TOWARDS A HOLISTIC INTERDISCIPLINARY EDUCATION IN CYBERSECURITY

by

Johanna Jacob, B.E

THESIS

Presented to the Faculty of

The University of Houston-Clear Lake

In Partial Fulfillment

Of the Requirements

For the Degree

MASTER OF SCIENCE

in Computer Science

THE UNIVERSITY OF HOUSTON-CLEAR LAKE

DECEMBER, 2018

TOWARDS A HOLISTIC INTERDISCPLINARY EDUCATION

IN CYBERSECURITY

by

Johanna Jacob

APPROVED BY

_____

T. Andrew Yang, PhD, Chair

_____

Wei Wei, PhD, Committee Member

_____

Sadegh Davari, PhD, Committee Member

RECEIVED/APPROVED BY THE COLLEGE OF SCIENCE AND ENGINEERING:

_____

Said Bettayeb, PhD, Interim Associate Dean

_____

Ju Hyo Kim, PhD, Interim Dean

ABSTRACT

TOWARDS A HOLISTIC INTERDISCPLINARY EDUCATION

IN CYBERSECURITY

Johanna Jacob
University of Houston-Clear Lake, 2018

Thesis Chair: Dr. T. Andrew Yang

The need for cybersecurity professionals continues to grow and education systems are responding in a variety of ways. This study focusses on the "interdisciplinarity" of cybersecurity in the light of current guidelines and frameworks that shape the growth and development of cybersecurity education and training. The study also significantly recognizes the contributions of other disciplines to the field of cybersecurity by the discussion of theories that contribute to understanding security in the context of legal, economics and criminology perspectives. A detailed discussion of the current guidelines in cybersecurity education is discussed to emphasize and indicate the changing needs and draws the importance of a multi-disciplinary approach. Finally, an extensive quantitative analysis is done to understand the existing knowledge of security behaviors and beliefs among students from technical and non-technical majors, and measure the interest fostered towards an academic pathway in cybersecurity. The results of the analysis will help understand the demand and need for a collaborative cybersecurity program in the Department of Computer Science.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

The term “cybersecurity” has been the highlight of academic literature for many years. With a significant rise in the proliferation of technology and the innovation that comes along with it, cybercrime has equally penetrated all aspects of human endeavor. The rising number of breaches and threats to personal, organizational and national safety have led to an increased focus on the defensive measures. It has in fact become the highest priority items on the global policy and national security agendas [1]. According to Cyber Security Business report, Cyber Crime damage costs will hit $6 trillion annually by 2021 [2]. In response, the Cybersecurity Policy Review [3] demanded for a national strategy to develop cybersecurity awareness and incorporate a cyber-secure workforce that is adequate in expertise and skills to be cyber-ready against the potential threats faced by the nation in different domains and avenues. There is a serious need for cybersecurity talent [1] to secure the infrastructure of federal and private entities against the growing cyber risks. Cyber-attacks are constantly progressing in frequency and sophistication. Cisco systems reported [43] that there is an unprecedented level of sophistication in deviousness and operation of the cyber criminals.

The treading complexity of cyber terrorism and hacking incidents portray the need for cybersecurity with a global perspective. A report from Frost, Sullivan and (ISC)2 depicts that more than 1.5 million positions will be unfilled in the global cybersecurity workforce [4]. One of the important reasons for such a dearth in cybersecurity talent is businesses looking for people with traditional technology credentials rather than absorbing potential candidates from non-traditional, non-computing backgrounds[5]. PayScale, a provider of on-demand compensation and software, states that 87% of recent graduates feel well prepared to hit the fast-paced

Cyber industry. However, for more than 51% of those graduates, underemployment is the reality [6]. This is contributed [6] by a massive gap in skills such as communication, ownership, leadership, teamwork, problem-solving, understanding cultural, social, legal, economic and political perspectives in the context of the problem at hand.

This work focusses on the "interdisciplinarity" of cybersecurity in the light of current guidelines and frameworks that shape the growth and development of cybersecurity workforce, and forms the foundation for curriculum development, training and certification. Also, it contributes significantly to understanding security behaviors and attitudes of students from technical and non-technical majors and measure the interest fostered towards an interdisciplinary approach in cybersecurity education through an extensive quantitative analysis.

Background and Problem

Cybersecurity has evolved into myriad avenues in the corporate and government sectors. Federal departments and agencies have been challenged with sophisticated and persistent cyber threats that pose strategic, economic and security challenges to the national infrastructure. This is due to the tremendous increase in the growth and usage of pervasive devices allowing accessibility and connectivity in every part of the world. The proliferation of cell phones and smart mobile applications have revolutionized the way people interact with devices. While all the technological innovations and advancements have paved the way to a "smart" world, they have innumerably increased the unintended consequences leading to an increase in cybercrime, threats and vulnerabilities in the infrastructure of the nation and private organizations. According to a report by the Berkley Research Group [7], infections from virus or malicious software account for about 39% of all data breaches, followed by system failures or data corruption accounting to 35% of breaches. And surprisingly, most organizations do not have a strategy to

combat cyber threats in emerging field as Internet of Things and Big Data. This leads to the cybersecurity workforce suffering from a fragmented cadre of training and development programs.

Due to the rising opportunities of accessing technology and devices, cybercriminals are on the rise to acquire Personally Identifiable Information through fraudulent means. A 2017 survey by Statista reports [8] that the greatest cybersecurity problem of the United States was hacking by foreign governments. The report also points out that "51 percent of U.S. adults believed that a cyber-attack on public infrastructure would probably happen in the next five years". The challenges posed by technology misuse and abuse are manifold and requires an equal contribution from computer science and social science researchers to better understand the dynamics of the attack and perpetrator and to propose a feasible solution to combat it. To exemplify this, consider phishing emails. Phishing emails can be blocked by email server software based on rules and classification strategies that are configured on the server end. However, it may still penetrate through to the end user. Potential recipients must be able to identify and understand these phishing messages as a threat to reduce the chances of being victimized. One needs to understand the behavioral and attitudinal differences that led some to respond to fraudulent messages while some others do not. On a much larger scale, it is important for organizations to understand the attack, the attacker and the dynamics around them.

Holt [9] in his journal, "Cybercrime through an interdisciplinary lens" points out that it is critical to situate a cybercrime threat or vulnerability in a multidisciplinary context. A holistic approach to cybersecurity is one that considers the many disciplines that produce cybersecurity professionals – technical and non-technical alike, in a coherent fashion. Such an approach respects the relative contributions of the different subfields

and recognizes that, prospective cybersecurity professionals must develop an expertise within their individual subfield while simultaneously understanding how their work fits into rest of the field.

However, such an approach to cybersecurity has been stove piped for decades in the education system of the nation. For instance, the disciplines of computer science and engineering are focused on developing algorithms and secure devices that support sensitive systems, and data/information processing while information technology and information assurance focus on better techniques, tools and process to protect information from being misused. While there is a higher emphasis on understanding the technical nature of the cyber environment, the networked systems, operating systems and the security threats around them, there is little to no emphasis on the human actors and their decision-making process that plays vital role in a cyber-attack being successful [10]. Knowing this will allow institutions or organizations to tailor educational programs accordingly.

Significance of the Study

This study will significantly recognize the contributions of other disciplines to the field of cybersecurity by the discussion of theories that contribute to the understanding security in the context of legal, economics and managerial perspectives. A detailed discussion of the current guidelines and frameworks in cybersecurity education is discussed to emphasize and indicate the changing needs and draws the importance of a multi-disciplinary approach. Finally, a quantitative analysis is done to understand the existing knowledge of security behaviors and beliefs and measure the interest fostered towards an academic pathway in cybersecurity. The results of the analysis will help to understand the demand and need for a collaborative cybersecurity program in the Department of Computer Science.

Research Purpose and Questions

Cybersecurity is a nascent and exploding field with a growing body of research. However, the research is rooted in traditional computer science but recently gained prevalence in other fields as legal studies, business, management and criminology as well as areas of technology that did not originally operate with the internet as internet of things, grid computing etc. In standards of research and collaboration with interdisciplinary subject area, cybersecurity has been given little attention because of the disciplines' standards of strictly being specified as technical.

The thesis is motivated by the observed sparsity of interdisciplinary research and collaboration in the existing frameworks which stands as a foundational groundwork for many cybersecurity initiatives. Outside the traditional computing space, there is an apparent lack of communication across disciplines, making the framework less inter-disciplinary. For example, there is a myriad of technical fields which offer solutions that support cyber security, but these solutions alone do not resolve cybersecurity challenges. Organizational, social, political, economic and other human dimensions are inevitably tied to them, but their contribution is overlooked in comparison to the technical avenues.

A recent internet fact sheet [11] shows that 76.5% of the US population access the internet from their home. Despite not being security experts, students from technical and non-technical majors are tasked with administering and making security decisions for their computers and devices. Understanding the mental models of security from a diverse sample of students helps model the educational resources towards a palliative approach and not as a curative approach. In this regard, the research primarily focusses on understanding the different types of security knowledge possessed by students from technical and non-technical majors by assessing their security behaviors and attitudes through an extensive quantitative analysis. The analysis also helps understand the interest

fostered towards an interdisciplinary education and career in cybersecurity. From the results and implications of the analysis, a multi-level, multi-discipline, multi-thread framework is proposed to understand the dimensions of interdisciplinary cybersecurity education and design of pluggable, drop in modules that could be cross pollinated into different courses across various majors along with pedagogical approaches for the same. Also, existing frameworks in cybersecurity education, as the National Cybersecurity Workforce Framework (NCWF) and the knowledge units of the Center for Academic Excellence in Cyber Defense (CAE-CD) are discussed in detail.

The following research questions guided the study with respect to understanding the different types of security behaviors and beliefs and measure the interest garnered towards an academic or career pathway in cybersecurity.

1. To what extent students from technical and non-technical majors perceive cybersecurity?
2. Is there a statistically significant mean difference in participants' perception of security behaviors?
3. Is there a statistically significant mean difference in participants' perception of security beliefs?
4. What are students' perceptions of pursuing an academic pathway in cybersecurity?
5. Is the National Cybersecurity Workforce Framework (NCWF) effective for a workforce comprised of interdisciplinary majors?

While the last research question is addressed in Chapter II, the rest of the research questions are discussed in detail in Chapter III.

Methodology

The purpose of this study is to examine existing knowledge of security, awareness of threats and vulnerabilities, and the interest fostered towards an interdisciplinary path in cybersecurity and workforce across students from technical and non-technical majors. Survey data were collected from a purposeful sample of respondents enrolled in different disciplines at the University of Houston - Clear Lake (UHCL). The survey was conducted across eight different majors (Criminology, Legal Studies, Management, Information Technology, Economics, Computer Science and Computer Information Systems) across the College of Science and Engineering (CSE) and the College of Human Sciences and Humanities (HSH). Each of the disciplines demonstrate a close relationship with cybersecurity and enough literature has been covered with respect to their significant contribution to cybersecurity in the consecutive chapter. The data were analyzed using frequencies, percentages, the Wilcoxon signed rank test, and paired sample t-tests. Chapter III presents an overview of the research problem, research purpose and questions, research design, population and sample, instrumentation, data collection and analysis, ethical considerations, and research design limitations.

Summary

This chapter identified the need to examine the importance of a holistic education in cybersecurity by the inclusion of other disciplines that contribute to the field and also indicate the importance of understanding existing knowledge in security practices across a wide range of students studying diverse subject matter. The research problem and significance of the study were reviewed, and research questions presented. In the next chapter, a review of literature expanding the breadth of theories.

CHAPTER II

REVIEW OF LITERATURE

The breathtaking pace of change in computing and technology and its widespread adoption in virtually every human endeavor has led to the dawn of a never seen era of Interdisciplinarity. Nearly all field of human activity require an understanding and application of that field within the context of one or more other fields. As Way [12] quotes it, “Interdisciplinarity is the combining of two or more disciplines into a single, cross-discipline learning experience”. This section will highlight the importance of an interdisciplinary education in cybersecurity followed by contributing theories from disciplines as criminology, legal studies and economics and detail on the theoretical framework which baselines the quantitative study.

Interdisciplinary Cybersecurity

A balanced cybersecurity workforce incorporates a basic understanding of technical skills along with non-technical abilities such as understanding, formulating policies, standards and practices, risk management, business standards, frameworks, practices, politics, governance and much more. In fact, the non-technical side of Cybersecurity has spread widely into avenues such as Criminology, Human psychology, Management, Law, Governance etc.

Cybersecurity education does not pertain to technical studies alone that surround network security, malware analysis, reverse engineering, application security and network security etc. In fact, the rising number of cyber terrorism and hacking incidents portray the need for Cybersecurity with a global perspective. A report from Frost, Sullivan and depicts that more than 1.5 million positions will be unfilled in the global cybersecurity workforce [4]. One of the important reasons for such a dearth in cybersecurity talent is businesses looking for people with traditional technology

credentials [5]. PayScale, a provider of on-demand compensation and software, states that 87% of recent graduates feel well prepared to hit the fast-paced Cyber industry. However, for more than 51% of those graduates, underemployment is the reality [5]. This is contributed by a massive gap in skills such as communication, ownership, leadership, teamwork, problem-solving, understanding cultural, social, legal, economic and political perspectives in the context of the problem at hand.

Society's dependence on information technology has created a "technological sovereignty" in the education curriculum and has outpaced non-technical skills [5].

To combat this, infusing political, ethical, social, cultural, religious and economic perspectives into cybersecurity education fosters a balance of technical and non-technical skills [13] and enhances preparedness to tackle a cyber-related threat or investigation in a better dimension. This calls for an "Interdisciplinary Cybersecurity".

Ghernaouti- Hélie [14] states that Cybersecurity education is "at the crossroads of technological, legal, sociological, economic and political fields, and is interdisciplinary by nature". This propels the need to leverage the effectiveness of the educational curriculum models [13]. Introducing a global perspective through interdisciplinary studies and employing "cross pollination" of disciplines closes the gap between "technically focused" cybersecurity and the non-technical, non-traditional backgrounds.

In response to this, a greater collaboration is initiated between education, research and industry fields. The collaboration has resulted in frameworks and guidelines that demonstrate an increased value for the Cybersecurity Workforce. Perhaps, the clearest indication of the evolving needs of cybersecurity education was posited by an NSF supported effort that brought together educators, government official and experts from the field to discuss the state of cybersecurity education. The report [15] from this gathering addressed the concerns and challenge of the state of cybersecurity education in

the United States. Of the six principles that were laid towards establishing cross-cutting principles for addressing cybersecurity education and training, three are noted for this work.

- Cybersecurity is an international issue. Strategic planning extends beyond the federal level, taking into consideration the needs, concerns and opportunities at the national and international levels
- Cybersecurity requires a multi-disciplinary approach. All educational efforts and academic instruction should be made to educate and partner with disciplines not always thought of as related to cyber security
- To address the continuing security breaches, curative not palliative approaches are needed

The National Initiative for Cybersecurity Education (NICE) [16] establishes a taxonomy and common lexicon for cybersecurity work across public, private and academic sectors. However, Cai [17] describes that the framework provides a burgeoning body of knowledge that consists of almost entirely of computing topics, though there are some policy and law areas addressed. The problem space presented while assessing the workplace requirements for a cybersecurity professional is daunting. With the advent of newer threats and technologies, it is characteristic of the cyber environment to evolve, leading to newer definitions of specific job roles and advanced skills. These are by large presumed to be the core skills as engineering, mathematics and computer science. Conversely, Robert [13] posits that the demand for cybersecurity expertise cannot be described with a set of uniform skills. Rather, it encompasses an ecosystem of interdisciplinary knowledge, skills and abilities.

Addressing cyber threats requires a reassessment of the way cybersecurity is approached as an academic discipline and requires a significant research in understanding

the frameworks and guidelines that form the basis of cybersecurity workforce and talent development. In this regard, traditional cybersecurity education has leveraged the technical approach of solving challenges in the cyber environment while overlooking factors influenced by humans and the decisions they make. According to Lomax Cook [18], "No solution for securing cyberspace is complete without the integration of research that examines how people behave in the complicated systems that constitute the Internet – from the users of Internet to the attackers who endanger networks"

Technology and behavior are intrinsically linked to each other. However, given that, technical measures alone cannot prevent any crime, it is critical that any cybercrime should be built around a global agenda. The Global Cybersecurity Agenda [19] is built on five work areas namely Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building and International Cooperation.

In support of this, Hoffman [20] points out that, "Examining the fundamentals of security and privacy from a multidisciplinary, sociotechnical perspective can lead to fundamentally new ways to design, build and operate cyber systems, protect existing infrastructure, and motivate and educate individuals about cybersecurity".

In this regard, encompassing social sciences into cybersecurity education by infusing economic, political, legal and social dimensions draws on globalization and sufficiently equips individuals with the full spectrum of global and local cybersecurity challenges. Building the cyber resilience of a nation resonates from such a sound education in cybersecurity rather than a traditional, techno-sovereign approach[20]. Albeit, there is a significant contention in defining "interdisciplinary cybersecurity" because of its multivariate nature, paucity of literature that situates cybersecurity in different contexts and differences in the nature of academic fields studying the phenomenon around it [21].

The following section discusses in brief some of the contributing theories from the field of social sciences as Criminology, Economics and Legal Studies to the field of cybersecurity.

Cybersecurity and Criminology

Thousands of Cyber-attacks are being launched against internet users across the world. These so-called cyber criminals, hacktivists or cyber adversaries have presented a full spectrum of the threats not only to the US government but also to private organizations and critical infrastructure sectors. In fact, cyber-attacks have become arduously frequent and highly expensive to individual users, businesses, organizations, economies and other infrastructural entities. In 2016, Symantec [22] discovered more than 430 million unique pieces of new malware, 91 percent of these attacks were originated by employing phishing techniques, while numerous high-profile breaches originated from a single phishing attack.

It is globally realized that humans are the weakest link in cybersecurity. Most of the system security organizations work on the premise that human factor is the weakest link in cybersecurity. In fact, humans have moved ahead of machines as the top target for cybercriminals. There were 3.8 billion internet users in 2017, up from 2 billion in 2015 [23]. According to Cybersecurity Ventures [24], there will be 6 billion internet users by 2022 and more than 7.5 billion internet users by 2030. This vast increase in the number of internet user's raises concern in terms of vulnerabilities and emerging threats by ideologically motivated offenders to cause harm and further their political and social agendas.

However, a lack of empirical research on cyber-attackers limits our knowledge of the factors that affect their behavior. As Sandeep [25] denotes, the "interaction between computers and humans is not a simple mechanism but is instead a complex interplay of

social, psychological, technical and environmental factors operating in a continuum of organizational internality and externality".

Cyber threats and attacks are becoming more sophisticated with the blend of the "once upon at a time" distinct types of attack into comprehensive, destructible and damaging forms. Further, it has been aggravated by a tremendous increase in the variety and volume of attacks along with the birth of strategic, financially and criminally motivated crime actors. As Choo [21] quotes, "Cybercrime has evolved into an entire economy rife with professionalization and filled with parallels to legitimate industries. The emergence of a complex and multi-layered cybercrime economy has also begun to suggest a fundamental shift in the very nature of crime itself".

The United States, United Kingdom and Australia, which have been identified as culturally and economically open nations, have tremendously thrived on the wealth that information and communication technologies have offered over the decades [26]. Though information and communication technologies have proliferated as a wide platform for businesses and private sectors to operate, it also poses an equal amount of opportunities for those with criminal intentions and poses a great risk to individuals, communities, organization and the nation.

Within the field of criminology, numerous theories exist to elucidate why crime occurs, why certain people engage in deviant behavior while others refrain from it and ways to help predict future crime behaviors and practices [27]. This below section presents some of the theories in the light of cybercrime as follows:

Akers' Social Learning Theory

Precisely used to explain a diverse body of criminal behaviors, this theory encompasses four fundamental avenues namely, differential association, definitions, differential reinforcement, and imitation. The theory reinforces the idea that individuals

develop motivation and skills to commit crime by associating themselves with those who are involved in crime (deviant peers). With respect to cybercrime, research indicates that this theory can help elaborate the issues of software piracy. Burruss et al [28], found that individuals who associate with software piracy peers learn and consequently follow the deviant conduct. Not only does the social learning theory explain for software piracy but also posits to other cybercrimes because of its ability to explain the rationalizations, skills and behavior that the criminals are reinforced with through their association with, and observation of others [28]. Thus, the main idea behind this theory is understanding the motives of delinquent peers and their functions in the context of various cyber-crimes.

Routine Activity Theory

Developed by Cohen and Felson, this theory posits that the behavior of most victims is repetitive and predictable and that the likelihood of victimization is dependent on three important elements - motivated offenders, suitable targets and the absence of capable guardians [29]. While the motivated offender is someone willing to commit a crime if an opportunity presents itself, the target is the one that the motivated offender values (e.g., credit card information) and the capable guardian is a person or an entity that obstructs the offender's ability to acquire the target.

Situational Crime Prevention Theory

The situational crime prevention theory is a strategy that addresses specific crimes by manipulating the environment in a way that increases the risk to the offender, while reducing the potential reward for committing the crime [29]. Unlike other criminology theories, this theory does not postulate on why the offender did the crime. Rather, it tends to focus more on the reducing the crime opportunities. Hardening the targets of crime by encrypting sensitive information, implementing access control mechanisms, securing off-site data and performing background checks on employees and restricting unauthorized

installations on computers are some of the examples of this theory. Situational Crime Prevention Theory is used to reduce cyber stalking and other online victimization crimes.

Ideally, criminal behavior cannot be explained by one theory but requires a conjunction of various theories to recompense for what each individual theory failed to explain. Although these crimes, by large help to explain the crimes in the real world, they are applicable to cybercrimes. However, while criminological theory in the physical realm enjoys a rich history with diverse contributions and clear paradigm development and shifts, explanatory research and studies with respect to digital and electronic crime and information security success remains relatively undeveloped.

Cybersecurity and Economics

The economics of cybersecurity or "cyber economics" as the newly evolved name, is one of the thriving interdisciplinary facets of growing cyber security issues in the United States. Conservatively, a total of 15 billion US dollars are spent every year by organizations in the United States to secure their communication and information systems [11]. Though the investments are higher, the economic impacts of cyber-attacks and breaches have set to surpass the cost of investment by large. In 2009, the cost of cyber-attacks was estimated by the then President of United States, Barack Obama, to be 1 trillion dollars per year or translated as 6 percent of the Gross Domestic Product of the United States [30]. However, the estimates have appeared to vary widely. In 2010, internet crime cost totaled to 560 million USD, out of which Phishing, one of the top social engineering attacks, accounted to 120 million dollar per quarter [11].

In order to effectively learn and understand the economically complex cyber-attacks, it is important to understand the interconnections and complexities in our economy that cyber attackers could devise combinations of attacks to cause greater destruction. In lieu of this, the following economical concepts are discussed as below,

Economic Redundancies

The first feature of our economy that's crucial to cyberattack consequences is the way systems can substitute for other systems. These redundancies are usually the main factor limiting the consequences of a cyberattack. Interfering with one business system usually does little damage to the economy, because other systems simply take over that system's function. To deal with redundancies, cyber attackers employ combinations of cyberattacks designed to produce Intensifier Effects. These are simultaneous attacks on different systems or businesses that could otherwise serve as substitutes for each other. When several systems could serve as substitutes, a successful cyberattack on the first of these systems will generally have extremely limited consequences. Further successful attacks on further systems that can substitute will produce only very small increases in destructiveness.

This continues until the capacity of the remaining systems is no longer enough to allow them to take over for the systems that have been attacked. The consequences of the cyberattacks will then go abruptly from being small to being huge. This has important implications for the planning of almost any cyberattacks. In this regard, Economic redundancies, and the potential for intensifier Effects to overcome them, will be a major consideration in choosing targets [30].

Economic Interdependencies

The second economic feature that's crucial to cyber-attack consequences is the way production is organized into value chains. For instance, one company might turn ore into metal. Another company will turn the metal into mechanical parts. Another company will incorporate the mechanical parts into airplanes. This interdependency is the basis for any kind of economic cooperation. But on the other hand, these interdependencies provide enormous opportunities for cyber attackers to find ways to exploit. The reason is

that mechanisms that companies employ to coordinate their value chains can also be used to make compensating adjustments if part of the value chain is disrupted [30]. The below flowchart diagrams the economic activities. The systems that make up the value chain are represented as channels that flow into each other. To exploit such value-chain attacks, cyber attackers need to employ a combination of cyber-attack to produce a Cascade Effect. By this mechanism, a successful attack on one set of businesses will affect numerous other businesses up and down the value chain [30].

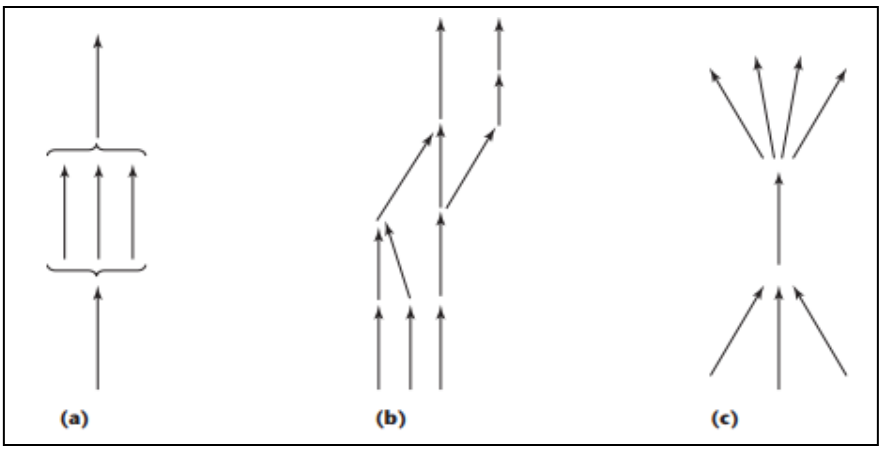

Figure 2.1

Economic complexities of cyber-attacks

(a) Economic redundancy (b) Economic interdependency

(c) Economic Monopoly

Economic near Monopolies

The third economic feature that's crucial to cyber-attack consequences are the facilitating capabilities that are leveraged to produce widespread benefits. Business and enterprises that are monopolies in their area of service are prone to a higher range of cyber-attacks. Because near monopolies produce large inputs through limited means, they

give attackers opportunities to produce limited effects with limited means. In Fig 2.1 (c), each monopoly is represented as a point at which numerous channels radiate out to connect with many other channels. To take advantage of such monopolies, cyber attackers employ combinations of attacks specifically designed to produce Multiplier effects. The sort of companies that could be attacked to produce Multiplier Effects would make especially tempting targets, because they are small sized. And their budgets for cybersecurity are small.

From the discussion of the above economic concepts, the structural analysis of an economy is a powerful tool for cyber attackers and it eventually becomes a more essential tool for cyber defenders [30]. An effective cyber defense program or training cannot be satisfied with identifying a few individual cyber-attack scenarios. Taking proper accountability of economics in security thinking requires an adjustment in outlook. Economics is therefore a powerful analytical tool to defend against cyber activities.

Cybersecurity and Legal Studies

The need for a comprehensive approach to cyber security deriving from the architecture of the internet and emerging cyber threats and incidents requires a systematic development, interpretation and application of legal areas and instruments. With politically motivated cyber incidents on the rise, cyber security has grown into an immediate area of concern for national governments and international organizations. In this regard, an approach combining considerations of threat, deterrence and response from different areas of authority and responsibility are significant to cater to the defensive actions against the attacks. This has led to the discussion of a coordinated legal approach. Defenses and responses to cyber-attacks will depend to a great extent on systems and security standards designed in peace time with primarily commercial interests in mind. From a legal perspective, this means that the national legal approaches

to data and consumer protection and due diligence will determine law enforcement and national defense capabilities [31]. Understanding these legal policies in the light of cybersecurity adds a holistic perspective to defending and responding to such attacks. Some of the categories of legal studies in the light of cybersecurity have been briefed in the following section.

Computer Crime Laws

These laws deal with a broad range of criminal offenses committed using a computer or similar electronic device as identify thefts, online stalking, bullying, sex crimes etc. This law typically includes procedural and legal ramifications for prohibition, investigation and prosecution of criminal activity [31]. Its application extends to a wide range of fields as computer hacking, viruses, internet gambling, encryption, online undercover operations, internet surveillance etc.

Information Privacy Laws

Information privacy laws includes the development of constitutional, tort, contract, property, and statutory law to address emerging threats to privacy. Laws under the information privacy law deal with privacy in the media, law enforcement, and online transactions, medical and genetic privacy and for personal privacy [31].

Homeland Security Law and Policy

These policies concern the Department of Homeland Security and the adoption of the Homeland Security Act of 2002 [31]. The laws under the Homeland Security define legal responses and actions for protection of critical infrastructure, information sharing, liability for terrorist attacks, risk insurance, threats to electronic infrastructure and combating the finance of terrorism.

Counterterrorism laws

These set of laws provide an analysis of legal mechanisms in the fields of criminal, civil, military, immigration, and administrative law used by the U.S. government to combat domestic and international terrorism. The laws also in detail charts out the effectiveness of government actions and alternatives for achieving public safety goals and the effect of such actions on U.S. citizens and citizens of other countries.

Intelligence Laws

These set of laws identify and analyze current legal questions that face intelligent practitioners. They also include constitutional, statutory and executive authorities that govern the intelligence community.

A comprehensive defense to cyber-attacks includes a strong contribution from a legal perspective. Instead of addressing a specific threat, cyber threats should be regarded as a spectrum where different stages and effects of cyber incidents are aligned. Depending on the motivation, effects and actors, a cyber-incident will be categorized as a breach of law short of cyber-crime, crime, national security relevant incident or cyber warfare [31]. An interdisciplinary, holistic education in Cybersecurity is borne out of understanding and applying these laws in context to the security issues learnt.

Multi-discipline, Multi-level, Multi-thread Model for Interdisciplinary Cybersecurity

Based on the discussion in the above section, the need for a comprehensive approach to cybersecurity is clear because the need for such an approach will cover the information society and the challenges tackled leading to comprehensive, palliative understanding rather than a stove piped approach [32].

In this regard, the newly developed model provides an opportunity to explore technical and non-technical content in a four-year program by integrating disciplinary

and interdisciplinary electives at different levels. The model called as “Multi-discipline, Multi-level, multi-thread model” allows potential candidates to specialize in subjects of Cybersecurity according to their level of interest. Figure 2.2 shows a diagrammatic representation of the proposed model. The model would accommodate electives from other disciplines that are relevant to the Cyber domain. The model works on a top-down approach, allowing different pedagogical methods to be employed in each level of advancement. A diagrammatic representation of the framework is shown in Figure 2.2. Elaborating the model, the following are taken into consideration,

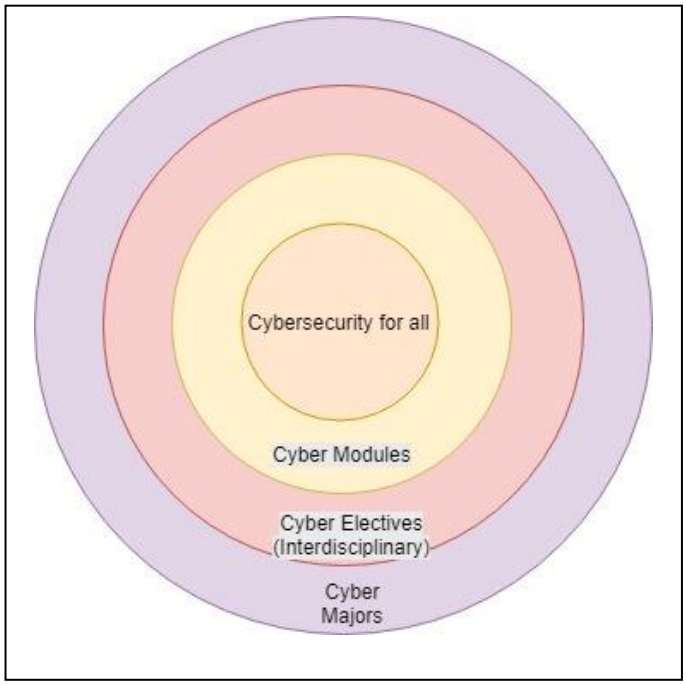

Figure 2.2

Multi-level, Multi-discipline and Multi-thread Model

Cybersecurity for All

The model is designed as a prototype to foster an inclusive, interdisciplinary approach in Cybersecurity Education. Although many four-year institutions have stringent requirements for general education, the idea of putting cyber into general education courses applies to any college or university. This approach that is named as "Cybersecurity for all" includes an introductory envisions a taxonomy for cyber education across the entire spectrum of curriculum, including non-technical, non-computing fields of study.

Cyber Modules

Cyber Modules will be the foundational element towards the "Cybersecurity for all" framework. The modules can be incorporated into courses to infuse knowledge about security measures and protocols. The modules are reusable, interdisciplinary and can be aggregated as a unit (or thread) to be pluggable into different disciplines, threads and electives. This will enable significant addition of cybersecurity into the core courses as well as in general education classes such as International Relations, Legal Studies, Business Administration, Management, Psychology etc.

Cyber Electives (Interdisciplinary)

Cyber electives include a myriad of courses that could be adopted into the curriculum to infuse a holistic education in Cybersecurity. In addition to the electives offered in Computer Science or Information Technology, the cyber electives contain interdisciplinary electives from across the spectrum of courses. These courses will include electives from Legal Studies, Business and Psychology.

Cyber Majors

Cyber Majors includes majors such as Computer Science, Information Technology, Software Engineering and Computer Information Systems that allow

students to choose chosen sub-topics within their desired major. The majors must present core cyber subjects across their curriculum. The major must be culminated by a Capstone Project in the Cyber Domain that gives students, an exposure to implement the knowledge gained through the coursework [43]. Other than the above elements, the model also greatly motivates enrichment opportunities by fostering student research groups, clubs and chapters of renowned cyber associations that is inclusive of all majors.

Explorative Analysis of Current Guidelines in Cybersecurity Education

This section discusses two of the important initiatives undertaken by the Department of Homeland Security with respect to Cybersecurity Education and Training. First, The National Initiative for Cybersecurity Education (NICE), aka the National Cybersecurity Workforce Framework (NCWF) [16], is a national focused resource that categorizes and describes cybersecurity work. In response to the evolving vulnerabilities in the cyber infrastructure, NICE along with the Department of Homeland Security formulated the NCWF framework which serves as a reference standard for workforce development, curricular development and much more. Also, NCWF serves as a foundation in establishing common taxonomy and lexicon for several key groups as cybersecurity staff, workers and students considering a career in the field. Second, is the Centers of Academic Excellence in Cyber Defense (CAE-CD), jointly sponsored by the National Security Agency (NSA) and the Department of Homeland Security (DHS) originated as an immediate response to the demands of the growing cybersecurity talent addressed in the Federal Cybersecurity Workforce Strategy.

The National Initiative for Cybersecurity Education (NICE) Framework

The NICE framework consists of several components – Category, Specialty areas, Work roles, Knowledge, Skills, Abilities and Tasks. Each category is composed of Specialty Areas, each of which is composed of one or more work roles. Work role

includes Skills, Knowledge, Abilities and Tasks [16]. While categories portray as the overarching, higher-level groupings in the framework, work roles are the most detailed grouping of cybersecurity related work. There are seven categories in the framework: Securely Provision, Operate and Maintain, Protect and Defend, Investigate, Collect and Operate, Analyze, and Oversight and Development. Each of the categories, the specialty areas and the work roles encompassed within them are detailed as follows:

Securely Provision

This category encapsulates the specialty areas responsible for overseeing, conceptualizing, designing, building and accrediting information systems using concrete security policies and processes [16]. The Specialty areas included are Risk Management, Software Development, Systems Architecture, Technology Research and Development, Systems Requirement Planning, Test and Evaluation and Systems Development. Work roles range from Information Assurance (IA) Compliance Analysts, Software Developers, and Programmers. It has a robust structure of work roles and technically sound KSAT descriptions.

Operate and Maintain

This category includes specialty areas responsible for providing support, administration and maintenance that is necessary to ensure effective and efficient information technology (IT) system performance and security. The specialty areas included are Data Administration, Knowledge Management, Customer Service and Technical Support, Network Services, Systems Administration and Systems Analysis [16]. Sample Job titles under this category range from Data Architect, Network engineer and server administrators.

Oversee and Govern

This category comprises of areas such as Legal Advice and Advocacy, Training Education and Awareness, Cybersecurity Management, Strategic Planning and Policy, Executive Cyber Leadership, Program/Project Management Acquisition. Oversee and Govern encompasses non-technical cybersecurity workforce who have job titles as Cyber Legal Advisor, Cyber Instructional Curriculum Developer etc. Work roles are not overtly technical in nature but require an understanding of behavioral and technical aspects of cybersecurity [16].

Protect and Defend

Comprising of specialty areas as Cyber Defense Analysis, Cyber Defense Infrastructure Support, Incident Response and Vulnerability Assessment and Management, this category aims at identifying, analyzing and mitigating threats to internal IT systems and networks. Job positions under this umbrella are Cybersecurity Intelligence Analyst, Incident Analyst, Ethical Hacker, Penetration Tester etc.

Analyze

Analyze covers specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence. Threat Analysis, Exploitation Analysis, All-Source Analysis, Targets, Language Analysis are the specialty areas under its cover [16]. The NICE work roles define for this category are Threat/Warning Analyst, Exploitation Analyst, All-Source Analyst etc.

Collect and Operate

This category is defined by Specialty Areas responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence. Collections Operations, Cyber Operational Planning and Cyber

Operations are the areas that extend into work roles such as All-Source Collection Manager, All Source-Collection Requirements Manager.

Investigate

This category includes specialty Areas responsible for investigating cyber events or crimes related to information technology (IT) systems, networks, and digital evidence [16]. Cyber Investigation and Digital Forensics are the specialty areas under its cover.

Analysis of Non-Technical Work Roles in NCWF

NCWF is established as a reference structure that provides a common, consistent lexicon to categorize and describe cybersecurity work [16]. The framework serves as the underlying protocol to identify, recruit, develop and maintain cybersecurity talent. It is used as a standard by educators to develop curriculum, certificate or degree programs, training programs, courses, seminars, exercises or challenges.

Discussion

People, Process and Technology form the inevitable triad of an organization's cybersecurity. Many organizations focus on technology to solve their security problems, hiring more security practitioners. Increasing the workforce does not solve problems [33]. The Commission of Enhancing National Cybersecurity recommends acknowledging the need for socially-focused security measures to improve the overall effectiveness of the NCWF framework. Though the framework demonstrates depth and breadth of scope for the technical roles, the non-technical roles are outpaced. In this regard, some of the observed discrepancies are documented as below:

Less Competencies for Non-Technical Workforce

The NCWF framework has a higher weightage for technical aptitude than the non-technical ones. This is explained by competencies. "Competency" is a new term that is introduced into NCWF and is defined as "skills or capabilities that are critical for

successful job performance across various Cyber roles and charts out the behaviors that elaborate the progressive levels of proficiency associated with those competencies" [16].

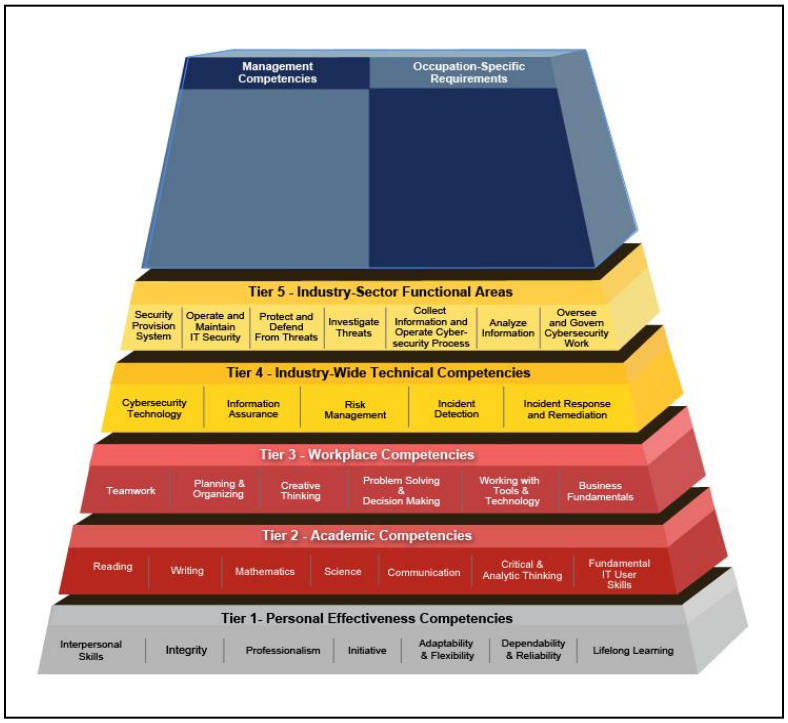

Figure 2.3

Cybersecurity Competency Model

The NCWF framework has a higher weightage for technical aptitude than the non-technical ones. This is explained by competencies. "Competency" is a new term that is introduced into NCWF and is defined as "skills or capabilities that are critical for successful job performance across various Cyber roles and charts out the behaviors that elaborate the progressive levels of proficiency associated with those competencies". The Cybersecurity competency model [34] complements the NICE framework by including competencies required by the average worker and cybersecurity professionals. Fig 2.3 shows the diagrammatic representation of the Competencies required at different levels. While the industry wide technical competencies are plugged into the NICE framework

extensively, the workplace and academic competencies are comparatively fewer. This creates a skills gap by generating a highly competent technical workforce and less incompetent non-technical workforce. Figure 2.4 shows the competencies for the specialty area, Legal Advice and Advocacy. Legal advisors provide sound advice and recommendations to leadership and staff on a variety of topics, advocate legal and policy changes and makes a case on behalf of client through extensive written and oral work.

Majorie and Sheldon [51] state that the core competencies required for successful advocacy include analysis and reasoning, creativity, problem solving, practical judgement, excellent communication skills which includes writing, speaking and listening, research analysis, time and stress management. Comparing the above critical factors with that of the NICE competencies (given in Figure 2.3 [33]), the latter appears to be uncritical. With evolving legal environments, it is important to embrace a holistic culture.

Item ID	KSA	Statement	Competency
27	KSA	Knowledge of cryptography and cryptographic key management concepts.	Cryptography
88	KSA	Knowledge of new and emerging Information Technology (IT) and cyber security technologies.	Technology Awareness
105	KSA	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code)	Vulnerabilities Assessment
282	KSA	Knowledge of emerging computer-based technology that has potential for exploitation by adversaries.	Technology Awareness
297	KSA	Knowledge of key industry indicators that are useful for identifying technology trends.	Technology Awareness
300	KSA	Knowledge of intelligence reporting principles, policies, procedures, and vehicles, including report formats, reportable criteria (requirements and priorities), dissemination practices, and legal authorities and restrictions.	Organizational Awareness
338	KSA	Knowledge of the principal methods, procedures, and techniques of gathering information and producing, reporting, and sharing intelligence.	Reasoning
339	KSA	Knowledge of the structure and intent of business or military operation plans, concept operation plans, orders, policies, and standing rules of engagement.	Organizational Awareness
377	KSA	Skill in tracking and analyzing technical and legal trends that will impact cyber activities.	Legal, Government, and Jurisprudence
954	KSA	Knowledge of import/export control regulations and responsible agencies for the purposes of reducing supply chain risk.	Contracting/Procurement
981	KSA	Knowledge of International Traffic in Arms Regulation (ITARs) and relevance to cybersecurity.	Criminal Law
1036	KSA	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed.	Criminal Law
1070	KSA	Ability to determine impact of technology trend data on laws, regulations, and/or policies.	Legal, Government, and Jurisprudence

Figure 2.4

NICE Competencies for Legal Advice and Advocacy

Job Descriptions and KSATs

While mobile exploitation analyst positions demand an extensive knowledge of networking and communication devices, data exploitation analysts are required to possess knowledge of data mining, trend analysis and financial structures. The framework states a generalized description for these "newer" work roles and the associated KSATs do not cover in breadth, the requisite knowledge needed to acquire specific roles. With the growing demand for technical and managerial roles, relative newcomer positions such as "exploitation analysts", "multi-discipline language analysts" have less vision and scope due to uncritical job descriptions and lessened awareness of requisite knowledge.

As a result, a sector of candidates aspiring to get into those work roles suffer due to a fragmented focus in education and skills development [33].

NICE Work Role Name	Recruiting Site Statistics	
	Number of Positions (as on 4/12/2018)	Diversity of Job Positions
Threat/Warning Analyst	424	Cyber Threat Analyst
Exploitation Analyst (EA)	32	Mobile Exploitation Analyst Financial Exploitation Analyst Digital Network Exploitation Analyst Audio/Video and Biometric Exploitation Analyst Cyber Operations Exploitation Analyst
All-Source Analyst (ASA)	252	Cyber Ops Military Planner
Mission Assessment Specialist (MAS)	0	
Target Developer (TD)	0	
Target Network Analyst	0	
Multi-Discipline Language Analyst	2	Multi-Discipline Language Analyst
All-Source Collection Manager		All-Source Requirements Collection Manager All-Source Intelligence Collection Manager
All-Source Collections Requirements Manager	4	
Cyber Intel Planner	1	
Cyber Ops Planner	1	Cyber Ops Military Planner
Partner Integration Planner	0	
Cyber Operator	9	
Cyber Crime Investigator	1	
Law Enforcement/Counterintelligence Forensics Analyst	5	Cyber Intelligence Analyst
Cyber Defense Forensics Analyst	1	

Figure 2.5

Statistics of Newer Work Roles

Exploring the NICCS initiative

The National Initiative for Cybersecurity Careers and Studies (NICCS)[36] is a preeminent online resource for Cybersecurity training. The NICCS was formed with a vision to help citizens find the required education and training needed to enhance skills and bridge the gap in the cybersecurity workforce. NICCS has an extensive repository of courses delivered by federal agencies, Centers of Academic Excellence, universities and private training providers. Each of the courses offered is mapped to the NICE framework categories.

Observing the learning objectives of one of the NICCS courses offered in Security Risk Management, it is seen that the learning objectives portray a mixture of organizational, technical and risk management knowledge. According to a Risk Management competency model of a top firm, some of the core competencies required for this position includes Business Insight, Communication, Collaboration and Consultation.

However, the courses delivered in the NICCS catalog are tied to a category level and their learning objectives are not refined to impart the expected non-technical competencies along with the program. This is contributed to the high-level notional connections between the NICCS courses and the NICE categories [37]. Previous research show that the mapping of the courses to the NICE categories is fluid since they were put through the best fit filter. Therefore, a much-refined re-mapping of the NICCS courses to the NICE categories is required (must incorporate industry wide competencies for work roles affiliated to that category). Secondly, the concentration of courses affiliated to the non-technical specialty areas are fewer in number. For technical Specialty Areas such as Software Development, Systems Administration, the number of courses and certifications are more in comparison to non-technical areas such as Threat Analysis, Exploitation

Analysis, All-Source Analysis etc. Overall, very few courses are mapped to the following categories – Analyze, Collect and Operate, and Investigate.

Reduced Emphasis on Human Elements

Attacks from human behavior or human attacks are inseparable from Cybersecurity. Training to prevent, respond and defend systems from those attacks depend heavily on technical aspects and de-prioritizes human factors [37]. Emphasizing technical aspects within Cyber Education prepares a workforce to respond to only a certain part of the problem. In connection to the NICE framework, this can be understood by the breadth of KSATs covered for each work role. It is logically not feasible to foster programs in cybersecurity that would extensively cover all the essential KSATs that are necessary to a field and to each specialization. Rather, it makes more sense to place emphasis on "human centric" skills such as problem-solving, innovation and self-directed inquiry, which benefits the non-technical workforce.

Lack of Interdisciplinarity Creates a Siloed Workforce

Historically, security was originated as a technical subfield of Computer Science. However, evolving pervasive computing technology has leveraged security integrating management and policies within its umbrella. In 2015, the European CAMINO Project [38] created the THOR acronym approach of "(T)echnical", "(H)uman", "(O)rganizational" and "(R)egulatory". The project ascertains that cyber security could be comprehensively perceived as a combination of the above four dimensions. In lieu of this, some of the areas that require a higher leverage in the framework are Usable Security, Cybersecurity Research, Criminology, Information Science and Behavioral Science. This is evident from the fact that cybersecurity as a multidisciplinary field is often misunderstood of requiring input only from Computer Science and not from other fields as Economics, Mathematics, Political Science, Social Science etc. As a result, the

workforce that result from such an education become siloed and stove-piped, keeping them within a shell of a specific career path (or a discipline) [39]. On a much higher level, previous research indicates that "Cybersecurity workforce members tend to be less bound to organizationally constructed career paths. Rather, they have a tendency towards a boundaryless career precisely motivated by personal achievement and external career dimensions, such as organizational position, mobility, flexibility and organizational goals". The NICE framework should consider such non-traditional conceptualizations of career management tool.

Explorative Analysis of Center of Academic Excellence in Cyber Defense (CAE-CD)

The CAE-CD Knowledge Unit Design and Analysis

Knowledge Units are "tightly targeted areas composed of a set of topics to be covered and expected student outcomes and masteries". The current version of the Centers of Academic Excellence in Cyber Defense (CAE–CD) designation requirements was published in June 2013. The 70 Knowledge Units (KUs) required in the current version are based on program type – precisely, a 2-year program and a 4+ year program.

A revised set of Knowledge Units for CAE-CD designation has been published by the governing body of CAE-CD; the new requirements are to be effective for the 2019 application cycle (1 Oct 2018 – 1 May 2019).

Structure of a Knowledge Unit

To allow for differentiation amongst the applying schools, the CAE-CD introduced the framework of Knowledge Units. This allows the applying institutions to immerse its curriculum in a specific track or path. Each knowledge unit in the CAE-CD is composed of a minimum list of topics to be covered and one or more outcomes or learning objectives. Some of the key terminologies that are used to constitute a KU are as follows,

Description

The description of the knowledge unit provides a high-level overview of what the Knowledge Unit contains. It basically communicates what the knowledge unit intends to impart to the users; whether the level of knowledge is basic, intermediate or advanced.

Outcome

The outcomes are chained to the knowledge unit. It precisely sums up the takeaways from the knowledge unit. The outcomes are more granular and connected to the topics within the knowledge unit.

Topics

Topics are the list of elements that together constitute the knowledge unit. Topics are hierarchically presented; Basic concepts leading to advanced topics within a knowledge unit. Each of the knowledge unit is mapped to the National Initiative for Cybersecurity Education Framework at a category level.

Specializations

This new terminology has been added to the revised version of CAE-CD 2019. Every KU is tied to a specialization.

Related Knowledge Units

These knowledge units are declared relevant to the primary knowledge unit under which it is specified. The following sections explain in detail, the CAE-CD KU design of the current (2014 version) and the revised version (2019 version).

The Current KU Structure

CAE-CD's current version of the Knowledge Unit was published in 2014 and was required of all applying institutions to incorporate them. The duration of the application cycle under this criterion is from 2014 through spring 2018. The current version of the CAE-CD KUs has separate CORE knowledge units for 2-year programs and 4-year

programs. The 2-year programs consist of CORE KUs that include Basic Data Analysis, Cyber Defense, Cyber Threats, Introduction to Cryptography, IT System Components, and Networking Concepts etc. An institution applying for a designation must map its curriculum to all the 2-year and 4-year KUs. In addition, 5 of the optional KUs must also be integrated into the institution's curriculum. The choice of optional KUs is at the discretion of the institution. A full list of the Optional KUs is presented in Table 2.1.

The Knowledge Units furnished by the CAE-CD are subject to revisions and are strengthened accordingly to keep pace with the evolving nature of the Cyber Defense industry and market. In accordance to this revision, a new framework for KUs has been proposed by the CAE-CD with significant changes in the Knowledge Units and its applicability to the applying institutions. The following section presents a glimpse of the revised CAE-CD KUs and the changes introduced therewith.

Table 2.1

List of Optional Knowledge Units in CAE-CD

Optional KUs	Optional KUs
Advanced Algorithms	Independent/Directed Study/Research
Advanced Cryptography	Introduction to Theory of Computation
Advanced Network Technology and Protocols	Intrusion Detection/Prevention Systems
Algorithms	Life-Cycle Security
Analog Telecommunications	LINUX System Administration
Basic Cyber Operations	Low Level Programming
Cloud Computing	Media Forensics
Cyber Crime	Mobile Technologies
Cybersecurity Ethics	Network Forensics
Data Administration	Network Security Administration
Database Management Systems	Network Technology and Protocols
Databases	Operating Systems Hardening
Data Structures	Operating Systems Theory
Device Forensics	Penetration Testing
Digital Communications	Privacy
Digital Forensics	QA/Functional Testing
Embedded Systems	Radio Frequency Principles
Forensic Accounting	Secure Programming Practices
Formal Methods	Software Assurance
Fraud Prevention and Management	Software Reverse Engineering
Hardware Reverse Engineering	Software Security Analysis
Hardware/Firmware Security	Supply Chain Security
Host Forensics	Systems Certification and Accreditation
IA Architectures	Systems Programming
IA Compliance	Systems Security Engineering
IA Standards	Virtualization Technologies
Wireless Sensor Networks	Vulnerability Analysis
	Windows System Administration

The Revised KU Structure

Figure 2.5[41] is the diagrammatic representation of the KU usage in the revised CAE-CD 2019 requirements. The schema is based on the following factors - Program Type, Everyone, Objective Driven and Program Choice.

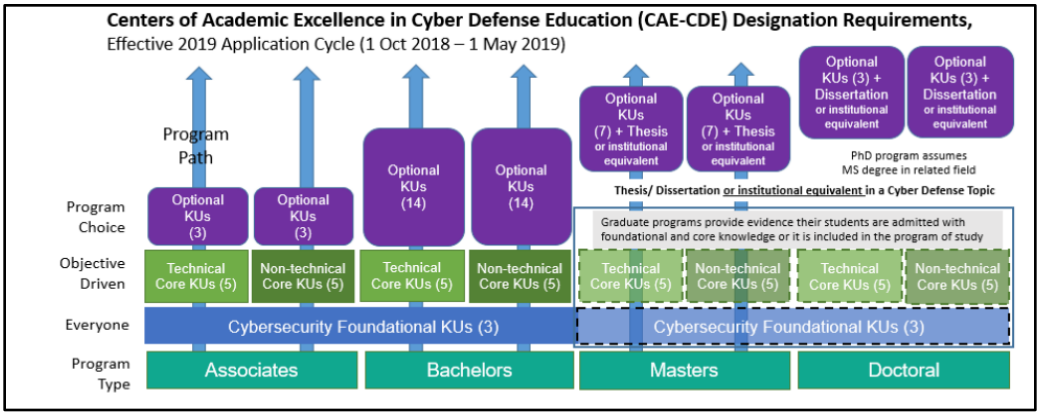

Figure 2.6

Structure of CAE-CD KU 2019 Revised Version

Unlike the current version of CAE-CD KU, the revised version is based on program type. The program types are Associates, Bachelors, Masters and Doctoral. Three Knowledge units have been deemed foundational and is required of all programs that are seeking a designation. Cybersecurity Foundations, Cybersecurity Principles, IT System Components are the foundational Knowledge Units established by CAE-CD. Further, each program type, in addition to the mandatory foundational KUs, has a set of five technical core KUs, five non-technical core KUs, and optional KUs.

Technical Core KUs

The technical core Knowledge Units are Basic Scripting and Programming, Basic Networking, Network Defense, Basic Cryptography and Operating System Concepts

Non-technical Core KUs

The non- technical core Knowledge Units are Cyber Threats, Policy, Legal ethics and Compliance, Security Program Management, Security Program Management and Cybersecurity Planning and Management [41].

For a given program to be certified as a CAE-CD, in addition to meeting the cybersecurity foundational KUs requirements, the program must choose to focus on either the technical or the non-technical core, by requiring KUs from either the technical core or the non-technical core in the program. Choosing KUs from the technical core prepares the students for technical jobs; choosing a program of study that has non-technical core KUs allows the students to aim for non-technical jobs. In addition, optional KUs (see Table 2.1) can be adopted by any program to supplement their program of study. Additionally, opposing core KUs could be used as optional KUs. For example, a program that chooses to require the technical core may use KUs in the non-technical core as optional KUs.

Analyzing Strengths, Weaknesses, Opportunities and Threats

The CAE-CD KUs have been designed by a panel of expert researchers, curriculum designers and representatives from the CAE-CD. The following section postulates the strengths, weaknesses, opportunities and threats existent in the revised version.

Bridging the Disconnects

A fundamental misunderstanding of the nature of the cybersecurity workforce challenge has led to a proliferation of educational programs focusing on traditional Information Assurance and Cybersecurity skills. This has sprung up because many of the cybersecurity educational programs offered by higher educational schools focus more on

technical skills and knowledge. Though these skills are real, they overshadow non-technical skills required by employers [42].

Cybersecurity is a field characterized by multi-layered challenges requiring a cross-discipline focus rather than a discipline-centric approach. This calls for a Comprehensive education in Cybersecurity. In this regard, the revised version of the CAE-CD KUs accommodates a comprehensive outlook on cybersecurity education by allowing institutions to choose KUs from one of the two core sections – Either the Technical Core KUs or the non-technical core KUs, in addition to the Cybersecurity Foundational KUs (mandatory to all program types).

The current version of CAE-CD designation requirements has a total of 11 KUs comprising both technical and non-technical KUs for a 2-year program and a total of 6

KUs for 4+ year programs. However, the revised version has a clear categorization - 3 foundational, 10 cores (5 technical and 5 non-technical) and 55 optional KUs [42].

The introduction of a separate category of non-technical core KUs is a significant improvement accommodated in the revised version. This allows institutions to offer programs that specialize in a path – either the technical stream or the non-technical stream.

Table 2.2

Comparison of KU names in the current and revised version

KU Names in the current version	KU names in the revised version
Information Assurance Fundamentals	Cybersecurity Fundamentals
Fundamental Security Design Principles	Cybersecurity Principles (Fundamental KU)
Introduction to Cryptography	Basic Cryptography (Technical Core KU)
Networking Concepts	Basic Networking (Technical Core KU)
Basic Scripting	Basic Scripting and Programming (Technical Core KU)
Overview of Cyber Operations	Basic Cyber Operations (Optional KU)

An increased leverage on the non-technical aspects such as Cyber Threats, Policy, law and Ethics, Risk Management, Cybersecurity Planning and Management (An administrative Cybersecurity), Security Program Management bridges the disconnect and misunderstanding that cybersecurity issues can be solved only through technology solutions [42].

Changed KU names in the Revised Version of CAE-CD

In the revised version of CAE-CD 2019, some of the KU names have been changed. The changes in the KU names between the current and the revised version is shown in Table 2.2. The modified names imply easier naming conventions and connects well with the contents covered within the KU (For instance, Basic Scripting and Programming).

Increase in the breadth of KU Topics

The revised version of CAE-CD has a well-defined detail of the sub topics that are to be covered within each KU. This helps cover a wide number of topics within a KU. For instance, comparing the IT System Components from the previous and the revised version, as listed in the below Figure 2.6, we observe that the revised version has a broader perspective of the sub-topics and intends to familiarize the users on the breadth

of topics that constitute the KU. However, the topics are subject only to a high-level introduction and not intended for in-depth learning.

Addition of New KUs

The introduction of new knowledge units (Optional KUs) is one of the striking features in the revised CAE-CD version. The newly introduced KUs include Cyber Crime, Cybersecurity Ethics, Privacy and Advanced Algorithms. Also, some of the knowledge units in the current version is broken down into one more knowledge unit. For instance, System Administration KU in the current version is separated into 2 KUs - LINUX Systems Administration and WINDOWS Systems Administration. This gives more breadth of topics in each KU and covers all the specifications of System Administration, overall.

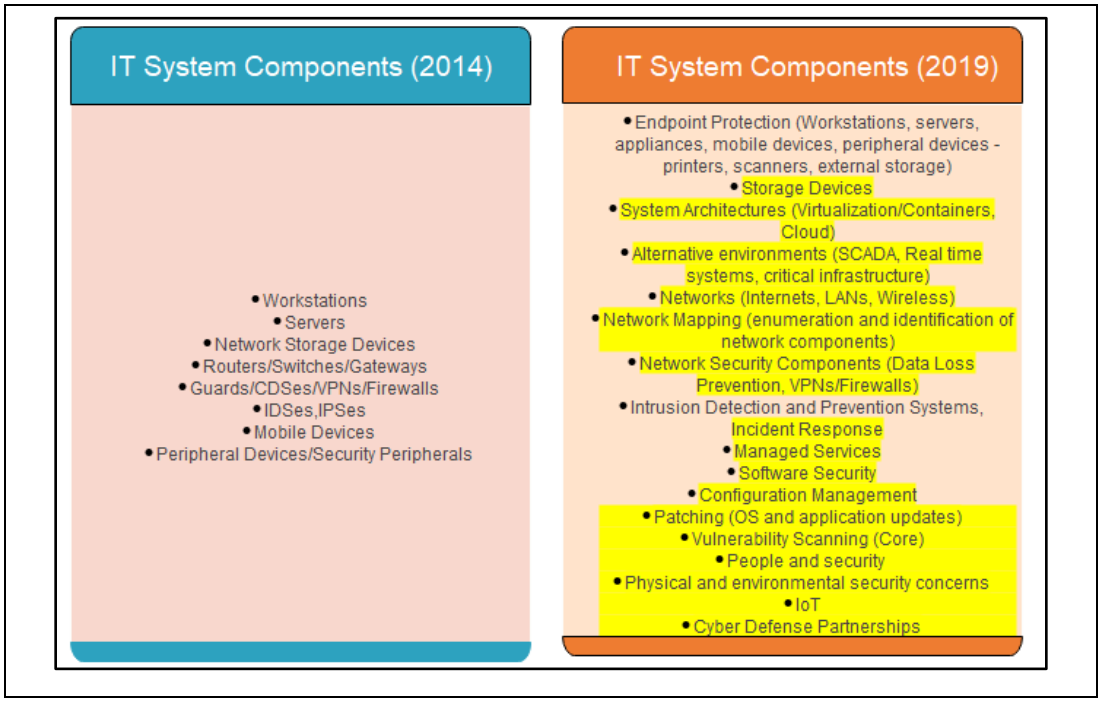

Figure 2.7

Knowledge Unit - IT System Components

Linking the current and revised versions of the KUs

The revised version of KU maps to the current version by specifying it in the Related Knowledge Unit section as indicated in the below Figure

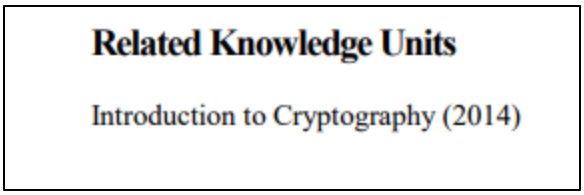

Figure 2.8

Structure of Related Knowledge Unit

Arbitrary Association to the NICE Framework

The NICE framework is tied to the foundational and core KUs at its category level. However, the connection is arbitrary as it does not pin to the specific knowledge, skills and competencies in that area. Each of the KUs in the Cybersecurity Foundational and Technical or Non-Technical Cores associates with all the NICE framework categories.

For instance, comparing the IT System Components, with the NICE framework categories, one can see that the topics map to more than one category. This is in a way, both advantageous and disadvantageous. Advantageous, because it associates with all the categories. Disadvantageous because it does not relate to specific work roles associated with the categories and the respective KSAs aimed towards them.

"Specializations" unassociated to the NICE Framework

The specializations mentioned as part of each KU infer to those areas where the Knowledge Unit is required. However, these specializations are not tied to the NICE framework. More Precision on association to NICE framework is necessary to be able to streamline the right Knowledge, Skills, Abilities and Tasks for a given KU [42].

Summary

This chapter discussed the importance of a holistic, interdisciplinary approach to Cybersecurity Education by the discussion of contributing disciplines and their theories, presented the multi-level, multi-discipline, multi-thread model for effective incorporation of interdisciplinary cybersecurity in course offerings spanning technical and non-technical majors, and presented a detailed analysis of the current guidelines that model cybersecurity education and training in the United States.

CHAPTER III

METHODOLOGY

The purpose of this study is to examine existing knowledge of security, awareness of threats and vulnerabilities, and the interest fostered towards an interdisciplinary path in cybersecurity and workforce across students from technical and non-technical majors. Survey data were collected from a purposeful sample of undergraduate students enrolled in different disciplines at the University of Houston - Clear Lake (UHCL). The survey was administered across eight different majors (Criminology, Legal Studies, Management, Information Technology, Economics, Computer Science and Computer Information Systems) within the College of Science and Engineering (CSE) and the College of Human Sciences and Humanities (HSH). The data were analyzed using frequencies, percentages, and paired sample t-tests. This chapter presents an overview of the research problem, research purpose and questions, research design, population and sample, instrumentation, data collection and analysis, ethical considerations, and research design limitations.

Overview of the Research Problem

Cybersecurity has become one of the most challenging issues of this digital age. In recent times, major retailers as Target and Neiman Marcus have been seriously exposed to data breaches, attack software such as the OpenSSL Heartbleed Bug have been used to expose secure websites and data of government agencies are at play in the hands of hacktivists groups as Anonymous. These events are emerging as commonplace events in academic, government, public and private sectors. According to Cisco's

Midyear Cybersecurity Report [43], “Business Email Compromise (BEC) has become a highly lucrative threat vector for attackers. U.S. $5.3 billion was stolen due to BEC fraud between October 2013 and December 2016 while ransomware exploits cost US$1 billion in 2016.” With emerging challenges and threats, it becomes imperative for preparing the talent in the pipeline with the required exposure in terms of training and skills. Also, to remedy the nation’s undeniable shortage of people with the knowledge, skills and abilities to perform the tasks required for cybersecurity work, a knowledgeable and experienced workforce staffed with both technical and interdisciplinary roles are needed [44].

Incorporating an interdisciplinary instructional design for students from technical and non-technical majors depends greatly on understanding the perceptions of cybersecurity risks, vulnerabilities, and practices that students bring to the classroom. Students are not categorized as “clear slates” when it comes to cybersecurity. Rather, students carry an initial understanding of security practices and risks that have been shaped through various means (e.g., social media, course offerings) and personal experiences. The basis of this research depends on the initial knowledge of cyber threats, risks, awareness and practices that they have developed over a period.

Research Purpose and Questions

The purpose of this study is to examine existing knowledge of security, awareness of threats and vulnerabilities, and the interest fostered towards a career path in cybersecurity education, and workforce across students from technical and non-technical majors. The study addressed the following research questions:

R1: To what extent do students perceive from technical and non-technical majors perceive cybersecurity?

R2: Is there a statistically significant mean difference in participants' perception of security behaviors before and after the intervention?

Ha: There is a statistically significant mean difference in participants' perception of security behaviors before and after the intervention

R3: Is there a statistically significant mean difference in participants' perception of security beliefs before and after the intervention?

Ha: There is a statistically significant mean difference in participants' perception of security beliefs before and after the intervention

Research Design

For purposes of this study, a survey design was employed. A purposeful sample of undergraduate students majoring in Economics, Computer Science, Information Technology, Legal Studies, Management, and Criminology at UHCL were administered the researcher-constructed *Integrated Approach to Cybersecurity Education Survey* to assess student perceptions on security behavior and beliefs, and measure the interest gathered towards an interdisciplinary approach. The data were analyzed using descriptive statistics (frequencies, percentages), and two-tailed paired sample t-tests.

Population and Sample

For this study, the population consisted of undergraduate students from the College of Business, College of Human Sciences and Humanities, and College of Science and Engineering at UHCL; a Hispanic-serving institution (HIS) with a current enrollment of 8,677 students. There are four colleges that function within its umbrella: College of Science and Engineering, College of Business, College of Human Sciences and Humanities, and the College of Education. Table 3.1 displays the student population of UHCL along with race/ethnicity and classification of students according to degrees for the previous academic school year (2017-2018).

Instrumentation

The *Integrated Approach to Cybersecurity Education Survey* was used to measure the existing knowledge of security practices and the awareness and interest fostered towards pursuing cybersecurity coursework and career. The survey was designed by the researcher through extensive design and consulting from methodologists and an expert panel consisting of faculty from UHCL and the Houston Baptist University. Stages of designing the instrument are described below.

1. Determining the primary goal/objective of designing the instrument – Measure existing knowledge in security awareness and practices, measure interest fostered to further their knowledge in the same by pursuing a minor in cybersecurity or desiring to enter the cybersecurity workforce.
2. Comprehensive Literature Review and Identifying Target Audience – a comprehensive literature review was carried out to understand the entities of

Table 3.1

Student Population at University of Houston - Clear Lake

	Students (n)	Percentage (%)
1. Degree		
Undergraduate	6,064	71.0
Graduate	2,478	29.0
2. Gender		
Male	3,176	37.2
Female	5,366	62.8
3. Enrollment by College		
College of Education	1,486	16.6
College of Business	2,564	30.0
College of Human Sciences and Humanities	2,228	26.1
College of Science and Engineering	2,219	26.0
4. Race/Ethnicity		
White	3,228	37.8
Hispanic/Latino	2,776	32.5
Black	689	8.1
International	894	10.5
Other	955	11.1

survey design and development with respect to Cybersecurity awareness and practices. The target audience was enumerated during this process.

3. Development – As an initial instrument, a survey was constructed based on a 4-point Likert-type scale from “Strongly Disagree” to “Strongly Agree” (items 4, 5, 7, 8, 9), 5-point Likert-type scale from “Never” to “Always” (item 6), and a 4-point Likert-type scale from “Not at all concerned” to “Very concerned” (item 3). These scales were selected due to their primary role in

understanding the respondents' behavior and attitudes with respect to the theory and practice of cybersecurity, and their focus on dynamic interaction between people, technology and process.

After determining the primary scales, a survey comprising of 17-items was constructed. Reliability and validity were evaluated as outlined in the following sections.

Determination of Validity – Expert Panel Review

The validity of the instrument was evaluated by using the content and context validity method. The content validity was used extensively to determine the relevance of the items in the instrument. In the first step, experts had to confirm that the items were valid. In the second step, a different group of experts were involved in asserting the validity of the entire instrument. The criteria for selecting the experts included knowledge and experience related to cybersecurity as well as education. By contrasts, experts with more than 5-years of experience in in the unit and those who were familiar with the concepts of security and education were included in the expert panel. The portfolio of the expert panel is included in Table 3.2.

The 17-item instrument was broken down into five subscales. The subscales, number of items, likert scales and Cronbach's Alpha pertaining to each are tabulated in Table 3.3. The Cronbach's Alpha calculated for the entire instrument is tabulated in Table 3.4.

Table 3.2

Demographics - Expert Panel Review

Name	Gender	Race/Ethnicity	Subject Matter Taught	Experience
Christina	Female	Asian	Systems Administration, Network Administration, Digital Forensics, Programming, Data Structures	19
Wilhelmina	Female	Asian	Information Systems, Database, Data Analytics	6
Chuck	Male	White/ Caucasian	Cyber Security, Computer Forensics, Programming (Java, MATLAB, Python, Basic), Computers in Society, Database, Information systems	30
Jannie	Female	White/ Caucasian	Instructional Technology, Educational Technology, Grant Writing, Web Design, Multimedia, Professional Writing	20+
Kim	Male	White/ Caucasian	Software Engineering, Engineering Management, Systems Engineering, Data Science	30+
Macey	Female	White/ Caucasian	Research Design, Survey Design, Statistics	20

Table 3.3

Reliability Statistics – Subscales

Subscale	Items	Example	Likert Scale	Cronbach's Alpha
Awareness of viruses	5	A virus erases personal files on the computer	Strongly Disagree to Strongly Agree	0.724
Awareness of protection measures against viruses	5	One can protect themselves from viruses by blocking pop-ups	Strongly Disagree to Strongly Agree	0.894
Frequency of protection measures	4	How often do you update your anti-virus software?	Never to Always	0.756
Awareness of hackers	9	Hackers target only home computer users	Strongly Disagree to Strongly Agree	0.677
Password practices	5	One should consider using the same password for all websites for consistency and ease	Strongly Disagree to Strongly Agree	0.912
Confidence to identify cyber attacks	4	I am confident I can identify phishing mails	Strongly Disagree to Strongly Agree	0.734

Table 3.4

Reliability Statistics - Instrument

Integrated Approach to Cybersecurity Education Survey	Cronbach's Alpha
No of items = 30	0.839

Data Collection Procedures

The researcher obtained permission from the University of Houston - Clear Lake (UHCL) Committee for the Protection of Human Subjects (CPHS) and fulfilling the training requirements enlisted by the Institutional Review Board (IRB) before collecting any data. Upon approval from both the entities, the student researcher reached out to the faculty from across the selected majors to gather interest to participate in the research. The emails that were sent out to invite faculty from across different colleges and majors in the UHCL included a short summary of the research, research goals and objectives, instructions explaining the survey instrument, intervention that was involved between the pre and the post survey (a short presentation) and the timeline enclosed for each of the activity which denoted the total class time that would be required to administer the survey. Appendix A and B includes a copy of the survey cover letter that states the purpose of the research, the duration of the survey, the contact information of the faculty sponsor and an acknowledgement for participation. Depending on the approval gained from the faculty and the time accommodated, a total of nine classes were selected. Prior to survey administration, the online links of the survey were sent to the instructor and was published on Blackboard for the students to access. Data were consolidated using

Qualtrics, exported, and stored electronically on a flash drive and a computer hard drive that was password protected. The data will remain with the researcher under secure conditions for a period of 5-years before it is destroyed.

Data Analysis

All data were analyzed using IBM SPSS. To answer research question one, descriptive statistics (frequencies and percentages) were calculated to understand and interpret the data in more depth. While descriptive statistics are employed to describe, show and summarize data in a meaningful way to study the emerging patterns obtained, they do not allow the researcher to make conclusions beyond the data analyzed or reach conclusions regarding the hypothesis made. To answer research question two, a two-tailed paired samples t-test was conducted to determine if there was a statistically significant mean difference from pre- to post-survey administration on security behaviors. To answer research question three, a paired sample t-test was conducted to determine if any statistically significant mean difference existed from pre- to post-survey administration on security beliefs. Effect was measured using Cohen's d and $r^{2.}$ A significance value of 0.05 was used for this study.

Privacy and Ethical Considerations

Prior to collection of data, the student researcher gained consent from UHCL's CPHS and IRB. The student researcher and the Faculty sponsor fulfilled required training criteria of the IRB. A survey cover letter was attached to the survey instrument enumerating the purpose of the study, ensuring that the participants were aware that their involvement in the survey was completely voluntary and that their responses are kept

confidential and anonymous. Completion of the survey implied the student's participation in the survey. All quantitative data were then transferred from Excel to SPSS and then verified it was transferred correctly. Data were stored electronically on a password protected flash drive and computer hard drive. The data will remain with the researcher under secure conditions for a period of 5-years before which it is destroyed.

Limitations of the study

There are several limitations for this study. First, the classes for survey administration were chosen depending on approvals sought and availability of the instructors across various classes. Therefore, the sample size across each major varies and is not in proximity to each other. For instance, most of the Legal studies courses at the UHCL are offered online. Given the nature of the classes for the survey were determined to be face to face, there was only one class from Legal Studies that was a core course and the sample size was much lower compared to the other classes. This has had an influence on the overall results due to an unequal representative distribution of the population on whom the overall results are generalized or transferred. Second, most of the classes chosen for the survey were core courses targeted in the sophomore or the junior level. However, there were a few elective courses that were part of the survey administration. Due to constraints of the nature of the classes, there is an unequal number of core and elective courses chosen for the survey. In accordance to this, Pew Research Center [63] states that the knowledge of cybersecurity is affected by respondents' age, educational attainment, and subject matter studied.

Conclusion

The purpose of this quantitative analysis was to draw a relationship between the subject matter learnt, and the security behaviors and beliefs that the respondents possess, and the interest fostered towards pursuing a path in cybersecurity career or workforce. These dimensions of research questions help explain the strong connection between cybersecurity and the other disciplines (Criminology, Legal Studies, Economics, Management, Information Technology) taken into consideration as part of this research. The next chapter provides the results of the data analysis of the research questions.

CHAPTER IV

RESULTS

The purpose of this study is to examine existing knowledge of security, awareness of threats and vulnerabilities, and the interest fostered towards an interdisciplinary path in cybersecurity and workforce across students from technical and non-technical majors. The survey was completed by 228 UHCL undergraduate students and administered to classes across six different disciplines: Criminology, Legal Studies, Management, Computer Science, Information Technology, and Economics. This chapter presents the data analysis for each of the three research questions. It concludes with a summary of the findings.

Participant Demographics

From the above given population, a purposeful sample of students across majors were selected to participate in the survey. These majors pose a significant connection and contribution to interdisciplinary cybersecurity and much of its significance has been covered in the literature review section. The majors include Criminology, Computer Science, Economics, Information Technology, Legal Studies and Management. The research participants were aimed at being undergraduate students whose majors were one of those mentioned. Several classes in each major were selected for the administration of the survey, depending on the support and accommodation extended by the faculty. Three classes in the criminology major (namely Criminology, Criminal Investigation and Race and Justice), one undergraduate class in Computer Science (Computer Security), two classes in Information Technology (namely Computer Forensics and Cybersecurity), one

class in Economics (Principles of Microeconomics), one class in Legal Studies (Legal Research) and one class in Management (Management Theory and Practice) were involved. Altogether, 228 students participated in the survey. Table 4.1 displays the participant demographics regarding gender, age, and race/ethnicity that took the selected classes. “n” represents the frequency, i.e., the number of students that fall in that particular category and “%” represents the percentage value for the same. Most students were female comprising of 56.4% (n = 128). Male participants comprised of 43.9% (n = 100) of the sample population.

About age classification, participants in the 18-24 age group constituted the majority of all the respondents, comprising of 66.7% (n = 152), followed by students in the 25-34 category, comprising of 28.1% (n = 64) of the total sample.

Regarding Ethnicity, most of the survey respondents identified themselves as White or Caucasian, comprising of 36.9% (n = 84). The Hispanic/Latino numbers were also close to that of White/Caucasian, comprising of 36.9% (n = 86).

In order to gain a better understanding of student perceptions, the survey included questions on number of hours students spend online in fulfilling personal and academic tasks. The data obtained is tabulated in Table 4.2. On an average, the data demonstrates that, almost three-fourth of students (65.8%, n = 150) spend 2 to 5 hours every day fulfilling academic tasks and 51.8% (n=118) of students spend the same number of hours in fulfilling their personal tasks.

Table 4.1

Overall Participant Demographics

	Crim.		CS		Econ.		IT		Legal Studies		Mgmt.	
	n	%	n	%	n	%	n	%	n	%	n	%
1. Gender												
Male	23	39.7	10	20.8	22	41.5	26	86.7	1	12.5	18	56.3
Female	35	60.3	37	77.1	31	58.5	4	13.3	7	87.5	14	43.8
2. Race												
Asian	4	6.9	8	16.7	6	11.3	4	13.3	0	0	1	3.1
Black	3	5.2	5	10.4	6	11.3	0	0	0	0	3	9.4
Hispanic	24	41.4	18	37.5	15	28.3	8	26.7	7	87.5	12	37.5
Native American	0	0	0	0	1	1.9	0	0	0	0	1	3.1
Other	0	0	2	4.2	0	0	0	0	0	0	0	0
Two or more	7	12.1	0	0	3	5.7	2	6.7	0	0	3	9.4
White	20	34.5	15	31.3	22	41.5	16	53.3	1	12.5	12	37.5
3. Age Classification												
18-24	41	70.7	28	58.3	40	75.5	13	43.3	5	62.5	25	78.1
25-34	13	22.4	17	35.4	9	17	15	50	3	37.5	7	21.9
35-44	3	5.2	3	6.3	4	7.5	1	3.3	0	0	0	0
45-54	1	1.7	0	0	0	0	1	3.3	0	0	0	0
55-64	0	0	0	0	0	0	0	0	0	0	0	0

Note. Crim. = Criminology, CS = Computer Science, Econ = Economics, I.T = Information Technology, Mgmt = Management

Table 4.2

Demographics of Hours Spent on the Internet

Majors	Hours spent - academic tasks		Hours spent - personal tasks	
	Mean	Standard Deviation	Mean	Standard Deviation
Computer Science	4.6	3.1	6.2	4.2
Criminology	4.1	2.4	4.6	3.0
Economics	4.4	2.8	6.4	12
Information Tech.	4.6	2.1	6.6	4.1
Legal Studies	6.0	4.2	8.3	13.1
Management	4.9	4	6.6	8.6

Comparatively, students from non-technical majors as Legal Studies (Mean = 6.0, S.D = 4.2) and Management (Mean = 4.9, S.D = 4) spend more time on the internet fulfilling academic tasks in comparison to the students from technical majors as Computer Science (Mean = 4.1, S.D = 3.1) and Information Technology (Mean = 4.6, S.D = 2.1).

Research Question One

Research Question One, *To what extent do students from technical and non-technical majors perceive cybersecurity?*, was measured using frequencies and percentages. With this research question, the survey questionnaire included 9 items using a 4-point Likert scale (*Strongly Disagree, Disagree, Agree, Strongly Agree*). The responses related to factors that influence the perception of cybersecurity among students are provided below and are tabulated in the tables that follow.

Concern for Security on the Internet

Table 4.3 points out that students in the technical majors were found to be much concerned about their security on the internet than students from the non-technical majors. Approximately 84.0 percent of the students in Computer Science, 87.5 percent of students in Computer Security and 100.0 percent of students in the Computer Forensics classes were *Somewhat Concerned/Very Concerned* about their security on the internet.

Not at all Concerned/Slightly Concerned were also reported by students from the technical majors. Twelve point five percent of students who took the Computer Security Course agreed that they were *Not at all Concerned/Slightly Concerned*. On the other hand, students from the non-technical majors were also found to be concerned about their security. Seventy percent of students from Criminology, 66.6 percent of students from Economics and 81.8 percent of students from Management classes were *Somewhat Concerned/Very Concerned* about their security on the internet. However, more students agreed to be *Not at all Concerned/Slightly Concerned*. Thirty percent of students from Criminology, 31.5 percent of students from Economics and 18.2 percent of students from Management were *Not at all Concerned/Slightly Concerned* about their security on the internet.

Awareness of Viruses

From Table 4.4, with respect to technical majors, all the students (100.0 percent) in the Computer Forensics class *Agreed/Strongly Agreed* that viruses cause computers to crash while 36.0 percent of students in the Computer Science class *Strongly Disagree/Disagree* the same. On the contrary, some students (11.1 percent) from the Criminal Investigation class *Strongly Disagree/Disagree* while 97.0 percent of students in the Management class *Agree/Strongly Agree* on the same. All the students in the Computer Security class *Agree/Strongly Agree* that a virus causes annoying problems, while all of the students from a non-technical class as Legal Studies also Agreed/Strongly Agreed the same. None of the students *Strongly Disagree/Disagree* that viruses cause annoying problems.

Most students (81.7 percent) in the Computer Forensics class *Agree/Strongly Agree* that viruses erase important files on the computer, while all the students from a non-technical class as Legal Studies also *Agreed/Strongly Agreed* the same. On the

contrary, 34.0 percent of students in the Computer Science class Strongly Disagree/Disagree that a virus erases important files on the computer while only 3.5 percent of student in a non-technical major as Economics Strongly Disagree/Disagree on the same. While three-fourths (75.0 percent) of students in the technical major as Computer Science Agree/Strongly Agree that viruses can be avoided by being aware of the websites that are visited, 25.0 percent of students from the same class also Disagree/Strongly Disagree on the same.

Table 4.3

Concern for Security on the Internet (%)

Classes	Not at all Concerned	Slightly Concerned	Somewhat Concerned	Very Concerned
Computer Science	4.0 (n = 1)	12.0 (n = 3)	36.0 (n = 9)	48.0 (n = 12)
Computer Security	4.2 (n = 1)	8.3 (n = 2)	33.3 (n = 8)	54.2 (n = 13)
Computer Forensics	0.0 (n = 0)	0.0 (n = 0)	36.4 (n = 4)	63.6 (n = 7)
Legal Studies	0.0 (n = 0)	12.5 (n = 1)	62.5 (n = 5)	25.0 (n = 2)
Criminology	10.0 (n = 1)	20.0 (n = 2)	30.0 (n = 3)	40.0 (n = 4)
Criminal Investigation	0.0 (n = 0)	11.5 (n = 3)	46.2 (n = 12)	42.3 (n = 11)
Race/Justice	4.3 (n = 1)	13.0 (n = 3)	43.5 (n = 10)	39.1 (n = 9)
Economics	5.6 (n = 3)	25.9 (n = 14)	29.6 (n = 16)	37 (n = 20)
Management	6.1 (n = 2)	12.1 (n = 4)	33.3 (n = 11)	48.5 (n = 16)

Table 4.4

Awareness of Viruses (%)

Survey Item	Course	Strongly Disagree	Disagree	Agree	Strongly Agree
1. A virus causes computers to crash	Comp. Sci	12.0 (n = 3)	24.0 (n = 6)	32.0 (n = 8)	32.0 (n = 8)
	Comp. Sec	0.0 (n = 3)	12.5 (n = 3)	41.7 (n = 10)	45.8 (n = 11)
	Comp. For	0.0 (n = 0)	0.0 (n = 0)	33.3 (n = 4)	66.7 (n = 8)
	Legal	0.0 (n = 0)	0.0 (n = 0)	25.0 (n = 2)	75.0 (n = 6)
	Criminology	0.0 (n = 0)	0.0 (n = 0)	55.6 (n = 5)	44.4 (n = 4)
	Crim. Inv	0.0 (n = 0)	11.1 (n = 3)	55.6 (n = 15)	29.6 (n = 8)
	Race/Justice	0.0 (n = 0)	6.8 (n = 4)	54.2 (n = 32)	35.6 (n = 21)
	Economics	0.0 (n = 0)	8.9 (n = 5)	48.2 (n = 27)	37.5 (n = 21)
	Management	0.0 (n = 0)	3.0 (n = 1)	36.4 (n = 12)	60.6 (n = 20)
2. A virus causes annoying problems	Comp. Sci	4.0 (n = 1)	4.0 (n = 1)	48.0 (n = 12)	44.0 (n = 11)
	Comp. Sec	0.0 (n = 0)	0.0 (n = 0)	29.2 (n = 7)	70.8 (n = 17)

Survey Item	Course	Strongly Disagree	Disagree	Agree	Strongly Agree
	Legal	0.0 (n = 0)	0.0 (n = 0)	25.0 (n = 2)	75.0 (n = 6)
	Criminology	0.0 (n = 0)	0.0 (n = 0)	40.0 (n = 4)	50.0 (n = 5)
	Crim. Inv	0.0 (n = 0)	0.0 (n = 0)	51.9 (n = 14)	44.4 (n = 12)
	Race/Justice	0.0 (n = 0)	0.0 (n = 0)	40.7 (n = 24)	55.9 (n = 33)
	Economics	0.0 (n = 0)	0.0 (n = 0)	41.1 (n = 23)	53.6 (n = 30)
	Management	0.0 (n = 0)	0.0 (n = 0)	30.3 (n = 10)	69.7 (n = 23)
3. A virus erases important files on the computer	Comp. Sci	8.0 (n = 2)	26.0 (n = 5)	36.0 (n = 9)	36.0 (n = 9)
	Comp. Sec	0.0 (n = 0)	8.3 (n = 2)	58.3 (n = 14)	33.3 (n = 18)
	Comp. For	0.0 (n = 0)	8.3 (n = 1)	16.7 (n = 2)	75 (n = 9)
	Legal	0.0 (n = 0)	0.0 (n = 0)	50.0 (n = 4)	50.0 (n = 4)
	Criminology	0.0 (n = 0)	0.0 (n = 0)	33.3 (n = 3)	66.7 (n = 6)

Survey Item	Course	Strongly Disagree	Disagree	Agree	Strongly Agree
	Race/Justice	0.0 (n = 0)	11.9 (n = 7)	50.8 (n = 30)	33.9 (n = 20)
	Economics	0.0 (n = 0)	3.6 (n = 2)	55.4 (n = 31)	35.7 (n = 20)
	Management	0.0 (n = 0)	0.0 (n = 0)	39.4 (n = 13)	60.6 (n = 20)
4. A virus steals personal/financial information	Comp. Sci	4.0 (n = 1)	8.0 (n = 2)	36.0 (n = 9)	52.0 (n = 13)
	Comp. Sec	0.0 (n = 0)	16.7 (n = 4)	50.0 (n = 12)	33.3 (n = 8)
	Comp. For	0.0 (n = 0)	8.3 (n = 1)	16.7 (n = 2)	75.0 (n = 9)
	Legal	0.0 (n = 0)	0.0 (n = 0)	25.0 (n = 2)	75.0 (n = 6)
	Criminology	0.0 (n = 0)	0.0 (n = 0)	33.3 (n = 3)	66.7 (n = 6)
	Crim.Inv	3.7 (n = 1)	3.7 (n = 1)	44.4 (n = 12)	44.4 (n = 12)
	Race/Justice	1.7 (n = 1)	3.4 (n = 2)	45.8 (n = 27)	45.8 (n = 27)
	Economics	0.0 (n = 0)	7.1 (n = 4)	39.3 (n = 22)	48.2 (n = 27)
	Management	0.0 (n = 0)	0.0 (n = 0)	39.4 (n = 13)	60.6 (n = 20)

Survey Item	Course	Strongly Disagree	Disagree	Agree	Strongly Agree
5. A virus can be avoided by being aware of which websites I go to	Comp. Sci	4.0 (n = 1)	20.0 (n = 5)	48.0 (n = 12)	28.0 (n = 7)
	Comp. Sec	0.0 (n = 0)	20.8 (n = 5)	33.3 (n = 8)	45.8 (n = 11)
	Comp. For	0.0 (n = 0)	0.0 (n = 0)	25.0 (n = 3)	75.0 (n = 9)
	Legal	0.0 (n = 0)	0.0 (n = 0)	25.0 (n = 2)	75.0 (n = 6)
	Criminology	0.0 (n = 0)	0.0 (n = 0)	33.3 (n = 3)	66.7 (n = 6)
	Crim. Inv	0.0 (n = 0)	7.4 (n = 2)	44.4 (n = 12)	44.4 (n = 12)
	Race/Justice	1.7 (n = 1)	3.4 (n = 2)	45.8 (n = 27)	45.8 (n = 27)
	Economics	1.8 (n = 1)	1.8 (n = 1)	55.4 (n = 31)	35.7 (n = 20)
	Management	3.0 (n = 1)	0.0 (n = 0)	30.3 (n = 10)	66.7 (n = 22)

Note. Comp. Sci = Computer Science, Comp. Sec = Computer Security, Comp. For = Computer Forensics, Legal = Legal Research and Studies, Crim. Inv = Criminal Investigation.

Awareness of Protection from Viruses

From Table 4.5, it is evident that all students from the technical classes as Computer Science, Computer Security and Computer Forensics *Agree/Strongly Agree*

that anti-virus protection is important, 14.3 percent of students from non-technical classes as Criminal Investigation, Race/Justice and Economics *Strongly Disagree/Disagree* the same. Most students (83.3 percent) from technical classes as Computer Science *Agree/Strongly Agree* that one can protect themselves from viruses by blocking pop-ups, 25.9 percent of students from a non-technical class as Criminal Investigation *Disagree/Strongly Disagree* on the same.

Table 4.5

Awareness of Protection from Viruses (%)

Survey Item	Course	Strongly Disagree	Disagree	Agree	Strongly Agree
1. One can protect themselves from viruses by keeping the anti-virus software up-to date	Comp. Sci	0.0 (n = 0)	4.0 (n = 1)	60.0 (n = 15)	36.0 (n = 9)
	Comp. Sec	0.0 (n = 0)	0.0 (n = 0)	54.2 (n = 13)	45.8 (n = 11)
	Comp. For	0.0 (n = 0)	0.0 (n = 0)	15.4 (n = 2)	69.2 (n = 9)
	Legal	0.0 (n = 0)	0.0 (n = 0)	12.5 (n = 1)	87.5 (n = 7)
	Criminology	0.0 (n = 0)	0.0 (n = 0)	22.2 (n = 2)	77.8 (n = 7)
	Crim.Inv	0.0 (n = 0)	7.4 (n = 2)	37.0 (n = 10)	51.9 (n = 14)
	Race/Justice	0.0 (n = 0)	5.1 (n = 3)	37.3 (n = 22)	54.2 (n = 32)
	Economics	0.0 (n = 0)	1.8 (n = 1)	51.8 (n = 29)	41.1 (n = 23)

Survey Item	Course	Strongly Disagree	Disagree	Agree	Strongly Agree
2. One can protect themselves from viruses by never downloading anything from the Internet	Management	0.0 (n = 0)	0.0 (n = 0)	22.1 (n = 7)	78.8 (n = 26)
	Comp. Sci	12.0 (n = 3)	44.0 (n = 11)	28.0 (n = 7)	12.0 (n = 3)
	Comp. Sec	0.0 (n = 0)	29.2 (n = 7)	33.3 (n = 8)	37.5 (n = 9)
	Comp. For	7.7 (n = 1)	15.4 (n = 2)	23.1 (n = 3)	38.5 (n = 5)
	Legal	12.5 (n = 1)	50 (n = 4)	0.0 (n = 0)	37.5 (n = 3)
	Criminology	0.0 (n = 0)	33.3 (n = 3)	44.4 (n = 4)	22.2 (n = 2)
	Crim.Inv	11.1 (n = 3)	44.4 (n = 12)	33.3 (n = 9)	7.4 (n = 2)
	Race/Justice	6.8 (n = 4)	39.0 (n = 23)	40.7 (n = 24)	10.2 (n = 6)
	Economics	5.4 (n = 3)	58.9 (n = 33)	21.4 (n = 12)	8.9 (n = 5)
	Management	0.0 (n = 0)	12.1 (n = 4)	45.5 (n = 15)	42.4 (n = 14)
	Legal	0.0 (n = 0)	62.5 (n = 5)	0.0 (n = 0)	37.5 (n = 3)
	Criminology	0.0 (n = 0)	11.1 (n = 1)	55.6 (n = 5)	33.3 (n = 3)
	Crim.Inv	7.4 (n = 2)	18.5 (n = 5)	48.1 (n = 13)	22.2 (n = 6)

Survey Item	Course	Strongly Disagree	Disagree	Agree	Strongly Agree
	Race/Justice	3.4 (n = 2)	18.6 (n = 11)	54.2 (n = 32)	20.3 (n = 12)
	Economics	0.0 (n = 0)	21.4 (n = 12)	60.7 (n = 34)	12.5 (n = 7)
	Management	0.0 (n = 0)	3.0 (n = 1)	51.5 (n = 17)	45.5 (n = 15)
3. One can protect themselves from viruses by being aware of what websites are visited	Comp. Sci	0.0 (n = 0)	0.0 (n = 0)	68.0 (n = 17)	28.0 (n =7)
	Comp. Sec	0.0 (n = 0)	4.2 (n = 1)	33.3 (n = 8)	62.5 (n = 15)
	Comp. For	0.0 (n = 0)	0.0 (n = 0)	15.4 (n = 2)	69.2 (n = 9)
	Legal	0.0 (n = 0)	62.5 (n = 5)	0.0 (n = 0)	37.5 (n = 3)
	Criminology	0.0 (n = 0)	0.0 (n = 0)	33.3 (n = 3)	66.7 (n = 6)
	Crim.Inv	0.0 (n = 0)	3.7 (n = 1)	55.6 (n = 15)	37.0 (n = 10)
	Race/Justice	0.0 (n = 0)	1.7 (n = 1)	44.1 (n = 26)	50.8 (n = 30)
	Economics	0.0 (n = 0)	1.8 (n = 1)	62.5 (n = 35)	30.4 (n = 17)
	Management	0.0 (n = 0)	0.0 (n = 0)	39.4 (n = 13)	60.6 (n = 20)
4. One can protect themselves	Comp. Sci	0.0 (n= 0)	4.0 (n = 1)	40.0 (n = 10)	56.0 (n = 14)

Survey Item	Course	Strongly Disagree	Disagree	Agree	Strongly Agree
from viruses by not clicking on email attachments from people you do not know	Comp. Sec	0.0 (n = 0)	0.0 (n = 0)	12.5 (n = 3)	87.5 (n = 21)
	Comp. For	0.0 (n = 0)	0.0 (n = 0)	8.3 (n = 1)	91.7 (n = 11)
	Legal	0.0 (n = 0)	0.0 (n = 0)	12.5 (n = 1)	87.5 (n = 7)
	Criminology	0.0 (n = 0)	11.1 (n = 1)	0.0 (n = 0)	88.9 (n = 8)
	Crim.Inv	0.0 (n = 0)	0.0 (n = 0)	33.3 (n = 9)	63.0 (n = 17)
	Race/Justice	0.0 (n = 0)	1.7 (n = 1)	27.1 (n = 16)	67.8 (n = 40)
	Economics	0.0 (n = 0)	8.9 (n = 5)	33.9 (n = 19)	51.8 (n = 29)
	Management	0.0 (n = 0)	0.0 (n = 0)	24.2 (n = 8)	75.8 (n = 25)

Note. Comp.Sci = Computer Science, Comp.Sec = Computer Security, Comp. For = Computer Forensics, Legal = Legal Research and Studies, Crim. Inv = Criminal Investigation.

Awareness of Hackers

From Table 4.6, it is evident that all students (100.0 percent) from technical classes as Computer Security *Agree/Strongly Agree* that hackers could intentionally put viruses on my computer. Six percent of students from a non-technical class as Management *Disagree/Strongly disagree* on the same. While all students (100.0 percent) from technical classes as Computer Security *Agree/Strongly Agree* that hackers could monitor what they are doing on their computers, 25.0 percent of students from a non-technical class as Legal Studies *Disagree/Strongly Disagree* on the same. Moreover,

students (35.0 percent) from technical classes as Computer Security *Agree/Strongly Agree* that hackers target only home computer users, while 36.3 percent of students from a non-technical class as Management *Agree/Strongly Agree* on the same.

Table 4.6

Awareness of Hackers (%)

Survey Item	Course	Strongly Disagree	Disagree	Agree	Strongly Agree
1. Hackers could watch what I am doing on my computer	Comp.Sci	0.0 (n = 0)	4.0 (n = 1)	44.0 (n = 11)	52.0 (n = 13)
	Comp.Sec	0.0 (n = 0)	0.0 (n = 0)	37.5 (n = 9)	62.5 (n = 15)
	Comp.For	0.0 (n = 0)	8.3 (n = 1)	50.0 (n = 6)	41.7 (n = 7)
	Legal Studies	0.0 (n = 0)	25.0 (n = 2)	0.0 (n = 0)	75.0 (n = 6)
	Criminology	0.0 (n = 0)	0.0 (n = 0)	22.2 (n = 2)	77.8 (n = 7)
	Crim.Inv	0.0 (n = 0)	3.7 (n = 1)	44.4 (n = 12)	48.1 (n = 13)
	Race/Justice	0.0 (n = 0)	3.4 (n = 2)	42.4 (n = 25)	50.8 (n = 30)
	Economics	0.0 (n = 0)	3.6 (n = 2)	57.1 (n = 32)	33.9 (n = 19)
	Management	6.1 (n = 2)	0.0 (n = 0)	27.3 (n = 9)	66.7 (n = 22)

Survey Item	Course	Strongly Disagree	Disagree	Agree	Strongly Agree
2. Hackers could intentionally put viruses on the computer	Comp.Sci	0.0 (n = 0)	12.0 (n = 3)	36.0 (n = 9)	52.0 (n = 13)
	Comp.Sec	0.0 (n = 0)	0.0 (n = 0)	33.3 (n = 8)	66.7 (n = 16)
	Comp.For	0.0 (n = 0)	8.3 (n = 1)	50.0 (n = 6)	41.7 (n = 5)
	Legal Studies	0.0 (n = 0)	0.0 (n = 0)	12.5 (n = 1)	87.5 (n = 7)
	Criminology	0.0 (n = 0)	0.0 (n = 0)	22.2 (n = 2)	77.8 (n = 7)
	Crim.Inv	0.0 (n = 0)	0.0 (n = 0)	55.6 (n = 15)	40.7 (n = 11)
	Race/Justice	0.0 (n = 0)	0.0 (n = 0)	44.1 (n = 26)	52.5 (n = 31)
	Economics	0.0 (n = 0)	5.4 (n = 3)	57.1 (n = 32)	32.1 (n = 18)
	Management	6.1 (n = 2)	0.0 (n = 0)	18.2 (n = 6)	75.8 (n = 25)
3. Hackers could record everything on the computer	Comp.Sci	0.0 (n = 0)	16.0 (n = 4)	32.0 (n = 8)	52.0 (n = 13)
	Comp.Sec	0.0 (n = 0)	0.0 (n = 0)	37.5 (n = 9)	62.5 (n = 15)
	Comp.For	0.0 (n = 0)	8.3 (n = 1)	50.0 (n = 6)	41.7 (n = 5)

Survey Item	Course	Strongly Disagree	Disagree	Agree	Strongly Agree
	Legal Studies	0.0 (n = 0)	0.0 (n = 0)	12.5 (n = 1)	87.5 (n = 7)
	Criminology	0.0 (n = 0)	0.0 (n = 0)	22.2 (n = 2)	77.8 (n = 7)
	Crim.Inv	0.0 (n = 0)	0.0 (n = 0)	51.9 (n = 14)	44.4 (n = 12)
	Race/Justice	0.0 (n = 0)	0.0 (n = 0)	47.5 (n = 28)	49.2 (n = 29)
	Economics	0.0 (n = 0)	8.9 (n = 5)	53.6 (n = 30)	32.1 (n = 18)
	Management	6.1 (n = 2)	0.0 (n = 0)	18.2 (n = 6)	75.8 (n = 25)
4. Hackers could target only home computer users	Comp.Sci	16.0 (n = 4)	32.0 (n = 8)	20.0 (n = 5)	32.0 (n = 8)
	Comp.Sec	41.7 (n = 10)	12.5 (n = 3)	29.2 (n = 7)	16.7 (n = 4)
	Comp.For	75.0 (n = 9)	0.0 (n = 0)	25.0 (n = 3)	0.0 (n = 0)
	Legal Studies	37.5 (n = 3)	25.0 (n = 2)	25.0 (n = 2)	12.5 (n = 1)
	Criminology	22.2 (n = 2)	33.3 (n = 3)	11.1 (n = 1)	33.3 (n = 3)
	Crim.Inv	29.6 (n = 8)	44.4 (n = 12)	7.4 (n = 2)	14.8 (n = 4)
	Race/Justice	25.4 (n = 15)	45.8 (n = 27)	11.9 (n = 7)	13.6 (n = 8)

Survey Item	Course	Strongly Disagree	Disagree	Agree	Strongly Agree
	Economics	23.2 (n = 13)	44.6 (n = 25)	14.3 (n = 8)	12.5 (n = 7)
	Management	33.3 (n = 11)	30.3 (n = 10)	12.1 (n = 4)	24.2 (n = 8)

Note. Comp.Sci = Computer Science, Comp.Sec = Computer Security, Comp. For = Computer Forensics, Legal = Legal Research and Studies, Crim. Inv = Criminal Investigation.

Password Ethics

Table 4.7 shows that while most students (96.0 percent) in the computer science class *Disagree/Strongly Disagree* that 'admin' or 'root' or 'administrator' could be used as passwords, 33.3 percent of students from a non-technical class as Criminology *Agree/Strongly Agree* on the same. While only 64.0 percent of students in technical classes as Computer Science *Disagree/Strongly Disagree* that passwords could be written down, 66.7 percent of students in Legal Studies, 62.9 percent of students from Criminal Investigation and 64.4 percent of students from Race/Justice Agree/Strongly Agree on the same.

Table 4.7

Password Ethics

Survey Item	Course	Strongly Disagree	Disagree	Agree	Strongly Agree
1. Use 'admin' and 'root' or 'administrator' as passwords	Comp. Sci	80.0 (n = 20)	16.0 (n = 4)	4.0 (n = 1)	0.0 (n = 0)
	Comp. Sec	62.5 (n = 15)	16.7 (n = 4)	12.5 (n = 3)	8.3 (n = 2)
	Comp. For	76.9 (n = 10)	7.7 (n = 1)	7.7 (n = 1)	0.0 (n = 0)

Survey Item	Course	Strongly Disagree	Disagree	Agree	Strongly Agree
	Legal Studies	50.0 (n = 4)	50.0 (n = 4)	0.0 (n = 0)	0.0 (n = 0)
	Criminology	22.2 (n = 2)	44.4 (n = 4)	22.2 (n = 2)	11.1 (n = 1)
	Crim.Inv	40.7 (n = 11)	44.4 (n = 12)	3.7 (n = 1)	7.4 (n = 2)
	Race/Justice	33.9 (n = 20)	49.2 (n = 29)	8.5 (n = 5)	5.1 (n = 3)
	Economics	30.4 (n = 17)	42.9 (n = 24)	17.9 (n = 10)	3.6 (n = 2)
	Management	78.8 (n = 26)	9.1 (n = 3)	0.0 (n = 0)	12.1 (n = 4)
2. Write it down so you can look it up when you forget	Comp. Sci	32.0 (n = 8)	32.0 (n = 8)	36.0 (n = 9)	0.0 (n = 0)
	Comp. Sec	41.7 (n = 10)	29.2 (n = 7)	20.8 (n = 5)	8.3 (n = 2)
	Comp. For	23.1 (n = 3)	46.2 (n = 6)	7.7 (n = 1)	15.4 (n = 2)
	Legal Studies	37.5 (n = 3)	37.5 (n = 3)	12.5 (n = 1)	12.5 (n = 1)
	Criminology	11.1 (n = 1)	22.2 (n = 2)	55.6 (n = 5)	11.1 (n = 1)
	Crim.Inv	14.8 (n = 4)	18.5 (n = 5)	40.7 (n = 11)	22.2 (n = 6)
	Race/Justice	13.6 (n = 8)	18.6 (n = 11)	40.7 (n = 24)	23.7 (n = 14)
	Economics	3.6 (n = 2)	23.2 (n = 13)	58.9 (n = 33)	8.9 (n = 5)

Survey Item	Course	Strongly Disagree	Disagree	Agree	Strongly Agree
3. A good mixture of upper case, lower case letters, numbers and special characters	Management	33.3 (n = 11)	33.3 (n = 11)	21.2 (n = 7)	12.1 (n = 4)
	Comp. Sci	0.0 (n = 0)	0.0 (n = 0)	24.0 (n = 6)	76.0 (n = 19)
	Comp. Sec	4.2 (n = 1)	0.0 (n = 0)	8.3 (n = 2)	87.5 (n = 21)
	Comp. For	0.0 (n = 0)	0.0 (n = 0)	7.7 (n = 1)	84.6 (n = 11)
	Legal Studies	0.0 (n = 0)	0.0 (n = 0)	12.5 (n = 1)	87.5 (n = 7)
	Criminology	0.0 (n = 0)	0.0 (n = 0)	22.2 (n = 2)	77.8 (n = 7)
	Crim.Inv	0.0 (n = 0)	0.0 (n = 0)	22.2 (n = 6)	74.1 (n = 20)
	Race/Justice	0.0 (n = 0)	0.0 (n = 0)	27.1 (n = 16)	69.5 (n = 41)
	Economics	0.0 (n = 0)	0.0 (n = 0)	35.7 (n = 20)	58.9 (n = 33)
4. Change once in a few years	Management	6.1 (n = 2)	0.0 (n = 0)	21.2 (n = 7)	72.7 (n = 24)
	Comp. Sci	24.0 (n = 6)	36.0 (n = 9)	28.0 (n = 7)	12.0 (n = 3)
	Comp. Sec	25.0 (n = 6)	29.2 (n = 7)	29.2 (n = 7)	16.7 (n = 4)
	Comp. For	23.1 (n = 3)	38.5 (n = 5)	23.1 (n = 3)	7.7 (n = 1)
	Legal Studies	25.0 (n = 2)	37.5 (n = 3)	12.5 (n = 1)	25.0 (n = 2)
	Criminology	0.0 (n = 0)	22.2 (n = 2)	55.6 (n = 5)	22.2 (n = 2)

Survey Item	Course	Strongly Disagree	Disagree	Agree	Strongly Agree
	Crim.Inv	3.7 (n = 1)	25.9 (n = 7)	44.4 (n = 12)	22.2 (n = 6)
	Race/Justice	3.4 (n = 2)	22.0 (n = 3)	50.8 (n = 13)	20.3 (n = 12)
	Economics	8.9 (n = 5)	25.0 (n = 14)	39.3 (n = 22)	21.4 (n = 12)
	Management	30.3 (n = 10)	27.3 (n = 9)	33.3 (n = 11)	9.1 (n = 3)
5. Use the same password for all websites for consistency and ease	Comp. Sci	48.0 (n = 12)	40.0 (n = 10)	12.0 (n = 3)	0.0 (n = 0)
	Comp. Sec	50.0 (n = 12)	45.8 (n = 11)	0.0 (n = 0)	4.2 (n = 1)
	Comp. For	84.6 (n = 11)	7.7 (n = 1)	0.0 (n = 0)	0.0 (n = 0)
	Legal Studies	50.0 (n = 4)	50.0 (n = 4)	0.0 (n = 0)	0.0 (n = 0)
	Criminology	44.4 (n = 4)	22.2 (n = 2)	22.2 (n = 2)	11.1 (n = 1)
	Crim.Inv	33.3 (n = 9)	48.1 (n = 13)	7.4 (n = 2)	7.4 (n = 2)
	Race/Justice	39.0 (n = 23)	42.4 (n = 25)	10.2 (n = 6)	5.1 (n = 3)
	Economics	32.1 (n = 18)	50.0 (n = 28)	8.9 (n = 5)	3.6 (n = 2)
	Management	72.7 (n = 24)	21.2 (n = 7)	0.0 (n = 0)	6.1 (n = 2)

Note. Comp.Sci = Computer Science, Comp.Sec = Computer Security, Comp. For = Computer Forensics, Legal = Legal Research and Studies, Crim. Inv = Criminal Investigation.

Confidence to Identify Vulnerabilities

As tabulated in Table 4.8, most of the students (95.9 percent) in a technical class as Computer Security *Agree/Strongly Agree* they can identify email scams, 22.2 percent of students in a non-technical class as Criminology *Disagree/Strongly Disagree* on the same. Seventy-seven percent of students from a technical class as Computer Forensics *Agree/Strongly Agree* that they are aware of local and national cyber-attacks, 41.7 percent of students from a non-technical class as Criminology and 48.1 percent of students from Criminal Investigation *Disagree/Strongly Disagree* on the same. While 87.5 percent of students from a technical major as Computer Security *Agree/Strongly Agree* that they are confident of identifying a virus on their personal computer or devices, 32.2 percent of students from a non-technical major as Economics *Disagree/Strongly Disagree* on the same.

Table 4.8

Confidence on identifying/handling security vulnerabilities

Survey Item	Course	Strongly Disagree	Disagree	Agree	Strongly Agree
1. I am confident I can identify email scams	Comp. Sci	0.0 (n = 0)	0.0 (n = 0)	52.0 (n = 13)	48.0 (n = 12)
	Comp. Sec	0.0 (n = 0)	4.2 (n = 1)	54.2 (n = 13)	41.7 (n = 10)
	Comp. For	7.7 (n = 1)	0.0 (n = 0)	38.5 (n = 5)	46.2 (n = 6)
	Legal Studies	0.0 (n = 0)	12.5 (n = 1)	62.5 (n = 5)	25.0 (n = 2)
	Criminology	0.0 (n = 0)	22.2 (n = 2)	55.6 (n = 5)	22.2 (n = 2)

Survey Item	Course	Strongly Disagree	Disagree	Agree	Strongly Agree
	Crim.Inv	3.7 (n = 1)	11.1 (n = 3)	66.7 (n = 18)	14.8 (n = 4)
	Race/Justice	3.4 (n = 2)	11.9 (n = 7)	62.7 (n = 37)	18.6 (n = 11)
	Economics	1.8 (n = 1)	12.5 (n = 7)	51.8 (n = 29)	28.6 (n = 16)
	Management	9.1 (n = 3)	9.1 (n = 3)	51.5 (n = 17)	30.3 (n = 10)
2. I am confident I can identify a virus on my personal computer/devices	Comp. Sci	0.0 (n = 0)	24.0 (n = 6)	40.0 (n = 10)	36.0 (n = 9)
	Comp. Sec	0.0 (n = 0)	12.5 (n = 3)	70.8 (n = 17)	16.7 (n = 4)
	Comp. For	0.0 (n = 0)	7.7 (n = 1)	53.8 (n = 7)	30.8 (n = 4)
	Legal Studies	12.5 (n = 1)	12.5 (n = 1)	62.5 (n = 5)	12.5 (n = 1)
	Criminology	0.0 (n = 0)	33.3 (n = 3)	44.4 (n = 4)	22.2 (n = 2)
	Crim.Inv	0.0 (n = 0)	18.5 (n = 5)	66.7 (n = 18)	11.1 (n = 3)
	Race/Justice	1.7 (n = 1)	28.8 (n = 17)	49.2 (n = 29)	16.9 (n = 10)
	Economics	3.6 (n = 2)	28.6 (n = 16)	44.6 (n = 25)	17.9 (n = 10)

Survey Item	Course	Strongly Disagree	Disagree	Agree	Strongly Agree
	Management	9.1 (n = 3)	12.1 (n = 4)	54.5 (n = 18)	24.2 (n = 8)
3. I am confident I can identify a phishing (fake) email	Comp. Sci	0.0 (n = 0)	4.0 (n = 1)	52.0 (n = 13)	40.0 (n = 10)
	Comp. Sec	0.0 (n = 0)	4.2 (n = 1)	58.3 (n = 14)	37.5 (n = 9)
	Comp. For	0.0 (n = 0)	0.0 (n = 0)	30.8 (n = 4)	61.5 (n = 8)
	Legal Studies	0.0 (n = 0)	0.0 (n = 0)	75.0 (n = 6)	25.0 (n = 2)
	Criminology	0.0 (n = 0)	11.1 (n = 1)	55.6 (n = 5)	33.3 (n = 3)
	Crim.Inv	0.0 (n = 0)	11.1 (n = 3)	66.7 (n = 18)	18.5 (n = 5)
	Race/Justice	0.0 (n = 0)	13.6 (n = 8)	57.6 (n = 34)	25.4 (n = 15)
	Economics	0.0 (n = 0)	10.7 (n = 6)	53.6 (n = 30)	30.4 (n = 17)
	Management	9.1 (n = 3)	12.1 (n = 4)	48.5 (n = 16)	30.3 (n = 10)
4. I am confident that I am aware of local and	Comp. Sci	4.0 (n = 1)	36.0 (n = 9)	32.0 (n = 8)	28.0 (n = 7)

Survey Item	Course	Strongly Disagree	Disagree	Agree	Strongly Agree
national cyber attacks	Comp. Sec	0.0 (n = 0)	29.2 (n = 7)	50.0 (n = 12)	20.8 (n = 5)
	Comp. For	0.0 (n = 0)	15.4 (n = 2)	38.5 (n = 5)	38.5 (n = 5)
	Legal Studies	25.0 (n = 2)	25.0 (n = 2)	50.0 (n = 4)	50.0 (n = 4)
	Criminology	0.0 (n = 0)	41.7 (n = 5)	16.7 (n = 2)	16.7 (n = 2)
	Crim.Inv	14.8 (n = 4)	33.3 (n = 9)	40.7 (n = 11)	7.4 (n = 2)
	Race/Justice	11.9 (n = 7)	35.6 (n = 21)	39.0 (n = 23)	10.2 (n = 6)
	Economics	1.8 (n = 1)	26.8 (n = 15)	42.9 (n = 24)	23.2 (n = 13)
	Management	9.1 (n = 3)	15.2 (n = 5)	45.5 (n = 15)	30.3 (n = 10)

Note. Comp.Sci = Computer Science, Comp.Sec = Computer Security, Comp. For = Computer Forensics, Legal = Legal Research and Studies, Crim. Inv = Criminal Investigation.

Knowledge of Interdisciplinary Application

In response to the knowledge of applying the students' major field of study to the field of cybersecurity, all the students in the technical major as Computer *Agree/Strongly Agree* while 24.3% of students in the Management class and 23.3% of students in the Economics class *Disagree/Strongly Disagree* for the same as tabulated in Table 4.9.

Table 4.9

Knowledge of Interdisciplinary Application (%)

Survey Item	Course	Strongly Disagree	Disagree	Agree	Strongly Agree
I think principles of my major field of study could be applied to Cybersecurity	Comp. Sci	0.0 (n = 0)	0.0 (n = 0)	52.0 (n = 13)	48.0 (n = 12)
	Comp. Sec	0.0 (n = 0)	0.0 (n = 0)	29.2 (n = 7)	70.8 (n = 17)
	Comp. For	0.0 (n = 0)	0.0 (n = 0)	15.4 (n = 2)	76.9 (n = 10)
	Legal	0.0 (n = 0)	12.5 (n = 1)	25.0 (n = 2)	62.5 (n = 5)
	Criminology	0.0 (n = 0)	33.3 (n = 3)	66.7 (n = 6)	0.0 (n = 0)
	Crim.Inv	0.0 (n = 0)	11.1 (n = 3)	63.0 (n = 17)	22.2 (n = 6)
	Race/Justice	0.0 (n = 0)	13.6 (n = 8)	57.6 (n = 34)	25.4 (n = 15)
	Economics	5.4 (n = 3)	17.9 (n = 10)	51.8 (n = 29)	19.6 (n = 11)
	Management	6.1 (n = 2)	18.2 (n = 6)	42.4 (n = 14)	33.3 (n = 11)

Note. Comp.Sci = Computer Science, Comp.Sec = Computer Security, Comp. For = Computer Forensics, Legal = Legal Research and Studies, Crim. Inv = Criminal Investigation.

Interest towards a Cyber Career

As tabulated in Table 4.10, a higher number of students in the technical majors as Computer Science (68.0 percent) and Information Technology (61.6 percent)

Disagree/Strongly Disagree to become a part of the growing cyber workforce, 33.3 percent of students in the Criminology class, 44.4 percent of students in the Criminal Investigation class, 42.4 percent of students in the Economics class and 45.4 percent of students in the Management *Agree/Strongly Agree* to pursue a career in given the desired knowledge and skills.

Interest to Pursue a Minor in Cybersecurity

As tabulated in Table 4.11, a higher number of students in technical majors as Computer Science (76.0 percent) and Information technology (75.0 percent) *Disagree/Strongly Disagree* to pursue a minor in cybersecurity, 62.5 percent of students in each of Legal Studies and Economics classes, 55.5 percent of students from Criminology and 45.4 percent of students from Management expressed a strong interest toward it.

Table 4.10

Interest towards a Cyber Career (%)

Survey Item	Course	Strongly Disagree	Disagree	Agree	Strongly Agree
Given the necessary skills and training, I desire to become a part of the growing cybersecurity workforce and contribute the knowledge gained through my coursework	Comp. Sci	28.0 (n = 7)	40.0 (n = 10)	24.0 (n = 6)	8.0 (n = 2)
	Comp. Sec	16.7 (n = 4)	66.7 (n = 16)	0.0 (n = 0)	16.7 (n = 4)
	Comp. For	38.5 (n = 5)	23.1 (n = 3)	7.7 (n = 1)	23.1 (n = 3)
	Legal	12.5 (n = 1)	25.0 (n = 2)	50.0 (n = 4)	12.5 (n= 1)
	Criminology	22.2 (n = 2)	44.4 (n = 4)	22.2 (n = 2)	11.1 (n = 1)
	Crim.Inv	7.4 (n = 2)	44.4 (n = 12)	37.0 (n = 10)	7.4 (n = 2)
	Race/Justice	10.2 (n = 6)	44.1 (n = 26)	39.0 (n = 23)	3.4 (n = 2)
	Economics	7.1 (n = 4)	46.4 (n = 26)	39.3 (n = 22)	1.8 (n = 1)
	Management	27.3 (n = 9)	27.3 (n = 9)	33.3 (n = 11)	12.1 (n = 4)

Note. Comp.Sci = Computer Science, Comp.Sec = Computer Security, Comp. For = Computer Forensics, Legal = Legal Research and Studies, Crim. Inv = Criminal Investigation.

Table 4.11

Interest to Pursue a Minor in Cybersecurity (%)

Survey Item	Course	Strongly Disagree	Disagree	Agree	Strongly Agree
I would consider pursuing a minor in Cybersecurity to know more about the fundamental concepts in securing information systems	Comp. Sci	24.0 (n = 6)	52.0 (n = 13)	16.0 (n = 4)	8.0 (n = 2)
	Comp. Sec	41.7 (n = 10)	33.3 (n = 8)	8.3 (n = 2)	16.7 (n = 4)
	Comp. For	30.8 (n = 4)	30.8 (n = 4)	7.7 (n = 1)	23.1 (n = 3)
	Legal	25.0 (n = 2)	12.5 (n = 1)	62.5 (n = 5)	0.0 (n = 0)
	Criminology	22.2 (n = 2)	22.2 (n = 2)	44.4 (n = 4)	11.1 (n = 1)
	Crim.Inv	3.7 (n = 1)	40.7 (n = 11)	40.7 (n = 11)	11.1 (n = 3)
	Race/Justice	8.5 (n = 5)	33.9 (n = 20)	42.4 (n = 25)	11.9 (n = 7)
	Economics	5.4 (n = 3)	26.8 (n = 15)	51.8 (n = 29)	10.7 (n = 6)
	Management	24.2 (n = 8)	30.3 (n = 10)	33.3 (n = 11)	12.1 (n = 4)

Note. Comp.Sci = Computer Science, Comp.Sec = Computer Security, Comp. For = Computer Forensics, Legal = Legal Research and Studies, Crim. Inv = Criminal Investigation.

Research Question Two

Research Question Two**,** *Is there a statistically significant mean difference in participants' perception of security behaviors before and after the intervention?,* was answered by students from technical and non-technical majors. Three sets of security behaviors were tested as part of this research question. The security behaviors that guided these tests are as follows: (a) Perception of protection measures against viruses, (b) Perception of frequency of protection measures, and (c) Perception of Password practices.

Perception of Protection Measures against Viruses

This consists of 5-items rated on a 4-point Likert scale (*Strongly Disagree, Disagree, Agree, and Strongly Agree*) presented in Table 4.12.

Table 4.12

Items for Protective Measures against Viruses

One can protect themselves from viruses by keeping the anti-virus up to date
One can protect themselves from viruses by blocking pop-ups
One can protect themselves from viruses by being aware of what websites are visited
One can protect themselves from viruses by not clicking on email attachments from people you do not know.
One can protect themselves from viruses by keeping the anti-virus up to date

The paired samples t-test indicated a *p-value* of 0.001. The results are presented in Table 4.13. Findings suggest that the perception of the respondents towards protection measures against viruses had changed before and after the intervention, $t(220) = 4.11$, $p = 0.001$. The post survey data reported a higher mean (M = 17.2) than the pre-survey mean (M =16.5) for the items pertaining to the protective measures against viruses.

Table 4.13

Perception of Protection Measures against Viruses

Security Behaviors	N	M	SD	t-value	df	*p*-value	d	r^2
Protection_pre	220	16.5	2.3	4.11	199	<0.001*	0.58	0.279
Protection_post	220	17.2	2.5					

*Statistically significant (p < .05)

Frequency of Protection Measures

This consists of 3-items rated on a 5-point Likert scale (*Never, Rarely, Sometimes, Often, Always)* presented in Table 4.14. The paired samples t-test indicated a p-value of 0.081. The results are displayed in Table 4.15. Findings suggest that the perception of the respondents towards the frequency of protection measures against viruses changed before and after the intervention, $t(220) = 4.23$, $p = 0.081$. The post survey data reported a higher mean (M = 14.3) than the pre-survey mean (M =13.2).

Table 4.14

Perception of Frequency of Protection Measures

How often do you scan the computer with Anti-virus software?
How often do you use anti-virus software?
How often do you use security software such as a firewall?

Table 4.15

Perception of Frequency of Protection Measures

Security Behaviors	N	M	SD	*t*-value	df	*p*-value	d	r^2
Frequency_protection_pre	220	13.2	4.9	4.235	202	0.081*	0.62	0.489
Frequency_protection_post	220	14.3	4.6					

*Statistically significant ($p < .05$)

Perception of Password Practices

This consists of 5-items rated on a 4-point Likert scale (*Strongly Disagree, Disagree, Agree, and Strongly Agree*) presented in Table 4.16. The paired samples t-test indicated a *p-value* of 0.002. The results are presented in Table 4.17. Findings suggest that the perception of the respondents the repostowards password practices changed before and after the intervention, $t(220) = 4.01$, $p = 0.081$. The post survey data reported a higher mean (M = 13.2) than the pre-survey mean (M =12.0).

Table 4.16

Items for Perception of Password Practices

Use 'admin' and 'root' or 'administrator' as passwords
Write the password down so you can look it up when you forget
A password must be a good mixture of upper case, lower case letters, numbers and special characters
Change your password once in a few years
Use the same password for all websites for consistency and ease

Table 4.17

Perception of Password Practices

Security Behaviors	N	M	SD	*t*-value	df	*p*-value	d	r^2
Password_practice_pre	220	12	2.5	4.01	199	0.002*	0.5	0.081
Password_practice_post	220	13.2	2.6					

*Statistically significant ($p < .05$)

Research Question Three

Research Question Three**,** *Is there a statistically significant mean difference in participants' perception of security beliefs before and after the intervention,* was answered by students from technical and non-technical majors. Two sets of security beliefs were tested as part of this research question. The security beliefs that guided these tests are as follows: (a) Perception of Hacker Beliefs, (b) Perceptions of Virus Beliefs

Perception of Hacker Beliefs

This consists of 5-items rated on a 4-point Likert scale (*Strongly Disagree, Disagree, Agree, and Strongly Agree*) presented in Table 4.18. The paired samples t-test indicated a *p-value* of 0.006. The results are presented in Table 4.19. Findings suggest that the perception of the respondents towards hacker beliefs changed before and after the intervention, $t(220) = 4.12$, $p = 0.006$. The post survey data reported a higher mean (M = 12.0) than the pre-survey mean (M =14.7).

Table 4.18

Items for Perception of Hacker Beliefs

Hackers could watch what I am doing on my computer
Hackers could intentionally put viruses on the computer
Hackers could record everything on the computer
Hackers could target only home computer users

Table 4.19

Hacker Beliefs

Security Behaviors	N	M	SD	*t*-value	df	*p*-value	d	r^2
Hacker_beliefs_pre	220	12	2.5	4.12	199	0.006*	0.6	0.244
Hacker_beliefs_post	220	14.7	2.6					

*Statistically significant ($p < .05$)

Perception of Virus Beliefs

This consists of 5-items rated on a 4-point Likert scale (*Strongly Disagree, Disagree, Agree, and Strongly Agree*) presented in Table 4.20. The paired samples t-test indicated a *p-value* of 0.011. The results are presented in Table 4.21. Findings suggest that the perception of the respondents towards virus beliefs had a significant change before and after the intervention, $t(220) = 4.12$, $p = 0.006$. The post survey data reported a relatively higher mean (M = 12.8) to that of the pre-survey mean (M =11.0).

Table 4.20

Items for Perception of Virus Beliefs

A virus causes computers to crash
A virus causes annoying problems
A virus erases important files on the computer
A virus steals personal/financial information
A virus can be avoided by being aware of which websites I go to

Table 4.21

Virus Beliefs

Security Behaviors	N	M	SD	*t*-value	df	*p*-value	d	r^2
Virus_beliefs_pre	220	11	2.3	4.22	199	0.007*	0.6	0.244
Virus_beliefs_post	220	12.8	2.5					

*Statistically significant ($p < .05$)

Conclusion

This chapter presented the quantitative analysis of the data collected from the surveys, participant demographics and processes of answering each of the research question. In the next chapter, findings will be presented to compare what was found through this study with existing literature. Implications of this study and future research will also be discussed.

CHAPTER V

SUMMARY, IMPLICATIONS, AND RECOMMENDATIONS

The purpose of this study is to examine the relationship between existing knowledge in security (beliefs versus behaviors), awareness of threats and vulnerabilities and the interest fostered towards an interdisciplinary approach in education and/or career from students across technical and non-technical majors. Participant demographics was enumerated in the previous chapter. Around 228 students participated in the survey, which was administered to classes across six different disciplines namely Criminology, Legal Studies, Management, Computer Science, Information Technology and Economics. This chapter presents the data analysis for each of the three research questions. It concludes with a summary of the findings. Within this chapter, the findings of this study are contextualized in the larger body of research literature. Implications as well as recommendations for future research are also included.

Summary

The following research questions guided the study with respect to understanding the different types of security behaviors and beliefs and measure the interest garnered towards an academic or career pathway in cybersecurity.

1. To what extent students from technical and non-technical majors perceive cybersecurity?
2. Is there a statistically significant mean difference in participants' perception of security behaviors?
3. Is there a statistically significant mean difference in participants' perception of security beliefs?

Security behaviors and beliefs were assessed individual in the survey. While security behaviors spanned questions related to security concerns on the internet,

protection from viruses, frequency of taking the necessary defensive actions against viruses, and password practices.

Research Question One

Security Concern

In general, the perceptions of internet users' security and trust have strong impacts on carrying out their day to day activities online. In terms of concern for their security on the internet, the results of the analysis demonstrate that the users' perceptions generally meet the expectation of their security concerns and lean towards the secure side. With respect to understanding the level of concerns between students from technical and non-technical majors, it is understood from the data that, students from technical majors were less unconcerned about their security on the internet than the students from the non-technical majors.

While only 9% of students from technical majors expressed their unconcern over their security on the internet, more than 25% of students from the non-technical majors expressed the same. Specifically, to denote, students from Criminal Investigation and Management classes peaked in numbers on the security concerns. This is of significance because from the demographics of internet usage, students from Criminology and Management topped the table.

This helps us understand that a relatively average number of students from the non-technical majors are susceptible to the attack of internet usage due to their expressed unconcern. This is also posited by Shropshire et al. [46], that there is a strong connection between the intent to comply with security rules and the traits of agreeableness and conscientiousness which means that accurate knowledge of security concerns would have been influenced by past experiences of making security decisions and executing the same.

Research Question Two

Protection from Viruses and Frequency of Defensive Actions

The sets of questions catered to understand the perception of the respondents in terms of their security behaviors are of concern in this section. This helped understand the types of security behaviors that participants exhibited. The actions were clustered into two categories – Behaviors that place trust-in-software and behaviors that trust-in-self.

While respondents in the first cluster agreed to have their anti-virus, firewall and security products up to date, most of the students from the technical and the non-technical majors claimed to do this to protect their devices against hackers. The second cluster of behaviors place trust in themselves, about their restraint to accessing websites, and carefulness to open email attachment or click on malicious downloads. 69.1% of the students fell in this category.

It is also of note that a statistical significance was observed from the pre and post survey data implying that the respondent's perceptions about defensive actions against viruses were changed. A statistical significance of 0.001 was obtained (Table 4.11).

Password Practices

Passwords are a key part of many security technologies and they are the most commonly used authentication method. For a password system to be secure, users must make conscious decisions about what passwords to use and where to re-use passwords.

From the results of the analysis, 33.3% of students from Criminology agree that they would use the same passwords for all the websites for consistency and ease while 66.6% of students in the Management class agreed to write down the passwords in some form, so they can look it up. This exhibits a sheer contradiction to the best practice in the field that passwords must be long, random and unique to each account. In this regard, Das et al. [47] estimated that 43-51% of user's re-use passwords across accounts and Ur et al.

[48] denotes that people re-use passwords because they have never personally experienced negative consequences stemming from re-use. This sheds some serious concern on incorporating and educating student of novel password practices.

Research Question Three

Virus Beliefs

This factor that is also categorized under research question one includes four different factors about viruses, namely, viruses causes computers to crash, viruses cause annoying problems, viruses erase important files on the computers and a virus can be avoided by being aware of which websites to go to. Most of the students express a strong concern about the malicious nature of viruses. This is precisely due to the attitude that they group all malicious software under "virus". Beliefs about how the viruses operate are likely to have an impact on the decisions that people make in order to protect their computers. This means that the users' beliefs about viruses and their protective measures to defend their devices against the same are directly correlated with each other. This was also evident through the bivariate Pearson Correlation coefficient that was derived between the virus beliefs and the protective actions against viruses, covered in Research Question Two. The population correlation coefficient ρ, was calculated to be 5.5, posits a perfectly positive linear relationship between both the factors.

A paired sample t-test performed between the composites of the pre and the post-survey data reveals there exists a statistical significance (Table 4.15) between the data. The statistically significant p-value refutes the null hypothesis that there is no relationship in users' perception of virus beliefs before and after the intervention that was administered as part of the survey. Post the intervention, it is observed that the respondents leaned more on the positive side of virus beliefs.

In specific, 24% of students from an undergraduate Computer Science class expressed a strong disagreement that, it is not necessary to be aware of the websites that are visited, in order to be protective of viruses. However, the intervention addressed some of the key concerns of unsecure websites and the strategies employed by hackers to exploit information from such websites. In the post-survey, there is less than 3% of students who polled for the same attitude. This posits a positive attitudinal difference in the way security is approached in website usage.

Hacker Beliefs

This factor that is also categorized under research question one includes five different factors about hackers, namely, hackers could watch what I am doing on my computer, hackers could intentionally put viruses on the computer, hackers could record everything on the computer and hackers could target only home computer users. While most of the users agree that hackers can monitor activity, most of them also believe that hackers target only home computer users.

From the data obtained in general about hacker beliefs, a close relationship is established between hacker beliefs and the defensive actions taken which are categorized as trust-in-software action, trust-in-self action and expert actions. The questions catered towards these actions are presented in Research Question Two. This implies that the more concerned students are about being hacked, the more effort they would be ready to take to protect themselves.

This is also evident from the statistically significant relationship that was proved through the Paired Sample T-Test as tabulated in Table 4.14. The statistically significant p-value refutes the null hypothesis that there is no relationship in users' perception of hacker beliefs before and after the intervention that was administered as part of the

survey. Post the intervention, it is observed that the respondents leaned more on the positive side of hacker beliefs.

Implications

As a result of this study about student's perceptions about security concerns, behaviors and attitudes, the following implications and recommendations are discussed in the below section.

Implications for Cybersecurity Awareness

There has been an exponential increase in the usage of internet, particularly among millennials and older generation. A fact sheet from the Pew Research Center [11] quotes that "Millennials have often led older Americans in their adoption and use of technology and this largely holds true today. But there has also been a significant growth in tech adoption in recent years among older generations". This denotes how reliance on internet usage in fulfilling personal and academic tasks demonstrates a paradigm shift. However, this increasing global population is one of the main contributing factors to changes in cyber threats.

In coping with the cyber threat landscape that has transitioned from the use of savvy hacking skills to sophisticated and well-planned strategies, cybersecurity awareness is deemed essential for internet users like youngsters as a counter-measure strategy to combat silent privacy invasion.

Cybersecurity awareness is defined as a methodology to educate internet users to be sensitive to the various cyber threats and the vulnerabilities of computers and data to these threats. Shaw et al. [49] defines cybersecurity as, "the degree of users' understanding about the importance of information security, and their responsibilities to exercise sufficient levels of information control to protect the organization's data and networks". These definitions help imply two significant things, alerting internet users of

cybersecurity issues and threats, and enhancing internet users' understanding of cyber threats so they can be fully committed to embracing securing during internet use.

From the analysis of the data gathered, a significant understanding of the security culture among students from technical and non-technical majors are understood. This forms the foundation for the design and development of a cybersecurity awareness program that enhances a security culture, reduces their lackadaisical attitude that causes them to be the weakest link in the security chain. This program must be tailored in a customized way to tailor the needs of target audiences depending on their background in security knowledge, behavior, mind-set towards online protection etc. Deployment of such a program across diverse disciplines and majors helps educate students on how to address specific threats and increases their resilience in defensive actions against them.

Implications for Interdisciplinary Collaboration

From the results of the analysis, students from non-technical majors that have a close association with the field of cybersecurity, expressed a higher interest to further their knowledge by pursuing a minor in Cybersecurity. This denotes that there is potential space for a collaborative program in cybersecurity that spans across disciplines and that encourages collaboration in areas as business, economics, public policy, criminology and even journalism.

Interdisciplinary cybersecurity programs provide multi-faceted learning by providing education in cybersecurity defense and countermeasures and training students in management, governance, and policy aspects of cybersecurity [48]. From a defense perspective, students acquire skills necessary to protect computer systems, networks, and online data from attack and compromise through courses that focus on computer science, computer engineering and Information technology. Coursework in cybersecurity analysis of vulnerabilities and threats to network environments offers students with skills required

in information technology technical project management. Law and criminal justice courses like cybercrime combined with digital forensics and courses from accounting and psychology make students a well- rounded product for the industry to absorb. The holistic perspective gained through such interdisciplinary training enables students to understand cybersecurity from a governance and management standpoint while possessing the necessary technical skills [48].

Recommendations for Future Research

Findings from this study involved obtaining feedback from students. Although the findings provided data and information about students' perceptions, recommendations for future research will help expand the knowledge on this topic. The following recommendations are based on data and findings from this study.

Firstly, the study was administered to ten classes spanning different disciplines and subject matter. The mode of research design employed was a quantitative study. For future research directives could focus on employing diverse research methodologies (Qualitative analysis and focus groups) and triangulate the analyses in order to obtain a higher precision on the user perspectives.

Conclusion

This study has significantly contributed to understanding the contribution of different disciplines to the field of cybersecurity and gather interest towards a holistic interdisciplinary understanding of the same. Further, a glance of the state of interdisciplinary cybersecurity education in the United States was provided along with contributing theories from disciplines closely related to cybersecurity. Finally, a quantitative study was conducted to understand user perceptions and draw significant attention to the current state of the dearth of security awareness that implies the need for an effective program for students in the technical and non-technical majors.

REFERENCES

[1] N. E. Insight. (2017, 9th May, 2018). *THE CYBERSECURITY THREAT - FIGHTING BACK*. Available: http://www.newsweek.com/insights/leading-cybersecurity-programs-2017

[2] S. Morgan. (2018, May 5th, 2018). *Top 5 cybersecurity facts, figures and statistics for 2018*. Available: https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html

[3] B. C. S.Donovan, M.Daniel, and T.Scott, "Strengthening the Federal Cybersecurity Workforce," in *Strengthening the Federal Cybersecurity Workforce*, ed: Obama White House, 2016.

[4] J. Peeler, Management, "(ISC)² Study: Workforce Shortfall Due to Hiring Difficulties Despite Rising Salaries, Increased Budgets and High Job Satisfaction Rate", (ISC)² Blog, 2018. [Online]. Available: http://blog.isc2.org/isc2_blog/2015/04/isc-study-workforce-shortfall-due-to-hiring-difficulties-despite-rising-salaries-increased-budgets-a.html. [Accessed: 10- Apr- 2018].

[5] M. v. Zadelhoff. (2017, 9th May 2018). *Cybersecurity Has a Serious Talent Shortage. Here's How to Fix It*. Available: https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it

[6] P. McNeice, "PAYSCALE AND FUTURE WORKPLACE RELEASE 2016 WORKFORCE-SKILLS PREPAREDNESS REPORT," 2016, Available:

https://www.payscale.com/about/press-releases/payscale-and-future-workplace-release-2016-workforce-skills-preparedness-report.

[7] B. R. Group, "Cybersecurity Preparedness Benchmarking Study Report," Online Source 2016, Available: https://ecommunications.thinkbrg.com/10/218/uploads/cspbs-report.pdf, Accessed on: 19th September, 2017.

[8] Statista. *U.S. government and cyber crime - Statistics & Facts*. Available: https://www.statista.com/topics/3387/us-government-and-cyber-crime/

[9] T. J. Holt, *Cybercrime Through an Interdisciplinary Lens*. Taylor & Francis, 2016.

[10] R. B. Ramirez, "Making cyber security interdisciplinary: recommendations for a novel curriculum and terminology harmonization," Massachusetts Institute of Technology, 2017.

[11] "Internet/Broadband Fact Sheet," 2018, Available: http://www.pewinternet.org/fact-sheet/internet-broadband/.

[12] T. Way and S. Whidden, "A Loosely-Coupled Approach to Interdisciplinary Computer Science Education," in *Proceedings of the International Conference on Frontiers in Education: Computer Science and Computer Engineering (FECS)*, 2014, p. 1: The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[13] W. A. Conklin, R. E. Cline, and T. Roosa, "Re-engineering cybersecurity education in the us: An analysis of the critical factors," in *System Sciences (HICSS), 2014 47th Hawaii International Conference on*, 2014, pp. 2006-2014: IEEE.

[14] S. Ghernouti-Hélie, "A National Strategy for an Effective Cybersecurity Approach and Culture", 2010 International Conference on Availability, Reliability and Security, 2010.

[15] N. Choucri, S. Madnick, and J. Ferwerda, "Institutions for Cyber Security: International Responses and Global Imperatives," *Information Technology for Development,* vol. 20, no. 2, pp. 96-121, 2014/04/03 2014.

[16] NIST, NICE Cybersecurity Workforce Framework Tutorial. National Initiative for Cybersecurity Education, 2018.

[17] Y. Cai and T. Arney, "Cybersecurity Should be Taught Top-Down and Case-Driven," presented at the Proceedings of the 18th Annual Conference on Information Technology Education, Rochester, New York, USA, 2017

[18] "NSF awards $74.5 million to support interdisciplinary cybersecurity research," ed, 2015.

[19] "ITU Global Cybersecurity Agenda," Geneva2017, Available: https://www.intgovforum.org/Substantive_2nd_IGF/ITU_GCA_E.pdf.

[20] L. J. Hoffman, D. Burley, and C. Toregas, "Thinking across stovepipes: Using a holistic development strategy to build the cybersecurity workforce," *IEEE Security and Privacy*, vol. 1, p. 13, 2011.

[21] K.-K. R. Choo, "A conceptual interdisciplinary plug-and-play cyber security framework," in *ICTs and the Millennium Development Goals*: Springer, 2014, pp. 81-99.

[22] Symantec Enterprises, "2018 Internet Security Threat Report," 2018, Available: https://www.symantec.com/security-center/threat-report.

[23] S. S. Tirumala, A. Sarrafzadeh, and P. Pang, "A survey on Internet usage and cybersecurity awareness in students," in *Privacy, Security and Trust (PST), 2016 14th Annual Conference on*, 2016, pp. 223-228: IEEE.

[24] G. Reid. (2018). *How Many Internet Users Will The World Have In 2022, And In 2030?* Available: https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/

[25] S. Mittal, "Understanding the Human Dimension of Cyber Security," *Indian Journal of Criminology & Criminalistics*, vol. Vol .34, pp. p.141-152, 2016.

[26] M. T. Siponen and H. Oinas-Kukkonen, "A review of information security issues and respective research contributions," *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, vol. 38, no. 1, pp. 60-80, 2007.

[27] K. Jaishankar, "Establishing a theory of cyber crimes," *International Journal of Cyber Criminology*, vol. 1, no. 2, pp. 7-9, 2007.

[28] T. J. Holt, G. W. Burruss, and A. M. Bossler, "Social learning and cyber-deviance: Examining the importance of a full social learning model in the virtual world," *Journal of Crime and Justice*, vol. 33, no. 2, pp. 31-61, 2010.

[29] T. C. Pratt, K. Holtfreter, and M. D. Reisig, "Routine online activity and internet fraud targeting: Extending the generality of routine activity theory," *Journal of Research in Crime and Delinquency*, vol. 47, no. 3, pp. 267-296, 2010.

[30] S. Borg, "Economically complex cyberattacks," *IEEE security & privacy*, vol. 3, no. 6, pp. 64-67, 2005

[31] A. Wilk, "Cyber Security Education and Law," in *Software Science, Technology and Engineering (SWSTE), 2016 IEEE International Conference on*, 2016, pp. 94-103: IEEE.

[32] D. Jacobson, J. Rursch, and J. Idziorek, "Security across the curriculum and beyond," in *Proceedings of the 2012 IEEE Frontiers in Education Conference (FIE)*, 2012, pp. 1-6: IEEE Computer Society.

[33] B. D. Caulkins, K. Badillo-Urquiola, P. Bockelman, and R. Leis, "Cyber workforce development using a behavioral cybersecurity paradigm," *International Conference on Cyber Conflict (CyCon U.S.)*, pp. 1-6, 2016.

[34] “Education - Risk Manager Core Competency Model", RIMS - The Risk Management Society, 2018. [Online]. Available: https://www.rims.org/education/Pages/RiskManagerCoreCompetencyModel.aspx. [Accessed: 10- Apr- 2018].

[35] M. Maguire Shultz and S. Zedeck, "Final Report - Identification, Development and Validation of Predictors for Successful Lawyering", SSRN Electronic Journal, 2009.

[36] *National Initiative for Cybersecurity Careers and Studies*. Available: https://niccs.us-cert.gov/

[37] Johanna Jacob, Wei Wei, Kewei Sha, Sadegh Davari, T. Andrew Yang, "Is The NICE Cybersecurity Workforce Framework (NCWF) Effective For A Workforce Comprised Of Interdisciplinary Majors? ," *Int'l Conf. Scientific Computing, CSC'18*, 2018.

[38] R. Ramirez and N. Choucri, "Improving Interdisciplinary Communication With Standardized Cyber Security Terminology: A Literature Review", IEEE Access, vol. 4, pp. 2216-2243, 2016.

[39] L. Hoffman, D. Burley and C. Toregas, "Holistically Building the Cybersecurity Workforce", IEEE Security & Privacy Magazine, vol. 10, no. 2, pp. 33-39, 2012

[40] X. Liu and D. Murphy, "Engaging females in cybersecurity: K through Gray," in *Intelligence and Security Informatics (ISI), 2016 IEEE Conference on*, 2016, pp. 255-260: IEEE.

[41] National Security Agency, "CAE CDE Criteria - 2019," 2018, Available: https://www.iad.gov/NIETP/CAERequirements.cfm.

[42] B. Technologies and B. Technologies, "Production Skills Gap | Burning Glass Technologies", Burning Glass Technologies, 2018. [Online]. Available: https://www.burning-glass.com/researchproject/production-skills-gap/. [Accessed: 10- Apr2018].

[43] CISCO, "Cisco 2017 Midyear Cybersecurity Report," 2017, Available: www.cisco.com/c/dam/global/es_mx/solutions/security/pdf/cisco-2017-midyear-cybersecurity-report.pdf.

[44] A. Rege, "Multidisciplinary experiential learning for holistic cybersecurity education, research and evaluation," *USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*, 2015

[45] A. Fink and M. S. Litwin, *How to assess and interpret survey psychometrics*. Sage, 2003.

[46] N. H. A. Rahim, S. Hamid, M. L. Mat Kiah, S. Shamshirband, and S. Furnell, "A systematic review of approaches to assessing cybersecurity awareness," *Kybernetes*, vol. 44, no. 4, pp. 606-622, 2015.

[47] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang. The Tangled Web of Password Reuse. In 12 Proceedings of the 2014 Network and Distributed System Security Symposium (NDSS), 2014.

[48] W. Melicher, B. Ur, S. M. Segreti, S. Komanduri, L. Bauer, N. Christin, and L. F. Cranor. Fast, lean and accurate: Modeling password guessability using neural networks. In Proceedings of USENIX Security, 2016

[49] C. C. Chen, R. Shaw, and S. C. Yang, "Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system," *Information Technology, Learning & Performance Journal*, vol. 24, no. 1, 2006.

[50] G. C. C. Centre. (2018, 9th October, 2018). *Global Cybersecurity Education – Lessons from the CMM*. Available: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/global-cybersecurity-education-%E2%80%93-lessons-cmm

[51] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining cybersecurity," *Technology Innovation Management Review*, vol. 4, no. 10, 2014.

[52] B. C. S.Donovan, M.Daniel, and T.Scott, "Strengthening the Federal Cybersecurity Workforce," in *Strengthening the Federal Cybersecurity Workforce*, ed: Obama White House, 2016.

[53] I. Douglas, "Blitzkrieg education: Finding a system for transforming education," in *Information Technology Based Higher Education and Training (ITHET), 2012 International Conference on*, 2012, pp. 1-5: IEEE.

[54] A. Setalvad, "Demand to fill cybersecurity jobs booming - Peninsula Press", Peninsula Press, 2018. [Online]. Available:

http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/. [Accessed: 10-Apr- 2018]

APPENDIX A

INTEGRATED APPROACH TO CYBERSECURITY EDUCATION (PRE-SURVEY)

Welcome to the research study!

We are interested in understanding the level of awareness, user security and interest gathered in an interdisciplinary program in cybersecurity education. You will be presented with information relevant to user awareness, good security practices and asked to answer some questions about it. Please be assured that your responses will be kept completely confidential.

The study should take you around 10 minutes to complete, and you will receive no incentive for your participation. Your participation in this research is voluntary. You have the right to withdraw at any point during the study, for any reason, and without any prejudice. If you would like to contact the Faculty Sponsor in the study to discuss this research, please e-mail Dr. T. Andrew Yang at yang@uhcl.edu.

By clicking the button below, you acknowledge that your participation in the study is voluntary, you are 18 years of age, and that you are aware that you may choose to terminate your participation in the study at any time and for any reason.

Please note that this survey will be best displayed on a laptop or desktop computer or a mobile device.

- ○ I consent, begin the study
- ○ I do not consent, I do not wish to participate

Q1 Enter your student ID

_____

Q2 I am majoring in :

- ○ Criminology
- ○ Legal Studies
- ○ Management
- ○ Economics
- ○ Computer Science/Computer Engineering/Information Technology
- ○ Other _____

Q3 In general, how concerned are you about your security on the internet (e.g., people reading your email or finding out what websites you visit). Keep in mind that "security" means privacy, confidentiality and/or proof of identity for you or someone else

- ○ Not at all concerned
- ○ Slightly concerned
- ○ Somewhat concerned
- ○ Very concerned

Q4 A virus...

	Strongly Disagree	Disagree	Agree	Strongly agree
causes computers to crash	○	○	○	○
causes annoying problems	○	○	○	○
erases important files on the computer	○	○	○	○
steals personal/financial information	○	○	○	○
can be avoided by being aware of which websites I go to	○	○	○	○

Q5 One can protect themselves from viruses by...

	Strongly Disagree	Disagree	Agree	Strongly Agree
keeping the anti-virus up-to date	○	○	○	○
never downloading anything from the internet	○	○	○	○
blocking pop-ups	○	○	○	○
being aware of what websites are visited	○	○	○	○
not clicking on email attachments from people you do not know	○	○	○	○

Q6 How often do you do the following?

	Never	Rarely	Sometimes	Often	Always
update Anti-virus software	○	○	○	○	○
regularly scan the computer with Anti-virus software	○	○	○	○	○
use anti-virus software	○	○	○	○	○
use security software such as a firewall	○	○	○	○	○

Q7 In general, hackers...

	Strongly Disagree	Disagree	Agree	Strongly agree
watch what I am doing on my computer	○	○	○	○
intentionally put viruses on the computer	○	○	○	○
record everything on the computer	○	○	○	○
target only home computer users	○	○	○	○

Q8 One should consider the following with respect to utilizing password techniques

	Strongly Disagree	Disagree	Agree	Strongly agree
Use 'admin' and 'root' or 'administrator' as passwords	○	○	○	○
Write it down so you can look it up when you forget	○	○	○	○
A good mixture of upper case, lower case letters, digits and punctuation	○	○	○	○
Change once in a few years	○	○	○	○
Use the same password for all websites for consistency and ease	○	○	○	○

Q9 I am confident...

	Strongly disagree	Disagree	Agree	Strongly agree
I can identify email scams	○	○	○	○
I can identify a virus on my personal computer/devices	○	○	○	○
I can identify a phishing (fake) email	○	○	○	○
I am aware of local and national cyber attacks	○	○	○	○

Q10 I think principles of my major field of study could be applied to Cybersecurity

- ○ Strongly Disagree
- ○ Disagree
- ○ Agree
- ○ Strongly agree

Q11 Given the necessary skills and training, I desire to become a part of the growing cybersecurity workforce and contribute the knowledge gained through my coursework

- ○ Strongly agree
- ○ Agree
- ○ Disagree
- ○ Strongly disagree

Q12 I would consider pursuing a minor in Cybersecurity to know more about fundamental concepts in securing information and systems

- ○ Strongly agree
- ○ Agree
- ○ Disagree
- ○ Strongly disagree

Q13 The number of hours I spend online everyday fulfilling academic tasks

_____

Q14 The number of hours I spend online everyday fulfilling personal tasks

_____

Q15 What is your gender?

- Male
- Female
- Other
- Do not wish to specify

Q16 Please specify your race/ethinicity

- White
- Hispanic or Latino
- Black or African American
- Native American or American Indian
- Asian/Pacific Islander
- two or more races
- Other

Q17 What is your age?

- 18-24
- 25-34
- 35-44
- 45-54
- 55-64
- Above 64

APPENDIX B

INTEGRATED APPROACH TO CYBERSECURITY EDUCATION (POST-SURVEY)

Welcome to the research study!

We are interested in understanding the level of awareness, user security and interest gathered in an interdisciplinary program in cybersecurity education. You will be presented with information relevant to user awareness, good security practices and asked to answer some questions about it. Please be assured that your responses will be kept completely confidential.

The study should take you around 10 minutes to complete, and you will receive no incentive for your participation. Your participation in this research is voluntary. You have the right to withdraw at any point during the study, for any reason, and without any prejudice. If you would like to contact the Faculty Sponsor in the study to discuss this research, please e-mail Dr. T. Andrew Yang at yang@uhcl.edu.

By clicking the button below, you acknowledge that your participation in the study is voluntary, you are 18 years of age, and that you are aware that you may choose to terminate your participation in the study at any time and for any reason.

Please note that this survey will be best displayed on a laptop or desktop computer or a mobile device.

- ○ I consent, begin the study
- ○ I do not consent, I do not wish to participate

Q1 Enter your Student ID

_____

Q2 I am majoring in :

- ○ Criminology
- ○ Legal Studies
- ○ Management
- ○ Economics
- ○ Computer Science/Computer Engineering/Information Technology
- ○ Other _____

Q3 In general, how concerned are you about your security on the internet (e.g., people reading your email or finding out what websites you visit). Keep in mind that "security" means privacy, confidentiality and/or proof of identity for you or someone else

- ○ Not at all concerned
- ○ Slightly concerned
- ○ Somewhat concerned
- ○ Very concerned

Q4 A virus...

	Strongly Disagree	Disagree	Agree	Strongly agree
causes computers to crash	○	○	○	○
causes annoying problems	○	○	○	○
erases important files on the computer	○	○	○	○
steals personal/financial information	○	○	○	○
can be avoided by being aware of which websites I go to	○	○	○	○

Q5 One can protect themselves from viruses by...

	Strongly Disagree	Disagree	Agree	Strongly Agree
keeping the anti-virus up-to date	○	○	○	○
never downloading anything from the internet	○	○	○	○
blocking pop-ups	○	○	○	○
being aware of what websites are visited	○	○	○	○
not clicking on email attachments from people you do not know	○	○	○	○

Q6 How often do you do the following?

	Never	Rarely	Sometimes	Often	Always
update Anti-virus software	○	○	○	○	○
regularly scan the computer with Anti-virus software	○	○	○	○	○
use anti-virus software	○	○	○	○	○
use security software such as a firewall	○	○	○	○	○

Q7 In general, hackers...

	Strongly Disagree	Disagree	Agree	Strongly agree
watch what I am doing on my computer	○	○	○	○
intentionally put viruses on the computer	○	○	○	○
record everything on the computer	○	○	○	○
target only home computer users	○	○	○	○

Q8 One should consider the following with respect to utilizing password techniques

	Strongly Disagree	Disagree	Agree	Strongly agree
Use 'admin' and 'root' or 'administrator' as passwords	○	○	○	○
Write it down so you can look it up when you forget	○	○	○	○
A good mixture of upper case, lower case letters, digits and punctuation	○	○	○	○
Change once in a few years	○	○	○	○
Use the same password for all websites for consistency and ease	○	○	○	○

Q9 I am confident...

	Strongly disagree	Disagree	Agree	Strongly agree
I can identify email scams	○	○	○	○
I can identify a virus on my personal computer/devices	○	○	○	○
I can identify a phishing (fake) email	○	○	○	○
I am aware of local and national cyber attacks	○	○	○	○

Q10 I think principles of my major field of study could be applied to Cybersecurity

- Strongly Disagree
- Disagree
- Agree
- Strongly agree

Q11 Given the necessary skills and training, I desire to become a part of the growing cybersecurity workforce and contribute the knowledge gained through my coursework

- Strongly agree
- Agree
- Disagree
- Strongly disagree Q12 I would consider pursuing a minor in Cybersecurity to know more about fundamental concepts in securing information and systems
- Strongly agree
- Agree
- Disagree
- Strongly disagree

APPENDIX C

INFORMED CONSENT

Informed Consent

Welcome to the research study!

We are interested in understanding the dynamics of interdisciplinary cybersecurity education. You will be presented with information relevant to user security awareness, behaviors and beliefs; and asked to answer some questions about it. Please be assured that your responses will be kept completely confidential.

The study should take you around 15 minutes (pre and post survey together) to complete, and you will receive no incentive for your participation. Your participation in this research is voluntary. You have the right to withdraw at any point during the study, for any reason, and without any prejudice. If you would like to contact the Faculty Sponsor in the study to discuss this research, please e-mail yang@uhcl.edu (281-283-3835)

By clicking the button below, you acknowledge that your participation in the study is voluntary, you are 18 years of age, and that you are aware that you may choose to terminate your participation in the study at any time and for any reason.

Please note that this survey will be best displayed on a laptop/desktop/mobile device.

- ○ I consent, begin the study
- ○ I do not consent, I do not wish to participate

APPENDIX D

APPLICATION TO THE CENTER OF PROTECTION FOR HUMAN SUBJECTS

University of Houston Clear Lake

COMMITTEE FOR THE PROTECTION OF HUMAN SUBJECTS

Faculty/Sponsor Application for Investigation Involving Human Subjects

2700 Bay Area Blvd. 281.283.3015 FAX 281.283.2143
Houston, TX 77058-1098 uhcl.edu/research

DATE: 08.20.2018

TITLE: TOWARDS A HOLISTIC APPROACH IN INTERDISCIPLINARY CYBERSECURITY EDUCATION

PRINCIPAL INVESTIGATOR(S):

STUDENT RESEARCHER(S): JOHANNA JACOB

FACULTY SPONSOR: DR.T. ANDREW YANG

PROPOSED PROJECT END DATE: DEC 2018

How will this project be funded:

If grant, this project is: ____ **Pending** _____ **Funded – Federal** ____ **Funded – Other**

Grant title and/or contract number (if available):

All applicants are to review and understand the responsibilities for abiding by provisions stated in the UHCL's Federal-wide Assurance (FWA 00004068), approved by the Office of Human Research Protections (OHRP) on March 9, 2004: (a) The Belmont Report provides ethical principles to follow in human subject research; and (b) Federal regulations 45 CFR 46 and all of its subparts A, B, C, and D are the minimum standards applied to all of UHCL's human subject research.
See http://www.uhcl.edu/research -- Protection of Human Subjects, Federal-wide Assurance.

For questions, contact the Office of Sponsored Programs (OSP) at 281-283-3015 or sponsoredprograms@uhcl.edu

Principal Investigator (PI) / Faculty Sponsor (FS) Responsibilities Regarding Research on Human Subjects:

- PI / FS acknowledges reviewing UHCL's FWA (Federal-wide Assurance) approved by the Office of Human Research Protections (OHRP). PI / FS understands the responsibilities for abiding by provisions of the Assurance.
- The PI / FS cannot initiate **any** contact with human subjects until final approval is given by CPHS.
- Additions, changes or issues relating to the use of human subjects after the project has begun must be submitted for CPHS review as an amendment and approved PRIOR to implementing the change.
- If the study continues for a period longer than one year, a continuing review must be submitted **PRIOR** to the anniversary date of the studies approval date.
- PI / FS asserts that information contained in this application for human subjects' assessment is complete, true and accurate.
- PI / FS agrees to provide adequate supervision to ensure that the rights and welfare of human subjects are properly maintained.
- Faculty Sponsors are responsible for student research conducted under their supervision. Faculty Sponsors are to retain research data and informed consent forms for three years after project ends.
- PI / FS acknowledges the responsibility to secure the informed consent of the subjects by explaining the procedures, in so far as possible, and by describing the risks and potential benefits of the project.
- PI / FS assures CPHS that all procedures performed in this project will be conducted in accordance with all federal regulations and university policies which govern research with human subjects.

A. DATA COLLECTION DATES:

1. From: **September 10th 2018**
2. To: **October 31st 2018**
3. Project End Date: **December 2018**

B. HUMAN SUBJECTS DESCRIPTION:

1. Age range: **18 - 65**
2. Approx. number: **100**
3. % Male: **50**
4. % Female: **50**

C. PROJECT SUMMARY:

Complete application using commonly understood terminology.

1. Background and Significance

Provide a **CONCISE** rationale for this project, based on current literature, information, or data. Include references as appropriate.

Cybersecurity has evolved into myriad avenues in the corporate and government sectors. Federal departments and agencies have been challenged with sophisticated and persistent cyber threats that pose strategic, economic and security challenges to the national infrastructure. This is due to the tremendous increase in the growth and usage of pervasive devices allowing accessibility and connectivity in every part of the world. The proliferation of cell phones and smart mobile applications have revolutionized the way people interact with devices. While all the technological innovations and advancements have paved the way to a "smart" world, they have innumerably increased the unintended consequences leading to an increase in cybercrime, threats and vulnerabilities in the infrastructure of the nation and private organizations. According to a report by the Berkley Research Group ([1], infections from virus or malicious software account for about 39% of all data breaches, followed by system failures or data corruption accounting to 35% of breaches. And surprisingly, most organizations do not have a strategy to combat cyberthreats in emerging field as Internet of Things and Big Data (Group 2016).

Due to the unmatched opportunities of accessing technology and devices, cybercriminals are on the rise to acquire Personally Identifiable Information through fraudulent means. A 2017 survey by Statista reports that the greatest cybersecurity problem of the United States was hacking by foreign governments (Statista). The report also points out that "51 percent of U.S. adults believed that a cyber-attack on public infrastructure would probably happen in the next five years" [2].

The challenges posed by technology misuse and abuse are manifold and requires an equal contribution from computer science and social science researchers to better understand the dynamics of the attack and perpetrator and to propose a feasible solution to combat it. To exemplify this, consider Phishing emails. Phishing emails can be blocked by email server software based on rules and classification strategies that are configured on the server end. However, it may

still penetrate through to the end user. Potential recipients must be able to identify and understand these phishing messages as a threat to reduce the chances of being victimized. One needs to understand the behavioral and attitudinal differences that lead some to respond to fraudulent messages while some others do not. On a much larger scale, it is important for organizations to understand the attack, the attacker and the dynamics around them. Holt [3] in his journal, "Cybercrime through an interdisciplinary lens" points out that it is critical to situate a cybercrime threat or vulnerability in a multidisciplinary context. However, such an approach to cybersecurity has been stove piped for decades in the education system of the nation. For instance, the disciplines of computer science and engineering are focused on developing algorithms and secure devices that support sensitive syst ems, and data/information processing while information technology and information assurance focus on better techniques, tools and process to protect information from being misused. While there is a higher emphasis on understanding the technical nature of the cyber environment, the networked systems, operating systems and the security threats around them, there is little to no emphasis on the human actors and their decision-making process that plays vital role in a cyber-attack being successful (Holt 2016).

Knowing this will allow institutions or organizations to tailor educational programs accordingly. To combat this, businesses and government sectors have begun to focus on comprehensive cyber security solutions. With these efforts in progress, a greater collaboration has been initiated between education, research and industry fields. The collaboration motivates a cross-disciplinary approach for cybersecurity education. In the light of this, two of the important initiatives undertaken by the Department of Homeland Security are briefed upon below.

The National Initiative for Cybersecurity Education (NICE), aka the National Cybersecurity Workforce Framework (NCWF), is a national focused resource that categorizes and describes cybersecurity work (NIST, 2017). In response to the evolving vulnerabilities in the cyber infrastructure, NICE along with the Department of Homeland Security formulated the NCWF

framework which serves as a reference standard for workforce development, curricular development and much more. Also, NCWF serves as a foundation in establishing common taxonomy and lexicon for several key groups as cybersecurity staff, workers and students considering a career in the field.

Addressing cyber threats requires a reassessment of the way cybersecurity is approached as an academic discipline and requires a significant research in understanding the frameworks and guidelines that form the basis of cybersecurity workforce and talent development.

[1] B. R. Group, "Cybersecurity Preparedness Benchmarking Study Report," Online Source 2016, Available: https://ecommunications.thinkbrg.com/10/218/uploads/cspbs-report.pdf, Accessed on: 19th September 2017.

[2] Statista. U.S. government and cyber-crime - Statistics & Facts. Available: https://www.statista.com/topics/3387/us-government-and-cyber-crime/

[3] T. J. Holt, Cybercrime Through an Interdisciplinary Lens. Taylor & Francis, 2016.

2. Specific Aims

Purpose, Hypotheses/Research Questions, Goals of the Project. **BRIEFLY** describe the purpose and goals of the project (include hypotheses or research questions to be addressed and the specific objectives or aims of the project. Describe or define terms or methods as needed for CPHS reviewer's understanding.

This thesis proposal is motivated by the observed sparsity of interdisciplinary research and collaboration in the NICE framework which stands as a foundational groundwork for many cybersecurity initiatives. Outside the traditional computing space, there is an apparent lack of communication across disciplines, making the framework less inter-disciplinary. For example, there is a myriad of technical fields which offer solutions that support cyber security, but these solutions alone do not resolve cybersecurity challenges. Organizational, social, political, economic and other human dimensions are inevitably tied

to them, but their contribution is overlooked in comparison to the technical avenues (2016). The main goal of this research is to empirically assess the contribution of such fields. In this regard, the following research questions are taken into focus,

- What are the different issues faced by cybersecurity professionals that require increased inter – disciplinary focus in cybersecurity education?
- What is the state of the art in emerging cybersecurity research and other avenues of cybersecurity that could be potentially incorporated into cybersecurity education?
- What are the predominant non – technological disciplines that are key to addressing complex cybersecurity challenges? What is their significance and contribution towards mitigating cyber misuse? Determine the level of awareness of good security practices across such disciplines?
- What are the disciplines that will enable an enhanced and enriched focus on inter-disciplinary cybersecurity education? How will their inclusion significantly impact the effectiveness of education in cybersecurity?
- Is existing training and certification adequate to employ an interdisciplinary workforce?
- How will developing pluggable, aggregable inter-disciplinary modules prove effective in enhancing collaboration between disciplines?

RESEARCH OBJECTIVES AND APPROACH

- Identify current programs in interdisciplinary studies in relevance to NIST/CAE-CDT standards
- Perform an extensive SWOT analysis of each of the programs
- Seek opportunities for filling the gaps in the existing programs by analyzing inclusion of counter attacks, criminology, psychological and information operations, legal components/international law, global internet law, politics, governance, business management, frameworks, practices, ethics and privacy.

• Depending on the results of the survey conducted, identify the specialty areas that have least adherence to interdisciplinary studies

RE**SEARCH GOALS**

The main goal of this research is to perform an explorative analysis of the state of research in interdisciplinary cybersecurity education and workforce in the light of existing underlying frameworks and guidelines. The research also focusses on measuring the interest fostered towards an interdisciplinary approach in cybersecurity through quantitative analysis. A multi-level, multi-discipline, multi-thread framework is proposed to understand the dimensions of interdisciplinary cybersecurity education and design of pluggable, drop in modules that could be cross pollinated into different courses across various majors along with proven pedagogical methods.

The research methods that will be extensively analyzed in the thesis are quantitative analysis, case study, empirical study and secondary analysis.

3. Research Method, Design and Procedures

(A) Provide an overview of research methodology and design; e.g., how the data are to be collected, analyzed, and interpreted.

(B) Provide step-by-step description of procedures and how they are to be applied. Procedures are to begin from CPHS approval and end when data compiled, and results reported. Possible information to include: What are participants asked to do? When and where are they to participate? How long will it take to participate? Describe type of research information gathered from participants, i.e., data being collected.

Note that ethical responsibility of researcher to participant does not end until participant's information has been destroyed. Research documentation cannot be destroyed for up to three years after completion of a study.

RESEARCH METHODOLOGY

The primary research methodology for the thesis includes collecting and analyzing quantitative data. The quantitative data includes closed-end information that undergoes statistical analysis and results in a numerical representation. Considering the research methods, quantitative methodologies provides a thorough understanding of a research problem.

- Validation of survey instrument through expert panel review for Context, Content and Culture
- Approval of survey instrument by CPHS
- Upon successful approval, collect data using the survey instrument by employing pre-and post-surveys
- The data gathered will be analyzed using SPSS tool for correlation, regression and other statistical data interpretation.

PROCEDURES

- Validation of survey instrument through expert panel review for Context, Content and Culture
- CPHS approval to be gained
- Upon successful approval, the survey is disseminated to the desired classes (subjects of interest) through an online link for pre-and post-survey. The pre-survey will be administered before the post-survey. A presentation emphasizing good security practices and user awareness will be given to the students preceding the post-survey. The presentation will be for a duration of 15 minutes. Manual copies of the survey/QR codes will also be available for students who do not have access to the link at the time of the post- survey.

- Upon collection of data, the data is run through SPSS to generate meaningful analysis and is interpreted in lieu of the research objectives
- The survey will test the knowledge of cybersecurity awareness and covers questions assessing their interest towards learning cybersecurity principles in the context of their discipline followed by a final section of gathering demographic information of the respondents.

4. Instruments for Research with Human Subject

Indicate instruments to be used.

(A) Submit copies electronically, if possible.

(B) Submit copy of copyrighted questionnaire for CPHS review. Copy kept on file by CPHS.

(C) Examples of instruments are as follows: (1) Educational Tests, (2) Questionnaires/Surveys, (3) Psychological Tests, (4) Educational Materials, i.e., curriculum, books, etc., (5) Interview or Phone Script, or (6) human subjects recruitment advertisements.

(C) (2) Surveys

5. Human Subject Source and Selection Criteria

Describe the procedures for the recruitment of the participants. Indicate when human subject involvement is expected to begin and end in this project. Example information to include:

(A) Characteristics of subject population, such as anticipated number, age, sex, ethnic background, and state of health.

(B) Where and how participants are drawn for subject selection criteria. Coercion or undue influence needs to be considered and eliminated.

(C) How ensuring equitable subject selection.

(D) If applicable, criteria for inclusion and/or exclusion and provide rationale.

(E) Children are classified as a vulnerable population. See Subpart D, §46.401, of federal guidelines for additional safeguards aimed to protect the rights and welfare of these subjects.

(A)The characteristics of the subject population are as follows: A total of 100 participants are to be involved in the survey. The audience of 100 participants for the survey are students between ages 18 through 65 in different disciplines as Criminology, Psychology, Legal Studies, Business and Information Technology. There are no reservations on sex, ethnic background and state of health. All students of the class are free to participate in the survey.

(B)Since students outside technical fields such as computer science would not have adequate knowledge of cybersecurity principles, the survey poses a fair subject selection as the audience would be spanning students from non-computing, non-technical majors.

(C) There are no criteria for inclusion and exclusion

(E) No children are involved in the survey

6. Informed Consent

For more details, see "Federal & University Guidelines" document, "Informed Consent" section.

(A) Describe procedure for obtaining informed consent.

(B) Use language that is appropriate for age or understandability of subjects.

(C) Attach informed consent page.

(D) If applicable, attach the following documents for review: (1) Parental permission form for participation of minors (under 18 years of age). (2) Assent form for children between ages 7 and 17: (2a) ages 12-17 must sign assent form; (2b) ages 7-11 must have witness sign attesting to child's positive assent.

(E) **Request CPHS waiver for documentation of informed consent, if appropriate**. Justification is required. See "Federal & University Guidelines."

(C)The informed consent will be available as a link for download along with the survey instrument

7. Confidentiality

Describe how data will be safeguarded: (a) how confidentiality maintained; use of personal identifiers or coded data; (b) how data collected and recorded; (c) how data stored during project; (d) who has access to data or participant's identifiers; (e) who is to receive data, if applicable; (f) what happens to data after research is completed.

Note that research documentation, including signed informed consent forms, are safeguarded for three years after completion of study for federal audit purposes. Faculty sponsors are responsible for safeguarding research documentation completed by students.

(a)The survey will be conducted as an anonymous and will be disseminated by the instructor the class through an online link to their student/personal email address (b)The data collected will be recorded on Qualtrics, a leading software that sophisticates research analysis. (c) The data is stored on Qualtrics during the project. (d) Other than the student researcher, there is none that can access the data during the project. (If applicable, the data will be received by the faculty sponsor Dr. T. Andrew Yang and the methodologist Dr. Michelle Peters, Department of Education) (f) The data will be retained by the student researcher on Qualtrics after the research is complete for future research directions and enhancements.

8. Research Benefits

Describe any anticipated benefits to subjects as well as reasonably expected general results.

There are no anticipated benefits to the subjects for participating in the survey. However, the thesis might result in a modulation of their course offerings to include cybersecurity modules in the future.

9. Risks

Describe any foreseeable risks to the subjects, whether physical injury, psychological injury, loss of confidentiality, social harm, etc., involved in the conduct of the research. Explain precautions taken to minimize these risks. If there are any foreseeable risks, provide contact information of organization(s) for professional treatment.

There are no foreseeable risks to the subjects during this survey.

10. Other Sites or Agencies Involved in Research Project

Indicate specific site if not UHCL, e.g., school districts or school, clinics.

(A) Obtain written approval from institution. Approval should be signed and on institution's letterhead. Other proof of documentation may be reviewed for acceptance by CPHS.

(B) Institution should include the following information: (B1) institution's knowledge of study being conducted on its site; (B2) statement about what research study involves; (B3) outline specific procedures to be conducted at site; and (B4) identify type of instrument(s) used to collect data and duration needed to complete instruments; (B5) statement that identities of institution and participants will be kept confidential; (B6) institution's permission granting the use of its facilities or resources; and (B7) include copy of Informed Consent document(s) to be used in recruiting volunteers from the institution.

(C) If at all possible, electronic copies of letter or other documentation are to be submitted with CPHS application.

(D) If letters are not available at time of CPHS review, approval will be contingent upon their receipt.

External agencies or institutions are not involved in the survey.

APPENDIX E

EXPERT PANEL DEMOGRAPHIC INFORMATION

Demographics of Expert Panel

This information is required to understand the demographics of the expert panel reviewing the survey instruments. Please fill in each field with the correct answers.

Q1 What is your name?

_____

Q2 What is your gender?

_____

Q3 What is your race/ethnicity?

_____

Q4 What are the different subjects you have taught?

_____

Q5 What is your total years of experience?

_____

APPENDIX F

PROTOCOL FOR SURVEY ADMINISTRATION

Dear Professor,

Thank you for your immense support and consideration to allow me to administer the survey in your class/es. To maintain consistency and to ensure the required data is obtained, I put together this short document that describes how the survey would be precisely administered in the class. I would greatly appreciate if you could inform the students (in advance) to bring a device to the class to take up the survey (If your class does not take place in a lab).

- The online links of the pre and post survey will be sent to the instructor 2 days before the survey is administered. Instructor will emphasize students to bring a portable device
  (Phone, Laptop, Tablet etc.,) to take up the survey
- The instructor must ensure the links are posted on blackboard but are NOT ACTIVE until the beginning of the class (If the instructor doesn't use blackboard for that class, the survey links would be mailed by the instructor right before the class starts)
- On the day of the survey, the links will be made active right before the class
- Once the informed consent is filled, the students will take up the pre-survey followed by a short presentation
- Upon completion of the presentation, the students will take up the post-survey

Primary source: The primary source of the survey would be an anonymous link that will be posted on the blackboard

Backup plan: In the event of inaccessibility to the survey, QR scan codes and hard copies of the survey would be available. In addition, additional laptops would be available to help the students take up the survey in the class.

Thank you for all the support shown in this regard! I am looking forward to seeing what the data entails.

Regards,

Johanna Jacob