. I am deeply grateful for their sacrifices and their unconditional love that has been a constant source of inspiration in my life. I also want to extend my thanks to my siblings, who have offered me love and praise every step of the way. I am grateful for your presence in my life.

To my beloved husband, Saleh, I want to express my deep and eternal gratitude for your unwavering love, support, and sacrifice. You have been my pillar throughout this journey, always there for me with a listening ear and a comforting embrace. Your patience, understanding, and sacrifices have been immeasurable, and I am so grateful for the way you have been my constant source of encouragement and support. You have been my partner in every sense of the word, always there to lift me up when I was down and celebrate with me in my triumphs. Your love and devotion have been the foundation of our relationship, and I am so blessed to have you in my life. I dedicate this dissertation to you as a token of my gratitude and utmost appreciation for everything you have done for me. This accomplishment would not have been possible without you by my side. Thank you for being my inspiration, my support, and my best friend.

To my children, Hamzeh, Jenna, Sara, Noor, and Hala, you have brought so much joy and light into my life. You have been my source of motivation and I am grateful for your love, understanding, and patience as I pursued this degree. I hope that by pursuing my dreams and reaching my goals, I can be a source of motivation for you and instill in you a love of learning and growing and the belief that you can accomplish anything you desire. This degree is not just a personal accomplishment, but a testament to the limitless potential that you have within you. I hope it will be a source of pride and inspiration for you as you navigate your own paths in life. Mama will always be there to celebrate your success, overcome your challenges, and cheer you on. I will always be proud of you and cherish the unique individuals you are growing up to be. My love for you is and will always be eternal. I love you, now and always.

Lastly, I want to thank my department and committee members, who have been my guides, mentors, and supporters. Their expertise, knowledge, and encouragement have been instrumental in helping me complete this dissertation, and I am deeply grateful for their help and support.

ACKNOWLEDGMENTS

I am grateful to God, the Almighty, for granting me the strength and perseverance to embark on this journey. Alhamdulilah.

I would like to express my heartfelt gratitude to all those who have supported me and made dua'a for me throughout the journey of writing this dissertation.

First and foremost, I would like to express my sincere gratitude to my advisor, Dr. John Springer, for his unwavering support, guidance, and encouragement throughout this project. Dr. Springer took on the role of Chair without hesitation and his invaluable insights and expertise were instrumental in shaping my thoughts and bringing this dissertation to fruition. I am forever grateful for his dedication, patience, and willingness to support me in every way possible.

I would also like to extend my gratitude to the members of my committee, Dr. Smriti Bhatt, Dr. Dawn Laux, Dr. Tatiana Ringenberg, for their insightful comments and constructive criticism, which have helped me to improve the quality of this work.

I would like to express my appreciation to my family, who have supported me in countless ways during the course of my academic pursuits. Their encouragement and understanding have been a constant source of motivation and inspiration throughout my life.

I would also like to thank the Purdue University for providing me with the resources and opportunities necessary to complete this dissertation.

This dissertation would not have been possible without the support of all these individuals.

Thank you all for your invaluable contributions and support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Human error is one of the most prominent challenges facing cybersecurity today. Attackers manipulate people's natural inclination to make mistakes using social engineering tactics to exploit psychological vulnerabilities, gain trust, and access sensitive information. Trust plays a critical role in human interaction, both in the physical and digital realms, making it an attractive target for attackers. However, cultural backgrounds, which reflect individual and societal beliefs and values, are often overlooked in cybersecurity risk assessments, despite significantly influencing human behavior. This study was conducted to investigate the relationship between trust and cybersecurity risks across diverse cultural groups. The study's findings could provide valuable insights into addressing and preventing human-related vulnerabilities by enhancing overall cybersecurity measures and examining cross-cultural differences in human behavior and their impact on cybersecurity risks. As human factors in cybersecurity become increasingly crucial, this study was performed to understand the differences in risky cybersecurity behaviors among various cultural groups and investigate the impact of different perceptions of trust on engaging in risky behaviors. The outcome of this research provides insights into the critical role cultural backgrounds play in shaping human behavior in the context of cybersecurity. The results of this study may have significant implications for enhancing overall cybersecurity measures by identifying and addressing human-related vulnerabilities that may be unique to specific cultural groups.

Keywords: cybersecurity, culture, trust, human factors, human error, human behaviors

CHAPTER ONE: INTRODUCTION

Background

Cybersecurity is the discipline of protecting and preventing network systems, devices, and data against unauthorized access or illegal, malicious use to preserve its confidentiality, integrity, and availability (CISA, 2019). Cybersecurity is widely recognized as a major global threat with significant impacts on all sectors of society, including industry, federal agencies, individuals, and public and private organizations (Stastny et al., 2022). As the world becomes increasingly digital and interconnected, protecting against cyber threats becomes paramount to the smooth functioning of daily operations. Undoubtedly, the emergence and reliance on technology are now part of everyday life. While technology has had many positive impacts on human existence, the reliance on technological digital assets has caused many areas of vulnerability to cybercrime. Cybercrimes are malicious acts that attempt to breach information and damage or disrupt digital life (Kaspersky, 2020). Cybercrime can occur in various forms, such as phishing scams, malware and ransomware attacks, social engineering tactics, massive data breaches, malicious insider activity, and cyber-terrorism, among other methods employed by cybercriminals (Alawida et al., 2022). According to the Global Risks Report of the World Economic Forum (2022), cybersecurity threats have increased by over 300% in 2020 alone. These threats are currently outpacing societies' capability to counteract to them efficiently and successfully. It is estimated that cybercrime attacks happen every 39 seconds, making it one of the most severe, challenging threats to the Nation's national security (Cukier, 2007). President Biden has made cybersecurity a necessary component of the Department of Homeland Security's primary mission and utmost importance to protect and secure all levels of the government, all public and private sectors, and the American people. In 2022, an

executive order was issued to strengthen and safeguard federal systems against cyber-attacks to establish more effective methods to report and respond to cyber incidents promptly and agilely (The White House, 2022).

Cybersecurity in 2022 is vastly different from twenty or even ten years ago. Its evolution is driven by the increasing reliance on information technology environments and its increasing incidence of cyberattacks that caused many disruptions of critical infrastructure. Cyberattacks' continuous evolution and strategic components have advanced in sophistication and will continue to do so in the upcoming years. The history of cybersecurity dates to the early 1970s, when most people did not have computers. Although cybersecurity was beginning to take shape, its primary focus was physical security, and threats were easily identifiable (Mutune, 2021). Bob Thomas, a researcher for BBN Technologies, developed the first computer worm, Creeper, which spread over the ARPANET network while leaving a trail behind it (Davies, 2021). His invention led to the beginning of the development of cybersecurity. The surge in popularity of Microsoft's Windows operating system in the early 1990s led to a corresponding rise in polymorphic virus activity. As a result, the market witnessed an increase of antivirus software to combat this growing threat (Clarke, 2008). This was a year when so much information was public and widely available, and new viruses and malware numbers were rising by the minute. The start of the 2000s is when there was a noticeably growing number of cyberattacks and a lack of available preventions to combat these threats (Chadd, 2020). The Department of Homeland Security (2003) outlined an initial framework to reduce vulnerabilities and support the Nation's critical infrastructures and make sure that cyber-attack disruptions are controllable and cause minor damage possible. With a computer device in every pocket and many significant data breaches emerging, the rise of cybersecurity is kicking off with no foreseeable end. A digital, connected world offers new and innovative opportunities for

cybercrimes; each additional connected device serves as a unique entry point that needs to be appropriately protected (Chadd, 2020). As technology advances, the risks, and vulnerabilities it presents will continue to expand and become more challenging to defend against.

As cyber-attacks continue to surge and become more sophisticated and innovative, they are on the rise, leading to an increased cost of cybercrimes. The cost is not simply in terms of the damages that occur during or after an attack; it also includes the time and resources that come before, during, and after a cyberattack (Fox, 2021). Examples of damages include opportunity and awareness costs, educational training, data destruction, decision-making developments, the impact of system downtime, loss of productivity, and reputational damages. Becoming a victim of cybercrime has shifted from a matter of "if" to "when," making it an almost inevitable occurrence (Madigan, 2014), reinforcing the need to take the consequences of cybercrimes and vulnerabilities seriously. The current global cost from cybercrimes surpassed one trillion dollars, a more than fifty percent increase from 2018 and an increase of fifteen percent yearly (Smith et al., 2020). This equates to an estimated cost of more than $500 billion a month, $16.4 billion a day, and $190,000 per second (Morgan, 2022). With the growing number of over six billion people connected to the internet worldwide, this high cost of cyber threats is unlikely to slow down anytime soon. It will expand to every profession, company, and industry worldwide.

New tactics and techniques used by cybercriminals are consistent with the growth of technology. Cybercriminals are growing at an alarming rate and are quick to keep up to date with ongoing cybersecurity flaws. A common significant contributor to cyber incidents is errors caused by human behavior (Nobles, 2018; Metalidou et al., 2014; Pollock, 2017), also known as the human factor. Human factors in a security context are the actions or events that result in a data breach. These actions may be unintentional or intentional, eventually allowing a security breach

to occur. Human factors have been identified as the primary area of vulnerability in cybersecurity (Mohan, 2016), and it is estimated that 90% of cybersecurity incidents are caused by human error (Kemper, 2019). Despite this, humans are still crucial in the fight against cyberattacks.

As organizations' reliance on information and data grows, protecting these assets against leaks, modifications, and damage becomes increasingly vital to prevent the costly consequences of cyberattacks. However, it's important to note that while technical factors play a crucial part in defending against these threats, human error is the highest area of vulnerability (Van-Zadelhoff, 2016). A single human error can be all it takes to circumvent and compromise all the technical safeguards that have been put in place. This emphasizes the need to address technical vulnerabilities and the potential for human error in cybersecurity strategies. Cybersecurity starts and ends with humans, and because people are the prime target for cyber-attacks, human error is considered the weakest link in the security chain (Wiederhold, 2014; Balozian et al., 2019; Gratian et al., 2018). Cyber-criminals and hackers will most likely attempt to attack individuals or even an entire company through the most vulnerable link – humans. This may seem far-fetched, but this type of cybercrime has been proven to be the most successful and the root cause of data breaches (Evans et al., 2016). Cybersecurity is ultimately a human challenge; incorporating human behavioral implications into risk mitigation solutions is essential to being proactive in cyberspace.

Human behavior is generally inconsistent, meaning many factors can influence individuals' behaviors, making it difficult to predict and manage. It is imperative to consider human behaviors critical for cybersecurity plans and procedures. Trust is a significant factor that heavily influences human behavior (Heyns, 2021; Sellaro et al., 2014). In simple terms, trust can be described as having faith in the ability, reliability, truth, and integrity of someone or something (Scott, 2012). The positive expectation allows an instance of a trusting moment towards others (Möllering, 2006,

p. 191). Trust is a trait that varies across different cultural backgrounds, and it should not be assumed that all cultures evaluate trust similarly (Klein et al., 2019). Culture is "the collective programming of the mind which distinguishes the members of one group from another" (Hofstede, 1984, p. 21). It includes the "knowledge, belief, art, morals, law, custom, and any other capabilities and habits acquired by man as a member of society" (Tylor, 1871, p. 1). Trust is fundamental in human relationships and communication, and cultural backgrounds influence human behaviors. Some cultures, including the United States, Germany, and Australia, consider trust established by an individual's confidence in another person's abilities and past performances (Meyer, 2017). Building trust in these cultures tends to be more of a cognitive process.

On the contrary, trust is perceived as an emotional and personal matter in cultures that place greater importance on relationships, such as those in China, Saudi Arabia, and Nigeria (Meyer, 2017). Trust is built through shared experiences and a solid emotional connection with others in these cultures; it is a more intuitive and holistic process. Cultural backgrounds can profoundly affect how trust is viewed and established. Certain cultures may focus more on a person's capabilities and track record in building trust, while others prioritize emotional bonds and shared experiences (Kwantes et al., 2021). Acknowledging these cultural distinctions in trust can aid in understanding cross-cultural interactions and behaviors.

Current research on human behaviors in cybersecurity is typically intended for the general audience without any consideration of the cross-cultural differences of individuals (Halevi et al., 2016). Research has suggested that cultural factors may directly impact cybersecurity risks since human behavioral decisions are highly influenced by cultural habits and values (Halevi et al., 2016). The focus on human factors in cybersecurity is gradually growing but is still wildly understudied in literature. There is an urgent need to understand how cultural backgrounds

influence human behaviors and how these behaviors may impact or overlook cybersecurity risks. It is essential to reveal gaps of potential cybersecurity breaches to enhance specialized training and further assess best practices. Although a considerable amount of research has been focused on the technical aspects of cybersecurity, there has been little to no focus on integrating the cross-cultural factors that influence human behavior within different cultural groups. By understanding the behaviors of individuals and the factors that influence their decisions, risk assessments can be tailored to promote secure behaviors and practices.

Problem Statement

The current state of cybersecurity is becoming increasingly complex, with no foreseeable end in sight. One of the challenges faced when approaching cybersecurity risk assessment practices and policies is the domination of technical properties while overlooking the characteristics of human-centric behaviors, specifically the cross-cultural aspects of these behaviors. Given that more than 90% of cyberattacks result from human faults, not technical errors (De Catalunya, 2022), the first significant line of defense must concentrate on the foundational components of cybersecurity: human-centric behaviors. However, present-day preventions of human factors only include homogenous solutions, which may not adequately address the diverse cultural characteristics that influence human behaviors and decision-making. This is a problem because trust, which is culturally specific and influences human behavior, contributes significantly to how individuals perceive and respond to cybersecurity risks. Using a standard approach to preventing human-related vulnerabilities in cybersecurity ignores cultural factors' role and may be ineffective in addressing these risks. Further research is needed to recognize the cultural differences in the perceptions of trust and their impact on risky cybersecurity behaviors. By examining these

differences, this study was performed to gain insights into the diverse cultural characteristics that influence human behaviors and how they may impact cybersecurity risks.

Significance

This research study aimed to provide a deeper understanding of human behaviors related to cybersecurity and how cultural influences may impact individuals' perceptions of risks. By exploring the differences in risky cybersecurity behaviors among various cultural groups and examining the potential correlation between these differences and the perception of trust, this research seeks to study an often-overlooked area of cybersecurity. The findings of this research could have significant implications for individuals and businesses, as they may help to identify and prevent human-related vulnerabilities in the future. Additionally, research into human factors in cybersecurity is becoming increasingly important in the rapidly expanding field, and this study has the possibility of adding to the enhancement of overall security measures. The current state of cybercrime is alarming, and humans are known to be the weakest link in cybersecurity, as they are the leading cause of cyberattacks (Alsharif et al., 2022). While technical measures are essential for preventing and raising awareness of cyberattacks, human behaviors can still compromise them.

Cultural characteristics strongly influence trust, which plays a significant role in shaping an individual's perceived level of trust and their related behaviors concerning cybersecurity (Parsons et al., 2010). Cross-cultural perspectives must be considered to reduce cyber risks related to human behavior and accurately examine human behaviors toward cybersecurity. Security policies and procedures can be modified and updated by identifying and examining these factors to assist in future cybersecurity risk assessments. Cultural differences can significantly impact how people perceive trust (Klein et al., 2019), and these differences can either hinder or foster trust.

More research is needed to explore how these cultural differences impact cybersecurity risks. By focusing on cross-cultural behaviors that may increase cybersecurity risks and improving our understanding of human behavioral cyber resilience, this study aims to contribute to cybersecurity to strengthen compliance and cybersecurity awareness significantly.

Purpose Statement

The purpose of this study was aimed to investigate cross-cultural differences in the perceptions of trust and their impact on cybersecurity risks and to examine any differences in risky behaviors towards cybersecurity across cultural groups. Given the increasing number of cyberattacks that exploit human vulnerabilities, it is essential to recognize the cultural factors influencing cybersecurity risks. By examining these differences, this study aims to understand better how culture may shape cybersecurity-related human behaviors. The findings of this study can offer valuable insights into the influences cultural backgrounds have on human behavior and cybersecurity risks and may provide helpful information for reducing these risks in the future.

Research Questions

The objective of this study aimed to answer the following hypothesis and research question:

RQ_1: What is the relationship between trust and cybersecurity risky behaviors among different cultural groups?

H_1: There are cultural differences in how people view or perceive trust.

H_2: There are cultural differences in cybersecurity risky behaviors.

H_3: There is a positive relationship between trust and cybersecurity risky behaviors among different cultural groups.

In this study, the level of significance was set at 0.05 for hypothesis H_1 and H_2, meaning that there is a less than 5% chance that any differences between the cultural groups in the study are due to chance. The level of significance for H_3 was set at 0.01, to obtain stronger evidence of association. A p-value of less than alpha level of significance would be considered statistically significant and would provide evidence to reject the null hypothesis.

Assumptions

The researcher made the following assumptions in this study:

1. The respondents understand the survey questions and provide honest answers.
2. The study was conducted objectively, with minimal researcher bias.
3. The instruments utilized to collect data are valid and reliable.
4. The survey questionnaire was constructed correctly to measure the respondents' perception of trust.
5. The results of the study may be generalized to a larger population of individuals from the selected cultural groups.
6. The collected data is representative of the sample.

Limitations

Research limitations refers to the factors that may negatively impact the results and are beyond the researcher's control. A few possible limitations of this study are the following:

1. The study was based on self-reported data, which may be subject to bias or error.
2. Cultures in the United States may answer differently than the same culture outside the United States, which could impact the generalizability of the outcomes.

3. The study was conducted in English and may not capture the nuances and complexities of trust and cybersecurity risks in other languages or cultures.
4. The study relied on a single measure of trust and may not capture other dimensions or facets of trust.

Delimitations

Research delimitation is a limitation set forth by the researcher to identify specific aspects of the study design and the focus of the research study. The delimitations for this research include the following:

1. This study was geographically limited to respondents located in the United States and may not be generalizable to other regions or countries.
2. The study was conducted using a specific set of cultural groups and may not be representative of or generalizable to other cultural groups.
3. The study was only collected and analyze quantitative data and does not include qualitative data such as experiences or perspectives from interviews or other sources.
4. The questionnaire used in this study was only be distributed to participants who choose to take the survey online and may exclude individuals without internet access or who prefer to complete the survey in person.

Organization

The dissertation is divided into five main chapters and appendices. The first chapter offers an overview of the research study, including the purpose statement, problem statement, research question, hypothesis, limitations, and delimitations. This chapter establishes the foundation for the

rest of the dissertation by introducing key concepts, outlining the research methods and population to be studied, and defining the scope of the study. The second chapter presents a thorough literature review, which examines previous research on the topic and identifies areas where the current study can contribute new insights. The literature review highlights key themes related to the research design, questions, and hypotheses. The third chapter discusses the research methodology, including the research objectives, design, data collection procedures, and data analysis strategies. Measures to ensure the reliability and validity of the data are also described. Chapter Four presents the study's results, including comprehensive data analysis. The research findings are presented logically and structured, with tables and graphs used to illustrate key points. The results are also compared to the research questions and hypotheses, highlighting areas where the study has achieved its aims and where further research may be needed. Chapter Five discusses the results and their implications for the field. This chapter explores the significance of the research findings, considering their theoretical and practical contributions and the extent to which they support or challenge existing literature. The chapter draws conclusions based on the overall results of the dissertation and suggests directions for future research. Finally, the appendices provide additional information, including the survey scales used in the study.

CHAPTER TWO: LITERATURE REVIEW

The literature review section serves as an organizational pattern of the research, which summarizes current knowledge of the topic, develops a theoretical framework and methodology, and identifies gaps in the current research. It includes a summary of the key findings of the research being studied and highlights the insights and importance of this study in relation to existing research on the topic. This section explores the relationship between human behavioral factors and cybersecurity among cultural groups, focusing on how trust may shape individuals' decisions and actions related to online security. The review draws heavily on articles and studies from the following sources: Purdue University library database, Google Scholar, Science Direct, and Elsevier. The selected articles and studies were carefully chosen for their relevance to the topic, specifically, human behaviors or factors in cybersecurity, the role culture has on human behavior and the differences in the perception of trust.

This literature review will start with a comprehensive overview of cybersecurity, including an analysis of common cyber-attacks, the impacts, and the goals of these attacks. Subsequently, an in-depth review of the relationship between human behaviors and cybersecurity will focus on the processes that shape decision-making and behavior in this domain. A review of current research on this topic will also be discussed. The following section will analyze culture's effect on human behaviors and how it impacts people's perceptions and evaluations of cybersecurity risks. The literature review will also explore how trust may influence decision-making and risky behavior in the realm of cybersecurity. Furthermore, the literature review will include an overview of previous questionnaires used to evaluate behaviors related to cybersecurity and scales used to measure the

perceptions of trust. The literature review process allows for identifying gaps in research and areas that require further investigation.

Cybersecurity Overview

The National Institute of Standards and Technology (NIST) (2020) defined cybersecurity as the "practice of protecting computers, servers, mobile devices, electronic systems, networks, and data from digital attacks, theft, and damage" (p. 1). The main goal of cybersecurity is to implement policies and use technological tools to secure systems and networks, prevent unauthorized use and access, and prevent cyber threats from occurring. This includes a wide range of technical and non-technical strategies such as using antivirus software and providing educational and training material, as well as implementing policies and best practices. Using a more technical explanation, cybersecurity aims to protect against cyber threats to prevent data breaches from occurring and to safeguard the three fundamental components of security, known as the confidentiality, integrity, and availability of sensitive information. Confidentiality, integrity, and availability, known as the CIA Triad, are the core of cyber and information security (Qadir et al., 2016) and serve as a guide for designing and assessing the efficacy of security measures (Henderson, 2015). The CIA security triad, shown in Figure 1, contains the three fundamental foundations of security: confidentiality – the protection of private information and unauthorized access, integrity – assuring that information is accurate and has not been tampered with, and availability – ensuring information and systems are available when needed. Incorporating all three principles of the CIA triad into security policies can provide a comprehensive approach to safeguarding businesses, organizations, and governments.

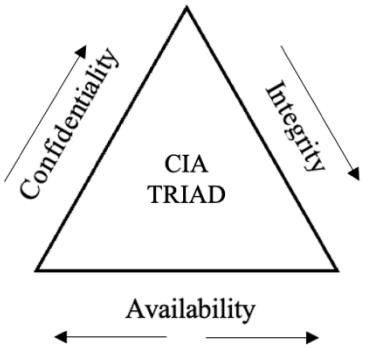

Figure 1. The CIA Triad

Note: This figure has been adapted from the original work of Qadir, S and Quadri, S (2016). The adaptation includes simple modifications made by the present author to better suit the context of this paper.

The CIA Triad model aids in understanding and evaluating the security measures of an organization and an assessment of its valuable resources. It helps identify weak points and minimize risks of security incidents from happening. It is also used to teach employees about good security practices. If a security incident happens, like a data breach, it means that one of the principles of the CIA Triad has been broken, no matter what or who caused the breach (Araiza, 2022). It is a widely recognized standard of guiding security policies and procedures in the field of cybersecurity. Although the triad has shaped a theoretical understanding and a solid foundation in cybersecurity, it has been criticized for mainly focusing on the technical controls and overlooking the socio-technical, human behavioral aspects of security (Harris, 2002; Oltramari et al., 2015; Kolkowska et al., 2009; Anderson, 2003). Additionally, it only represents a subset and addresses a limited aspect of risks (Veale et al., 2020). Nonetheless, the CIA Triad plays a vital role in cybersecurity and information security practices.

While cybersecurity is a commonly used term for the protection against attacks, there are several other areas within the field of cybersecurity that play a role in protecting different types of cyberthreats and cyberattacks. These areas include network security, endpoint security, information security, application security, cloud security, and data security. Each area has its own

responsibilities and protect a specific area of the digital world. This paper mainly focused on the general approach of cybersecurity. The terms cybersecurity and information security have been commonly used interchangeably in the literature; however, the meaning and purpose of the two terms are quite different. Information security, as defined by NIST, is “protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide integrity, confidentiality, and availability” (Barker, 2003). Cybersecurity, on the other hand, is known as the techniques and processes that are established to defend the digital environment of users, companies, and organizations against cyber threats. The International Telecommunications Union (2008) defined cyber security as “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets” (p. 2). Cyber-attackers when taking advantage of cyberthreats, have a main goal, which is to either gain entry to, manipulate, obliterate sensitive and private data, demand payment from users, or interfere with standard business operations.

Cyber threats may have many negative impacts and severe consequences. The result of such threats could result in the loss or theft of private information, disruption of operations and productivity, financial loss, and damage to an organization's social status and reputation (Venkatachary, 2017). Cyber threats are known to be either intentional or unintentional actions that pose risks to individuals, computing devices, networks, and the information stored on them. Present-day life is primarily technology-driven, meaning that most financial, commercial, and social activities and interactions at all levels, individual, corporate, and governmental, are carried out in cyberspace (Aghajani et al., 2018). These threats are constantly changing and keeping up to speed with technological advancements. Threats can take on many forms and come from various

sources. Some common types of cyber threats include malware, phishing, denial of service (DoS) attacks and man-in-the-middle (MitM) attacks.

Cyberthreats are a significant concern in the current era of technology, the internet, and digital communication, as they can have extensive impacts on individuals, businesses, and governments. Cyber threats are potential risks or vulnerabilities that, if not properly mitigated, can lead to a cyber-attack. Cyber-attacks are the actualization of these risks or vulnerabilities – the deliberate and targeted efforts which can have significant consequences for organizations, individuals, governments, and critical infrastructures. More information on such attacks will be discussed in more detail further in this section. The goal of cybersecurity is to restrain cyber-attacks from happening or to minimalize their impact if they do occur. By identifying and addressing potential cyber threats, organizations can proactively protect themselves and their systems from harm (NIST, 2014). For example, suppose a cyber threat in the form of a malware infection is detected on a computer. In this specific example, the appropriate cybersecurity measures in position would be installing and updating antivirus software to help prevent the malware from infecting the system and causing damage.

Similarly, suppose a cyber threat in the form of a phishing scam is detected. In that case, cybersecurity measures include implementing supplemental education classes and training to prevent employees from falling victim to fraud and being more cautious about giving away private information. This is how cybersecurity and cyber threats interconnect, with cybersecurity measures serving as a defense against potential threats. By understanding the threats and vulnerabilities that the digital world faces, it is possible to reduce the risks of being targeted by cyberattacks to ensure that systems and data remain secure.

Cyberattacks

Cyberattacks, or cybercrime, are the main concerns in the growing field of cybersecurity, as they can compromise the security of individuals and businesses. A cyberattack is an electronic attack on individuals, systems, enterprises, and networks that intends to disrupt, steal, or corrupt assets. The purpose of a cyberattack is to compromise the confidentiality, integrity, and availability of digital data, services, and assets in cyberspace (Hodges, 2015). The motivations and methods behind cyberattack can vary widely, but they all aim for a common goal which is to gain unauthorized access or control over computing systems and networks. Another common motivation, which may be the most common reason, is financial gain by selling valuable data or stealing bank account information. Cyberattacks may be perpetrated by individuals or small groups, while others may be carried out with the backing of large organizations with greater resources, funds, and expertise to carry on these types of attacks. Despite differences in the size, the impact, or resources used to conduct such attacks, the ultimate purpose of any cyberattack remains the same.

Cyberattacks can be broadly categorized into two types of attacks: technical and non-technical attacks (Baror et al., 2019). Technical cyberattacks use malicious code that seeks to alter computer code, resulting in compromised systems and identity theft of private information. In contrast, non-technical cyberattacks use various psychological manipulation methods to influence a particular behavior and trick people into giving up valuable information or performing a risky action, such as gaining unauthorized access a computer network or system. The following discussion will delve into the most common technical and non-technical cyberattacks, emphasizing the latter.

Technical cyberattacks heavily rely on technical means, such as exploiting software and hardware systems vulnerabilities. These attacks require a deep understanding of networks and computer systems, programming capabilities, cryptography skills, and expertise in the field of engineering. Common technical cyberattacks include malware, denial of service, network intrusions, viruses, worms, ransomware, and SQL injection attacks (Aqeel et al., 2022). Malware, short for malicious software, is a program or file purposely intended to damage and penetrate a computer system or network (Harford, 2021). These malicious codes could disable and interrupt the performance and functioning of a system, giving hackers the ability to attain access to confidential information. Malware varies in its methods of destruction. It is specifically made to be hidden so it can remain inside a system for long periods without being noticed by the system owner (Speed, 2012). In fact, most industry reports state that the average time elapsed between incidents of security breaches and their detection is between 200 and 300 days (Pogue, 2018).

Rootkits, botnets, worms, spyware, and trojan horses are the most dominant forms of malware that can cause significant damage to networks and operating systems (Feizollah et al., 2015). Rootkits are a type of software made to hide their presence from detection while maintaining privileged access to a user's system to leak sensitive information (Yin et al., 2007). Botnets are networks of hijacked computer devices that are under the control of an adversary used to carry out attacks (Stone-Gross et al., 2009). Worms and trojan horse malware are similar and spread across a network by propagating and self-replicating from one computer to another (Mishra et al., 2012). Spyware tracks and invades devices by monitoring, tracking, and collecting information such as locations, contacts, emails without the user's knowledge (Ahvanooey et al., 2017). To tackle these types of attacks, anti-malware and antivirus applications use detailed and pre-defined algorithms and patterns to detect malware (Razak et al., 2016) and stop potential

attacks. Malware can also use social engineering tactics to take advantage of and attract target users to run the malicious code through email attachments or messaging applications that allow malware to spread (Fruhlinger, 2022). A denial of service (DoS) attack is a form of cyberattack created to disrupt a network system's operation by overloading it with high traffic volume preventing requests from accessing the network infrastructure (Kumari et al., 2022). This type of cyberattack takes advantage of servers by sending overwhelming requests to make the network inaccessible and non-functional for its intended users (CISA, 2022). These large numbers of requests typically use many interconnected machines and take advantage of security vulnerabilities to carry out one target. The more sophisticated the DoS attacks are, the greater the chances of bypassing cybersecurity measures and increasing their chances of success (Gebreyes, 2020).

Network intrusion attacks are the act of penetrating a computer system and can be presented in two forms: passive, in which penetration is gained discreetly and unnoticed, or active, in which modifications to a network are made (West, 2009). Such attacks include worms, computer viruses that typically spread through email attachments, traffic flooding, and trojan horse malware (Gaylord, 2019). Traffic flooding involves excessive loads that exceed the system's capacity, while trojan horse viruses establish a network backdoor that enables attackers to gain unauthorized access to the network and data. Ransomware attacks come in the form of malware that encrypts the victim's confidential data and then threatens and blackmails the victim by demanding a ransom in exchange for the information back (Hull et al., 2019).

The most recent ransomware attack was against Accenture in 2021, in which attackers demanded a $50 million ransom for the stolen information (Freed, 2022). Most ransomware attacks seek financial gain; when unsuccessful, they typically vow to release proprietary information. SQL injection attacks are malicious code injected into application/user input specifications and later

carried to a back-end server for decoding and execution (Clarke, 2009). SQL injections exploit vulnerabilities to access and manipulate the data stored in a website's database to steal information, interrupt services, or obtain unauthorized access to sensitive data. Using security software and regularly updating it can help to protect against malware and other threats. By being aware of the risks posed by non-technical cyberattacks and taking the necessary precautions, individuals and businesses can better protect themselves against these threats, even when technical measures may not be sufficient. This entails exercising caution when dealing with emails or messages from unfamiliar sources, validating the legitimacy of websites before inputting sensitive information, and utilizing security software to safeguard against malware. By cautiously following these steps, individuals and businesses can better defend themselves against non-technical cyberattacks that may go undetected by technical measures. To effectively prevent and defend against cyberattacks, it is necessary to invest in technical resources and provide training for individuals with the technical skills and expertise required for cyber defense.

Non-technical cyberattacks target users of a system rather than the system itself by using manipulation techniques to influence specific behaviors of victims, also known as social engineering. Social engineering attacks are currently cybersecurity's most significant risks (Chargo, 2018; Libicki, 2018; Costantino et al., 2018). Social engineering attacks require various steps in which the attacker collects as much information as possible about their victims using emotional manipulation. Attackers usually conduct substantial research on the target, such as their name, job location, title, contact information, or recent vacations from their social media. They tend to develop a relationship with these victims, plan and exploit a vulnerability, execute the attack, and disappear without leaving any evidence (Kaspersky, 2020).

Social engineering tactics are highly effective because these types of attacks take advantage of the human inclination to trust others. People generally assume that others have good intentions and act in good faith, making them vulnerable to such attacks (Salahdine et al., 2019). Figure 2 provides a visual representation of a common approach employed by attackers in user-oriented cyber-attacks. The attackers plan the attack and rely on unsuspecting victims to unwittingly participate. The victims interact with the attack, for example by clicking on a malicious link, thereby enabling the attack to propagate across systems and networks. As a result, critical assets become compromised and private, sensitive data may be stolen. Cybercriminals favor this method as it allows them to circumvent firewalls and intrusion detection systems. Targeting users, the attacker can gain access to valuable assets such as databases and sensitive files. Once the user's device is compromised, the attacker can use it to spread malware and steal sensitive information throughout the network.

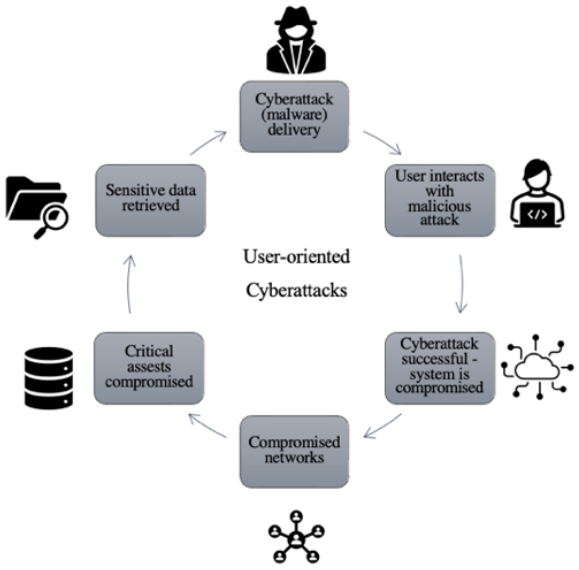

Figure 2. User-oriented Cyberattack

Note: This figure has been adapted from the original work of Hamoud et al. (2020). The adaptation includes simple modifications made by the present author to better suit the context of this paper.

The most common social engineering cyberattacks are phishing, baiting, and pretexting (Kaspersky, 2020). A staggering 90% of data breaches are caused by phishing scams (Cybertalk, 2022), and the percentage of such attacks is expected to increase 400% year after year (Federal Bureau of Investigation, 2021). Phishing, also known as phishing scams, is well-crafted email or text messages that appear to be from a legitimate source, such as a well-known person of a company, government agency, bank, or business. An example of a phishing scam email is shown in Figure 3. The email is crafted in a way that would be difficult for an average user to detect because cyberattacks typically target individuals unaware of the risks and how to identify a phishing attempt correctly. Phishing scams, through emails or messages, convince the victim to give up private information, transfer money, or click on a malicious link. Phishing scams use persuasive and deceptive language and trust-building tactics to establish credibility with the victim. Cybercriminals frequently use strategies such as posing as tech support, claiming to be a representative from the IRS, and sending emails from well-known businesses to inform recipients of suspicious activity. These attacks can be persuasive and difficult to distinguish from legitimate messages, which is why they are often successful (Salahdine et al., 2019).

It is also essential to be careful of email or text messages from unidentified sources and verify websites' authenticity before entering sensitive information. As shown in Figure 3, logos, graphics, font, and the opt-out instructions indicate that this phishing attempt originated from an authentic source. However, there are a few signs that indicate this email is a phishing scam: sender's email address does not match the company it claims to be from, and there are a few grammatical mistakes, the sender is requesting immediate, urgent action to be made, email contains links and attachments.

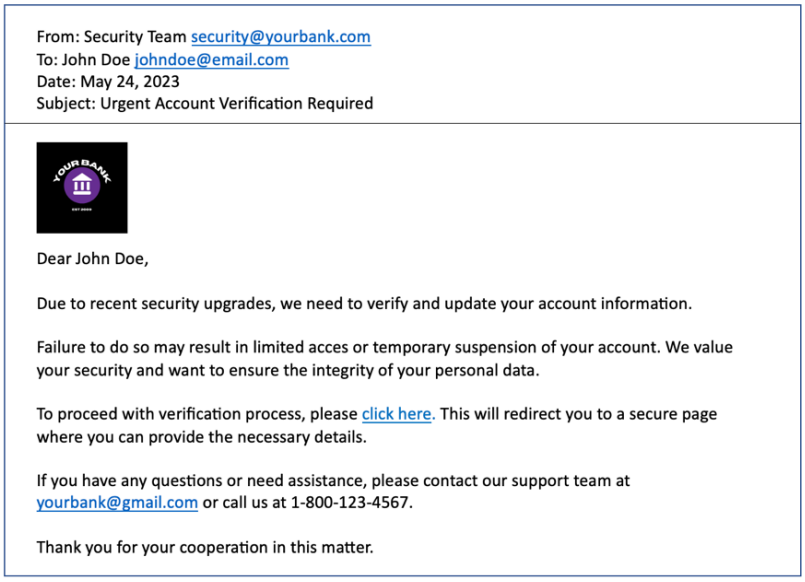

Figure 3. Phishing Scam Email Example

Baiting attacks use manipulation techniques by offering tempting agreements or promises, such as exclusive access to certain services or attractive financial gain, stimulating curiosity and convincing the victim to take a particular action (Iuga et al., 2016). Baiting often employs similar tactics to phishing scams, using persuasive language and a sense of urgency to persuade victims to disclose sensitive information or carry out behaviors or tasks. Upon successful manipulation, victims enter their private information into the site under the false belief that it is legitimate (Iuga et al., 2016). Pretexting presents a false identity and inventing a scenario to request information and gather desired material by personally interacting with the victim, either over the phone or in person (Wilhelm, 2013). To illustrate the concept of pretexting, an attacker looks up a victim of a particular company and gathers as much information as possible about the victim. In this attack, the attacker disguises themselves as a UPS delivery driver and goes to the front desk of a business, claiming to have a package for the victim. The attacker may gather information about the victim and the business through online sources such as social media accounts or searching through a recycled waste bin for sensitive information. Consequently, organizations face a range of primary

cybersecurity risks, including malware, ransomware, and insider threats, which involve the utilization of deceptive tactics, manipulation, and the exploitation of human trust as part of human-driven cyber threats (Eira, 2023).

Cyberattacks are a growing problem and can affect individuals and businesses. According to a recent report distributed by Cybersecurity Ventures, the worldwide expense of cybercrime is projected to range from over $10.5 trillion annually by 2025, up by three trillion dollars in 2015 (Cybersecurity Ventures, 2020). Another study by the Center for Strategic and International Studies (2018) found that the average cost of a single data breach is an estimated $3.92 million. Personal information, among other valuable data, may be compromised in cyberattacks, potentially resulting in identity theft and financial harm to individuals. For businesses, cyberattacks can easily disrupt operations and damage reputation. According to the National Cybersecurity Alliance (2022), small businesses are the target of 43% of cyberattacks, and within six months of being attacked, 60% of small businesses go out of business. The future of cybersecurity will likely be shaped by the increasing sophistication and frequency of cyber-attacks and the growing use of artificial intelligence, machine learning, and the Internet of Things (IoT) (Markets and Markets, 2020). These technologies automate identifying and exploiting vulnerabilities by identifying targets and generating new forms of malware (NIST, 2019). The continued growth of technology and the increasing number of interconnected devices make cybersecurity a constant necessity and will remain a top priority.

Human Behaviors

The terms human element and human behavior are commonly referred to as *human factors*. Human factors in cybersecurity refer to how human behaviors, capabilities, and restrictions can

impact the effectiveness of cybersecurity measures. Behaviors may include situations of careless or uninformed behavior, such as clicking on a malicious link, neglecting security measures, frequently using weak or easily guessable passwords, providing private and sensitive information to unauthorized individuals, and failing to recognize or follow cybersecurity best practices (Parsons et al., 2010; Connolly et al., 2019; Moody et al., 2018). According to the Pew Research Center (2017), while many have been affected by security breaches, the average American has limited knowledge of cybersecurity issues. In view of current technological advancements, a holistic view that prioritizes the human behavioral factors that shape security decisions is needed to understand and address cybersecurity from a human perspective.

The cyber domain is an interdisciplinary field that integrates various branches of knowledge, including engineering, computer science, sociology, technology, mathematics, psychology, and law (Dawson et al., 2018). A critical aspect of the cyber field is the need for cybersecurity, which involves technical and non-technical measures to minimize and safeguard against cyberattacks, protect data and ensure business continuity. Traditionally, the field of cybersecurity has had a technology-centric approach, meaning that it has mainly focused on technical solutions to protect systems and networks from cyber-attacks. However, this approach does not consider the human factors and motivations that play a role in cybersecurity incidents. Studies by Abawajy (2014), Aoyama et al. (2015), and Glaspie (2018) have emphasized the importance of considering human factors, influences, and motivations in cybersecurity and how this can be used to develop more effective security measures.

Human errors are widely recognized as the leading cause of cybersecurity breaches and are considered the weakest link in the security chain (Cybersecurity Ventures, 2020; Risto, 2016). Despite the importance of addressing human factors in cybersecurity risk assessments, research in

this area is very limited. According to a study by Gillam et al. (2020), only four percent of peer-reviewed cybersecurity research studies published between 1996 and 2018 focused on human behaviors/factors in cybersecurity. To continue to be increasingly effective against cyber-attacks and dangers, a paradigm shift from "humans are part of the issue" to "humans are part of the solution" is required (Zimmermann et al., 2019). As such, humans remain a crucial, inescapable, and unavoidable component of cybersecurity (Pollini et al., 2022).

Human behavior in relation to cybersecurity is a complex topic with various contributing factors. Studies have shown that individual traits significantly influence how people make decisions regarding online security risks. A study conducted by Russell et al. (2017) found that personality attributes, such as neuroticism and conscientiousness, were positively correlated with cybersecurity behavior. Similarly, Bulgurcu et al. (2010) found that individuals who have higher levels of trust in technology and self-efficacy were less likely to engage in risky cybersecurity behavior. Furthermore, research has discovered differences in secure behavior compliance among different ethnicities. For instance, Hovav et al. (2012) found that individuals who are more collectivistic in nature were more likely to comply with organizational policies related to information security. Studies such as Shappie et al. (2019) and McCormac et al. (2017), and Ifinedo (2022) also found a positive correlation between individual traits and cybersecurity risky behavior. Other studies have investigated predictors of risky behaviors toward cybersecurity, such as impulsiveness (Aivazpour et al., 2018), educational level (Chua et al., 2018), and work experience (Hadlington, 2018). Still, the influences of cultural factors received limited attention.

The internet’s worldwide reach and interconnectedness enables for vulnerabilities to increase and gives cybercriminals opportunities to promote their attacks to broader target audiences in less time and at meager costs (Canadian Centre for Cybersecurity, 2018). Research

has demonstrated a direct relationship between human factors and the occurrence of data breaches (Hughes-Lartey et al., 2021), meaning that most successful cyberattacks result from human error (Kelly, 2017; El-Bably, 2021; Kobis, 2021); regardless of how sophisticated and advanced technical measures are, security will continue to be confined by human factors (Threatcop, 2021; Karachı, 2017).

Human factors play a vital role in designing and implementing cybersecurity measures. It is fundamental to consider how humans will use and understand these measures to make them effective. Business and organizational leaders need to give proper focus to human behavior to develop cybersecurity strategies, leading to a lack of adaptability to emerging threats and risks (Triplett, 2022). The Healthcare Cybersecurity Survey conducted by SANS indicated that 51% of threats were caused by neglect from an insider, however, within the same documentation of future security recommendations, human factors were not mentioned as a strategy for enhancing security measures (Evans et al., 2016). This lack of focus on human behavior can lead to a lack of resiliency and flexibility regarding emerging threats and risks and a lack of awareness about the individual's role in protecting against those threats. As a result, organizations may struggle to maintain pace with evolving cybersecurity threats and vulnerabilities and may be more vulnerable to attacks. This highlights the importance of not only human behaviors but also incorporating individual differences when developing cybersecurity plans and protocols (Jaferian et al., 2011), as it can help organizations stay ahead of emerging threats and better protect against attacks.

Previous research on measuring and evaluating human behavior in the realm of cybersecurity has utilized a variety of methods, such as surveys and interviews to gather data on individuals' attitudes and risk-related behaviors (Faklaris et al., 2019). Other studies have used experiments, such as theoretical games, to observe cognitive processes in decision-making settings

and evaluate risky behaviors (Beuran et al., 2018). Additionally, monitoring software and security incident log flow have been installed to observe and measure employee behavior and gather information on user behavior in the cyber domain to improve security efforts (Lalonde Levesque et al., 2013). Furthermore, security training and educational programs have been implemented and evaluated through pre-and post-training assessments, measuring changes in employee knowledge and attitudes towards cybersecurity (McCrohan et al., 2010). These methods are valuable ways to understand the human behavioral aspect of cybersecurity. To gain insights into the influences of human behavior related to cybersecurity and examine cultural differences in these behaviors, this study employed a widely used form of surveys. Furthermore, this study aims to investigate the diverse perspectives on trust across cultural groups and explore any possible links to cybersecurity risk behaviors.

Culture

Culture is a complex, multifaceted term that encompasses many factors influencing how people interact with one another and the world around them. Researchers have extensively studied culture (Kluckhohn, 1951; Schein, 1990; Bodley, 2017; Walsham, 2002), many of whom have proposed various definitions highlighting its many dimensions and nuances. At its most basic level, culture can be described as the unique experiences, language, personal views, practices, values, and social norms that individuals have been exposed to and internalized through their upbringing and life experiences (Brislin, 1970). While these terms are commonly used interchangeably, the terms *culture, race,* and *ethnicity* have distinct definitions (Arora et al., 2017). Race signifies socially constructed classifications based on physical qualities. In contrast, ethnicity signifies individuals' affiliation with a particular group based on shared history, clothing, food, literature, location, language, or religion (Johnson, 2000). Through their shared practices and interactions,

people create their culture, which shapes how they engage with the world and build their communities (Causadias, 2020).

Cross-cultural studies generally aim to understand the link between cultural context and variations in human behavior through systematic comparisons of different cultures (Papayiannis et al., 2011). Cultural backgrounds influence how individuals perceive and interpret the world around them through their own cultural lens (Bourrelle, 2015) and are known to highly guide human behavior (Han et al., 2015; Lugrin et al., 2015; Bourrelle, 2015). This can alter certain behaviors, attitudes, and habits (Kastanakis et al., 2014), but generally, cultural practices and behaviors tend to remain consistent across generations (Snowdon, 2018). Similarly, culture may significantly influence human behavior in the realm of cybersecurity (Crespo-Pérez, 2021). While much research has been conducted on cybersecurity-related educational programs and policies, there is insufficient attention given to the cultural factors that influence human behavior in this domain. This gap in understanding can limit the effectiveness of cybersecurity strategies in diverse cultural environments. Cross-cultural research can provide valuable insights into how cultural values and beliefs shape individuals' risk-taking behaviors and perceptions of cybersecurity. Future studies can further delve into the specific cultural influences on decision-making styles, information interpretation, attention, and risk-taking behaviors, which would inform the development of more effective cybersecurity strategies that consider individuals' cultural differences.

Cross-cultural research has pursued to recognize the specific cultural differences that influence human behavior in various areas, including decision-making, information interpretation, communication, and attention differences (Yates et al., 2016). Studies have shown that people from different cultures often have distinct decision-making styles. Culture plays a significant role

in shaping an individual's perception and framing their understanding of certain events and situations that in turn influences their behavior (Oyserman et al., 2011; Weber et al., 2010). It determines how people construct and interpret meaning from a given scenario based on prior experiences and cultural norms (Weber et al., 2010). According to several theorists and researchers, every person belongs to at least one cultural group, and some may even carry several levels of cultural categories (Trompenaars et al., 1994; Hofstede, 1980). Fredrick Erickson (1985), a well-known theorist who studied cultural differences of ways people communicate in learning environments. He emphasized the importance of acknowledging and understanding the cultural context in which communication takes place. He highlighted that cultural differences shape how individuals experience and understand the world around them. Similarly, anthropologist Edward Hall (1976) proposed the Cultural Dimensions Theory which supports Erickson's (1985) theory in terms of cultural impacts of how individuals interpret the world and is greatly influenced by situations and past experiences. He argues that communication contexts – high context and how context – is greatly dependent on the cultural background of individuals. In high-context cultures, which are prevalent in Asia and Africa, the nonverbal context of a message is highly significant. People have a more indirect communication style. In contrast, in low-context cultures, like United States, people have a more direct communication style. According to Hall (1976), it is fundamental to acknowledge and understand these differences for effective cross-cultural communication.

Studies have demonstrated that individualism and collectivism have a significant impact on cultural disparities in the consideration of certain situations (Masuda et al., 2001). One study discovered, for instance, that people from Eastern cultures, such as Japanese and Chinese, typically have a more holistic attentional style, which means they concentrate more on personal connections and contexts of a situation rather than specific details or individual features (Varnum et al., 2010).

People from Western cultures, such as those in the United States and Europe, on the other hand, typically have a more analytical attentional style, which means they are more inclined to concentrate on details and individual components within a situation (Nisbett et al., 2001; Chua et al., 2005). Culture significantly impacts individuals' perspectives, affecting how they understand and interpret their environment. It can also shape decision-making, perceptions of situations and events, problem-solving approaches, and meaning construction and interpretation by individuals within their society or community. By analyzing the distribution of this dimension, it may provide insights on how individualism and collectivism affects the way people pay attention to specific situations, i.e., in the context of cybersecurity.

Recently, there has been an increasing interest in exploring the effects of cultural differences on various aspects of society through research studies. This attraction is due to the recognition that cultural differences play a significant role in shaping individuals' perceptions, perspectives, behaviors, and decision-making and can significantly impact different areas such as education, business, healthcare, and technology. Examples of research methods used to evaluate and measure cultural differences include questionnaires, interviews, case studies, observations, and assessments. One of the most widely used studies measuring cultural differences is Hofstede's (1980) Cultural Dimensions Theory framework. His theory is based on research he conducted using the Values Survey Model (VSM), a survey instrument used on a large company to measure cultural differences in work-related values and to describe how culture influences behavior. Hofstede's (1990) theory identifies six dimensions of culture, each of which describes the impacts of cultural backgrounds on the behavior of people who live within that culture.

These dimensions identified by Hofstede (1990) include Power Distance, Individualism vs. Collectivism, Masculinity vs. Femininity, Uncertainty Avoidance, Long-term Orientation vs.

Short-term Orientation, and Indulgence vs. Restraint. Each dimension represents a fundamental concern for any society, and a variety of possible solutions can be found for each dimension. Due to their relevance in identifying cultural differences in human behavior between individuals, individualism and collectivism have received the most attention as fundamental dimensions of cultural variation in cross-cultural research (Brewer et al., 2007; Dumont, 1986; Fatehi et al., 2020). The primary emphasis of this study revolves around the concept, or dimension of individualism and collectivism, which describes the extent to which individuals in a community are incorporated into social groups (Hofstede, 2010). Refer to Table 1 for a description of the model's individualistic and collectivist dimensions.

Table 1. Dimensions of Culture: The Hofstede Model of Individualism and Collectivism

Individualism	Collectivism
Everyone is supposed to take care of him or herself and his or her immediate family only	People are born into extended families or clans which protect them in exchange for loyalty
"I" – consciousness	"We" – consciousness
Right of privacy	Stress on belonging
Speaking one's mind is healthy	Harmony should always be maintained
Others classified as individuals	Others classified as in-group or out-group
Personal opinion expected: one person one vote	Opinions and votes predetermined by in-group
Transgression of norms leads to guilt feelings	Transgression of norms leads to shame feelings
Languages in which the word "I" is indispensable	Language in which the word "I" is avoided
Purpose of education is learning how to learn	Purpose of education is learning how to do
Task prevails over relationships	Relationship prevails over task

Note: Hofstede (2010) model of individualism and collectivism

Individualism refers to an emphasis on individual goals and needs, while collectivism emphasizes the interests and objectives of the group, rather than on an individual (Triandis et al., 1998). This dimension has received the most attention because it gives insights into understanding how behavior is shaped and further identifies patterns and trends in behavior across cultures.

Similarly, understanding how culture influences and impacts human behavior towards cybersecurity may provide insights into how individuals and groups may be more or less likely to engage in risky online behaviors that may increase their susceptibility to cyber risks and threats. This can be achieved through the study of cross-cultural patterns and trends, which allows for identification of the cultural factors that shape human behavior and develop cultural theories and models that can help better understand and anticipate the actions and behaviors of individuals and groups (Cronk, 2017) and identify common behaviors that are more prone to risky security practices. These insights may assist researchers and cybersecurity experts to develop targeted educational efforts and tailored security measures to minimize vulnerabilities and threats (Gratian et al., 2018). This study's findings utilized Hofstede's (1990) categorization of countries to classify cultural groups as either individualistic or collectivistic in nature. Hofstede (1990) classified Western nations such as the United States, Canada, Sweden, and New Zealand as having a strong inclination towards individualism. On the other hand, most Eastern countries such as Russia, Mauritania, and Algeria were identified as more collectivistic in nature.

The dimension of individualism and collectivism is particularly relevant to this research study as it relates to decision-making and understanding how cultural differences shape how people and groups make decisions. Different cultural values and beliefs can shape how people view the importance of protecting against cyber threats and can modify their perspectives and habits toward cybersecurity. In other words, cultural values and beliefs can impact an individual's likelihood of engaging in risky online behaviors, such as sharing work laptops, clicking on suspicious links, or sharing sensitive information (Williams et al., 2017). Comparably, the cultural context in which an individual was brought up, may influence how they perceive the value of

personal information and the risks associated with sharing it online, as well as how they view the role of the individual versus the community in protecting against cyber threats.

There is evidence to suggest that culture shapes how humans approach cybersecurity and impacts security and risky human behavior (Kharlamov et al., 202), but research on this topic is limited. Research on human behavior in cybersecurity has focused mainly on educational programs for safe online behavior, developing policies and procedures (Aldawood et al., 2019), and cybersecurity measures' legal and ethical implications. Research has not adequately addressed the role of cultural backgrounds in influencing and shaping certain human behaviors. This leaves a significant gap in understanding culturally influenced human behaviors in cybersecurity and highlights the need for further research on this topic. This lack of understanding can potentially limit the effectiveness of cybersecurity strategies, particularly in culturally diverse environments. Considering cultural factors in the field of cybersecurity is crucial in understanding and addressing the complexities of human behavior and decision-making in this context. It enables the design of more effective and culturally appropriate cybersecurity programs and policies, leading to a more comprehensive and inclusive approach to protecting against cyber threats.

Trust

Trust has been a popular research topic across various fields and has gained significant attention in recent years (Mitchell et al., 2009). Trust is of utmost importance in cybersecurity, affecting how people approach and manage online security and privacy issues. Many factors can influence trust, and one of these is cultural background. Cultural backgrounds can influence how people perceive trust and how they approach problems related to trust. Trust is a multifaceted concept with many layers of meaning and implications. According to three online dictionaries, Websters, Random House, and Oxford, the definition of trust has an average of 17 definitions,

whereas similar terms, such as confidence, have an average of 4.7 (McKnight et al., 2000). There is much difficulty narrowing down the definition of trust to one specific domain, hence the high number of definitions of trust currently available. Generally, trust is understood as the belief and ability that someone or something is reliable and truthful (Marsh et al., 2005). The most commonly cited definition of trust, proposed by Mayer and colleagues (1995) is defined as "the aspect of relationships, the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action necessary to the trustor, irrespective of the ability to monitor or control that other party" (p. 712). Mayer et al.'s (1995) definition stemmed from a review of literature from various fields that provided many insightful perspectives on trust, which resulted in combining these concepts into one single model (Schoorman, 2007).

Traditionally, trust is described as the involvement of two people: the trustor and the trustee, and is dependent on three elements: integrity, ability, and benevolence. Integrity is the perception of the trustor to the trustee that both parties will adhere to principles and values the trustor finds reasonable (Mayer et al., 1995). Ability is services offered relative to the trustor's background, experience, and knowledge in essential areas (Matheson, 2004). Benevolence is wanting to do good without expecting anything in return. According to Mayer et al. (1995), these three characteristics may likely vary independently of each other but emphasized that without these three elements, trust does not exist. More recent studies of trust use the definition put forward by (Krebs et al., 2006), which defines *trust* as the "confidence that members have in each other's dependability and expertise" (p.723). Each team member holds certain expectations of others to fulfill their required and predetermined responsibilities. This definition implies trust is not easily achieved and is developed over time through repeated, continuous social interaction (Krebs et al., 2006).

Other researchers defined *trust* as "a personality trait of people interacting with peripheral environments of an organization" (Farris et al., 1973, p. 145). This definition views trust as a trait that leads to certain expectations of trustworthiness also referred to as the propensity to trust. A slightly different approach, acquired by McKnight (2001), defined trust as "the extent to which one displays a consistent tendency to be willing to depend on others in general, across a broad spectrum of situations and persons" (p. 45). This suggests trust is developed when one is generally willing to depend on others. Lewis et al. (1985) defined *trust* as "the undertaking of a risky course of action in the confident expectation that all persons involved in the action will act competently and dutifully" (p. 971). Trust is a complex term with numerous connotations; as the well-known saying goes, trust is hard to gain but easy to lose. Despite the efforts of scholars to enhance comprehension of trust in specific fields, it remains difficult to identify a universally accepted definition that can be applied across the various contexts and scenarios explored in the literature. For this study, *trust* will be defined as the willingness to expose oneself to vulnerability by another individual, considering past experiences, future roles, cultural backgrounds, positive mutual interactions, and the belief that all parties involved will act responsibly and fulfill their obligations.

Research has also shown that trust levels can vary significantly among individuals from different cultural backgrounds (Ariss et al., 2002; Mayer et al., 1995). The complexity of examining trust among various cultural groups is this: each culture has what is known as a 'cultural sphere,' and each sphere shapes how a person thinks and is independent of other spheres (Bryk et al., 2003). The interactions with different 'cultural spheres' that dominate in some instances and subside in others unravel the complexity of maintaining trust among unfamiliar parties (Saunders et al., 2010). People who share similar cultural norms tend to trust each other more because they follow similar processes for determining trustworthiness. In other words, the steps the target takes

to earn trust are the same steps that the trustor takes to determine whether the target is trustworthy (Doney et al., 1998). Trust is mainly socially positioned, meaning it changes depending on the time and place and is highly dependent on cultural and sociopolitical factors (Marková et al., 2004).

Moreover, trust is developed differently across various cultures (Zaheer et al., 2006; Fukuyama, 1996). This can be seen in how people communicate, express feelings, and resolve conflicts. For example, in some cultures, direct communication and confrontation may be seen as a sign of respect, while indirect communication or avoidance may be preferred in others. In cultural groups that prioritize task-oriented behaviors, such as those found in the United States, Germany, and Australia, trust is often established on a cognitive level, where individuals associate trust with their confidence in another person's abilities and accomplishments. In cultures that place greater emphasis on building relationships, such as those found in China, Jordan, and Nigeria, trust is often established on a more personal and emotional level (Meyer, 2017). According to Javidan et al. (2019), in many cultures worldwide, trust is often based on reputation and character. Riemhofer (2019) notes that Germans place high value on credibility and reliability, while Scroope (2017) explains that in French culture, trust is established through proper behavior and demonstration of courtesy and formality. West Asians tend to view trust based on its impact on caution (Kwantes et al., 2021), and Brazilians require social interaction strategies (jeitinho) to grasp the meaning of trust (Kwantes et al., 2021). From an African perspective, trust implies hope, reliance, and the expectation that others will behave conscientiously (Kwantes et al., 2021). In Iran, trust is viewed as honesty, secrecy, religious devotion, and protection of both material and nonmaterial possessions (Talaei et al., 2013). Trust in the United States tends to be more complex due to its large and diverse population, with higher levels of trust in the workplace than in general society (Kwantes et al., 2021).

Research has also shown how trust levels varied significantly between cultures. For example, 49% of respondents in Saudi Arabia expressed overall trust in business leaders, while in Spain, only 14% of respondents did so (IPSOS, 2021). Similarly, 72% of respondents in Great Britain reported trust in doctors, while only 38% of respondents in South Korea did so (IPSOS, 2021). The findings of this study show that cultural backgrounds shapes people's understanding and perceptions of trust, which is reflected in the different views of trust within different cultures (Lane, 1997; Lane et al., 1996; Doney, 1998).

Trust is a foundational aspect of human interactions and influences decision-making, risk perceptions, knowledge-sharing, and communication (Mayer et al., 1995). Similarly, trust may likely influence cultural behaviors, which pose security risks in cyberspace. The cultural influences on human behavior in cybersecurity have received limited attention in the literature. This dissertation proposal aims to address this gap in knowledge and the findings of this study may provide valuable insights into the cross-cultural differences of influences on human behaviors and how they may impact cybersecurity risks. These insights may address and prevent human-related vulnerabilities in the future and contribute to a deeper understanding of the role of cultural factors in cybersecurity.

Cybersecurity Risk Assessment Frameworks

Cybersecurity risk assessment frameworks are a crucial part of strategic management, as they help prioritize threats and ensure that the most pressing issues are dealt with promptly to prevent disruptions. This study focuses on human behavioral factors that may impact cybersecurity risks, and as such, will examine assessment frameworks that take human behavior into account. Many popular frameworks, such as the National Institute of Standards and Technology (NIST), do not account for the vulnerabilities brought about by human behavior and the attackers who exploit

them (Henshel et al., 2016; King et al., 2018). Is important to consider and integrate human factors into cybersecurity risk assessments to understand the influences of human behavior on the protection of network systems (Cains et al., 2022). The following subsection evaluates the top three most common cybersecurity risk assessment frameworks, specifically those that consider the human element as part of the assessment.

The Human Affected Cyber Security Framework (HACS)

The Human Affected Cyber Security (HACS) Framework aims to address the human behavioral factors that contribute to cybersecurity vulnerabilities at both the individual and organizational level by providing potential solutions for these risky behaviors. Human risky behaviors are classified into seven categories: user validation violations, information sharing, misuse of technology, training, poor monitoring, and incident management, neglecting physical environment security, and deliberate, malicious attack. For instance, user validation violations may include poor password management practices, such as using the same password on multiple online platforms, not continuously updating passwords, and storing passwords in browsers. These practices increase the risk of data breaches and identity theft. Information sharing encompasses the ways in which vulnerability increases when information is shared, such as through personal emails, social media, shared in public areas, and USB memory drives. Misuse of technology encompasses the use of unauthorized equipment, downloading unapproved software, and using public Wi-Fi, which increases the risk of vulnerabilities in organizations.

The framework highlights the overlaps between the categories and how a failure to provide appropriate policies/procedures could lead to other risky behaviors. Additionally, it also considers how organizational culture can play a role in encouraging or neglecting certain behaviors, potentially leading to malicious attacks. While the HACS Framework considers the human factors

that enables cybersecurity risks and vulnerabilities, it falls short in addressing the underlying influences of these risky behaviors. It fails to consider the cross-cultural differences in human behaviors and the role it plays in influencing decisions.

Threat Modeling Approaches to Human Behavior/Factors (STRIDE-HF)

The Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of privilege – Human Factor (STRIDE-HF) is an extension of the existing framework, STRIDE and has been revised to address the human element as a possible source of cybersecurity risks. It evaluates potential impacts of human behaviors and provides ways to mitigate risks (Ferro et al., 2022). Each element of the STRIDE-HF model has been considered in the context of human error and identified ways it's related to each aspect of STRIDE. The elements of STRIDE-HF provide an overview of how the model could be used to address potential threats in the context of human behavior. For example, tampering threats may be a human factor risk behavior identified as a lack of awareness of the consequences and distraction due to job-related stress. Behaviors associated with tampering threats may be purposefully modifying files to documents and the response may include implementing a program where forms must be uploaded with a complete record containing username or ID, dates, and dates times logs. Elements such as trust, cross-cultural differences, and workplace culture are all factors that increase the likelihood that certain risky behaviors might differ from one employee to another (Ferro et al., 2022). This model provides a base outline that organizations may use to detect human behaviors that may be commonly overlooked. Future considerations with this model include iterations of various human factors, such as trust and character traits, especially in cyber environments.

The Human Factors Framework of Cybersecurity Risk Assessment (HFF)

Henshel et al. (2015) developed a cybersecurity risk assessment framework, known as the HFF framework, to incorporate trust as a critical factor of human influences on cybersecurity risks. According to Henshel (2016), trust in human factors is directly linked to assessments of risky behaviors and investigating trust can offer valuable understanding into the kind of behavior that is commonly associated with it. The framework divides human factors into two main categories: inherent characteristics that impact trust, which is based on the trustor's perception and can be influenced by external and internal factors, and situational characteristics, which pertain to the level of access granted by an organization through policies, software, and hardware. Inherent characteristics are further categorized into behavioral and knowledge skill characteristics. Behavioral characteristics capture rational/irrational behaviors, malevolent/benevolent, and integrity, while knowledge skills characteristics include expertise and attention-related influences.

Trust, the primary drive in this framework, is captured by public reputation and personal interaction– perceived honesty, credibility, and predictability. The level of trust an individual possesses from others is directly related to the level of trust they instill in others. Trust is an efficient defender and primarily depends upon the years of experience individuals possess, their educational background, and skills (Henshel et al., 2015). The HFF framework helps to identify these risky behaviors by evaluating, studying, and measuring how different perceptions of trust are generated and influenced among individuals with different cultural backgrounds.

The HFF framework is an effective tool for analyzing the correlation between trust and human factors that can affect cybersecurity risks, among other factors such as training, policies, and organizational culture. Trust is a key aspect of this framework, highlighting the significance of considering human behavior when evaluating cybersecurity risks. Additionally, the framework's focus on examining cultural variations in trust attitudes can give valuable perspectives on how

trust is perceived and affected by culture. The HFF offers a thorough method for including human behavior variations into a structure; however, its broad and general approach may not entirely capture the complexity and diversity of human behavior. By specifically investigating cultural factors that shape human behavior, organizations can gain valuable insight into how different groups perceive and approach cybersecurity risks. Additionally, by integrating cultural influences into the HFF, cybersecurity strategies can effectively customize their cybersecurity strategies to meet the specific needs of their workforce and anticipate the human factors that may contribute to cybersecurity risks. The HFF provides valuable contribution to the field of human factors in cybersecurity. However, this study differs from the HFF in that it focuses more on the perspective of the victims of a cyberattack rather than the behaviors of cyber-attacks. The HFF aims to characterize and examine the behaviors of attackers to develop predictive risk models, whereas this study seeks to examine the behaviors of the victims and how they perceive and respond to cybersecurity risks. By taking a victim-centered approach, this study provides a complementary perspective to the HFF and highlights the importance of considering both sides of the coin: the attacker and the victim in understanding and managing cybersecurity risks.

Previous Work

Measurement of Trust

Following the review of cybersecurity, culture, and trust, it is necessary to examine previous research on these subjects. This section provides a foundation for the current study to build and add to the existing knowledge in these areas. By understanding the work done in the past, it is possible to recognize gaps in the literature and address them in the current study. The previous

research on trust, cybersecurity, and culture can guide for creating of hypotheses and designing the current study. Therefore, a thorough review of prior work is essential to the research process.

Previous studies have measured trust in various contexts, including trust in virtual work teams (Tan et al., 2019), social trust (Gheorghiu et al., 2009), and social interactions (Watabe et al., 2015). Survey instruments such as questionnaires or interviews are commonly used to gather information on individuals' beliefs, attitudes, and trust-related experiences, and the data collected can be analyzed to understand how trust differs among cultural groups and how it relates to other variables such as social support, communication patterns, and relationship satisfaction. A popular trust scale frequently used in literature is the Generalized Trust Scale (GTS) (Yamagishi et al., 1994). The GTS was developed to measure trust in social interactions and consists of a self-report questionnaire with nine statements about trust, which participants are asked to rate their level of agreement with. These questions aim to assess an individual's general inclination to trust others and their expectations for the reliability of others. The GTS is a self-reported questionnaire designed to be completed independently by participants. Participants must rate their level of agreement with each statement on a scale from 1 (Strongly Disagree) to 5 (Strongly Agree).

The Generalized Trust Scale (GTS) is a widely used measure of trust in literature and has been found to have strong validity and reliability. The GTS has demonstrated good levels of internal consistency and strong test-retest reliability and has significant relationships with other trust-related constructs and measures. It has also been found to be a reliable predictor of various outcomes in different contexts. Table 2 presents a summary of the studies that have utilized the GTS scale to assess individuals' general level of trust. The use of the GTS in this study allows for a deeper understanding of trust and its relationship to other constructs outcomes.

Table 2. Summary of Studies Utilized the GTS

Study	Reference	Description
1	Jasielska et al., 2021	This study aims to present a Spanish adaptation of GTS to achieve a measure of propensity to trust that may enable applied and theoretical research on trust in Spanish. Results revealed good psychometric properties of the instrument, and the internal consistency analysis showed a Cronbach's alpha of .862.
2	Montoro et al., 2014	This study aimed to test whether the structure of the GTS is invariant across two countries representing more collectivist and more individualist cultures (Poland and the United States). Results of the study show the reliability was good for both American and Polish samples, with Cronbach's alpha of .83 and .82, respectively.
3	Lin et al., 2021	This study translated the GTS into Persian and validated its psychometric properties. Results indicated test-retest reliability was good, with an intraclass correlational coefficient of 0.865, and internal consistency was good, with a Cronbach's alpha of 0.881.
4	Ahorsu et al., 2022	This study aims to see the mediational role of trust in the healthcare system in the association between generalized trust and willingness to get COVID-19 vaccination in Iran. Results show the tool had an acceptable Cronbach's alpha reliability coefficient of 0.770.
5	Carlander et al., 2020	This study aims to validate the GTS, assuming that individuals' levels of trust and coping can buffer psychological stress. Findings show that GTS considers trust as a remedy for stress and could potentially be explained mainly as a proxy for a beneficial combination of personality, coping, and socioeconomic background.
6	Gobin et al., 2014	This study aims to measure the impact of betrayal trauma on the tendency to trust others. The GTS was used in this study, and results showed a strong internal consistency of Cronbach's alpha of 0.87, a strong convergent validity, and has shown strong correlations with other measures of the GTS.

Measurement of Cybersecurity Risks

The Risky Cybersecurity Behaviors Scale (RScB) is a tool that helps assess a person's inclination to engage in risky cybersecurity behaviors. The RScB is a self-reported questionnaire that comprises of series of statements about potentially dangerous cybersecurity habits, such as sharing passwords, clicking on links in suspicious emails, and connecting to unsecured Wi-Fi networks. The RScB is a useful tool for assessing the cybersecurity habits of individuals in various settings, including schools, businesses, and government agencies. Participants are asked to rate their level of agreement with each statement on a scale ranging from 1 (Strongly Disagree) to 4

(Strongly Agree). The RScB is used to identify areas where an individual may need to be more cautious in their online activities and to determine how likely they are to engage in risky cybersecurity behaviors. Several studies have found that the Risky Cybersecurity Behaviors Scale (RScB) has strong validity and reliability (Wijayanto et al., 2020; Hadlington et al., 2018; Nunes et al., 2021). This suggests that the RScB effectively measures the intended construct of risky cybersecurity behavior. In addition to its strong validity and reliability, the RScB may also have applicability, as it is practical, easy to administer, and used in various contexts. The RScB can provide valuable insights into cybersecurity behavioral habits and evaluate the cybersecurity awareness level of individuals. Table 3 provides a summary of previous research that has utilized the RScB scale and a brief description of the conducted study. The use of the RScB in this study allows for a richer understanding of risky cybersecurity behavior and its relationship to other constructs and outcomes.

Table 3. Studies that Used the Risky Cybersecurity Behaviors Scale (RScB)

Study	Reference	Description
1	Wijayanto et al., 2020	Researched assessed the cybersecurity weaknesses in universities during the Covid-19 outbreak. To analyze the conduct of internet and computer users, the RScB was employed. The findings showed a decent level of dependability with a Cronbach alpha coefficient of 0.721
2	Hadlington et al., 2018	Research used the RScB scale to investigate the essential actions that might result in individuals being at risk due to inadequate cybersecurity habits. Scale showed excellent internal consistency with a Cronbach's alpha of 0.823
3	Nunes et al., 2021	Research assessed the attitudes and actions related to cybersecurity within healthcare organizations in Portugal. The RScB scale was utilized in the study and produced a Cronbach’s alpha value of 0.745
4	Hadlington et al., 2018	Research investigated how media multitasking is linked to cognitive lapses in people's everyday lives in terms of their risky cybersecurity behaviors. Results indicate that everyday cognitive failures are strong indicators of risky cybersecurity behaviors. The study measured a high degree of internal consistency Cronbach’s alpha of 0.73
5	Aivazpour, et al., 2022	Research assessed the connection between impulsiveness and dangerous cybersecurity practices. Findings revealed that a person's addiction to the internet can forecast risky cybersecurity behaviors and a positive association between attentional impulsiveness and engaging in such hazardous online activities. The study obtained a Cronbach's alpha score of 0.70

In conclusion, previous research has shown that trust measurement has been conducted in various contexts and with the help of survey instruments, such as questionnaires or interviews, to gather information on individuals' beliefs, attitudes, and trust-related experiences. The GTS is a widely used and accepted measure in literature and has been found to have strong validity and reliability in different cultural and language groups. This information is a fundamental starting point for the current research, providing a foundation upon which the study can build and add to the existing knowledge in this area. This information makes it clear that the RScB scale can be effectively used to measure behaviors toward inclusive cybersecurity behaviors. With their strong validity and reliability, these scales can provide accurate and reliable data to support the research aims and objectives.

CHAPTER THREE: RESEARCH METHODOLOGY

Research Design

The research design is an integral part of a study as it delivers the evidence needed to answer the research question and hypotheses as precisely and clearly as possible (Chandra et al., 2018). It serves as the plan and strategy implemented for conducting a study. The plan outlines the process of selecting specific research questions, identifying study participants, and determining data collection and analysis methods. The research design also allows readers to assess the research's reliability and validity. This study utilized a quantitative research method, incorporating ANOVA and correlation techniques to explore the correlation between trust, cybersecurity risks among cultural groups. The results of the study can provide valuable insights into how trust and cybersecurity risks are perceived within different cultural contexts.

This study aimed to investigate the potential link between trust and cybersecurity risky behaviors, with a focus on cultural groups. Human factors in cybersecurity are a relatively new area of research, yet it is crucial to understand how human behavior can contribute to cyber vulnerabilities. Unfortunately, there is a lack of research that examines the cultural differences in human behavior as it pertains to cybersecurity. Additionally, little consideration has been given to the role of trust and how it may overlook or impact cybersecurity risks. Therefore, this study sought to address these gaps in the literature and reveal the relationship between trust and cybersecurity risky behaviors across various cultural groups**.**

Methods for Testing Research Questions & Hypothesis

As previously stated, this study aimed to answer the following research question:

RQ_1: What is the relationship between trust and cybersecurity risky behaviors among different cultural groups?

H_1: There are cultural differences in how people perceive trust.

H_2: There are cultural differences in how people perceive cybersecurity risky behaviors.

H_3: There is a positive relationship between trust and cybersecurity risky behaviors among cultural groups.

In this study, a survey was distributed to qualified participants. They were asked to provide information about their cultural group they most associate with, their gender, their level of education, and their computer user proficiency level, such as whether they are a novice or an expert. The cultural groups identified in this study were based on the standards set forth by Stanford University (n.d.), which are widely recognized and used in previous cross-cultural studies. This decision was made to ensure consistency and comparability of the results. Descriptive data serves and provide an overview of the sample population. The GTS scale was used to gather data on individuals' perceptions of trust across different cultures. (See Appendix A). ANOVA was used to compare the means of trust perceptions across cultural groups. Assumptions for normality and homogeneity of variance was tested before ANOVA tests were conducted to check if the assumptions were met and to determine the type of test that is required.

The RScB scale was used to gather data on individuals' tendency to engage in cybersecurity risky behavior within each cultural group. (See Appendix B). The GTS scale was used to gather data on individuals' perceptions of trust within each cultural group. Person's correlation coefficient determines the correlation between trust and cybersecurity risky behaviors within each cultural group. ANOVA was used to compare the correlation coefficients across the cultural groups. By investigating both trust perceptions and cybersecurity risky behaviors within

different cultural groups, this study seeks to contribute to a better understanding of cross-cultural differences and similarities in these important factors. The results can inform efforts to enhance trust and promote safer cybersecurity practices in diverse contexts.

Data Collection Method

Data for this study was collected using a survey designed with Qualtrics software. The study recruited participants through Amazon Mechanical Turk (MTurk), which is an online platform that facilitates the recruitment of individuals for data collection purposes. The survey was completed online, and it took participants an estimated 10-15 minutes to complete. To compensate participants for their time, they were offered $1 upon completion of the survey, with payments made via direct deposit.

Sampling Method

For this study, a convenience sampling method was utilized, which is a non-probabilistic approach to recruit participants who are readily accessible, were eligible based the inclusion criteria, and those who were willing to participate. The total sample size for the study is 392 participants. To be eligible to participate in this study, participants needed to meet the following inclusion criteria:

- Individuals located in the United States
- Individuals who are 18 years of age or older
- Individuals who are currently using a computer or have used a computer in the past.
- Individuals who are currently students or have a job (or were students or have had a job in the past). This could be any job: full-time, part-time, temporary, seasonal, or intern.

Ethical Considerations

Ethical considerations ensure that the research is conducted responsibly and transparently and can help maintain the integrity and credibility of the study. To ensure that the rights and well-being of participants are protected, several ethical considerations were considered in this study. First, all participants were given comprehensive details regarding the study, including its purpose, procedures, and potential risks and benefits, before deciding whether to participate. Participation in the survey was entirely voluntary, and participants were able to withdraw from participating at any time without penalty. Second, to protect the confidentiality of participants, no names or identifying numbers were collected. There is minimal risk to participants; the survey did not require disclosing of any personal information. To protect the confidentiality of participants, the survey was conducted anonymously, ensuring that there was no way to link the collected data to any specific participant. The study's results may be published in academic journals in the future, but all data collected was restricted to the researchers involved in the study. Finally, this research has been approved by the IRB, ensuring its adherence to ethical guidelines.

Survey Design

This study utilized a convenience sampling method with a closed-ended survey to gather specific, quantifiable data. This survey includes a total of seven questions, using a combination of multiple choice, rating scale, and Likert scale questions. Rating scale questions consisted of options ranging from “Never” and “Rarely” to “Sometimes” and “Very Often.” Likert scale questions consisted of options ranging from "Strongly Disagree" to "Strongly Agree" and "Never" to "Very Often," and participants were asked to rate their level of agreement with each statement.

This study used a set of pre-validated survey scales to measure participants' perceptions and measurements of trust and cybersecurity risks. The survey comprised a total of seven questions, with three of them being carefully selected to elicit in-depth information on the studied constructs. In comparison, the other five questions serve to gather descriptive statistics. These scales have been frequently used in previous research and proven to be reliable and valid measures of these constructs. The use of these established scales allows the researcher to ensure the quality and consistency of the collected data, as well as to compare the results to previous research and add to the current knowledge on trust and cybersecurity risks.

General Trust Scale

The General Trust Scale was designed to assess people's level of trust in others within the context of social relationships and interactions (Yamagishi et al., 1994). It consists of a series of trust statements, and respondents are asked to indicate their level of agreement with each statement using a 4-point Likert scale ranging from "Strongly Disagree" to "Strongly Agree." The scores on the scale are used to evaluate an individual's overall level of trust and how it may impact their social interactions and relationships. The survey was conducted using all the original questions of the GTS without any modifications or omissions. The complete survey is included in Appendix A.

Risky Cybersecurity Behaviors Scale (RScB)

The RScB scale is a tool used to measure an individual's risky cybersecurity behaviors. It is based on the Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS), the original scale from which the RScB scale was derived. In this revised version of the scale, participants were asked to rate, on a scale of 1 to 4 (with 1 indicating "Never" and 4

indicating "Very Often"), the frequency with which they engaged in specific behaviors. A higher score on the RScB scale suggests that the individual participates in more risky cybersecurity behaviors. The complete survey ins included in Appendix B.

Instrument Reliability

In this study, the instrument's reliability used was determined by calculating the Cronbach's alpha coefficient for the both the RScB and GTS scales. This is a widely used internal consistency measure that evaluates the coherence of responses within a set of questions. The results of the analysis for the RScB scale, as presented in Table 4, show the Cronbach's alpha for the instrument is 0.940, indicating very high internal consistency. The Cronbach's alpha based on standardized items is also very high at 0.937. The survey consisted of 20 items.

Table 4. Instrument Reliability for the RScB Scale

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.940	0.937	20

The results of the analysis for the GTS scale, as presented in Table 5, show the Cronbach's alpha for the instrument is 0.816 indicating high internal consistency. The Cronbach's alpha based on standardized items is also high at 0.816. The survey consisted of 12 items. The high level of instrument reliability suggests that the survey instrument is a valid tool for measuring trust among different cultural groups.

Table 5. Instrument Reliability for the GTS Scale

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.832	0.816	12

Measures of Analysis

Descriptive statistics were used to provide an overview of the sample population, including measures of central tendency (e.g., mean, median) and variability (e.g., standard deviation, range). Inferential statistics were used to test the research questions and hypotheses, specifically the relationship between trust and cybersecurity risky behaviors among different cultural groups. The GTS scale was used to gather data on individuals' perceptions of trust across different cultures and the RScB scale was used to gather data on individuals' tendency to engage in cybersecurity risky behavior within each cultural group. For this study, ANOVA is an appropriate measure for comparing means across three or more groups, while correlation analysis is useful for exploring relationships between variables. Normality and homogeneity of variance tests was conducted to check if assumptions were met. A one-way ANOVA was used to compare the means across three or more groups for hypothesis one. For hypothesis two, a Welch's test was conducted to examine the mean difference in cybersecurity risky behaviors among cultural groups. Correlational analysis was used for hypothesis three to determine the correlational association between the two variables of this study: trust and cybersecurity risky behaviors within each cultural group.

Additionally, other measures of analysis were utilized in this study to provide a comprehensive understanding of the data. Specifically, regression analysis was also conducted to confirm the results of the relationship between trust perceptions and cybersecurity risks within each cultural group. The coefficient ranges from -1 to 1, where -1 represents a perfect negative

correlation between trust perceptions and cybersecurity risks, 0 represents no correlation, and 1 represents a perfect positive correlation. The regression coefficient can provide insight into the strength and direction of the relationship between trust perceptions and cybersecurity risks within each cultural group. If the coefficient is positive, it suggests that higher levels of trust are associated with higher levels of cybersecurity risks. Conversely, if the coefficient is negative, it suggests that higher levels of trust are associated with lower levels of cybersecurity risks.

All measures of analysis were chosen to provide a thorough and rigorous examination of the data and to ensure that the findings are both statistically and practically significant. The use of IBM SPSS statistical software enables the researchers to conduct complex analyses and generate accurate results that will inform the study's conclusions.

CHAPTER FOUR: RESULTS

This quantitative study aimed to examine the relationship between trust and cybersecurity risky behaviors among different cultural groups. The relationship between trust and cybersecurity risky behaviors can vary among different cultural groups. In some cultures, trust may be seen as a fundamental value and may be extended more easily to others, including online interactions. In contrast, in other cultures, trust may be more challenging to establish and limited to a smaller group of people, leading to more cautious online behavior. This research report sought to understand these dynamics, specifically the relationships between trust and risky cybersecurity behaviors.

Qualtrics was used to host the survey and collect data from anonymous participants. Primary data was used in this research study. The data was obtained through a structured survey administered to respondents from various cultural backgrounds. The survey used two previously validated surveys; the GTS to measure the perceptions of trust and the RScB to measure risky cybersecurity behaviors. To examine the potential connection between trust and cybersecurity risky behavior across different cultural groups, the study employed statistical analysis, utilizing both ANOVA and correlational techniques. Pearson's correlation coefficient was used to assess the correlation between the GTS and RScB scores, with a two-tailed test used to determine statistical significance. By analyzing the correlation between trust and cybersecurity risky behavior among a sample size of 392 participants, the study sought to gain insight into any variations between cultural groups.

Descriptive Statistics

Descriptive statistics are essential to any research study as they provide valuable insights into the collected data. This step allows researchers to understand better the characteristics and

features of the sample population they're studying. By summarizing and describing the data using various methods, such as the mean, median, and mode, researchers can identify patterns and trends to draw meaningful conclusions about the collected data. In addition, descriptive Statistics can be used to describe relationships between variables in a dataset, help make sense of large amounts of data, and make predictions or draw conclusions from a dataset.

Cultural Groups

This study examined cultural groups to explore the differences in their attitudes toward trust and risky cybersecurity behaviors. Based on the data collected, the most significant cultural group in the sample population is Caucasian, with 252 individuals (65.3% of the sample). The largest groups in the sample population are Black or African American, with 26 individuals (6.7% of the sample), and Hispanic, Latino, or Spanish origin, with 27 individuals (7%). The remaining cultural groups have a smaller representation in the sample population: Asian with 24 individuals (6.2% of the sample), Middle Eastern or North African with 26 individuals (6.7% of the sample), American Indian or Alaska Native with 22 individuals (5.7% of the sample), Other with seven individuals (1.8% of the sample), and Native Hawaiian or other Pacific Islander with two individuals (0.5% of the sample). Six participants did not respond to this question. See Figure 4.

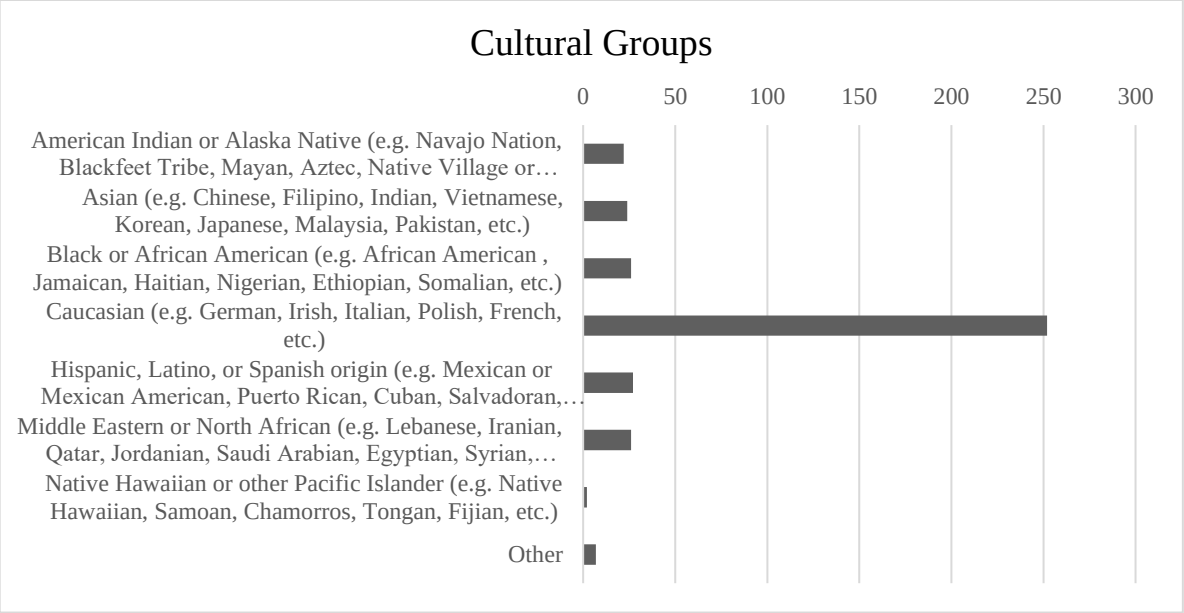

Figure 4. Cultural Groups

Gender, Level of Education, and Computer User

Data were collected about gender to identify the gender distribution of the total sample population. Of the total participants who completed the survey, five did not indicate their gender, 170 individuals (44.0% of the sample) identified as female, and 216 individuals (56.0% of the sample) identified as male. No individuals selected "Other" or "Prefer not to say" as their gender.

Information on participants' education level was collected to provide insights into how educational attainment may influence certain behaviors and decision-making in the area of study. Out of the total sample population, the largest group is individuals who hold a bachelor's degree, with 274 individuals (70% of the sample) having attained this level of education. The next largest group is individuals with a Postgraduate Degree, with 67 individuals (17.1% of the sample) having achieved this level of education. There are also individuals with an associate degree, with 12 individuals (3.1% of the sample) and individuals with a High School education, with 33 individuals

(8.4% of the sample) having attained this level of education. Six participants did not respond to this question. See Table 6.

Table 6. Descriptive Statistics for Gender, Level of Education, and Computer User

Descriptive	Statistics	Frequency	Percent	Cumulative Percent
Gender	Male	216	55.2	56.0
	Female	170	43.5	98.7
	Missing	5	1.3	100.0
Education	High School	33	8.4	8.5
	Associate's Degree	12	3.1	11.7
	Bachelor's Degree	274	70.1	82.6
	Postgraduate Degree	67	17.1	98.7
	Missing	5	1.3	100.0
Computer User	Novice user (you just started using computers)	35	9.0	9.0
	Average user (you use spreadsheets, emails, surf the web)	110	28.1	37.3
	Advanced user (you can install software and setup configurations)	145	37.1	74.6
	Expert user (you can set up operating systems and know programming languages)	99	25.3	99.5
	Missing	2	0.5	100.0

Information about the participant's level of computer use ranging from expert to novice, was collected to help understand how individuals' level of computer proficiency may influence specific behaviors. Out of the total sample, the largest group is individuals who identified as advanced users, with 145 individuals (37.1% of the sample) falling into this category. The next largest group is individuals who identified as average users, with 110 individuals (28.1% of the sample) falling into this category. Some individuals identified as expert users, with 99 individuals (25.3% of the sample) falling into this category, and individuals who identified as novice users,

with 35 individuals (9.0%) falling into this category. Three participants did not respond to this question.

Form of Trust

Table 7. Descriptive Statistics - Trust

Which form of trust do you associate yourself with the most?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Cognitive-based trust: trust based on the confidence you feel in another person's accomplishments, degrees, skills, and reliability.	287	73.2	76.7	76.7
	Affective-based trust: trust that arises from feelings of emotional closeness, empathy, or friendship.	87	22.2	23.3	100.0
	Total	374	95.4	100.0	
Missing	System	18	4.6		
Total		392	100.0		

This research paper focuses on trust and collecting data on different forms of trust – cognitive-based or affective-based – is essential because trust plays a vital role in shaping individuals' behaviors and decision-making. Table 7 shows that out of the total sample, the largest group is individuals who associate themselves with cognitive-based trust, with 287 individuals (76.7% of the sample) falling into this category. The next largest group is individuals who associate themselves with affective-based trust, with 87 individuals (23.3% of the sample) falling into this category. Based on the data provided, most respondents across all cultural groups identified with cognitive-based trust. The highest percentage of respondents who identified with cognitive-based

trust was among Asian respondents at 82.6%, followed by Caucasian respondents at 80.6%. The lowest percentage was among other respondents at 57.1%. Regarding affective-based trust, the highest rate of respondents identifying with this form of trust was among Native Hawaiian or other Pacific Islander respondents at 36.0%, followed by Hispanic, Latino, or Spanish-origin respondents at 38.5%. The lowest percentage was among Caucasian respondents, at 19.4%. Eighteen participants did not respond to this question.

Table 8. Forms of Trust Among Cultural Groups

Cultural Group	Cognitive	Affective
Caucasian (e.g., German, Irish, Italian, Polish, French, etc.)	195	47
Hispanic, Latino, or Spanish origin (e.g., Mexican, Mexican American, Puerto Rican, Cuban, Salvadoran, Dominican, Columbia, etc.)	16	10
Black or African American (e.g., African American, Jamaican, Haitian, Nigerian, Ethiopian, Somalian, etc.)	18	7
Asian (e.g., Chinese, Filipino, Indian, Vietnamese, Korean, Japanese, Malaysia, Pakistan, etc.)	19	4
American Indian or Alaska Native (e.g., Navajo Nation, Blackfeet tribe, Mayan, Aztec, Native Village of Barrow Inupiat Traditional Government, Nome Eskimo Community, etc.)	16	5
Middle Eastern or North African (e.g., Lebanese, Iranian, Qatar, Jordanian, Saudi Arabian, Egyptian, Syrian, Moroccan, Algerian, etc.)	16	9
Native Hawaiian or Pacific Islander (e.g., Native Hawaiian, Samoan, Chamorros, Tongan, Fijian, etc.)	0	2
Other	4	3

Most of the respondents, shown in Table 8, indicated they associate most with cognitive-based trust. This was about (73.2%) of the participants. The remaining (22.2 %) associate most with affective-based trust. Regarding the forms of trust among cultural groups, most participants associated trust with cognitive components (n=374, 100%). In terms of affective trust, the majority

of the participants associated affective trust with the Caucasian cultural group (n=47, 15.9%), followed by Hispanic, Latino, or Spanish origin (n=10, 3.4%), Black or African American (n=7, 2.4%), Asian (n=4, 1.1%), American Indian or Alaska Native (n=5, 1.3%), Middle Eastern or North African (n=9, 2.4%), Native Hawaiian or Pacific Islander (n=2, 0.5%), and Other (n=3, 0.8%).

In contrast, for cognitive trust, the majority of the participants associated cognitive trust with Caucasian cultural group (n=195, 52.6%), followed by Asian (n=19, 5.1%), Black or African American (n=18, 4.9%), American Indian or Alaska Native (n=16, 4.3%), Middle Eastern or North African (n=16, 4.3%), Hispanic, Latino, or Spanish origin (n=16, 4.3%), Native Hawaiian or Pacific Islander (n=0, 0%), and Other (n=4, 1.1%).

General Trust Scale

The General Trust Scale (GTS) was used to measure participants' trust in others. The original scale consists of five response options on a Liker-scale. In this study, the scale was modified to a 4-point Likert scale to reduce respondent confusion, which still provides sufficient variation in the responses for meaningful analysis. An overall higher score indicates more significant levels of trust. Respondents were asked to rate their agreement with a series of statements on a 4-point Likert scale, ranging from "Strongly Disagree" to "Strongly Agree.” For the statement "Most people are honest," (68.4%) of respondents agreed or strongly agreed, with the highest agreement among Asians (87.5%) and the lowest among Hispanics/Latinos/Spanish origin (59.3%). For the statement "Most people are trustworthy," (79.9%) of respondents agreed or strongly agreed, with the highest agreement among Black/African Americans (89.2%) and the lowest among American Indian/Alaska Natives (72.7%). For the statement "Most people are good, and kind," 88.3% of respondents agreed or strongly agreed, with the highest agreement among

Asians (91.7%) and the lowest among Hispanics/Latinos/Spanish origin (58%). For the statement "Most people are trustful of others," (77.8%) of respondents agreed or strongly agreed, with the highest agreement among American Indian/Alaska Natives (92.9%) and the lowest among Asians (62.5%). For the statement "I am trustful," 87.8% of respondents agreed or strongly agreed, with the highest agreement among Caucasians (92.8%) and the lowest among Asians (83.3%). The response to all the trust questions was analyzed separately to gain insights into the participants view on trust. This was achieved by computing the summary statistics of the variables (mean and standard deviation). See Table 9.

Table 9. Summary Statistics of the General Trust Scale

General Trust Scale Items	**N**	**Mean**	**Std. Deviation**
Most people are basically honest	386	3.03	.646
Most people are trustworthy	386	3.13	.784
Most people are basically good and kind	386	3.11	.641
Most people are trustful of others	385	3.01	.743
I am trustful	384	3.28	.669
Most people will respond with kindness when they are trusted by others	386	3.14	.697
Valid N (listwise)	383		

Upon examining the mean values of all the questions related to trust, it is evident that they are almost identical, with each hovering around the value of 3. This indicates that most participants either agreed or strongly agreed with all the trust-related questions. Most respondents agreed or strongly agreed that most individuals are inherently honest, trustworthy, kind, and virtuous.

Furthermore, they agreed or strongly agreed that people tend to trust others, are trustworthy themselves, and that individuals typically respond to being trusted with kindness.

Cybersecurity Risky Behaviors

The data for this question was collected using the RScB scale, which consists of a series of questions to understand individuals' cybersecurity-related behaviors. Under this variable, 20 questions revolved around cybersecurity behaviors. The scale was from 1 to 4, implying the combined variable has values ranging from 20 to 80. The summary statistics for the combined variable are highlighted below.

The respondents rated their behavior on a 4-point Likert scale, with 1 indicating "Never" and 4 indicating "Very Often." Higher values for this variable indicate a higher likely of behaving in risky cybersecurity behavior. The mean value is 56.405, greater than the variable's central value, which is 40. Values around 40 and below are considered low values, whereas those below this threshold are deemed high values. Since the mean value of the variable is 56.08, as shown in Table 10, it is evident that most respondents to the cybersecurity questions responded “Often” or “Very Often”. This clearly indicates that most study participants are likely to behave in risky cybersecurity behavior.

Table 10. RScB Descriptive Statistics

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Cybersecurity Score	381	20.00	80.00	56.0892	12.8179
Valid N (listwise)	381				

Hypothesis Testing

Hypothesis 1: There are cultural differences in how people view or perceive trust.

To test this hypothesis, testing for normality and homogeneity of variance is necessary to check if these assumptions are met before conducting an ANOVA test. Welch's ANOVA test will be performed if the data violates these assumptions. A one-way ANOVA approach will be used if the assumptions are met. The tests for assumptions will help to determine if the mean differences across various cultural groups are the same or different regarding trust. The null hypothesis states that the mean difference across cultural groups is the same, and the alternative hypothesis states that the mean difference across the groups is different.

Table 11. Test for Normality – Hypothesis Two

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Trust	.147	386	.000	.929	386	.000

a. Lilliefors Significance Correction

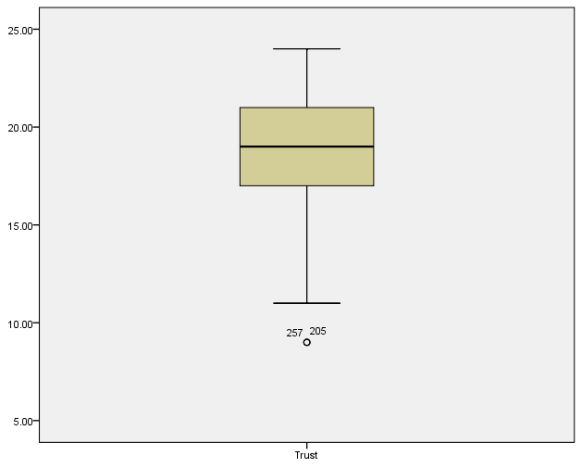

Figure 5. Box Plot Normality – Hypothesis One

The assumptions of normality and homogeneity of variance were tested before conducting a one-way ANOVA. In Table 11, the normality result shows that the Shapiro-Wilk test was statistically significant $F=.929$, $p<.05$, hence it was concluded that perceived trust did not follow a normal distribution. Figure 5 displays the box plot with a few outliers in the trust variable, while the shape of the box plot shows an approximately normal distribution.

Table 12. Test of Homogeneity of Variance - Trust

Test of Homogeneity of Variances

Trust			
Levene Statistic	df1	df2	Sig.
1.209	7	375	.297

Table 12 displays the homogeneity of variance assumption in which Leven's test was not statistically significant $F_{7,375}=1.209$, $p=.297$ ÞÈ Å Î ïÃ Åwas concluded that the cultural differences have equal variances of trust. The homogeneity of variance assumption was met; therefore, a one-way ANOVA test was used to examine the mean trust difference among different cultural groups.

Table 13. ANOVA - Hypothesis One

ANOVA

Trust					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	317.142	7	45.306	6.720	.000
Within Groups	2528.116	375	6.742		
Total	2845.258	382			

The ANOVA results in Table 13 show the results were statistically significant F 7,375 =6.720, p<.05 ηÔ È Å Ò ÃÆ Æ ï Ò Å was concluded that there are mean differences in the trust among different cultural groups. Thus, hypothesis 1 holds cultural differences exist in how people view or perceive trust.

Hypothesis 2: There are cultural differences in risky cybersecurity behaviors.

The assumptions of normality and homogeneity of variance were tested before conducting a one-way ANOVA test. In Table 14, the normality result shows that the Shapiro-Wilk test was statistically significant F=.942, p<.05 ηÈ Å Î ÃÅ was concluded that risky cybersecurity behaviors did not follow a normal distribution.

Table 14. Test for Normality Hypothesis 2

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Cybersecurity	.124	381	.000	.942	381	.000

a. Lilliefors Significance Correction

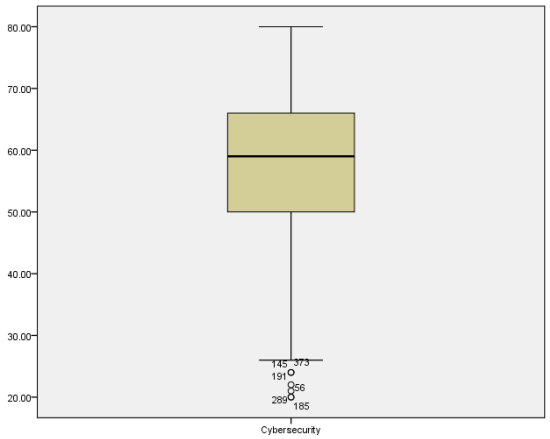

Figure 6. Box Plot Normality - Hypothesis Two

Table 15. Test for Homogeneity of Variance - Hypothesis Two

Test of Homogeneity of Variances

Cybersecurity

Levene Statistic	df1	df2	Sig.
2.622	7	371	.012

The box plot in Figure 6 does not show normal distribution, and Table 15 shows the homogeneity of variance assumption in which Levene's test was statistically significant $F_{7,371} = 2.622$, $p = .012$. Therefore, it was concluded that cultural differences do not have equal variances in risky cybersecurity behaviors. The homogeneity of variance assumption was unmet, so Welch's ANOVA test was conducted to examine the mean differences in cybersecurity risky behaviors among different cultural groups.

Table 16. Welch's Test

Robust Tests of Equality of Means

Cybersecurity

	Statistic[a]	df1	df2	Sig.
Welch	35.442	7	18.506	.000

a. Asymptotically F distributed.

The Welch's test, shown in Table 16, was statistically significant as the statistic equals $F_{7,18.5} = 35.442$. At the same time, the p-value was statistically significant $p < .05$, while the result in Table 17 shows that the one-way ANOVA was statistically significant $F_{7,371} = 8.800$, $p < .05$, therefore the null hypothesis was rejected and concluded that there are cultural differences in cyber security risky behaviors.

Table 17. ANOVA - Hypothesis Two

ANOVA

Cybersecurity

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	8844.132	7	1263.447	8.800	.000
Within Groups	53266.549	371	143.576		
Total	62110.681	378			

Correlational Analysis

Hypothesis 3: There is a positive relationship between trust and cybersecurity risky behaviors among different cultural groups.

Correlation and regression analysis were performed to test this hypothesis to confirm the findings. From correlation analysis, it can be observed that the correlation coefficient of the two significant variables is 0.511. This correlation value also has a p-value of 0.000, signifying a strong positive relationship between the variables. Higher levels of trust are closely associated with a higher likelihood of cybersecurity risky behaviors. See Table 18.

Table 18. Correlational Analysis Hypothesis Three

		Cybersecurity Score	Trust Score
Cybersecurity Score	Pearson Correlation	1	.511**
	Sig. (2-tailed)		.000
	N	3386	380
ChaTrust Score	Pearson Correlation	.511**	1
	Sig. (2-tailed)	.000	
	N	380	381

**. Correlation is significant at the 0.01 level (2-tailed).

Regression Analysis

The analysis of Table 19 suggests that the coefficient of Trust Score is positively associated with risky cybersecurity behaviors. The positive coefficient is statistically significant $F\ 1,378 = 133.921, p < .01$, which indicates that the relationship between trust and risky cybersecurity behaviors is not due to chance alone. Furthermore, the standardized coefficient of Trust Score, shown in Table 20, is 0.511, which suggests that a one-unit increase in Trust Score leads to a 0.511 unit increase in cybersecurity risky behaviors (when trust increases, risky cybersecurity behaviors also increase). This finding supports the third hypothesis that there is a positive relationship between trust and cybersecurity risky behaviors.

Table 19. Regression Analysis

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.511[a]	.262	.260	2.33657

a. Predictors: (Constant), Cybersecurity

Table 20. Parameter Estimates of Regression Model

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	12.649	.538		23.510	.000
	Cybersecurity	.108	.009	.511	11.572	.000

a. Dependent Variable: Trust

CHAPTER FIVE: DISCUSSION & CONCLUSION

Introduction

As technological advancements have rapidly integrated into all aspects of life, cybersecurity has become essential to protecting individuals and businesses from cyberattacks. Technology's increasing use and sophistication has heightened the need for cybersecurity to protect computer systems, networks, and data from unauthorized use or damage. However, despite technical implementations' role in protecting against cyberattacks, considering human factors in cybersecurity is often overlooked and under-researched. As cybersecurity is no longer solely a technical issue, human factors in cybersecurity have emerged as an essential factor mutually dependent on technical aspects. Human behavior plays a crucial role in cybersecurity and must be considered when assessing cybersecurity risks. Therefore, understanding human factors in cybersecurity has become increasingly important, as it could help prevent and mitigate the impact of cyberattacks.

A significant limitation in understanding the importance of human factors in cybersecurity is the lack of literature on this topic. While technical aspects such as firewalls, encryption, and intrusion detection systems have been extensively researched and are the focus of businesses, human factors in cybersecurity should not be taken lightly and have not received the same attention. This gap in knowledge between technical and human factors can lead cybersecurity experts to overlook the significance of the critical role of human factors when developing and implementing cybersecurity policies and solutions. Consequently, systems and data are left vulnerable, presenting a pathway for cyber-attacks. To address this limitation, this research emphasizes the importance of human factors in cybersecurity and explores how cultural backgrounds influence certain behaviors that may overlook risks. The study also examines the role of trust and how

variations in the perception of trust can impact risky cybersecurity behaviors. This research could help enhance cybersecurity measures and prevent potential cyber threats by shedding light on these critical issues.

Chapter Five presents the results obtained in Chapter Four and discusses the study, which aims to address the research question and hypotheses outlined in Chapter One. The study aimed to explore the differences in the perceptions of trust and cybersecurity risky behaviors among cultural groups and to examine whether there is a correlation between trust and cybersecurity risky behaviors. The GTS scale was used to measure trust, and the RScB scale was used to investigate cybersecurity-related risky behaviors. Analyzation techniques were used to test the relationship between the two variables, and a discussion of the results will be provided in this chapter. To give an overview, the chapter begins with a summary of the study's objectives and an outline of the research methodology, including valuable insights into the sample characteristics of the data. It then provides a detailed analysis of the key findings, examining their implications for the study's research question and objectives. In the final stretch of the chapter, a summary of the main results and conclusions is provided, highlighting their significance to future research on this topic. Furthermore, recommendations for future research based on the findings of this study will be presented, mainly focusing on the recommendations in the field of human factors in cybersecurity.

This study provides insights into the following research question and hypotheses:

RQ_1: What is the relationship between trust and cybersecurity risky behaviors among different cultural groups?

H_1: There are cultural differences in how people perceive trust.

H_2: There are cultural differences in how people perceive risky cybersecurity behaviors.

H_3: There is a positive relationship between trust and risky cybersecurity behaviors among cultural groups.

Review of the Methodology

This study used a quantitative online survey methodology to collect data from a diverse sample of participants. Data collection for this study employed an online survey methodology using Qualtrics and was distributed through Amazon Mechanical Turk. The survey was administered electronically to maximize the reach and accessibility of the survey to a large and diverse sample. The survey consisted of a series of questions designed to assess the participants' perceptions of trust and their behaviors related to cybersecurity. Participants were compensated for their time with a monetary incentive provided through amazon mechanical Turk's payment system. The data collected from the survey were exported from Qualtrics to a spreadsheet and then imported into IBM SPSS. Descriptive and inferential statistics were used to analyze the data and draw conclusions.

Discussion of Results

Descriptive Statistics

The descriptive statistics offer an overview of the sample population, predominantly Caucasians, accounting for (65.3%) of the total sample population. As per the U.S. Census Bureau (2022), this wasn't unexpected as Caucasians comprise approximately (75.8%) of the U.S. population. However, it should also be acknowledged that the rest of the cultural groups represented in the sample were diverse: Hispanic and Latino (7%), Black or African American (6.7%), Asian (6.2%), American Indian (5.7%), Middle Eastern or North African (6.7%), Native Hawaiian (.5%), and those who indicated Other (1.8%). For future studies, it would be advisable

to aim for a better representation of all cultural groups to ensure a more balanced, diverse sample to capture the population's diversity accurately.

Regarding educational level, most participants hold a bachelor's degree (70%), and (37%) identified as advanced computer users. This high percentage highlights the study participants' educational level and computer proficiency, which may not be fully representative of the general population, including individuals with a wide range of academic backgrounds and computer proficiency use. Future studies may consider recruiting participants from a broader range of educational backgrounds and computer skill levels to ensure the generalizability of the findings to a broader population. The descriptive statistics also reveal that more males than females participated in the survey (55%) and (43%). While the reasons for this disparity are not clear from the data alone, it is possible that this could be attributed to the differences in the level of interest in cybersecurity, where males in the United States account for 83% of cybersecurity positions (Zippia, 2023), which may reflect underlying gender differences in interest, exposure, or educational opportunities in this field.

Trust

Previous research has provided evidence that indicates an association between cultural influences and trust and highlighted the differences in how individuals perceive trust among cultural groups (Chatterjee et al., 2002; Wang et al., 2002). This study aimed to investigate the differences in the perceptions of trust among cultural groups. The GTS scale was used to measure the various perceptions of trust among the sample population, specifically among the cultural groups specified in Chapter One.

The ANOVA analysis in Table 13 shows a statistically significant difference in the mean levels of trust among different cultural groups. This suggests that the cultural group to which an

individual belongs may play a role in how they perceive trust. The F-statistic of 6.720 indicates that the variance in trust levels between cultural groups is larger than the variance within each cultural group. This implies that the differences in trust perceptions among the cultural groups are more significant than the variations observed within each cultural group. This suggests that trust levels are more influenced by the cultural group to which an individual belongs rather than by individual differences within the same cultural group. In simpler words, these results indicate that individuals from the same cultural group are likelier to have similar perceptions of trust than individuals from different cultural groups. This is highly likely due to the similar values, experiences, and norms that have shaped their perceptions and expectations of trust. As such, it highlights the need to consider cultural backgrounds when developing effective strategies to design and implement cybersecurity policies.

The p-value of 0.000 suggests that the probability of obtaining such a result by chance is very low. This indicates strong evidence to support the alternative hypothesis, which states a significant difference in mean levels of trust among cultural groups. The results suggest that cultural factors are crucial in shaping how individuals perceive trust, indicating that trust is not a universal, unanimous concept. How trust is built and viewed highly depends on the cultural background the individual associates with. This finding supports hypothesis 1, which states that statistically significant cultural differences exist in how individuals perceive or view trust. These differences are consistent with previous studies on the differences in trust across cultures (Fukuyama, 1995; Yamagishi et al., 1998; Dyer et al., 2003).

A statistically significant and higher mean trust difference was found in Caucasians with Middle Eastern or Northern African $d=3.229, p<.05$, while in Caucasians, there was not a statistically significant mean difference with all the other cultures. This is consistent with the

Worlds Values Survey of 2022, as countries such as Norway and Sweden had higher levels of trust than countries such as Columbia and Brazil (Inglehart, 2022). It is important to note that the findings of this World's Values Survey solely pertain to one specific question from the GTS, specifically in response to the statement, “Most people can be trusted.”

Post hoc test, particularly Fisher’s Least Significant Difference (LSD), was used to compare the means to determine if there were statistically significant differences in trust between cultural groups. The tests revealed that Hispanic, Latino, or Spanish origin had a statistically significant mean trust difference with American Indian or Alaska Native $d=-1.8064$, $p<.05$ and Middle Eastern or Northern African $d=2.4174$, $p<.05$. Black or African American had a statistically significant mean trust difference with American Indian or Alaska Native $d=-1.5699$, $p<.05$ and Middle Eastern or Northern African $d=2.6538$, $p<.05$. Asian culture had a significant mean trust difference with the Middle Eastern or Northern African $d=3.3109$, $p<.05$, while it has insignificant mean trust difference with all the other cultures. These findings contradicted the World Values Survey (2022) outcomes, which suggested that China, as a representative of the Asian cultural group, also exhibited significant levels of trust. It is essential to recognize that the World Values Survey (2022) results cannot be uniformly applied to all Asian countries, making it impractical to generalize these findings to the entire Asian cultural group. As previously stated, these findings pertain to one specific question from the GTS, specifically in response to the statement, “Most people can be trusted.”

Higher trust was found in cultural groups of American Indian or Alaska Native with Middle Eastern or North African $d=4.2237$, $p<.05$ and Native Hawaiian or Pacific Islanders $d=4.4545$, $p<.05$ Because there was a statistically significant mean trust difference among the cultural groups 8Middle Eastern or Northern African had a statistically significant mean trust

difference with Hispanic, Latino or Spanish origin $d=-2.4174$, $p<.05$, Black or African American $d=-2.6539$, $p<.05$ and Other $d=-3.5550$, $p<.05$ groups. The current study's findings of these cultural groups lack sufficient support from existing literature. The absence of previous studies supporting these findings raises questions about their generalizability and warrants caution in their interpretation.

The present study's findings highlight the importance of considering cultural backgrounds in shaping individuals' perceptions of trust, particularly when examining the nature of individualistic and collectivistic cultures. Many interconnected factors, such as social norms, shared beliefs, values and experiences, and communication styles, may influence the role of trust and its fluctuations based on cultural backgrounds. Previous studies have strongly correlated trust attitudes with religious affiliation and upbringing (Guiso et al., 2006). Religious beliefs and upbringing influence an individual’s trust formation and behavior. Specifically, people from collectivistic cultures tend to have higher trust levels in their in-groups but lower trust in outsiders than those from individualistic cultures (Triandis, 1995). This strong in-group trust stems from the belief that members will prioritize the collective well-being and act in the group's best interests. As a result, individualistic cultures tend to exhibit lower trust in outsiders than their collectivistic counterparts (Triandis, 1995). This lower level of trust towards outsiders may be attributed to the belief that individuals from different cultural backgrounds may prioritize their interests over their collective well-being. Individualistic cultures emphasize personal independence and achievements more than those from collectivistic cultures. Consequently, individualistic cultures may approach interactions with others with greater caution and skepticism. This opposite personal inclination can potentially create conflict or tension in their trust formation and behavior towards others.

Shared cultural norms and values can also foster the development and cultivation of trust, resulting in consistent assumptions and expectations toward other people. When people share a common belief about their perceptions of what trustworthy behavior is, it establishes a foundation for social communication and interactions (Doney et al.,1998; Hofstede, 1980). This means that if a group mutually values honesty and integrity, individuals within the same group are highly likely to trust each other. Trust assumes that others will adhere to the same set of values, which in turn informs decision-making processes (Triandis, 1972). The convergence of shared presumptions and expectations creates an environment of predictability and dependability, fostering heightened interpersonal trust (Deutsch, 1973). The relationship between trust and cultural norms and values lies in shaping individuals' perceptions and expectations of what constitutes trustworthy behavior, and it creates a mutual understanding of interpersonal interactions. These findings may help establish a common expectation of cybersecurity norms and create a predictable and effective environment for more accessible collaboration efforts on implementing strong cybersecurity measures and robust security practices.

Communication styles also play a pivotal role in shaping trust and serve as a guide for choices and behaviors (Easton, 2016). Direct and unambiguous communication is often favored in individualistic cultures, promoting clarity and transparency (Ting-Toomey, 1988). In these cultures, trust is built upon open and honest dialogue, where individuals express their thoughts, concerns, and intentions openly and explicitly (Gudykunst et al., 1996). On the other hand, collectivistic cultures tend to emphasize indirect communication, relying on contextual cues, facial signals, nonverbal gestures, and shared understandings (Sanoubari et al., 2018). While this communication style may appear less explicit, it fosters trust by respecting the harmony and social dynamics within the group. The differences in communication styles and their relationship to trust

may help cybersecurity professionals tailor their strategies to address these differences by promoting clear and transparent communication and raising awareness about the risks associated with implicit transmission.

The findings of this study carry significant implications for cross-cultural interactions, specifically within the realm of cybersecurity, where trust plays a pivotal role in information sharing and collaborative endeavors. An awareness of the cultural variations in trust perception can significantly assist in developing enhanced communication strategies and collaborative practices among culturally diverse groups. Cybersecurity professionals can formulate more effective approaches to tackle security challenges within various cultural contexts by acknowledging and comprehending the impact of cultural factors on trust dynamics. By doing so, they can foster a stronger foundation of trust and facilitate more secure and productive interactions in an increasingly interconnected and culturally diverse digital landscape.

Cybersecurity Risky Behaviors

Cybersecurity risky behaviors are the actions that increase the likelihood of a cyberattack from occurring. These behaviors include many activities, such as clicking on a malicious links, using weak passwords, or sharing private information with unauthorized individuals. Behaviors towards cybersecurity vary, depending on many factors, such as cultural backgrounds. This study aimed to examine the cultural differences in risky cybersecurity behaviors. To analyze these risky behaviors, the RScB scale was used to measure individuals' attitudes toward cybersecurity. Hypothesis 2 indicates that there are cultural differences in risky cybersecurity behaviors. Individuals who participated in the survey were asked to answer questions regarding their cybersecurity behaviors.

The data analyzed in Chapter Four was used to examine the differences in these behaviors among different cultural groups. An ANOVA test in Table 17, a statistical method used to compare the means of multiple groups, was used to test this hypothesis. The p-value of the ANOVA table was less than 0.05, leading to the rejection of the null hypothesis in favor of the alternative hypothesis. Therefore, hypothesis 2 holds: cultural differences exist in how people perceive risky cybercrime behaviors. This suggests that the ANOVA results support hypothesis two and indicate a statistically significant difference in the means of the measured groups. It would be unlikely to have occurred by chance alone. By confirming that hypothesis 2 holds, the study adds to our understanding of how cultural factors can influence risky cybercrime behaviors. The results suggest that cultural differences may play an essential role in shaping attitudes toward cybercrime and informing interventions and policies aimed at reducing crime rates. While technical solutions play a critical role in mitigating risks, cultural factors can significantly influence behaviors and attitudes toward cybercrime, thereby influencing risky behaviors.

Post hoc test, specifically the Games-Howell test, is mainly designed for unequal variances to provide more accurate pairwise comparisons between the groups and shed light on the variations in risky behavior exhibited by different cultural groups. The Games-Howell post hoc test revealed significant differences in risky cybersecurity behavior between multiple pairs of cultural groups. Specifically, the test revealed a statistically significant and higher mean difference in risky cyber security behavior among various cultural groups. Specifically, compared to the Caucasian cultural group, American Indian or Alaska Native cultural group exhibited a significantly higher mean difference in cyber security risky behavior ($d = -7.9238$, $p < .05$). Similarly, the Middle Eastern or Northern African cultural group ($d = 15.7314$, $p < .05$) and Native Hawaiian or other Pacific

Islanders cultural group ($d = 23.4397$, $p < .05$) showed statistically significant and higher mean differences in cyber security risky behavior compared to Caucasian cultural groups.

In addition, Hispanic, Latino, or Spanish origin cultural groups demonstrated a statistically significant mean difference in cyber security risky behavior compared to American Indian or Alaska Native ($d = -10.1229$, $p < .05$), Middle Eastern or Northern African ($d = 13.5324$, $p < .05$), and Native Hawaiian or other Pacific Islanders ($d = 21.2407$, $p < .05$) cultural groups.

Furthermore, the Black or African American cultural group exhibited a statistically significant mean difference in cyber security risky behavior compared to Middle Eastern or Northern African ($d = 17.9455$, $p < .05$) and Native Hawaiian or other Pacific Islanders ($d = 25.6538$, $p < .05$) cultural groups.

Asian cultural groups displayed a significant mean difference in cyber security risky behavior compared to Middle Eastern or Northern African ($d = 13.7917$, $p < .05$) and Native Hawaiian or other Pacific Islanders ($d = 21.500$, $p < .05$) cultural groups. At the same time, it did not show a statistically significant mean difference in cyber security risky behavior with other cultures.

Additionally, Middle Eastern or Northern African cultural groups exhibited a statistically significant mean difference in cyber security risky behavior compared to Hispanic, Latino, or Spanish origin ($d = -2.4174$, $p < .05$), Black or African American ($d = -2.6539$, $p < .05$), and Other ($d = -3.5550$, $p < .05$) cultural groups.

While there is a lack of studies explicitly supporting these cultural differences in risky cybersecurity behavior among cultural groups within a cybersecurity context, general cultural differences can offer potential explanations based on cultural differences in human behavior. These

reasons may help shed light on potential factors contributing to varying attitudes and behaviors towards cyber security within different cultural groups.

Disparities in social structures and enduring values across diverse groups could have far-reaching implications for cybersecurity, particularly concerning risky human behavior. Social norms dictate how interactions will be perceived (Sanoubari et al., 2018). Weber et al. (1999) theorized that the variations in human behavior observed across different cultures may have roots in these very dissimilarities. Studies have found that personality traits contribute to higher susceptibility to phishing attacks (Parker et al., 2020; Cho et al., 2016) and influence perceived risk and trust levels contributing to phishing vulnerability (Cho et al., 2016). In collectivistic cultures, communal harmony and interdependence are emphasized and often prioritize the group's well-being over personal desires (Tov et al., 2017).

Consequently, individuals from such cultures tend to exhibit behavior that is likely approved by society (Gilbert, 2000) and that complies with collectivistic norms (Carlo et al., 2017). This emotional evaluation can influence their decision-making processes and may include their approaches and behaviors toward cybersecurity. For instance, in collectivistic cultures, where maintaining social cohesion and preserving relationships is paramount, individuals may be more susceptible to social engineering attacks that exploit their emotional vulnerabilities. Cybercriminals may exploit the trust and empathy prevalent in these cultures to manipulate individuals into revealing sensitive information or performing actions unfavorable to their cybersecurity protocols and policies. On the other hand, individualistic cultures tend to prioritize personal independence and self-reliance (Cybersecurity Insiders, 2021; Snibbe et al., 2005). In such cultures, people are more likely to include emotions in their evaluation of the situations and environment, as they make decisions based on their personal preferences, desires, and interests

(Yates et al., 2016). This preference for individual autonomy can also impact how individuals from individualistic cultures behave in the context of cybersecurity. People from individualistic cultures may engage in riskier online behaviors, such as freely sharing personal information or neglecting security measures. This behavior stems from their emphasis on individual freedom and a potentially lesser concern for collective security. As a result, they may become more susceptible to cybersecurity threats like phishing and malware attacks.

Another factor contributing to the differences in behavior among cultural groups, which may impact cybersecurity risks, is how people from specific cultural groups deal with power, also referred to as power distance. Power distance refers to the extent to which members of a society accept and expect power and authority to be distributed; essentially, the way a culture deals with hierarchical relationships and the level of inequality that is considered normal and acceptable (Daniels et al., 2014). Hofstede's cultural dimensions theory is one of the most widely recognized frameworks for understanding power distance among cultural groups (Hofstede, 1980). Dealing with power is not universal and varies significantly across different cultures. Cultures characterized by high power distance, such as India and Singapore, tend to exhibit behaviors that involve demonstrating respect and acceptance towards individuals of higher social status without questioning their authority (Yang et al., 2017). In these cultures, hierarchical structures are deeply ingrained, and individuals generally adhere to established authority figures.

Conversely, cultures with low power distance, like the United States and Denmark, adopt a different perspective. They value equal power and respect, irrespective of an individual's social status. In such cultures, individuals question authority and believe in equal principles. Power is perceived as being distributed more evenly, emphasizing the importance of individual rights and autonomy (Javidan et al., 2001). These divergent approaches to power have implications for

cybersecurity risks within cultural groups. In high power distance cultures, where individuals tend to defer to authority figures, there is a greater likelihood of unthinkingly following instructions without questioning their legitimacy (Hofstede, 2001). This can make individuals more susceptible to social engineering attacks, where hackers exploit the trust and respect accorded to those in positions of power.

On the other hand, low power distance cultures may exhibit a more independent and critical mindset toward authority (Hofstede, 2001). When people have a greater tendency to question and carefully examine requests or instructions, it can help protect against potential cybersecurity risks. This cautious behavior can act as a defense mechanism, making it harder for cyber threats to succeed. Understanding the impact of power distance on cybersecurity is crucial for organizations operating in culturally diverse environments. By recognizing these cultural differences, organizations can better tailor their cybersecurity strategies and awareness programs to address different cultural groups' specific needs and behaviors. Implementing measures that promote a balance between respect for authority and critical and analytical thinking can help mitigate cybersecurity risks, regardless of the prevalent power distance within a particular cultural context.

Recognizing and understanding these cultural variations in human behavior becomes crucial for cybersecurity professionals as it underscores the importance of targeted education and awareness campaigns that address the unique challenges different cultural groups face. By customizing cybersecurity practices and interventions to align with diverse cultures' values and social structures, organizations can effectively reduce the risks associated with human behavior and bolster overall cybersecurity readiness.

In conclusion, the disparities in human behaviors observed across cultures, rooted in distinct social structures and enduring values, can have significant implications for cybersecurity.

Recognizing these differences and adapting cybersecurity strategies accordingly can aid in reducing vulnerabilities stemming from risky human behavior in an increasingly interconnected world. Overall, the results provide crucial evidence to support the study's conclusions and contribute to advancing knowledge in cybercrime research.

Trust and Cybersecurity Risky Behaviors

The study results show a significant positive correlation between trust and risky cybersecurity behaviors among all cultural groups. The study found that trust significantly correlates with these behaviors, indicating that trust plays a role in the likelihood of engaging in risky cybersecurity behaviors. The Pearson correlation coefficient (r) is a statistical measure used to determine the strength and direction of a linear relationship between the two continuous variables of a study. It ranges between -1 and +1, where values close to +1 indicate a strong positive correlation, meaning that as one variable increases, the other also increases. As trust increases, so do risky cybersecurity behaviors. When the value of (r) is close to -1, it indicates a strong negative correlation, meaning that as one variable increases, the other variable decreases. When (r) is close to 0, it suggests no correlation between the two variables (LaMorte, 2021). The (r) of the two scores on the GTS and the RScB was 0.511, with a p-value of 0.000, indicating a strong positive relationship between the variables. This suggests the likelihood of risky cybersecurity behaviors increases as trust levels increase.

In contrast, as trust levels decrease, the likelihood of engaging in risky cybersecurity behaviors decreases. In other words, higher levels of trust are closely associated with a higher probability of risky cybersecurity behaviors. This may suggest that individuals with higher levels of trust are more likely to be less guarded, as opposed to individuals with lower levels of trust may be more cautious and vigilant (Cheshire et al., 2010).

The study also found significant differences in trust and risky cybersecurity behaviors between cultural groups. Specifically, the results show that Caucasians and Middle Eastern or North African participants had the highest levels of trust. This is consistent with the World Values Survey that used the GTS scale across various regions worldwide (Inglehart et al., 2022). In contrast, American Indian or Alaska Native participants had the lowest levels of trust. Due to the lack of accessible information to support this result, asserting their alignment with previous studies is difficult. In addition, American Indian or Alaska Native and Black or African American participants had the highest levels of risky cybersecurity behaviors.

In contrast, Caucasian participants had the lowest levels of risky cybersecurity behaviors. The lack of prior studies in cybersecurity of risky behaviors makes it challenging to ascertain the degree to which these findings support existing research. The correlation was stronger for some cultural groups, such as Caucasians and Middle Eastern or North African individuals than for others, such as Native Hawaiian or Pacific Islander individuals.

Culture influences people's thinking processes and instructs them to act and interact with others. It provides a foundation for people on how to behave and interpret the behaviors of others. As discussed in Chapter Two, Hofstede's (1984) model recognizes individualism and collectivism as two fundamental dimensions of culture that influence human behavior and decision-making. Individuals from collectivistic cultures, such as Asians, may be likelier to exhibit affective-based trust due to their high value on interpersonal relationships and social harmony (Leung, 1988). On the other hand, individualistic cultures, such as Caucasians, may be more likely to exhibit cognitive-based trust due to their high value of personal independence and rational decision-making (Marshall, 2003). To better support Hofstede's Cultural Dimensions Theory of individualism and collectivism, it is necessary to have a more diverse range of participants from

other cultural groups as part of the study. The study's limited participation of individuals from different cultural backgrounds made it challenging to determine whether they were collectivistic or individualistic. Therefore, to further validate Hofstede's theory, it is necessary to include more samples from all cultural groups, in addition to incorporating cultures from around the world. This would allow a more comprehensive understanding of how different cultures exhibit individualistic and collectivistic behaviors and decision-making styles. By having participants from various cultural backgrounds, we can gain a deeper insight into the impact of culture on human behavior and decision-making. While a larger sample size is necessary to fully incorporate Hofstede's model into this study, utilizing information on the dimension of individualism and collectivism can enhance our understanding of human behavior differences and their potential integration within a cybersecurity context.

As previously discussed, individuals with a more individualistic outlook are more likely to develop cognition-based trust, while those with a more collectivistic perspective tend to foster affect-based trust (Chen et al., 1998). While the findings of this study may support the influences of cultural backgrounds on the development of cognition and affect-based trust, it is essential to note that more information is needed to draw a definitive conclusion. To clarify, the data used in this study may not be sufficient to draw a conclusive result, and more data may be needed to validate the study's findings. Additionally, limited participants from cultural groups other than Caucasians made it challenging to determine whether the results of this study supported Hofstede's (1990) theory. Overall, the differences in the development of cognition and affect-based trust can reflect the different cultural values and norms prominent in individualistic and collectivistic societies, as suggested by Hofstede (1990).

The results also revealed that cognitive-based trust is more prevalent than affective-based trust across all cultural groups. The higher prevalence of cognitive-based trust suggests that individuals tend to trust others based on their competence and reliability rather than their emotional connection (Washington, 2013). This finding has important implications for cybersecurity risk assessments. It highlights the need to develop effective strategies that enhance individuals' cognitive-based trust and reduce their dependence on affective-based trust.

The study also found that factors such as gender and level of education did not significantly influence the relationship between trust and risky cybersecurity behaviors, meaning there was no variation in the degree of the perceptions of trust and their likelihood to engage in risky cybersecurity behaviors among individuals' gender and level of education. However, the level of computer use was found to be a significant predictor of risky cybersecurity behaviors. Specifically, novice and expert users were likelier to engage in risky cybersecurity behaviors than average and advanced users. Based on these results, it may suggest that cybersecurity education and training programs should be tailored to the specific needs of individuals based on their level of computer use and their awareness of cybersecurity risks. The reason for this is unknown as there may be many possible explanations. It could be that novice users are unaware of the risks involved with online behavior, and expert users typically spend a significant amount of time online and may have developed a false sense of security or overconfidence in their abilities and may tend to overlook risks. More research in this area is needed to understand the relationship between the level of computer use and risky cybersecurity behaviors to tailor education and training to the specific needs of individuals and organizations to protect assets better and reduce cyber-attack risks.

Implications for Cybersecurity

The findings of this study have significant implications for future cybersecurity risk assessments and procedures, particularly for organizations and policymakers. The results reveal a strong positive correlation between trust and risky cybersecurity behaviors, indicating that increasing trust levels leads to an increase in risky cybersecurity behaviors. The higher trust levels individuals have towards other people, the more likely they will be involved in risky cybersecurity behaviors. The results also suggest that trust is not a universal concept and varies significantly among cultural groups. Considering the analysis results, exploring the implications for cybersecurity is crucial.

Role of Trust

Trust plays a vital role in cybersecurity, specifically in social engineering attacks. Social engineering is a method used by cyber-attackers to manipulate their victims to perform specific actions. The success of such attacks relies on the ability to establish trust of their victims by using deceptive methods to gain unauthorized access to sensitive information and systems. Recognizing the impact trust has on risks and understanding the relationship between trust and risky cybersecurity behaviors can help organizations and businesses develop more effective and targeted strategies to prevent and mitigate the impact of these attacks. Security measures can be tailored to address the risks and vulnerabilities that arise from misplaced trust. By bringing awareness to computer users and employees about the tactics used by social engineering attackers through educational initiatives, organizations can enhance their security posture and limit the possibility of being victims of these attacks.

Additionally, trust impacts cybersecurity risky behaviors and may potentially overlook risks. Organizations and policymakers should acknowledge that trust is not a one-size-fits-all

concept, and cultural backgrounds influence how individuals perceive trust. Therefore, designing cybersecurity policies recognizing these cultural differences in trust perception could lead to greater trust in cybersecurity practices among various cultural groups. Developing interventions may also include initiatives that promote transparency and accountability in cybersecurity practices, such as providing clear communication on how personal data is being used and how cybersecurity risks are being mitigated.

Cybersecurity Policies and Interventions

Cybersecurity policies and interventions must consider the cultural differences that influence behaviors and attitudes toward cybersecurity. These differences may be affected by variations in societal norms, beliefs, and practices related to technology and security. Understanding human behavior is instrumental in addressing and minimizing unsafe cybersecurity behaviors (Wiederhold, 2014). By recognizing and understanding these cultural nuances, organizations and policymakers can develop more effective strategies that resonate with diverse populations and encourage responsible cybersecurity practices.

Moreover, cybersecurity policies and interventions should aim to foster a culture of security that aligns with the values and beliefs of different cultural groups. This requires a tailored approach considering each community's specific needs and preferences. By promoting cybersecurity practices that are culturally sensitive and relevant, organizations can increase the adoption and compliance with security measures, reducing the vulnerability to social engineering attacks and other cybersecurity threats and minimizing potential risks.

Incorporating cultural considerations into cybersecurity policies and interventions may potentially enhance their effectiveness. Recognizing and addressing cultural differences in behaviors and attitudes towards cybersecurity allows for developing inclusive, relevant strategies

that resonate with diverse populations. By tailoring interventions to specific cultural contexts and fostering a culture of security that aligns with different communities, organizations can enhance cybersecurity practices and strengthen their defense against cyber threats.

Cultural Differences

The findings also indicate that cultural background can significantly influence how it shapes individuals' perceived trust levels and attitudes toward risky cybersecurity behaviors. Therefore, gaining an understanding of these cultural differences becomes crucial in the development of effective cybersecurity policies and strategies that are tailored to specific cultural groups. Cybersecurity remains a critical concern for individuals, organizations, and governments alike. However, cultural factors such as norms, beliefs, individualism, and collectivism can impact how people approach cybersecurity. In individualistic cultures, individuals may prioritize their personal privacy and data protection.

In contrast, in collectivistic cultures, people may be more inclined to share personal information for the benefit of the group. Recognizing these cultural variations enables us to design cybersecurity strategies and policies better aligned with specific cultural groups' values and behaviors. For instance, policies that foster trust within cultures that place a high value on trust may be more likely to reduce risky cybersecurity behaviors. Additionally, in individualistic cultures, security measures might need to be framed to safeguard personal privacy and data, while in collectivistic cultures, the emphasis might be on protecting the entire community's well-being.

Limitations

While Chapter Five provides valuable insights into the relationship between trust and risky cybersecurity behaviors among various cultural groups, it is important to acknowledge several

limitations. Firstly, the sample population's demographic characteristics, such as predominantly Caucasians with a bachelor's degree and advanced computer skills, limit the generalizability of the study's findings to a more diverse population with varying education and cybersecurity knowledge levels. This lack of diversity may not accurately represent different cultural groups' cybersecurity behaviors and attitudes.

Secondly, the use of self-reported measures in the study is subject to bias and may not accurately reflect participants' cybersecurity behaviors. Participants may have provided socially desirable responses, which could skew the results and limit the accuracy of the findings.
Moreover, the study's cross-sectional design limits the ability to establish causal relationships between trust and risky cybersecurity behaviors among different cultural groups. The results may only provide a snapshot of participants' attitudes and behaviors at a specific time, and therefore, it may not capture changes in attitudes or behaviors over time.

Lastly, the study's focus on cultural groups' perceptions of trust and cybersecurity risky behaviors may not account for other factors that influence these behaviors, such as age, gender, and socioeconomic status. Future research should address these limitations by considering more diverse populations, employing different research methodologies, and accounting for other factors influencing cybersecurity behaviors. This could further expand knowledge in the field of human factors in cybersecurity and help to develop more effective cybersecurity strategies.

Recommendations for Future Research

Drawing upon the results presented in Chapter Five, which focused on answering the research question and hypotheses, there are several recommendations for future research in the growing field of human factors in cybersecurity. Firstly, given the sample characteristics of the study, which primarily consisted of Caucasian individuals, it is recommended that future research

expand the sample population to include a more diverse range of individuals from various cultural groups instead of having most participants dominating the sample population. This can be achieved by using quota sampling methods – setting a specific number of participants from each cultural group – and using various recruitment strategies to recruit participants until the quota has been reached. This ensures that there are enough participants in each cultural group and would better represent the sample population. By doing so, a more comprehensive understanding of the differences in perceptions of trust and cybersecurity risky behaviors can be obtained, allowing for more accurate generalizations of all cultural groups to enhance and develop a more inclusive conclusion.

An added limitation of the current study was the focus on the prevalence of one form of trust: cognitive-based trust and affective-based trust across cultural groups in the context of cybersecurity. There are many other factors of trust they may influence specific responses and impact the results of the data. Therefore, further research should delve deeper into other cultural factors that influence trust and cybersecurity behaviors, such as the impact of cultural values, beliefs, and norms on individual perceptions of behaviors. Incorporating Hofstede's Cultural Dimensions may help guide future research on this topic and lead to more effective cybersecurity risk management strategies tailored to different cultural backgrounds.

Thirdly, the study did not investigate the effectiveness of interventions, such as developing culturally tailored educational materials and training programs that address the cultural factors that influence trust and cybersecurity behaviors. The study gathered insights into how cybersecurity risks are approached among different cultural backgrounds. It measured the relationship between trust and cybersecurity risks to guide future human factors in cybersecurity research. By assessing and studying the efficacy of interventions tailored to the cultural context, organizations can use

this knowledge to help improve the effectiveness of their cybersecurity risk management strategies. For example, studies can gather data on the effectiveness of educational materials and training programs to build awareness of cybersecurity risks and the importance of trust in different cultural contexts. This data could potentially provide practical guidance on reducing risky cybersecurity behaviors. By investigating the effectiveness of interventions to improve trust and reduce risky cybersecurity behaviors, organizations can develop more effective cybersecurity risk management strategies tailored to different cultural contexts. This could lead to more secure and resilient organizations better prepared to deal with the growing threats posed by cybercrime.

Additionally, conducting qualitative research, mainly through interviews, can provide valuable insights into the reasons behind the influences of perceived trust. Researchers can engage in more personal, in-depth conversations through interviews to understand the underlying reasons, motivations, and thought processes when trusting others. These interviews can uncover factors that may not have been considered in this study or prior studies. Qualitative studies can also be conducted to understand the reasoning behind behaviors and attitudes that may shape their decisions to engage in risky cybersecurity behaviors. This will allow researchers to identify potential weak points, which will help enhance strategies and cybersecurity awareness and response and provide a more in-depth assessment of cultural factors and behaviors to help better understand the complex relationship between culture, trust, and risky cybersecurity behaviors.

Lastly, given the significant positive correlation between trust and risky cybersecurity behaviors, as identified in this study, future research should include other factors influencing risky behaviors. This could include exploring the impact of social, developmental, and other cognitive factors on the relationship between trust and its impact on risky cybersecurity behaviors. Additionally, exploring deeper into the influences of trust on decision-making processes may lead

to impacting cybersecurity risks. Exploring how trust affects decision-making processes could be essential for future technological and cybersecurity-focused research.

Overall, the recommendations above aim to advance current knowledge of human factors in cybersecurity, allowing for a more comprehensive understanding of the relationship between cultural factors, trust, and risky cybersecurity behaviors that may lead to overlooking risks.

Conclusion

This study explored how trust and cultural background affect risky cybersecurity behaviors. Despite the importance of cultural factors in shaping responses to cybersecurity risks, existing literature has overlooked this aspect. By investigating the human behavioral aspect of cybersecurity risks and the impact of trust on these risks, this study sought to fill this gap. Trust is a complex concept that can significantly influence decision-making and behavior. By gaining a better understanding of trust and its impact, it may be possible to identify situations where different levels of trust can result in overlooking cybersecurity risks.

The study revealed that trust is perceived differently among people from different cultures. Additionally, there are differences in risky cybersecurity behaviors among other cultural groups, which suggests cultural backgrounds are crucial in shaping attitudes and behaviors toward cybersecurity risks. Furthermore, the study identified a positive association between trust and risky cybersecurity behaviors among the different cultural groups examined. This finding is particularly significant because it suggests that a high level of trust may lead to higher tendencies to engage in risky cybersecurity behaviors. One possible explanation for this is that when people have a high level of trust in others, they may be more likely to let their guard down, which can result in overlooking potential risks.

The implications of these findings are significant for both academia and industry. For the academic sector, this study highlights the need for more consideration of incorporating cultural factors' influences in cybersecurity research. Future studies should aim to explore cultural differences in greater depth to understand better the nuances of trust and its impact on human behaviors in cybersecurity. These findings suggest that cybersecurity strategies, risk assessments, and policies must be tailored to specific cultural contexts for the industry sector. By considering cultural differences, cybersecurity professionals can develop more effective risk mitigation strategies that account for the impact of trust on cybersecurity behaviors.

The results showed a statistically significant difference in the mean levels of trust among different cultural groups. This supports the first hypothesis that cultural differences exist in how people perceive trust. The findings suggest that cultural factors are crucial in shaping how individuals perceive trust, indicating that trust is not a universal, unanimous concept. Therefore, how trust is built and perceived, and maintained is highly influenced by cultural backgrounds. The study's results align with previous research highlighting the differences in trust across cultures.

The analysis of risky cybersecurity behaviors using the RScB scale showed that there are cultural differences in these behaviors among different cultural groups. This supports the second hypothesis that cultural differences exist in how people perceive risky cybersecurity behaviors. The findings indicate that individuals from different cultural backgrounds have other behaviors toward cybersecurity, and cultural backgrounds are highly likely to influence these behaviors. This implies that cybersecurity training and awareness programs must consider cultural differences to change people's behaviors effectively.

Lastly, the study found a significant positive correlation between trust and risky cybersecurity behaviors among the cultural groups specified in chapter one. This finding supports

the third hypothesis, indicating that trust plays a role in the likelihood of engaging in risky cybersecurity behaviors. The results suggest that individuals who trust others are more likely to engage in risky cybersecurity behaviors, which can increase their vulnerability to cyberattacks. Therefore, educating and understanding the risks associated with higher perceptions of trust and promoting healthy distrust towards online activities is essential.

In conclusion, the study's findings highlight the need for future research on the influences and differences of human behaviors that may impact cybersecurity risks among various cultural groups. The influences of cultural backgrounds on cybersecurity risks have not yet been studied in the literature. There is a need to study cultural backgrounds' role in how individuals perceive trust and its relation to risky cybersecurity behaviors. The study's results suggest that policies, risk assessments, cybersecurity education, training, and awareness programs should consider cultural differences to understand the variations in people's behaviors effectively. The study's findings also indicate that trust plays a role in the likelihood of risky cybersecurity behaviors, suggesting the need to educate individuals on the importance of understanding how trust is perceived among individuals, the risks associated with over-trusting others, and its impact on cybersecurity. Overall, this study contributes to the field of human factors in cybersecurity and provides valuable insights into future research on this topic.

REFERENCES

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behavior & Information Technology*, 33(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787

Aghajani, G., & Ghadimi, N. (2018). Multi-objective energy management in a micro-grid. *Energy Reports*, 4, 218–225. https://doi.org/10.1016/j.egyr.2017.10.002

Ahorsu, D. K., Lin, C.-Y., Yahaghai, R., Alimoradi, Z., Broström, A., Griffiths, M. D., & Pakpour, A. H. (2022). The mediational role of trust in the healthcare system in the association between generalized trust and willingness to get COVID-19 vaccination in Iran. *Human Vaccines & Immunotherapeutics*, 18(1), 1–8. https://doi.org/10.1080/21645515.2021.1993689

Ahvanooey, M. T., Li, Q., Rabbani, M., & Ahmed Raza Rajput. (2017). A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks. International Journal of Advanced Computer Science & Applications, 8(10). https://doi.org/10.14569/IJACSA.2017.081005

Aivazpour, A., & Rao, V. (2018). Impulsivity and risky cybersecurity behaviors: A replication. *Proceedings of the 24th American Conference on Information Systems (AMCIS)*, 1–9. https://doi.org/10.1145/3380799.3380803

Aivazpour, Z., & Rao, V. S. (2022). A Replication Study of the Impact of Impulsivity on Risky Cybersecurity Behaviors. *AIS Transactions on Replication Research*, 8, 3–. https://doi.org/10.17705/1atrr.00074

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University. Computer and Information Sciences*, 34(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003

Aldawood, H., & Skinner, G. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. *Future Internet*, 11(3), 73–. https://doi.org/10.3390/fi11030073

Alsharif, M., Mishra, S., & AlShehri, M. (2022). Impact of Human Vulnerabilities on Cybersecurity. *Computer Systems Science and Engineering*, 40(3), 1153–1166. https://doi.org/10.32604/csse.2022.019938

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security*, 22(4), 308–313. https://doi.org/10.1016/S0167-4048(03)00407-3

Antunes, M., Silva, C., & Marques, F. (2021). An Integrated Cybernetic Awareness Strategy to Assess Cybersecurity Attitudes and Behaviours in School Context. *Applied Sciences*, 11(23), 11269–. https://doi.org/10.3390/app112311269

Aoyama, T., Naruoka, H., Koshijima, I., & Watanabe, K. (2015). How Management Goes Wrong? – The Human Factor Lessons Learned from a Cyber Incident Handling Exercise. *Procedia Manufacturing*, 3, 1082–1087. https://doi.org/10.1016/j.promfg.2015.07.178

Aqeel, M., Ali, F., Iqbal, M. W., Rana, T. A., Arif, M., & Auwul, M. R. (2022). A Review of Security and Privacy Concerns in the Internet of Things (IoT). *Journal of Sensors*, 2022, 1–20. https://doi.org/10.1155/2022/5724168

Araiza, R. (2022) *Everything you need to know about the CIA triad*. Digital Guardian. https://digitalguardian.com/blog/everything-you-need-know-about-cia-triad

Ariss, S., Nykodym, N., & Cole-Laramore, A. A. (2002). Trust and technology in the virtual organization. S.A.M. *Advanced Management Journal*, 67(4), 22–.

Arora, P. G., Godoy, L., & Hodgkinson, S. (2017). Serving the Underserved: Cultural Considerations in Behavioral Health Integration in Pediatric Primary Care. *Professional Psychology, Research and Practice*, 48(3), 139–148. https://doi.org/10.1037/pro0000131

Balozian, P., Leidner, D., & Warkentin, M. (2019). Managers' and Employees' Differing Responses to Security Approaches. *The Journal of Computer Information Systems*, 59(3), 197–210. https://doi.org/10.1080/08874417.2017.1318687

Barker, W. C. (2003). *Guideline for identifying an information system as a national security system.* U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, p. 15

Baror, S. O., & Venter, H. (2019). A taxonomy for cybercrime attack in the public cloud. In *International conference on cyber warfare and security* (pp. 505-X). Academic Conferences International Limited

Beuran, R., Tang, D., Pham, C., Chinen, K., Tan, Y., & Shinoda, Y. (2018). Integrated framework for hands-on cybersecurity training: CyTrONE. *Computers & Security*, 78, 43–59. https://doi.org/10.1016/j.cose.2018.06.001

Bodley, J. H. (2017). *Cultural anthropology: tribes, states, and the global system* (Sixth edition.). Rowman & Littlefield, a wholly owned subsidiary of The Rowman & Littlefield Publishing Group, Inc.

Bourrelle, S. J. (2015, July 10). *How Culture Drives Behaviors* [Video]. YouTube. https://youtu.be/l-Yy6poJ2zs

Brewer, M. B., & Chen, Y.-R. (2007). Where (Who) Are Collectives in Collectivism? Toward Conceptual Clarification of Individualism and Collectivism. *Psychological Review*, 114(1), 133–151. https://doi.org/10.1037/0033-295X.114.1.133

Brislin, R. W. (1970). Back-Translation for Cross-Cultural Research. *Journal of Cross-Cultural Psychology*, 1(3), 185–216. https://doi.org/10.1177/135910457000100301

Bryk, A. S., & Schneider, B. (2003). Trust in schools: a core resource for school reform. *Educational Leadership*, 60(6), 40–.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, 34(3), 523–548. https://doi.org/10.2307/25750690

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. *Risk Analysis*, 42(8), 1643–1669. https://doi.org/10.1111/risa.13687

Canadian Centre for Cybersecurity (2018, August 15). *An introduction to the Cyber Threat Environment*. https://cyber.gc.ca/sites/default/files/ncta-2022-intro-e.pdf

Carlander, A., & Johansson, L.-O. (2020). Should Trust Be Stressed? General Trust and Proactive Coping as Buffers to Perceived Stress. *Frontiers in Psychology*, 11, 554962–554962. https://doi.org/10.3389/fpsyg.2020.554962

Carlo, G., Roesch, S. C., Knight, G. P., & Koller, S. H. (2001). Between or within-culture variation? Culture group as a moderator of the relations between individual differences and resource allocation preferences. *Journal of Applied Developmental Psychology*, 22(6), 559–579.

Causadias, J. M. (2020). What is culture? Systems of people, places, and practices. *Applied Developmental Science*, 24(4), 310–322. https://doi.org/10.1080/10888691.2020.1789360

Center for Strategic and International Studies (2018, February 21). *The economic impact of cybercrime*. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180906_Cybercrime_Economic_Impact_web.pdf

Chadd, K. (2020, December 5). *The history of cybercrime and cybersecurity, 1940-2020*. Cybercrime Magazine. https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/

Chandra, V., & Hareendran, A. (2018*). Research methodology* (1st edition). Pearson India Education Services.

Chargo, M. A. (2018). You've Been Hacked: How to Better Incentivize Corporations to Protect Consumers' Data. Transactions: Tenn. J. Bus. L., 20, 115

Chatterjee, S.R. and Pearson, C.A. (2002). Trust and managerial transition: evidence from three small Asian economies. *Cross Cultural Management: An International Journal*. 9(4), 19-28

Chen, C. C., Chen, X.-P., & Meindl, J. R. (1998). How Can Cooperation Be Fostered? The Cultural Effects of Individualism-Collectivism. *The Academy of Management Review*, 23(2), 285–304. https://doi.org/10.2307/259375

Cheshire, C., Antin, J., Cook, K. S., & Churchill, E. (2010). *General and Familiar Trust in Websites.* Knowledge in Society, 23(3-4), 311–331. https://doi.org/10.1007/s12130-010-9116-6

Cho, J., Çam, H., & Oltramari, A. (2016). Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis. *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, 7-13.

Chua, H. F., Boland, J. E., & Nisbett, R. E. (2005). Cultural Variation in Eye Movements during Scene Perception. *Proceedings of the National Academy of Sciences - PNAS*, 102(35), 12629–12633. https://doi.org/10.1073/pnas.0506162102

Chua, H. N., Wong, S. F., Low, Y. C., & Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. *Telematics and Informatics*, 35(6), 1770–1780. https://doi.org/10.1016/j.tele.2018.05.005

Clarke, J. (2009). *SQL Injection Attacks and Defense, 2nd Edition* (2nd ed.). Syngress. https://doi.org/10.1016/C2011-0-08480-6

Clarke, R., & Tsar, F. U. C. (2008). Network attack and defense. *Security Engineering: A Guide to Building Dependable Distributed Systems*,, 633-678

Connolly, L. Y., Lang, M., & Wall, D. S. (2019). Information Security Behavior: A Cross-cultural Comparison of Irish and US Employees. *Information Systems Management*, 36(4), 306-332. https://doi.org/10.1080/10580530.2019.1651113

Costantino, G., La Marra, A., Martinelli, F., & Matteucci, I. (2018). CANDY: A Social Engineering Attack to Leak Information from Infotainment System. *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, 1–5. https://doi.org/10.1109/VTCSpring.2018.8417879

Crespo--Pérez, G. (2021). *Factors that Influence the Cybersecurity Behavior: A Cross-Cultural Study*. ProQuest Dissertations Publishing.

Cronk, L. (2017). Culture's Influence on Behavior: Steps Toward a Theory. *Evolutionary Behavioral Sciences*, 11(1), 36–52. https://doi.org/10.1037/ebs0000069

Cukier, M. (2007, February 9). Hackers Attack Every 39 seconds. *University of Maryland*. https://eng.umd.edu/news/story/study- hackers-attack-every-39-seconds.

Cybersecurity & Infrastructure Security Agency (CISA) (2019). *Security Tip (ST04-001). What is Cybersecurity*. Cybersecurity and Infrastructure Security Agency CISA. https://www.us-cert.gov/ncas/tips/ST04-001

Cybersecurity & Infrastructure Security Agency (CISA). (2022, October 22). *Security Tip (ST04-015) – Understanding Denial-of-Service Attacks*. https://www.cisa.gov/uscert/ncas/tips/ST04-015

Cybersecurity Insiders (2021). Insider threat report, 1-24

CyberTalk (2022, April). *Phishing attack statistics 2022*. Cybertalk https://www.cybertalk.org/2022/03/30/top-15-phishing-attack-statistics-and-they-might-scare-you/

Daniels, M. A., & Greguras, G. J. (2014). Exploring the nature of power distance: Implications for micro- and macro-level theories, processes, and outcomes. *Journal of Management, 40*(5), 1202–1229

Davies, V. (2021, October 4). *The History of Cybersecurity*. Cyber Magazine. https://cybermagazine.com/cyber-security/history-cybersecurity

Dawson, J., & Thomson, R. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in Psychology*, 9, 744–744. https://doi.org/10.3389/fpsyg.2018.00744

De Catalunya, U. O. (2022, June 9). *More than 90% of cyberattacks are made possible by human error.* Tech Xplore. https://techxplore.com/news/2022-06-cyberattacks-human-error.html

Department of Homeland Security. (2003, February). National Strategy to Secure Cyberspace. Department of Energy. https://www.energy.gov/sites/default/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf

Deutsch, M. 1973. The resolution of conflict: constructive and destructive processes. New Haven: Yale University Press

Doney, P. M., Cannon, J. P., & Mullen, M. R. (1998). Understanding the Influence of National Culture on the Development of Trust. *The Academy of Management Review*, 23(3), 601–620. https://doi.org/10.2307/259297

Dumont, L. (1986). *Essays on individualism: modern ideology in anthropological perspective*. University of Chicago Press.

Dyer, J.H. and Chu, W.J. (2003). *The role of trustworthiness in reducing transaction costs and improving performance: empirical evidence from the United States, Japan, and Korea*. Organization Science 14 (1): 57–68

Easton, D. (2016, June 14). *What is the Impact of Your Communication Style on Others? | Kent State University*. www.kent.edu. https://www.kent.edu/yourtrainingpartner/what-impact-your-communication-style-others

Eira, A. (2023, January 9). *16 latest Cybercrime Trends & Predictions for 2022/2023 and beyond*. 16 Latest Cybercrime Trends & Predictions for 2022/2023 and Beyond. https://financesonline.com/cybercrime-trends/

El-Bably, A. Y. (2021). Overview of the Impact of Human Error on Cybersecurity based on ISO/IEC 27001 Information Security Management. *Journal of Information Security and Cybercrimes Research*, 4(1), 95–102. https://doi.org/10.26735/WLPW6121

Elbelekia, M. S. S. (2020). *Attitudes of employees towards cybersecurity*. [Unpublished master's thesis]. Near East University.

Erickson, F. (1985). *Qualitative methods in research on teaching* (pp. 119-62). Institute for Research on Teaching

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks*, 9(17), 4667–4679. https://doi.org/10.1002/sec.1657

Faklaris, C., Dabbish, L. A., & Hong, J. I. (2019). A Self report: measure of end-user security attitudes (SA-6). *Fifteenth Symposium on Usable Privacy and Security*. 61-77.

Farris, G. F., Senner, E. E., & Butterfield, D. A. (1973). Trust, Culture, and Organizational Behavior. *Industrial Relations* (Berkeley), 12(2), 144–157. https://doi.org/10.1111/j.1468-232X.1973.tb00544.x

Fatehi, K., Priestley, J. L., & Taasoobshirazi, G. (2020). The expanded view of individualism and collectivism: One, two, or four dimensions? *International Journal of Cross Cultural Management:* CCM, 20(1), 7–24. https://doi.org/10.1177/1470595820913077

Federal Bureau of Investigation (2021). *Internet Crime Report*. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Feizollah, A., Anuar, N. B., Salleh, R., & Wahab, A. W. A. (2015). A review on feature selection in mobile malware detection. *Digital Investigation*, 13, 22–37. https://doi.org/10.1016/j.diin.2015.02.001

Ferro, L. S., & Sapio, F. (2020). Another Week at the Office (AWATO) – An Interactive Serious Game for Threat Modeling Human Factors. *In HCI for Cybersecurity, Privacy and Trust* (pp. 123–142). Springer International Publishing. https://doi.org/10.1007/978-3-030-50309-3_9

Fox, J. (2021, December 27). *Business cost of Cybercrime.* Cobalt. https://www.cobalt.io/blog/business-cost-of-cybercrime

Freed, A. M. (2022, January 24). *Ten of the Biggest Ransomware Attacks of 2021*. Cybereason. https://www.cybereason.com/blog/ten-of-the-biggest-ransomware-attacks-of-2021

Fruhlinger, J. (2022, April 12). *What is phishing? Examples, types, and techniques*. CSO Online. https://www.csoonline.com/article/2117843/what-is-phishing-examples-types-and-techniques.html

Fukuyama, F. (1995) Trust: The Social Virtues and the Creation of Prosperity, The Free Press: New York

Fukuyama, F. (1996). *Trust: the social virtues and the creation of prosperity* (1st Free Press). Free Press Paperbacks.

Gaylord, I. (2019, November 13). *Network Intrusion: How to Detect and Prevent It*. United States Cybersecurity Magazine. https://www.uscybersecurity.net/network-intrusion/

Gebreyes, A. (2020). *Denial of Service Attacks: Difference in Rates, Duration, and Financial Damages and the Relationship Between Company Assets and Revenues*. ProQuest Dissertations Publishing.

Gheorghiu, M. A., Vignoles, V. L., & Smith, P. B. (2009). Beyond the United States and Japan: Testing Yamagishi's Emancipation Theory of Trust across 31 Nations. *Social Psychology Quarterly*, 72(4), 365–383. https://doi.org/10.1177/019027250907200408

Gilbert, P. (2000). The relationship of shame, social anxiety and depression: the role of the evaluation of social rank. *Clinical Psychology & Psychotherapy, 7*, 174-189.

Gillam, A. R., & Foster, W. T. (2020). Factors affecting risky cybersecurity behaviors by U.S. workers: An exploratory study. *Computers in Human Behavior*, 108, 106319–. https://doi.org/10.1016/j.chb.2020.106319

Glaspie, H. W., & Karwowski, W. (2017). Human Factors in Information Security Culture: A Literature Review. *Advances in Human Factors in Cybersecurity*, 269–280. https://doi.org/10.1007/978-3-319-60585-2_25

Gobin, R. L., & Freyd, J. J. (2014). The Impact of Betrayal Trauma on the Tendency to Trust. *Psychological Trauma*, 6(5), 505–511. https://doi.org/10.1037/a0032452

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, 73, 345–358. https://doi.org/10.1016/j.cose.2017.11.015

Gudykunst, W.B., Matsumoto, Y., Ting-Toomey, S., Nishida, T., Kim, K., & Heyman, S. (1996). The Influence of Cultural Individualism-Collectivism, Self Construals, and Individual Values on Communication Styles Across Cultures. *Human Communication Research, 22*, 510-543.

Guiso, L., Sapienza, P., & Zingales, L. (2006). Does culture affect economic outcomes? *The Journal of Economic Perspectives*, 20(2), 23-48

Hadlington, L. (2018). Employees Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom. *International Journal of Cyber Criminology*, 12(1), 269–281. https://doi.org/10.5281/zenodo.1467909

Hadlington, L., & Murphy, K. (2018). Is Media Multitasking Good for Cybersecurity? Exploring the Relationship Between Media Multitasking and Everyday Cognitive Failures on Self-Reported Risky Cybersecurity Behaviors. *Cyberpsychology, Behavior and Social Networking*, 21(3), 168–172. https://doi.org/10.1089/cyber.2017.0524

Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N., Aloul, F., & Chen, J. (2016). Cultural and psychological factors in cyber-security. *Proceedings of the 18th International Conference on Information Integration and Web-Based Applications and Services*, 318–324. https://doi.org/10.1145/3011141.3011165

Hall, E. T. (1976). *Beyond culture* (1st ed.). Anchor Press.

Hamoud, A., & Aïmeur, E. (2020). Handling User-Oriented Cyber-Attacks: STRIM, a User-Based Security Training Model. *Frontiers of Computer Science*.

Han, S., & Ma, Y. (2015). A Culture–Behavior–Brain Loop Model of Human Development. *Trends in Cognitive Sciences*, 19(11), 666–676. https://doi.org/10.1016/j.tics.2015.08.010

Harford, I. (2021, December). *10 common types of malware attacks and how to prevent them*. SearchSecurity. https://www.techtarget.com/searchsecurity/tip/10-common-types-of-malware-attacks-and-how-to-prevent-them

Harris, S. (2002). *CISSP all-in-one certification exam guide.* New York, USA: McGraw-Hill/Osborne

Henderson, A. (2015, July 5). *The CIA Triad: Confidentiality, Integrity, Availability*. Panmore Institute. https://panmore.com/the-cia-triad-confidentiality-integrity-availability

Henshel, D., Cains, M. G., Hoffman, B., & Kelley, T. (2015). Trust as a Human Factor in Holistic Cyber Security Risk Assessment. *Procedia Manufacturing*, 3, 1117–1124. https://doi.org/10.1016/j.promfg.2015.07.186

Henshel, D., Sample, C., Cains, M., & Hoffman, B. (2016). Integrating Cultural Factors into Human Factors Framework and Ontology for Cyber Attackers. *In Advances in Human Factors in Cybersecurity*, *Springer International Publishing.* 123–137. https://doi.org/10.1007/978-3-319-41932-9_11

Heyns, M., & Rothmann, S. (2021). Trust Profiles: Associations with Psychological Need Satisfaction, *Work Engagement, and Intention to Leave. Frontiers in Psychology*, 12, 563542–563542. https://doi.org/10.3389/fpsyg.2021.563542

Hodges, D., & Creese, S. (2015). Understanding cyber-attacks. *In Cyber Warfare* (1st ed., pp. 33–60). Routledge. https://doi.org/10.4324/9781315761565-3

Hofstede, G. (1984). *Culture's consequences: international differences in work-related values* (Abridged ed.). Sage Publications.

Hofstede, G. (2001), Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations Across Nations, 2nd ed. Sage, Thousand Oaks, CA.

Hofstede, G. H. (1980). *Culture's consequences: international differences in work-related values.* Sage Publications.

Hofstede, G., Hofstede, G. J. & Minkov, M. (2010). Cultures and Organizations: Software of the Mind (3rd ed.). New York: McGraw-Hill.

Hofstede, G., Neuijen, B., Ohayv, D. D., & Sanders, G. (1990). Measuring organizational cultures: A qualitative and quantitative study across twenty cases. *Administrative Science Quarterly, 35*(2), 286–316. https://doi.org/10.2307/2393392

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management,* 49(2), 99–110. https://doi.org/10.1016/j.im.2011.12.005

Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*, 7(3), e06522–e06522. https://doi.org/10.1016/j.heliyon.2021.e06522

Hull, G., John, H., & Arief, B. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. *Crime Science*, 8(1), 1–22. https://doi.org/10.1186/s40163-019-0097-9

Hulley, S., Cummings, S., Browner, W., Grady, D., Hearst, N., & Newman, T. (2013). *Designing clinical research* (4th ed.). Philadelphia, PA: Wolters Kluwer Health/Lippincott Williams & Wilkins

Ifinedo, P. (2022). Effects of Security Knowledge, Self-Control, and Countermeasures on Cybersecurity Behaviors. *The Journal of Computer Information Systems, ahead-of-print*(ahead-of-print), 1–17. https://doi.org/10.1080/08874417.2022.2065553

Inglehart, R., C. Haerpfer, A. Moreno, C. Welzel, K. Kizilova, J. Diez-Medrano, M. Lagos, P. Norris, E. Ponarin & B. Puranen (eds.). 2022. World Values Survey: All Rounds - Country-Pooled Datafile. Madrid, Spain & Vienna, Austria: JD Systems Institute & WVSA Secretariat. Dataset Version 3.0.0. doi:10.14281/18241.17

International Telecommunications Union (ITU). (2008). *X.1205 Overview of cybersecurity*. Series X: Data Networks, Open System Communications and Security – Telecommunication Security. https://www.itu.int/rec/T-REC-X.1205-200804-I

IPSOS (2021, October 12). *Global Trustworthiness Index 2021.* https://www.ipsos.com/en/global-trustworthiness-index-2021

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. https://doi.org/10.1186/s13673-016-0065-2

Jaferian, P., Hawkey, K., Sotirakopoulos, A., & Beznosov, K. (2011). Heuristics for evaluating IT security management tools. *CHI '11 Extended Abstracts on Human Factors in Computing Systems*, 1633–1638. https://doi.org/10.1145/1979742.1979820

Jasielska, D., Rogoza, R., Zajenkowska, A., & Russa, M. B. (2021). General trust scale: Validation in cross-cultural settings. *Current Psychology*, 40(10), 5019–5029. https://doi.org/10.1007/s12144-019-00435-2

Javidan, M., & House, R. J. (2001). Cultural acumen for the global manager: Lessons from Project GLOBE. *Organizational Dynamics*, 29: 289-305.

Javidan, M., Zaheer, A. (2019, May 2). *How Leaders Around the World Build Trust Across Cultures.* Harvard Business Review. https://hbr.org/2019/05/how-leaders-around-the-world-build-trust-across-cultures

Johnson, A. G. (2000). *The Blackwell dictionary of sociology: A user's guide to sociological language*. Wiley-Blackwell.

Karacı, A., Akyüz, H.İ., & Bilgici, G. (2017). Investigation of Cyber Security Behaviors of University Students. 25(6), 2079-2094.

Kaspersky (2020, August 26). *What is Social Engineering?* Kaspersky https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering

Kastanakis, M. N., & Voyer, B. G. (2014). The effect of culture on perception and cognition: A conceptual framework. *Journal of Business Research*, 67(4), 425–433. https://doi.org/10.1016/j.jbusres.2013.03.02

Kelly, R. (2017, May 7). *Almost 90% of Cyber Attacks are Caused by Human Error or Behavior*. Chief Executive. https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/

Kemper, G. (2019). Improving employees' cyber security awareness. *Computer Fraud & Security*, 2019(8), 11–14. https://doi.org/10.1016/S1361-3723(19)30085-5

Kharlamov, A. & Pogrebna, G. (2019). Using human values-based approach to understand cross cultural commitment toward regulation and governance of cybersecurity. *Policy & Regulation & Governance* forthcoming. https://doi.org/10.1111/rego.12281

King, Z. M., Henshel, D. S., Flora, L., Cains, M. G., Hoffman, B., & Sample, C. (2018). Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment. *Frontiers in Psychology*, 9, 39–39. https://doi.org/10.3389/fpsyg.2018.00039

Klein, H. A., Lin, M.-H., Miller, N. L., Militello, L. G., Lyons, J. B., & Finkeldey, J. G. (2019). Trust Across Culture and Context. *Journal of Cognitive Engineering and Decision Making*, 13(1), 10–29. https://doi.org/10.1177/1555343418810936

Kluckhohn, C. (1951) *Values and Value-Orientations in the Theory of Action: An Exploration in Definition and Classification*. Toward a General Theory of Action, Harvard University Press, Cambridge, 388-433. http://dx.doi.org/10.4159/harvard.9780674863507.c8

Kobis, P. (2021). Human factor aspects in information security management in the traditional IT and cloud computing models. *Operations Research and Decisions*, 31(1), 61–76. https://doi.org/10.37190/ord210104

Kolkowska, E., Hedström, K., & Karlsson, F. (2009*). Information security goals in a Swedish hospital*. In Security, assurance and privacy: organizational challenges. 8th Annual Security Conference, 15-16 April 2009, Las Vegas, USA

Krebs, S. A., Hobman, E. V., & Bordia, P. (2006). Virtual teams and group member dissimilarity: consequences for the development of trust. *Small Group Research*, 37(6), 721–741. https://doi.org/10.1177/1046496406294886

Kumari, K., & Mrunalini, M. (2022). Detecting Denial of Service attacks using machine learning algorithms. *Journal of Big Data*, 9(1), 1–17. https://doi.org/10.1186/s40537-022-00616-0

Kwantes, C. T., & Kuo, B. C. (2021). *Trust and Trustworthiness across Cultures*. Springer International Publishing

Kwantes, C.T., McMurphy, S. (2021). *Contextual Influences on Trust and Trustworthiness: An Etic Perspective.* In: Kwantes, C.T., Kuo, B.C.H. (eds) Trust and Trustworthiness across Cultures. Springer Series in Emerging Cultural Perspectives in Work, Organizational, and Personnel Studies. Springer, Cham. https://doi.org/10.1007/978-3-030-56718-7_1

Lalonde Levesque, F., Nsiempba, J., Fernandez, J., Chiasson, S., & Somayaji, A. (2013). A clinical study of risk factors related to malware infections. *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, 97–108. https://doi.org/10.1145/2508859.2516747

LaMorte, W. W. (2021, October 7). *Correlation and Linear Regression*. https://sphweb.bumc.bu.edu/otlt/mph-modules/bs/bs704_correlation-regression/bs704_correlation-regression2.html

Lane, C. (1997). The social regulation of inter-firm relations in Britain and Germany: market rules, legal norms and technical standards. *Cambridge Journal of Economics*, 21(2), 197–215. https://doi.org/10.1093/oxfordjournals.cje.a013666

Lane, C. and Bachmann, R. (1996). The social constitution of trust: supplier relations in Britain and Germany. *Organization Studies* 17(3), 365–395

Lanier, S. T. (2022). *The Financial Implications of Information Security: A Correlational Study*. ProQuest Dissertations Publishing.

Leung, K., & Stephan, W. G. (1998). Perceptions of injustice in intercultural relations. *Applied & Preventive Psychology*, 7(3), 195–205. https://doi.org/10.1016/S0962-1849(05)80022-8

Lewis, J. D., & Weigert, A. (1985). Trust as a Social Reality. *Social Forces*, 63(4), 967–. https://doi.org/10.2307/2578601

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Libicki, M. (2018). Could the Issue of DPRK Hacking Benefit from Benign Neglect? *Georgetown Journal of International Affairs*, 19(1), 83–89. https://doi.org/10.1353/gia.2018.0010

Lin, C.-Y., Imani, V., Griffiths, M. D., & Pakpour, A. H. (2021). Psychometric Properties of the Persian Generalized Trust Scale: Confirmatory Factor Analysis and Rasch Models and Relationship with Quality of Life, Happiness, and Depression. *International Journal of Mental Health and Addiction*, 19(5), 1854–1865. https://doi.org/10.1007/s11469-020-00278-0

Lin, C., Namdar, P., Griffiths, M. D., & Pakpour, A. H. (2021). Mediated roles of generalized trust and perceived social support in the effects of problematic social media use on mental health: A cross-sectional study. *Health Expectations : an International Journal of Public Participation in Health Care and Health Policy*, 24(1), 165–173. https://doi.org/10.1111/hex.13169

Lugrin, B., Frommel, J., & Andre, E. (2015). Modeling and Evaluating a Bayesian Network of Culture-Dependent Behaviors. *International Conference on Culture and Computing (Culture Computing)*, 33–40. https://doi.org/10.1109/Culture.and.Computing.2015.30

Madigan, L. (2014, August 20). *Cybercrime inevitable, so protect yourself*. The State Journal-Register. https://www.sj-r.com/story/opinion/columns/2014/08/21/cybercrime-inevitable-so-protect-yourself/36631985007/

Markets and Markets. (2020). *Artificial intelligence in cybersecurity market*. (No. SE5851). https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-security-market-220634996.html

Marková, I. (2004). Introduction: Trust/Risk and Trust/Fear. *In Trust and Democratic Transition in Post-Communist Europe.* British Academy. https://doi.org/10.5871/bacad/9780197263136.003.0001

Marsh, S., & Dibben, M. R. (2005). Trust, Untrust, Distrust and Mistrust – An Exploration of the Dark(er) Side. *Lecture Notes in Computer Science*, 3477, 17–33. https://doi.org/10.1007/11429760_2

Marshall, R. S. (2003). Building trust early: the influence of first and second order expectations on trust in international channels of distribution. *International Business Review*, 12(4), 421–443. https://doi.org/10.1016/S0969-5931(03)00037-4

Masuda, T., & Nisbett, R. E. (2001). Attending holistically versus analytically: Comparing the context sensitivity of Japanese and Americans. *Journal of Personality and Social Psychology*, 81(5), 922–934. https://doi.org/10.1037//0022-3514.81.5.922

Matheson, D. (2004). *The complete guide to good governance in organizations and companies*. New Zealand Management, 51(9), 72-72.

Matsumoto, D., & Juang, L. (2016). *Culture and psychology*. Cengage Learning.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709-734

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior*, 69, 151–156. https://doi.org/10.1016/j.chb.2016.11.065

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of Awareness and Training on Cyber Security. *Journal of Internet Commerce*, 9(1), 23–41. https://doi.org/10.1080/15332861.2010.487415

McKnight, D.H and Chervany, N.L (2000). What is trust? A conceptual analysis and an interdisciplinary model. *Proceedings of the 2000 Americas Conference on Information Systems*, 827-833.

Megira, S., Pangesti, A. R., & Wibowo, F. W. (2018). Malware Analysis and Detection Using Reverse Engineering Technique. *Journal of Physics*. 1140(1), 12042–. https://doi.org/10.1088/1742-6596/1140/1/012042

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. Procedia, *Social and Behavioral Sciences*, 147, 424–428. https://doi.org/10.1016/j.sbspro.2014.07.133

Meyer, E. (2017, January 23). *Building Trust Across Cultures*. Global Leadership Network. https://globalleadership.org/articles/leading-others/building-trust-across-cultures-erin-meyer-2/?locale=en

Mishra, B. K., & Ansari, G. M. (2012). Differential Epidemic Model of Virus and Worms in Computer Network. *Int. J. Netw. Secur.*, *14*(3), 149-155.

Mitchell, A., & Zigurs, I. (2009). Trust in virtual teams: solved or still a mystery? *ACM SIGMIS Database: The Database for Advances in Information Systems*, 40(3), 61–83. https://doi.org/10.1145/1592401.1592407

Mohan, S. (2016, September 16). *The greatest security vulnerability: Humans*. Application Security Blog. https://www.synopsys.com/blogs/software-security/greatest-security-vulnerability/

Möllering, G. (2006) *Trust: Reason, Routine, Reflexivity*. Oxford: Elsevier, 191–.

MonsterCloud. (2020, August 11). *Top cyber security experts report: 4,000 cyber attacks a day since COVID-19 pandemic*. MonsterCloud. https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html

Montoro, A., Shih, P.-C., Román, M., & Martínez-Molina, A. (2014). Spanish adaptation of Yamagishi General Trust Scale. *Anales de Psicología*, 30(1), 302–. https://doi.org/10.6018/analesps.30.1.122471

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly: Management Information Systems*, 42(1), 285-311. https://doi.org/10.25300/MISQ/2018/13853

Morgan, S. (2021, April 27). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Cybercrime Magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Morris, G. (2020, December 30). *Top cybercrimes of 2020 - how to prevent them in 2021*. Datalink Networks. https://www.datalinknetworks.net/dln_blog/top-cybercrimes-of-2020-and-how-to-prevent-them

Mutune, G. (2021, December 31). *The quick and dirty history of cybersecurity*. CyberExperts. https://cyberexperts.com/history-of-cybersecurity/

National Cyber Security Alliance. (2022). Cybersecurity: 3 Things Every Small Business Owner Should Know. Stay Safe Online. https://staysafeonline.org/small-business/cybersecurity/

National Institute of Science and Technology (NIST). (2019). *Cybersecurity for the Internet of Things*. NIST. https://www.nist.gov/cybersecurity-technology-advancement/cybersecurity-internet-things

National Institute of Standards and Technology (NIST). (2014). Cybersecurity framework. Gaithersburg, MD: National Institute of Standards and Technology.

National Institute of Standards and Technology (NIST). (2020). *Cybersecurity Framework* (Version 1.1). Gaithersburg, MD: National Institute of Standards and Technology, U.S. Department of Commerce.

Nisbett, R. E., Pens, K., Incheol Choi, & Norenzayan, A. (2001). Culture and systems of thought: Holistic versus analytic cognition. *Psychological Review*, 108(2), 291–310. https://doi.org/10.1037//0033-295X.108.2.291

Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. *Holistica: Journal of Business and Public Administration*, 9(3), 71–88. https://doi.org/10.2478/hjbpa-2018-0024

Nunes, P., Antunes, M., & Silva, C. (2021). Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions. *Procedia Computer Science*, 181, 173–181. https://doi.org/10.1016/j.procs.2021.01.118

Oltramari, A., Henshel, D. S., Cains, M., & Hoffman, B. (2015). Towards a Human Factors Ontology for Cyber Security. *Semantic Technologies for Intelligence, Defense, and Security*, 26-33

Oyserman, D. (2011). Culture as situated cognition: Cultural mindsets, cultural fluency, and meaning making. *European Review of Social Psychology*, 22(1), 164–214. https://doi.org/10.1080/10463283.2011.627187

Papayiannis, S., Anastassiou-Hadjicharalambous, X. (2011). *Cross-Cultural Studies*. In: Goldstein, S., Naglieri, J.A. (eds) Encyclopedia of Child Behavior and Development. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-79061-9_738

Parker, H. J., & Flowerday, S. V. (2020). Contributing factors to increased susceptibility to social media phishing attacks. *South African Journal of Information Management*, *22*(1), 1-10.

Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). Human Factors and Information Security: Individual, Culture and Security Environment. *DSTO Formal Reports*, TR(2484)

Pew Research Center's Internet, Science & Tech division released a report, "Americans and Cybersecurity." (2017). *Information Today*, 34(2), 3–.

Pogue, C. (2018). *The 2018 Black Report. Decoding the Minds of Hackers.* https://cdn2.hubspot.net/hubfs/85462/2018/THIS%20WEEK/report_nuix_black_report_2018_web_us.pdf

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, technology & work*, 24(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y

Pollock, T. (2017*). Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS)*. 2017 KSU Conference on Cybersecurity Education, Research and Practice, Kennesaw State University, GA, United States

Qadir, S., & Quadri, S. M. K. (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. *Journal of Information Security*, 7(3), 185–194. https://doi.org/10.4236/jis.2016.73014

Quiñones, D., & Rusu, C. (2017). How to develop usability heuristics: A systematic literature review. *Computer Standards and Interfaces*, 53, 89–122. https://doi.org/10.1016/j.csi.2017.03.009

Razak, M. F. A., Anuar, N. B., Salleh, R., & Firdaus, A. (2016). The rise of "malware": Bibliometric analysis of malware study. *Journal of Network and Computer Applications*, 75, 58–76. https://doi.org/10.1016/j.jnca.2016.08.022

Riemhofer, A. (16, July 2019). *Three things you should do so Germans develop trust in you*. Intercultural business facilitation. https://andra-ibf.com/2019/07/16/trust-across-cultures-advice-for-germany/

Risto, J. (2016). *Success Rates for Client Side Vulnerabilities* [White Paper]. SANS Institute. https://sansorg.egnyte.com/dl/TQJGXAAIK0

Russell, J. D., Weems, C. F., Ahmed, I., & Richard III, G. G. (2017). Self-reported secure and insecure cyber behaviour: factor structure and associations with personality factors. *Journal of Cyber Security*, 1(3-4), 163–174. https://doi.org/10.1080/23742917.2017.1345271

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, 11(4), 89–. https://doi.org/10.3390/fi11040089

Sanoubari, E., & Young, J.E. (2018). Explicit, Neutral, or Implicit: A Cross-cultural Exploration of Communication-style Preferences in Human Robot Interaction. *Companion of the 2018 ACM/IEEE International Conference on Human-Robot Interaction*.

Saunders, M. N. K., Skinner, D., Dietz, G., Gillespie, N., & Lewicki, R. J. (2010). *Organizational trust: a cultural perspective*. Cambridge University Press

Schein, E. H. (1990). Organizational culture. *American Psychologist, 45*(2), 109–119. https://doi.org/10.1037/0003-066X.45.2.109.

Schoorman, F.D., Mayer, R.C., & Davis, J.H. (2007). An Integrative Model of Organizational Trust: Past, Present, and Future. *Academy of Management Review*, 32, p. 344-354.

Schultz, E. (2005). The human factor in security. *Computers & Security*, 24(6), 425–426. https://doi.org/10.1016/j.cose.2005.07.002

Scott, C. L., & Byrd, M. Y. (2012). Leveraging Workforce Diversity in Practice: Building Successful Global Relationships with Minority-Owned Suppliers. In *Handbook of Research on Workforce Diversity in a Global Society: Technologies and Concepts*, 323–340). IGI Global. https://doi.org/10.4018/978-1-4666-1812-1.ch019

Scroope, C. (2017). *French culture - business culture*. Cultural Atlas. https://culturalatlas.sbs.com.au/french-culture/french-culture-business-culture

Sellaro, R., Hommel, B., de Kwaadsteniet, E. W., van de Groep, S., & Colzato, L. S. (2014). Increasing interpersonal trust through divergent thinking. *Frontiers in psychology*, 5, 561.

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2020). Personality as a Predictor of Cybersecurity Behavior. *Psychology of Popular Media*, 9(4), 475–480. https://doi.org/10.1037/ppm0000247

Smith, Z. M., & Lostri, U. (2020). *The Hidden Costs of Cybercrime*. McAfee. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

Snowdon, C. T. (2017). *Introduction to Animal Culture: Is Culture Uniquely Human?* John Wiley & Sons, Inc. https://doi.org/10.1002/9781119181361.ch4

Speed, T. J. (2012). *Asset protection through security awareness* (1st edition). CRC Press, 213-226. https://doi.org/10.1201/b11355

Stanford University. (n.d.). *Survey Definitions*. IDEAL Diversity Equity and Inclusion Survey. https://idealdeisurvey.stanford.edu/faq/survey-definitions

Stastny, P., & Stoica, A.-M. (2022). Protecting aviation safety against cybersecurity threats. IOP Conference Series. *Materials Science and Engineering*, 1226(1), 012025. https://doi.org/10.1088/1757-899X/1226/1/012025

Stastny, P., & Stoica, A.-M. (2022). Protecting aviation safety against cybersecurity threats. IOP Conference Series. *Materials Science and Engineering*, 1226(1), 12025–. https://doi.org/10.1088/1757-899X/1226/1/012025

Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., Kruegel, C., & Vigna, G. (2009). Your botnet is my botnet: analysis of a botnet takeover. *Proceedings of the 16th ACM Conference on Computer and Communications Security*, 635–647. https://doi.org/10.1145/1653662.1653738

Talaei, A., Lin, I., & Kwantes, C. T. (2013). *The History of Cybersecurity*. Future of Tech. https://www.futureoftech.org/cybersecurity/2-history-of-cybersecurity/

Tan, E., & Cox, A. (2019). Trusted Teammates: Commercial Digital Games Can Be Effective Trust-Building Tools. *Extended Abstracts of the Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts*, 705–713. https://doi.org/10.1145/3341215.3356296

The White House (2022, March 21). *Statement by President Biden on our Nation's Cybersecurity* [Press release]. https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/

Threatcop (2021, June 17). *Humans are the Weakest Link in Cyber Security Chain*. Medium. https://threatcop.medium.com/humans-are-the-weakest-links-in-cyber-security-of-any-organisation-ac04c6e6e71

Ting-Toomey, S. (1988). Intercultural conflict styles: A face-negotiation the- ory. In Y. Y. Kim & W. Gudykunst (Eds.), *Theories in intercultural commu- nication* (pp. 213-235). Newbury Park, CA: Sage

Tov, W., & Nai, Z. L. S. (2017). Cultural differences in subjective well-being: How and why. In *Subjective well-being and life satisfaction* (pp. 50-73). Routledge.

Triandis, H. C. (1972). The analysis of subjective culture

Triandis, H. C. (1989). The Self and Social Behavior in Differing Cultural Contexts. *Psychological Review*, 96(3), 506–520. https://doi.org/10.1037/0033-295X.96.3.506

Triandis, H. C., & Gelfand, M. J. (1998). Converging Measurement of Horizontal and Vertical Individualism and Collectivism. *Journal of Personality and Social Psychology*, 74(1), 118–128. https://doi.org/10.1037/0022-3514.74.1.118

Triandis, H.C. (1995) Individualism and Collectivism. Westview Press, Boulder.

Triplett, W. J. (2022). Addressing Human Factors in Cybersecurity Leadership. *Journal of Cybersecurity and Privacy*, 2(3), 573–586. https://doi.org/10.3390/jcp2030029

Trompenaars, A. (1994). *Riding the waves of culture: understanding diversity in global business*. Irwin Professional Pub.

Tylor, E. B.-. (1871*). Primitive culture: researches into the development of mythology, philosophy, religion, art, and custom*. J. Murray, 1871.

U.S Census Bureau (2022). *Quick Facts*. The Census Bureau. https://www.census.gov/quickfacts/fact/table/US/RHI125221#RHI125221

Van-Zadelhoff, M. (2016, September 19). *The biggest cybersecurity threats are Inside your company*. Harvard Business Review. https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company

Vance, A., Siponen, M. T., & Straub, D. W. (2020). Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. *Information & Management*, 57(4), 103212–. https://doi.org/10.1016/j.im.2019.103212

Varnum, M. E. W., Grossmann, I., Kitayama, S., & Nisbett, R. E. (2010). The Origin of Cultural Differences in Cognition: Evidence for the Social Orientation Hypothesis. *Current Directions in Psychological Science : a Journal of the American Psychological Society*, 19(1), 9–13. https://doi.org/10.1177/0963721409359301

Veale, M. & Brown, I. (2020). Cybersecurity. *Internet Policy Review*, 9(4). https://doi.org/10.14763/2020.4.1533

Venkatachary, S. K., Prasad, J., & Samikannu, R. (2017). Economic impacts of cyber security in energy sector: A review. *International Journal of Energy Economics and Policy*, *7*(5), 250.

Walsham, G. (2002). Cross-Cultural Software Production and Use: A Structurational Analysis. *MIS Quarterly*, 26(4), 359–380. https://doi.org/10.2307/4132313

Wang, K.Y. and Clegg, S. (2002). Trust and decision making: are managers different in the people's Republic of China and in Australia. *Cross Cultural Management: An International Journal*. 9(1) 30-45.

Washington, M. G. (2013). *Trust and Project Performance: The Effects of Cognitive-Based and Affective- Based Trust on Client-Project Manager Engagements*. [Master of Science in Organizational Dynamics Theses, The University of Pennsylvania]. https://repository.upenn.edu/od_theses_msod/67

Watabe, M., Kato, T. A., Teo, A. R., Horikawa, H., Tateno, M., Hayakawa, K., Shimokawa, N., & Kanba, S. (2015). Relationship between trusting behaviors and psychometrics associated with social network and depression among young generation: a pilot study. *PloS One*, 10(3), e0120183–e0120183. https://doi.org/10.1371/journal.pone.0120183

Weber, E. U., & Hsee, C. K. (1999). Models and mosaics: investigating cross-cultural differences in risk perception and risk preference. *Psychonomic bulletin & review*, *6*(4), 611–617. https://doi.org/10.3758/bf03212969

Weber, E. U., & Morris, M. W. (2010). Culture and Judgment and Decision Making: The Constructivist Turn. *Perspectives on Psychological Science*, 5(4), 410–419. https://doi.org/10.1177/1745691610375556

West, M. (2009). *Chapter 3 - Preventing System Intrusions*. In Computer and Information Security Handbook, 9–51 Elsevier Inc. https://doi.org/10.1016/B978-0-12-374354-1.00003-0

White House Press Release (2009). Remarks by the President on Securing our Nation's Cyber Infrastructure. https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure

Wiederhold, B. K. (2014). The Role of Psychology in Enhancing Cybersecurity. *Cyberpsychology, Behavior and Social Networking*, 17(3), 131–132. https://doi.org/10.1089/cyber.2014.1502

Wijayanto, H., & Prabowo, I. A. (2020). Cybersecurity Vulnerability Behavior Scale in College During the Covid-19 Pandemic. *Jurnal Sisfokom*, 9(3), 395–399. https://doi.org/10.32736/sisfokom.v9i3.1021

Wilhelm, T., & Neely, M. (2013*). Professional penetration testing creating and learning in a hacking lab* (2nd ed.). Syngress, an imprint of Elsevier.

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, 72, 412–421. https://doi.org/10.1016/j.chb.2017.03.002

World Economic Forum (2022) *The Global Risks Report 2022*. Weforum. https://www.weforum.org/reports/global-risks-report-2022

Yamagishi, T., & Yamagishi, M. (1994). Trust and commitment in the United States and Japan. *Motivation and Emotion*, 18(2), 129–166. https://doi.org/10.1007/BF02249397

Yamagishi, T., Cook, K. S., & Watabe, M. (1998). Uncertainty, trust, and commitment formation in the United States and Japan. The American Journal of Sociology, 104(1), 165–194. https://doi.org/10.1086/210005

Yang, J., Mossholder, K. W., & Peng, T. K. 2007. Procedural justice climate and group power distance: An examination of cross-level interaction effects. Journal of Applied Psychology, 92: 681-692.

Yates, J. F., & de Oliveira, S. (2016). Culture and decision making. *Organizational Behavior and Human Decision Processes*, 136, 106–118. https://doi.org/10.1016/j.obhdp.2016.05.003

Yin, H., Song, D., Egele, M., Kruegel, C., & Kirda, E. (2007). Panorama: capturing system-wide information flow for malware detection and analysis. *Conference on Computer and Communications Security: Proceedings of the 14th ACM Conference on Computer and Communications Security*; 28-31 Oct. 2007, 116–127. https://doi.org/10.1145/1315245.1315261

Zaheer, A., & Zaheer, S. (2006). Trust across Borders. *Journal of International Business Studies*, 37(1), 21–29. https://doi.org/10.1057/palgrave.jibs.8400180

Zimmermann V, Renaud K. Moving from a ‘human-as-problem” to a ‘human-as-solution” cybersecurity mindset. *International Journal of Human Computer Studies*, 131, 169–187. https://doi: 10.1016/j.ijhcs.2019.05.005

Zippia (2022, September 9). *Cyber Security Specialist Demographics and Statistics [2023]: Number of cyber security specialists in the US*. Zippia. https://www.zippia.com/cyber-security-specialist-jobs/demographics/

APPENDIX A: GENERAL TRUST SCALE (GTS)

Using the following scale, please indicate how much you agree or disagree with the following statements:

1 *Strongly Disagree*	*2* *Disagree*	*3* *Agree*	*4* *Strongly Agree*

1. Most people are basically honest.
2. Most people are trustworthy.
3. Most people are basically good and kind.
4. Most people are trustful of others.
5. I am trustful.
6. Most people will respond in kind when they are trusted by others.

APPENDIX B: RISKY CYBERSECURITY BEHAVIOR SCALE (RSCB)

Participants were asked to rate, on a scale of 1 to 4 (with 1 indicating "Never" and 4 indicating "Very Often"), the frequency with which they engaged in specific behaviors.

1. Sharing passwords with friends and colleagues.
2. Using or creating passwords that are not very complicated (e.g., family name and date of birth).
3. Using the same password for multiple websites.
4. Using online storage systems to exchange and keep personal or sensitive information.
5. Entering payment information on websites that have no clear security information/certification.
6. Using free-to-access public Wi-Fi
7. Relying on a trusted friend or colleague to advise you on aspects of online security.
8. Downloading free anti-virus software from an unknown source.
9. Disabling the anti-virus on my work computer so that I can download information from websites.
10. Bringing in my own USB to work in order to transfer data on to it.
11. Checking that software for your smartphone/tablet/laptop/PC is up to date.
12. Downloading digital media (music, films, games) from unlicensed sources
13. Sharing my current location on social media.
14. Accepting friend requests on social media because you recognize the photo.
15. Clicking on links contained in unsolicited emails from an unknown source.
16. Sending personal information to strangers over the Internet.
17. Clicking on links contained in an email from a trusted friend or work colleague.
18. Checking for updates to any anti-virus software you have installed.
19. Downloading data and material from websites on my work computer without checking its authenticity.
20. Storing company information on my personal electronic device (e.g., smartphone/tablet/laptop).

APPENDIX C: DEMOGRAPHIC QUESTIONS

Q1 Which cultural group best describes you?

- Caucasian (e.g.: German, Irish, Italian, Polish, French, etc.)
- Hispanic, Latino, or Spanish origin (e.g., Mexican, or Mexican American, Puerto Rican, Cuban, Salvadoran, Dominican, Columbia, etc.)
- Black or African American (e.g., African American, Jamaican, Haitian, Nigerian, Ethiopian, Somalian, etc.)
- Asian (e.g., Chinese, Filipino, Indian, Vietnamese, Korean, Japanese, Malaysia, Pakistan, etc.)
- American Indian or Alaska Native (e.g., Navajo nation, Blackfeet tribe, Mayan, Aztec, Native Village or Barrow Inupiat Traditional Government, Nome Eskimo Community, etc.)
- Middle Eastern or North African (e.g., Lebanese, Iranian, Qatar, Jordanian, Saudi Arabian, Egyptian, Syrian, Moroccan, Algerian, etc.)
- Native Hawaiian or Pacific Islander (e.g. Native Hawaiian, Samoan, Chamorros, Tongan, Fijian, etc.)
- Other

Q2 What is your gender?

- Male
- Female
- Other
- Prefer not to say

Q3 Current level of education

- High School
- Associate's Degree
- Bachelor's Degree
- Postgraduate Degree

Q4 What kind of computer user are you?

- Novice user (you just started using computers)
- Average user (you use spreadsheets, emails, surf the web)
- Advanced user (you can install software, setup configurations)
- Expert user (you can setup operating systems, know programming languages)